

개인정보 보호 법령 및 지침·고시 해설

2020. 12

제1장 총칙

[제1조] 목적 3
 [제2조] 정의 8
 [제3조] 개인정보 보호 원칙 30
 [제4조] 정보주체의 권리 33
 [제5조] 국가 등의 책무 36
 [제6조] 다른 법률과의 관계 37

제2장 개인정보 보호정책의 수립 등

[제7조] 개인정보 보호위원회 43
 [제7조의2] 보호위원회의 구성 등 45
 [제7조의3] 위원장 45
 [제7조의4] 위원의 임기 45
 [제7조의5] 위원의 신분보장 45
 [제7조의6] 겸직금지 등 45
 [제7조의7] 결격사유 45
 [제7조의8] 보호위원회의 소관 사무 50
 [제7조의9] 보호위원회의 심의·의결 사항 등 50
 [제7조의10] 회의 53
 [제7조의11] 위원의 제적·기피·회피 53
 [제7조의12] 소위원회 53
 [제7조의13] 사무처 53
 [제7조의14] 운영 등 53
 [제8조의2] 개인정보 침해요인 평가 58
 [제9조] 기본계획 60
 [제10조] 시행계획 62
 [제11조] 자료제출 요구 등 63
 [제12조] 개인정보 보호지침 66
 [제13조] 자율규제의 촉진 및 지원 68
 [제14조] 국제협력 76

목 차

제3장 개인정보의 처리

제1절 개인정보의 수집, 이용, 제공 등

[제15조] 개인정보의 수집·이용	79
[제16조] 개인정보의 수집 제한	102
[제17조] 개인정보의 제공	105
[제18조] 개인정보의 목적 외 이용·제공 제한	117
[제19조] 개인정보를 제공받은 자의 이용·제공 제한	131
[제20조] 정보주체 이외로부터 수집한 개인정보의 수집 출처 등 고지	133
[제21조] 개인정보의 파기	137
[제22조] 동의를 받는 방법	144

제2절 개인정보의 처리 제한

[제23조] 민감정보의 처리 제한	157
[제24조] 고유식별정보의 처리 제한	165
[제24조의2] 주민등록번호 처리의 제한	170
[제25조] 영상정보처리기기의 설치·운영 제한	174
[제26조] 업무위탁에 따른 개인정보의 처리 제한	203
[제27조] 영업양도 등에 따른 개인정보의 이전 제한	213
[제28조] 개인정보취급자에 대한 감독	218

제3절 가명정보 처리에 관한 특례

[제28조의2] 가명정보의 처리 등	221
[제28조의3] 가명정보의 결합 제한	225
[제28조의4] 가명정보에 대한 안전조치의무 등	240
[제28조의5] 가명정보 처리 시 금지의무 등	243
[제28조의6] 가명정보 처리에 대한 과징금 부과 등	245
[제28조의7] 적용범위	248

제4장 개인정보의 안전한 관리

[제29조] 안전조치의무	253
[제30조] 개인정보 처리방침의 수립 및 공개	272

[제31조] 개인정보 보호책임자의 지정 279
 [제32조] 개인정보파일의 등록 및 공개 287
 [제32조의2] 개인정보 보호 인증 299
 [제33조] 개인정보 영향평가 323
 [제34조] 개인정보 유출 통지 등 350
 [제34조의2] 과징금의 부과 등 359

제5장 정보주체의 권리 보장

[제35조] 개인정보의 열람 365
 [제36조] 개인정보의 정정·삭제 374
 [제37조] 개인정보의 처리정지 등 380
 [제38조] 권리행사의 방법 및 절차 등 384
 [제39조] 손해배상책임 391
 [제39조의2] 법정손해배상의 청구 398

제6장 정보통신서비스 제공자등의 개인정보 처리 등 특례

개관 405
 [제39조의3] 개인정보의 수집·이용 동의 등에 대한 특례 414
 [제39조의4] 개인정보 유출등의 통지·신고에 대한 특례 421
 [제29조, 제39조의5] 개인정보의 보호조치에 대한 특례 427
 [제39조의6] 개인정보의 파기에 대한 특례 442
 [제39조의7] 이용자의 권리 등에 대한 특례 450
 [제39조의8] 개인정보 이용내역의 통지 453
 [제39조의9] 손해배상의 보장 456
 [제39조의10] 노출된 개인정보의 삭제·차단 461
 [제39조의11] 국내대리인의 지정 463
 [제39조의12] 국외 이전 개인정보의 보호 467
 [제39조의13] 상호주의 471
 [제39조의14] 방송사업자등에 대한 특례 472
 [제39조의15] 과징금의 부과 등에 대한 특례 473

목 차

제7장 개인정보 분쟁조정위원회

[제40조] 설치 및 구성	485
[제41조] 위원의 신분보장	490
[제42조] 위원의 제척·기피·회피	490
[제43조] 조정의 신청 등	492
[제44조] 처리기간	492
[제45조] 자료의 요청 등	492
[제46조] 조정 전 합의 권고	492
[제47조] 분쟁의 조정	492
[제48조] 조정의 거부 및 중지	492
[제49조] 집단분쟁조정	497
[제50조] 조정절차 등	504

제8장 개인정보 단체소송

[제51조] 단체소송의 대상 등	509
[제52조] 전속관할	509
[제53조] 소송대리인의 선임	509
[제54조] 소송허가신청	514
[제55조] 소송허가요건 등	514
[제56조] 확정판결의 효력	517
[제57조] 「민사소송법」의 적용 등	518

제9장 보칙

[제58조] 적용의 일부 제외	523
[제58조의2] 적용제외	531
[제59조] 금지행위	532
[제60조] 비밀유지 등	538
[제61조] 의견제시 및 개선권고	541
[제62조] 침해사실의 신고 등	544

[제63조] 자료제출 요구 및 검사	546
[제64조] 시정조치 등	553
[제65조] 고발 및 징계권고	553
[제66조] 결과의 공표	553
[제67조] 연차보고	559
[제68조] 권한의 위임·위탁	560
[제69조] 벌칙 적용 시의 공무원 의제	562

제10장 벌칙

[제70조~제73조] 벌칙	565
[제74조] 양벌규정	569
[제74조의2] 몰수·추징 등	571
[제75조] 과태료	572
[제76조] 과태료에 관한 규정 적용의 특례	582

제1장 총칙

- 제1조 목적
- 제2조 정의
- 제3조 개인정보 보호 원칙
- 제4조 정보주체의 권리
- 제5조 국가 등의 책무
- 제6조 다른 법률과의 관계



제1조 | 목적

법률	제1조(목적) 이 법은 개인정보의 처리 및 보호에 관한 사항을 정함으로써 개인의 자유와 권리를 보호하고, 나아가 개인의 존엄과 가치를 구현함을 목적으로 한다.
시행령	제1조(목적) 이 영은 「개인정보 보호법」에서 위임된 사항과 그 시행에 관하여 필요한 사항을 규정함을 목적으로 한다.
표준지침	제1조(목적) 제1조(목적) 이 지침은 「개인정보 보호법」(이하 “법”이라 한다) 제12조제1항에 따른 개인정보의 처리에 관한 기준, 개인정보 침해의 유형 및 예방조치 등에 관한 세부적인 사항을 규정함을 목적으로 한다.

1. 법 제정 배경 및 연혁

가 법 제정 배경

4차 산업혁명 시대에 있어, 데이터를 핵심 자원으로 하는 인공지능(AI)·클라우드(Cloud), 사물인터넷(IoT) 등 신산업 활성화와 개인정보의 안전한 활용을 위한 사회적 규범 정립이 시급한 상황이다. 이에 따라 공공부문과 민간부문을 망라하여 국제 수준에 부합하는 개인정보 처리 원칙 등을 규정하고, 개인정보 침해로 인한 국민의 피해 구제를 강화하여 국민의 사생활의 비밀을 보호하며, 개인정보에 대한 권리와 이익을 보장하려는 것이다.

나 법의 연혁



2011.3.29., 법의 제정(법률 제10465호)

공공부문과 민간부문을 모두 규율하는 개인정보 보호에 관한 일반법 제정에 대한 논의가 있었고, 17대 국회에서 노회찬 의원안(민노당, 2004. 11.), 이은영 의원안(우리당, 2005. 7.), 이혜훈 의원안(한나라당, 2005. 12.) 등 3건의 「개인정보 보호법(안)」이 의원 발의되었으나 17대 국회 폐회로 폐기되었다. 18대 국회에서 이혜훈 의원안(2008. 8. 8.), 변재일 의원안(2008. 10. 27.) 등 2건의 「개인정보 보호법(안)」이 의원 발의되었고, 2008. 11. 28. 「개인정보 보호법 정부(안)」이 국회에 제출되었다. 2009. 2. 20. 국회 행정안전위원회에서 3개 의원안과 정부안을 병합하여 상정하였고 이후 공청회, 법안심사소위 등을 거쳐 2011. 3. 11. 본회의에서 의결되었고 같은 해 9. 30.부터 시행되었다.



2013.8.6., 일부개정(법률 제11990호)

대량의 주민등록번호 유출 및 악용에도 불구하고 이러한 유출 사고가 발생한 대기업 등에 대해서 민·형사상 책임이 제대로 부과되지 않고 있어 모든 개인정보처리자에 대하여 원칙적으로 주민등록번호의 처리를 금지하고, 주민등록번호가 분실·도난·유출·변조·훼손된 경우 5억원 이하의 과징금을 부과·징수할 수 있도록 하며, 개인정보 보호와 관련된 법규의 위반행위가 있다고 인정될 만한 상당한 이유가 있을 때는 대표자 또는 책임 있는 임원을 징계할 것을 권고할 수 있도록 명확히 하여 주민등록번호 유출사고를 방지하는 한편, 기업이 주민등록번호 등 개인정보 보호를 위한 책임을 다하도록 하였다.

제16조(개인정보의 수집 제한) 제2항 “개인정보처리자는 정보주체의 동의를 받아 개인정보를 수집하는 경우 필요한 최소한의 정보 외의 개인정보 수집에는 동의하지 아니할 수 있다는 사실을 구체적으로 알리고 개인정보를 수집하여야 한다.” 를 신설하고, 제24조 제2항과 제4항을 삭제하는 대신 제24조의2(주민등록번호 처리의 제한)를 신설하였다.



2014.3.24., 일부개정(법률 제12504호)

제1조(목적)를 “이 법은 개인정보의 수집·유출·오용·남용으로부터 사생활의 비밀 등을 보호함으로써 국민의 권리와 이익을 증진하고, 나아가 개인의 존엄과 가치를 구현하기 위하여 개인정보 처리에 관한 사항을 규정함을 목적으로 한다.” 에서 “이 법은 개인정보의 처리 및 보호에 관한 사항을 정함으로써 개인의 자유와 권리를 보호하고, 나아가 개인의 존엄과 가치를 구현함을 목적으로 한다.” 로 개정하였다.

제2조제2호 “처리” 에 대한 정의에서 “연계, 연동” 을 추가하고, 제6조(다른 법률과의 관계)를 “개인정보 보호에 관하여는 「정보통신망 이용촉진 및 정보보호 등에 관한 법률」(이하 “「정보통신망법」” 이라 한다), 「신용정보의 이용 및 보호에 관한 법률」(이하 “「신용정보법」” 이라 한다) 등 다른 법률에 특별한 규정이 있는 경우를 제외하고는 이 법에서 정하는 바에 따른다.” 에서 “개인정보 보호에 관하여는 다른 법률에 특별한 규정이 있는 경우를 제외하고는 이 법에서 정하는 바에 따른다.” 로 개정하였다.



2015.7.24. 일부개정(법률 제13423호)

2014년 1월 카드사 개인정보 유출사고를 계기로 대통령 소속 개인정보보호 위원회의 총괄·조정 기능 강화, 개인정보 보호 인증기관 지정 근거 마련 등 현행법의 운용상 미비사항을 보완하고, 징벌적 손해배상과 법정손해배상 제도를 도입하여 개인정보 유출에 대한 피해구

제를 강화하는 한편, 개인정보 불법 유통으로 얻은 범죄 수익을 몰수·추징하고, 부정한 방법으로 개인정보를 취득하여 영리 등의 목적으로 타인에게 제공한 자에 대한 벌칙을 신설하는 등 개인정보 범죄에 대한 제재수준을 강화하였다.



2016.3.29. 일부개정(법률 제14107호)

개인정보처리자가 민감정보를 처리하는 경우 안전성 확보에 필요한 조치를 하도록 명시하고, 행정자치부장관은 고유식별정보를 처리하는 개인정보처리자가 안전성 확보조치를 하였는지 정기적으로 조사하도록 하는 등 안전성 확보를 위한 규정을 강화하였다.

또한 주민등록번호를 수집할 수 있는 법령의 범위를 법률·대통령령·국회규칙·대법원규칙·헌법재판소규칙·중앙선거관리위원회규칙 및 감사원규칙으로 한정하고, 해당 법률 등의 제·개정 현황을 개인정보 보호 연차보고서에 포함하도록 함으로써 주민등록번호의 사용을 보다 엄격히 관리·통제하도록 하였다.

대통령령으로 정하는 기준에 해당하는 개인정보처리자가 정보주체 이외로부터 개인정보를 수집하여 처리하는 때에는 정보주체에게 수집 출처·처리 목적 등을 고지하도록 하였다.

또한, 영상정보처리기기 안내판 설치 관련 규정을 법률에 상향 규정하고, 개인정보 처리 방침에 포함해야 하는 항목을 추가하는 등 일부 미비사항을 보완하였다.



2017. 4. 18. 일부개정(법률 제14765호)

개인정보처리자가 서면 등으로 정보주체의 동의를 받을 때 정보의 수집·이용 목적, 수집·이용하려는 개인정보의 항목 등 대통령령으로 정하는 중요한 내용을 행정자치부령으로 정하는 방법에 따라 명확히 표시하여 알아보기 쉽게 하도록 개정하였다.



2020. 2. 4. 일부개정(법률 제16930호)

4차 산업혁명 시대를 맞아 핵심 자원인 데이터의 이용 활성화를 통한 신산업 육성이 범국가적 과제로 대두되고 있고, 특히 신산업 육성을 위해서는 인공지능, 클라우드, 사물인터넷 등 신기술을 활용한 데이터 이용이 필요한 바, 안전한 데이터 이용을 위한 사회적 규범 정립이 시급한 상황이 도래하였다.

그러나 기존법상 개인정보 보호 감독기능은 행정안전부·방송통신위원회·개인정보 보

호위원회 등으로, 개인정보 보호 관련 법령은 이 법과 「정보통신망 이용촉진 및 정보보호 등에 관한 법률」 등으로 각각 분산되어 있어 데이터 이용 활성화를 지원하고 데이터 이용으로부터 정보주체의 권리를 보호하는 데 한계가 있었다.

이에 따라 정보주체의 동의 없이 과학적 연구, 통계작성, 공익적 기록보존 등의 목적으로 가명정보를 이용할 수 있는 근거를 마련하되, 관련하여 개인정보처리자의 책임성 강화 등 개인정보를 안전하게 보호하기 위한 제도적 장치를 마련하는 한편, 당초 수집 목적과 합리적으로 관련된 범위 내에서 개인정보의 추가적인 이용·제공이 가능하도록 할 여지를 마련하였다.

또한, 개인정보의 오용·남용 및 유출등을 감독할 감독기구는 개인정보 보호위원회로, 「정보통신망의 이용촉진 및 정보보호 등에 관한 법률」과의 유사·중복 규정은 「개인정보 보호법」으로 일원화함으로써 개인정보의 보호와 관련 산업의 발전이 조화될 수 있도록 개인정보 보호 관련 법령을 체계적으로 정비하였다.

2. 법의 목적

이 법은 개인정보의 처리 및 보호에 관한 사항을 정함으로써 개인의 자유와 권리를 보호하고, 나아가 개인의 존엄과 가치를 구현함을 목적으로 한다. 이에 따라 개인정보의 수집·이용, 제공 등 개인정보 처리 기본원칙, 개인정보의 처리 절차 및 방법, 개인정보 처리의 제한, 개인정보의 안전한 처리를 위한 관리·감독, 정보주체의 권리, 개인정보 권리 침해에 대한 구제 등에 대하여 규정하고 있다.

헌법재판소는 인간의 존엄과 가치 및 행복추구권을 규정하고 있는 「헌법」 제10조 제1문에서 도출되는 일반적 인격권과 제17조에 의하여 보호받고 있는 사생활의 비밀과 자유를 근거 규정으로 하여 우리나라 「헌법」 상으로도 ‘개인정보자기결정권’이 기본권으로 보장되고 있다고 보고 있다.

개인정보자기결정권이란 자신에 관한 정보가 언제 누구에게 어느 범위까지 알려지고 또 이용되도록 할 것인지를 그 정보주체가 스스로 결정할 수 있는 권리, 즉 정보주체가 개인정보의 공개와 이용에 관하여 스스로 통제·결정할 수 있는 권리를 말한다.

참고 1 대한민국 헌법 제10조

모든 국민은 인간으로서의 존엄과 가치를 가지며, 행복을 추구할 권리를 가진다. 국가는 개인이 가지는 불가침의 기본적 인권을 확인하고 이를 보장할 의무를 진다.

참고 2 대한민국 헌법 제17조

모든 국민은 사생활의 비밀과 자유를 침해받지 아니한다.

판례 개인정보자기결정권

인간의 존엄과 가치, 행복추구권을 규정한 「헌법」 제10조 제1문에서 도출되는 일반적 인격권 및 「헌법」 제17조의 사생활의 비밀과 자유에 의하여 보장되는 개인정보자기결정권은 자신에 관한 정보가 언제 누구에게 어느 범위까지 알려지고 또 이용되도록 할 것인지를 그 정보주체가 스스로 결정할 수 있는 권리이다. 즉 정보주체가 개인정보의 공개와 이용에 관하여 스스로 결정할 권리를 말한다. 개인정보자기결정권의 보호대상이 되는 개인정보는 개인의 신체, 신념, 사회적 지위, 신분 등과 같이 개인의 인격주체성을 특징짓는 사항으로서 그 개인의 동일성을 식별할 수 있게 하는 일체의 정보라고 할 수 있고, 반드시 개인의 내밀한 영역이나 사사(私事)의 영역에 속하는 정보에 국한되지 않고 공적 생활에서 형성되었거나 이미 공개된 개인정보까지 포함한다. 또한 그러한 개인정보를 대상으로 한 조사·수집·보관·처리·이용 등의 행위는 모두 원칙적으로 개인정보자기결정권에 대한 제한에 해당한다(헌법재판소 2005. 7. 21. 2003헌마282, 425 결정).

제2조(정의) 이 법에서 사용하는 용어의 뜻은 다음과 같다.

1. “개인정보”란 살아 있는 개인에 관한 정보로서 다음 각 목의 어느 하나에 해당하는 정보를 말한다.
 - 가. 성명, 주민등록번호 및 영상 등을 통하여 개인을 알아볼 수 있는 정보
 - 나. 해당 정보만으로는 특정 개인을 알아볼 수 없더라도 다른 정보와 쉽게 결합하여 알아볼 수 있는 정보. 이 경우 쉽게 결합할 수 있는지 여부는 다른 정보의 입수 가능성 등 개인을 알아보는 데 소요되는 시간, 비용, 기술 등을 합리적으로 고려하여야 한다.
 - 다. 가목 또는 나목을 제1호의2에 따라 가명처리함으로써 원래의 상태로 복원하기 위한 추가 정보의 사용·결합 없이는 특정 개인을 알아볼 수 없는 정보(이하 “가명정보”라 한다)
- 1의2. “가명처리”란 개인정보의 일부를 삭제하거나 일부 또는 전부를 대체하는 등의 방법으로 추가 정보가 없이는 특정 개인을 알아볼 수 없도록 처리하는 것을 말한다.
2. “처리”란 개인정보의 수집, 생성, 연계, 연동, 기록, 저장, 보유, 가공, 편집, 검색, 출력, 정정(訂正), 복구, 이용, 제공, 공개, 파기(破棄), 그 밖에 이와 유사한 행위를 말한다.
3. “정보주체”란 처리되는 정보에 의하여 알아볼 수 있는 사람으로서 그 정보의 주체가 되는 사람을 말한다.
4. “개인정보파일”이란 개인정보를 쉽게 검색할 수 있도록 일정한 규칙에 따라 체계적으로 배열하거나 구성한 개인정보의 집합물(集合物)을 말한다.
5. “개인정보처리자”란 업무를 목적으로 개인정보파일을 운영하기 위하여 스스로 또는 다른 사람을 통하여 개인정보를 처리하는 공공기관, 법인, 단체 및 개인 등을 말한다.
6. “공공기관”이란 다음 각 목의 기관을 말한다.
 - 가. 국회, 법원, 헌법재판소, 중앙선거관리위원회의 행정사무를 처리하는 기관, 중앙행정기관(대통령 소속 기관과 국무총리 소속 기관을 포함한다) 및 그 소속 기관, 지방자치단체
 - 나. 그 밖의 국가기관 및 공공단체 중 대통령령으로 정하는 기관
7. “영상정보처리기기”란 일정한 공간에 지속적으로 설치되어 사람 또는 사물의 영상 등을 촬영하거나 이를 유·무선망을 통하여 전송하는 장치로서 대통령령으로 정하는 장치를 말한다.
8. “과학적 연구”란 기술의 개발과 실증, 기초연구, 응용연구 및 민간 투자 연구 등 과학적 방법을 적용하는 연구를 말한다.

제2조(공공기관의 범위) 「개인정보 보호법」(이하 “법”이라 한다) 제2조제6호나목에서 “대통령령으로 정하는 기관”이란 다음 각 호의 기관을 말한다.

1. 「국가인권위원회법」 제3조에 따른 국가인권위원회
- 1의2. 「고위공직자범죄수사처 설치 및 운영에 관한 법률」 제3조제1항에 따른 고위공직자범죄수사처
2. 「공공기관의 운영에 관한 법률」 제4조에 따른 공공기관
3. 「지방공기업법」에 따른 지방공사와 지방공단
4. 특별법에 따라 설립된 특수법인
5. 「초·중등교육법」, 「고등교육법」, 그 밖의 다른 법률에 따라 설치된 각급 학교

제3조(영상정보처리기기의 범위) 법 제2조제7호에서 “대통령령으로 정하는 장치”란 다음 각 호의 장치를 말한다.

1. 폐쇄회로 텔레비전 : 다음 각 목의 어느 하나에 해당하는 장치
 - 가. 일정한 공간에 지속적으로 설치된 카메라를 통하여 영상 등을 촬영하거나 촬영한 영상정보를 유무선 폐쇄회로 등의 전송로를 통하여 특정 장소에 전송하는 장치
 - 나. 가목에 따라 촬영되거나 전송된 영상정보를 녹화·기록할 수 있도록 하는 장치
2. 네트워크 카메라 : 일정한 공간에 지속적으로 설치된 기기로 촬영한 영상정보를 그 기기를 설치·관리하는 자가 유무선 인터넷을 통하여 어느 곳에서나 수집·저장 등의 처리를 할 수 있도록 하는 장치

「개인정보 보호법」은 개인정보 보호에 관한 일반법이므로 사람·장소·사항 등에 특별한 제한이 없이 일반적으로 적용되지만, 개인과 관련된 모든 정보를 규율대상으로 하기는 어렵다. 따라서 개인정보 보호의 사각지대를 해소하면서도 개인의 사생활 영역에 대한 지나친 규제가 되지 않도록 하는 등 적절한 수준에서 보호대상과 규율범위를 정하고자 하였다.

제1호 | 개인정보

법률

1. “개인정보”란 살아 있는 개인에 관한 정보로서 다음 각 목의 어느 하나에 해당하는 정보를 말한다.
 - 가. 성명, 주민등록번호 및 영상 등을 통하여 개인을 알아볼 수 있는 정보
 - 나. 해당 정보만으로는 특정 개인을 알아볼 수 없더라도 다른 정보와 쉽게 결합하여 알아볼 수 있는 정보. 이 경우 쉽게 결합할 수 있는지 여부는 다른 정보의 입수 가능성 등 개인을 알아보는 데 소요되는 시간, 비용, 기술 등을 합리적으로 고려하여야 한다.
 - 다. 가목 또는 나목을 제1호의2에 따라 가명처리함으로써 원래의 상태로 복원하기 위한 추가 정보의 사용·결합 없이는 특정 개인을 알아볼 수 없는 정보(이하 “가명정보”라 한다)

1. 개인정보

가 ‘살아 있는’ 개인에 관한 정보이어야 한다.

개인정보 보호 법령상 개인정보는 ‘살아 있는’ 자연인에 관한 정보이므로 사망했거나 실종 선고 등 관계 법령에 의해 사망한 것으로 간주되는 자에 관한 정보는 개인정보로 볼 수 없다. 다만, 사망자의 정보라고 하더라도 유족과의 관계를 알 수 있는 정보는 유족의 개인정보에 해당한다.

나 ‘개인에 관한’ 정보이어야 한다.

개인정보의 주체는 자연인이어야 하며, 법인 또는 단체에 관한 정보는 개인정보에 해당하지 않는다. 따라서 법인 또는 단체의 이름, 소재지 주소, 대표 연락처(이메일 주소 또는 전화번호), 업무별 연락처, 영업실적 등은 개인정보에 해당하지 않는다. 또한, 개인사업자의 상호명, 사업장 주소, 전화번호, 사업자등록번호, 매출액, 납세액 등은 사업체의 운영과 관련한 정보로서 원칙적으로 개인정보에 해당하지 않는다.

그러나 법인 또는 단체에 관한 정보이면서 동시에 개인에 관한 정보인 대표자를 포함한 임원진과 업무 담당자의 이름·주민등록번호·주택주소 및 개인 연락처, 사진 등 그 자체로 개인을 식별할 수 있는 정보는 개별 상황에 따라 법인 등의 정보에 그치지 않고 개인정보로 취급될 수 있다.

사람이 아닌 사물에 관한 정보는 원칙적으로 개인정보에 해당하지 않는다. 그러나 해당 사물

등의 제조자 또는 소유자 등을 나타내는 정보는 개인정보에 해당한다. 예를 들어, 특정 건물이나 아파트의 소유자가 자연인인 경우, 그 건물이나 아파트의 주소가 특정 소유자를 알아보는데 이용된다면 개인정보에 해당한다.

‘개인에 관한 정보’는 반드시 특정 1인만에 관한 정보이어야 한다는 의미가 아니며, 직·간접적으로 2인 이상에 관한 정보는 각자의 정보에 해당한다. SNS에 단체 사진을 올린다면 사진의 영상정보는 사진에 있는 인물 모두의 개인정보에 해당하며, 의사가 특정 아동의 심리치료를 위해 진료 기록을 작성하면서 아동의 부모 행태 등을 포함하였다면 그 진료기록은 아동과 부모 모두의 개인정보에 해당한다. 다만, 특정 개인에 관한 정보임을 알아볼 수 없도록 통계적으로 변환된 ‘○○기업 평균연봉’, ‘○○대학 졸업생 취업률’ 등은 개인정보에 해당하지 않는다.

이처럼 개인정보 해당하는지 여부는 구체적 상황에 따라 다르게 평가될 수 있다. 예를 들어 ‘휴대전화번호 뒤 4자리’를 개인정보라고 본 판례가 있으나, 이는 다른 정보와의 결합가능성 등을 고려하여 개인 식별가능성이 있으므로 개인정보로 본 것이다. 만약 다른 결합 가능 정보가 일체 없이 오로지 휴대전화번호 뒤 4자리만 있는 경우에는 개인정보에 해당하지 않는다고 보아야 할 것이다.

판례 휴대전화번호 뒤 4자리

대전지법 논산지원(2013고단17 판결)은 「휴대전화번호 뒷자리 4자」에 대하여, “휴대전화번호 뒷자리 4자만으로도 그 전화번호 사용자가 누구인지를 식별할 수 있는 경우가 있고, 특히 그 전화번호 사용자와 일정한 인적 관계를 맺어온 사람이라면 더욱더 그러할 가능성이 높으며, 설령 휴대전화번호 뒷자리 4자만으로는 그 전화번호 사용자를 식별하지 못한다 하더라도 그 뒷자리 번호 4자와 관련성이 있는 다른 정보(생일, 기념일, 집 전화번호, 가족 전화번호, 기존 통화내역 등)와 쉽게 결합하여 그 전화번호 사용자가 누구인지를 알아볼 수도 있다”고 하여 「개인정보 보호법」 제2조제1호에 규정된 개인정보에 해당된다고 판시하고 있다. (대전지법 논산지원 2013.8.9. 2013고단17 판결)

다 ‘정보’의 내용·형태 등은 제한이 없다

정보의 내용·형태 등은 특별한 제한이 없어서 개인을 알아볼 수 있는 모든 정보가 개인정보가 될 수 있다. 즉, 디지털 형태나 수기 형태, 자동 처리나 수동 처리 등 그 형태 또는 처리방식과 관계없이 모두 개인정보에 해당할 수 있다.

정보주체와 관련되어 있으면 키, 나이, 몸무게 등 ‘객관적 사실’에 관한 정보나 그 사람에 대한 제3자의 의견 등 ‘주관적 평가’ 정보 모두 개인정보가 될 수 있다. 또한, 그 정보가 반드시 ‘사실’이거나 ‘증명된 것’이 아닌 부정확한 정보 또는 허위의 정보라도 특정한 개인에 관한 정보이면 개인정보가 될 수 있다.

판례 공적 생활에서 형성된 정보, 이미 공개된 정보의 개인정보 해당하는지 여부

개인정보는 개인의 신체, 신념, 사회적 지위, 신분 등과 같이 인격주체성을 특징짓는 사항으로서 개인의 동일성을 식별할 수 있게 하는 일체의 정보를 의미하며, 반드시 개인의 내밀한 영역에 속하는 정보에 국한되지 않고 공적 생활에서 형성되었거나 이미 공개된 개인정보까지도 포함한다. (대법원 2016.03.10. 선고 2012다105482 판결)

라 성명, 주민등록번호 및 영상 등을 통하여 개인을 ‘알아볼 수 있는’ 정보이어야 한다.

‘알아볼 수 있는’의 의미는 해당 정보를 ‘처리하는 자’의 입장에서 합리적으로 활용될 가능성이 있는 수단을 고려하여 개인을 알아볼 수 있다면 개인정보에 해당한다. 현재 처리하는 자’ 외에도 제공 등에 따라 ‘향후 처리가 예정된 자’도 포함된다. 여기서 ‘처리’란 법 제2조제2호에 따른 개인정보의 수집, 생성, 연계, 연동, 기록, 저장, 보유, 가공, 편집, 검색, 출력, 정정(訂正), 복구, 이용, 제공, 공개, 파기(破棄), 그 밖에 이와 유사한 행위를 말한다.

한편, 주민등록번호와 같은 고유식별정보는 해당 정보만으로도 정보주체인 개인을 알아볼 수 있지만, 생년월일의 경우에는 같은 날 태어난 사람이 여러 사람일 수 있으므로 다른 정보 없이 생년월일 그 자체만으로는 개인을 알아볼 수 있다고 볼 수 없다.

마 해당 정보만으로는 특정 개인을 알아볼 수 없더라도 다른 정보와 ‘쉽게 결합’하여 알아볼 수 있는 정보도 포함된다.

다른 정보와 쉽게 결합하여 특정 개인을 알아볼 수 있으면 개인정보에 해당한다. 여기서 ‘입수 가능성’은 두 개 이상의 정보를 결합하기 위해 그 결합에 필요한 다른 정보에 합법적으로 접근하여 이에 대한 지배력을 확보할 수 있어야 하며 해킹·절취(切取) 등 불법적인 방법으로 취득한 정보까지 포함한다고 볼 수 없다.

아울러, 다른 정보와 쉽게 결합할 수 있는지 여부는 입수 가능성 외에 현재의 기술 수준이나 충분히 예견될 수 있는 기술 발전 등을 고려하여 시간이나 비용, 노력이 비합리적으로 과다하게 수반되지 않아야 한다. 따라서 일반적으로 사업자가 구매하기 어려운 정도로 고가의 컴퓨터가 필요한 경우라면 ‘쉽게 결합’하기 어렵다고 보아야 한다.

바 가명정보

가명정보란 법 제2조제1호가목 또는 나목에 따른 개인정보를 제1호의2에 따른 가명처

리를 하여 원래의 상태로 복원하기 위한 추가 정보의 사용·결합 없이는 특정 개인을 알아볼 수 없는 정보(이하 ‘가명정보’)로서 이러한 가명정보도 개인정보에 해당한다.

가명정보는 데이터의 안전한 활용을 위해 도입된 개념으로 기본적으로 개인정보에 해당한다는 점에서 법 제58조의2에 규정된 “시간·비용·기술 등을 합리적으로 고려할 때 다른 정보를 사용하여도 더 이상 개인을 알아볼 수 없는 정보”와 다르다. 또한, 가명정보와 제2조제1호나목의 개인정보는 모두 해당 정보만으로는 특정 개인을 알아볼 수 없지만, 가명정보는 추가 정보의 사용·결합을 통해 특정 개인을 알아볼 수 있는 정보라는 점에서 다른 정보와 쉽게 결합하여 특정 개인을 알아볼 수 있는 정보인 제2조제1호나목의 개인정보와 구분된다.

추가 정보란 가명처리 과정에서 개인정보의 전부 또는 일부를 대체하는데 이용된 수단이나 방식(알고리즘 등), 가명정보와의 비교·대조 등을 통해 삭제 또는 대체된 개인정보 부분을 복원할 수 있는 정보를 말한다. 제2조제1호나목의 다른 정보와 추가 정보는 해당 정보와 결합하여 특정 개인을 알아볼 수 있도록 하는 정보에 해당한다. 하지만, 다른 정보는 해당 정보와 결합하여 특정 개인을 알아볼 수 있도록 하는 정보라면 처리하는 자가 보유하고 있거나 합법적으로 접근·입수할 수 있는 정보 모두가 다른 정보가 될 수 있지만, 추가 정보는 가명처리 과정에서 생성·사용된 정보로 제한된다. 또한, 추가 정보는 해당 정보를 가명처리 전 정보로 되돌릴 수 있는 정보(복원(復元)할 수 있는 정보)인 점에서 특정 개인을 식별 가능하게 하는 다른 정보와 구분된다.

2. 관련 법률

「신용정보법」은 개인신용정보의 개념에 대해 규정하고 있다. 어떠한 정보가 개인신용정보에 해당하기 위해서는 먼저 신용정보에 해당하여야 하지만, 신용정보에 해당하지 않더라도 개인정보에는 해당할 수 있다. 예를 들어, 거래내역 등 개인의 상거래정보의 경우 거래 상대방의 신용을 판단할 때 필요한 정보만 신용정보에 해당하고 이에 해당하지 않는 상거래정보는 「개인정보 보호법」 상 개인정보에 해당한다.

신용정보법	<p>제2조 (정의) 이 법에서 사용하는 용어의 뜻은 다음과 같다.</p> <p>2. “개인신용정보”란 기업 및 법인에 관한 정보를 제외한 살아 있는 개인에 관한 신용정보로서 다음 각 목의 어느 하나에 해당하는 정보를 말한다.</p> <p>가. 해당 정보의 성명, 주민등록번호 및 영상 등을 통하여 특정 개인을 알아볼 수 있는 정보</p> <p>나. 해당 정보만으로는 특정 개인을 알아볼 수 없더라도 다른 정보와 쉽게 결합하여 특정 개인을 알아볼 수 있는 정보</p>
-------	--

법률

1의2. “가명처리”란 개인정보의 일부를 삭제하거나 일부 또는 전부를 대체하는 등의 방법으로 추가 정보가 없이는 특정 개인을 알아볼 수 없도록 처리하는 것을 말한다.

1. 가명처리

가명처리란 개인정보의 일부를 삭제하거나 일부 또는 전부를 대체하는 등의 방법으로 추가 정보가 없이는 특정 개인을 알아볼 수 없도록 처리하는 것을 말한다(제2조제1호의2). 가명처리의 기술이나 방식에는 제한이 없다. 다만, 가명정보(가명처리된 정보)는 해당 정보만으로는 특정 개인을 알아볼 수 없어야 하므로 단순히 개인정보의 일부를 삭제하거나 일부 또는 전부를 대체하는 등 기술적 처리를 한 것만으로는 가명처리가 완료되었다고 볼 수 없고, 처리 결과 해당 정보만으로는 특정 개인을 알아볼 수 없어야 제대로 된 가명처리가 이루어졌다고 볼 수 있다. 즉, 성명이나 주민등록번호, 주소 중 일부를 삭제하고 휴대전화번호와 전자우편주소는 다른 정보로 대체하였으나 해당 정보를 통해 특정 개인을 알아볼 수 있다면 가명처리가 제대로 이루어졌다고 볼 수 없다.

2. 관련 법률

「개인정보 보호법」과 「신용정보법」에서 가명처리 및 가명정보의 개념은 법률상 표현이 다소 다르게 되어 있으나, 데이터 분석·이용의 활성화라는 동일한 입법목적 하에 도입된 개념으로 법률 해석상 그 내용은 동일하다고 보아야 한다.

<p>신용정보법</p>	<p>제2조 (정의) 이 법에서 사용하는 용어의 뜻은 다음과 같다.</p> <p>15. “가명처리”란 추가정보를 사용하지 아니하고는 특정 개인인 신용정보주체를 알아볼 수 없도록 개인신용정보를 처리(그 처리 결과가 다음 각 목의 어느 하나에 해당하는 경우로서 제40조의2제1항 및 제2항에 따라 그 추가정보를 분리하여 보관하는 등 특정 개인인 신용정보주체를 알아볼 수 없도록 개인신용정보를 처리한 경우를 포함한다)하는 것을 말한다.</p> <p>가. 어떤 신용정보주체와 다른 신용정보주체가 구별되는 경우</p> <p>나. 하나의 정보집합물(정보를 체계적으로 관리하거나 처리할 목적으로 일정한 규칙에 따라 구성되거나 배열된 둘 이상의 정보들을 말한다. 이하 같다)에서나 서로 다른 둘 이상의 정보집합물 간에서 어떤 신용정보주체에 관한 둘 이상의 정보가 연계되거나 연동되는 경우</p> <p>다. 가목 및 나목과 유사한 경우로서 대통령령으로 정하는 경우</p> <p>16. “가명정보”란 가명처리한 개인신용정보를 말한다.</p>
--------------	---

제2호 | 처리

법률	2. “처리”란 개인정보의 수집, 생성, 연계, 연동, 기록, 저장, 보유, 가공, 편집, 검색, 출력, 정정(訂正), 복구, 이용, 제공, 공개, 파기(破棄), 그 밖에 이와 유사한 행위를 말한다.
표준지침	1. “개인정보 처리”란 개인정보를 수집, 생성, 연계, 연동, 기록, 저장, 보유, 가공, 편집, 검색, 출력, 정정(訂正), 복구, 이용, 제공, 공개, 파기(破棄), 그 밖에 이와 유사한 행위를 말한다.

1. 처리

개인정보를 활용하기 위해서는 수집, 생성에서부터 연계, 연동, 기록, 저장, 보유, 가공, 편집, 검색, 출력, 정정, 복구, 이용, 제공, 공개, 파기 등 다양한 처리 과정을 거치게 된다. 이 법은 이러한 일련의 과정을 포괄하는 개념으로 ‘처리’라는 용어를 사용하고 있다.

처리는 정의에서 규정한 행위 외에도 ‘그 밖에 이와 유사한 모든 행위’가 포함되는데, 여기에는 개인정보의 전송, 전달, 이전, 열람, 조회, 수정, 보완, 삭제, 공유, 보존, 파쇄 등이 포함될 수 있다.

다만, 다른 사람이 처리하고 있는 개인정보를 단순히 전달, 전송 또는 통과만 시켜주는 행위는 처리에 해당하지 않는다. 예컨대 우편배달사업자나 인터넷서비스제공자는 다른 사람의 개인정보를 확인할 수는 없고 단순히 전달 또는 전송하는 업무만 담당하게 되는데 이 때 우편배달사업자 등의 전달 또는 전송행위는 개인정보의 처리로 보지 않는다.

2. 관련 법률

한편, 「신용정보법」도 정의 조항에서 ‘처리’를 규정하고 있는데 이 법과 달리 ‘수집’에 조사를 포함한다는 취지를 명시하고 있고, ‘결합’을 처리의 개념에 포함하고 있다.

신용정보법	제2조제13호 “처리”란 신용정보의 수집(조사를 포함한다. 이하 같다), 생성, 연계, 연동, 기록, 저장, 보유, 가공, 편집, 검색, 출력, 정정(訂正), 복구, 이용, 결합, 제공, 공개, 파기(破棄), 그 밖에 이와 유사한 행위를 말한다.
-------	--

3. “정보주체”란 처리되는 정보에 의하여 알아볼 수 있는 사람으로서 그 정보의 주체가 되는 사람을 말한다.

1. 정보주체

정보주체란 처리되는 정보에 의하여 알아볼 수 있는 사람으로서 그 정보의 주체가 되는 사람을 말한다. 이 법에 의한 권리의 귀속 및 행사주체라고도 할 수 있다. 이 법의 보호를 받는 정보주체가 되기 위해서는 첫째, 처리되는 정보에 의하여 알아볼 수 있는 사람이어야 하고, 둘째, 법인이나 단체가 아닌 살아있는 사람이어야 하며, 셋째, 처리되는 정보의 주체가 되는 자이어야 한다.

그가 살아 있는 사람인 한 국적이거나 신분에 관계 없이 누구나 정보주체가 될 수 있다. 다시 말해 대한민국 국적을 가지고 있지 않은 외국인도 이 법에 따라 개인정보가 처리되는 경우에는 정보주체가 될 수 있고, 소비자, 근로자, 학생, 교사, 군인, 공무원, 환자, 피의자, 수형자, 행정조치 대상자 등 누구든지 공평하게 이 법에 의해 보호를 받는 정보주체가 될 수 있다.

2. 관련 법률

「신용정보법」은 「개인정보 보호법」의 정보주체 개념과 유사하게 처리된 신용정보로 알아볼 수 있는 자로서 그 신용정보의 주체가 되는 자를 신용정보주체로 규정하고 있다. 한편, 「개인정보 보호법」상 정보통신서비스 제공자등에 적용되는 특례 조항은 보호대상을 「정보통신망법」상 이용자로 규정하고 있어(제18조제2항 단서 참조) 서비스의 이용관계에 있는 자로 한정하고 있다.

정보통신망법	제2조제4호 “이용자”란 정보통신서비스 제공자가 제공하는 정보통신서비스를 이용하는 자를 말한다.
신용정보법	제2조제3호 “신용정보주체”란 처리된 신용정보로 알아볼 수 있는 자로서 그 신용정보의 주체가 되는 자를 말한다.

제4호 | 개인정보파일

법률

4. “개인정보파일”이란 개인정보를 쉽게 검색할 수 있도록 일정한 규칙에 따라 체계적으로 배열하거나 구성한 개인정보의 집합물(集合物)을 말한다.

개인정보를 쉽게 검색할 수 있도록 일정한 규칙에 따라 체계적으로 배열하거나 구성한 개인정보의 집합물을 의미한다. 즉 개인의 이름이나 고유식별정보, ID 등을 색인(index)이나 검색 값으로 하여 쉽게 검색할 수 있도록 체계적으로 배열·구성한 집합물을 말한다.

개인정보파일은 일반적으로 전자적 형태로 구성된 데이터베이스(database; DB)를 의미하는 경우가 많지만, 그 외에 체계적인 검색·열람을 위한 색인이 되어 있는 수기(手記) 문서 자료 등도 포함된다.

개인정보파일의 대표적인 예로는 기업에서 고객의 성명, ID 등으로 검색·활용이 가능하도록 구성된 고객정보 데이터베이스, 병원에서 환자에 대해 작성된 진료기록부 파일, 공공기관에서 관리하는 각종 행정처분 내역 파일 등을 들 수 있다. 그러나 개인정보가 기재되어 있는 문서의 단순한 집합물에 불과하고 체계적으로 배열·검색할 수 있도록 구성되어 있지 않은 경우는 개인정보파일에 해당하지 않는다.

결정례 블랙박스로 촬영된 영상의 개인정보파일 해당 여부

‘개인정보 파일’이란 개인정보를 쉽게 검색할 수 있도록 규칙에 따라 체계적으로 배열하거나 구성한 개인정보의 집합물을 말하는데(제2조제3호 참조), 블랙박스로 촬영된 영상정보는 촬영일시 등에 따라 체계적으로 배열하여 저장되므로 개인정보파일에 해당한다(보호위원회 결정 제2017-13-100호).

제5호 | 개인정보처리자

법률

5. “개인정보처리자”란 업무를 목적으로 개인정보파일을 운용하기 위하여 스스로 또는 다른 사람을 통하여 개인정보를 처리하는 공공기관, 법인, 단체 및 개인 등을 말한다.

표준지침

2. “개인정보처리자”란 업무를 목적으로 법 제2조제4호에 따른 개인정보파일을 운용하기 위하여 개인정보를 처리하는 모든 공공기관, 영리목적의 사업자, 협회·동창회 등 비영리기관·단체, 개인 등을 말한다.

1. 개인정보처리자

이 법의 수범자는 기본적으로 개인정보처리자이다. ‘개인정보처리자’는 업무를 목적으로 개인정보파일을 운용하기 위하여 스스로 또는 다른 사람을 통하여 개인정보를 처리하는 공공기관, 법인, 단체, 사업자 및 개인 등을 말한다.

개인정보처리자는 ‘개인정보취급자’와 구분된다. 개인정보처리자는 개인정보를 처리하는 공공기관이나 사업자·단체 등을 의미하지만, 개인정보취급자는 개인정보처리자의 지휘·감독을 받아 개인정보를 처리하는 임직원, 파견근로자, 시간제 근로자 등을 말한다(제28조제1항 참조).

가 업무를 목적으로 하여야 한다.

개인정보처리자가 되기 위해서는 ‘업무를 목적으로’ 개인정보를 처리하여야 한다. 순수한 개인적인 활동이나 가사 활동을 위해서 개인정보를 수집·이용·제공하는 자는 개인정보처리자가 아니다. 예를 들어 사적인 친분관계를 위하여 휴대폰에 연락처 정보, 이메일 주소록 등을 저장하는 경우는 개인정보처리자에 해당하지 않는다.

‘업무’란 직업상 또는 사회생활상의 지위에 기하여 계속적으로 종사하는 사무나 사업의 일체를 의미하는 것으로 보수 유무나 영리 여부와는 관계가 없으며, 단 1회의 행위라도 계속·반복의 의사가 있다면 업무로 볼 수 있다.

한편, 업무란 직업상 또는 사회생활상 지위에 기하여야 하므로 지인들에게 모임을 안내하기 위해 전화번호 및 이메일주소를 수집하는 행위나 결혼을 알리기 위해 청첩장을 돌리는 행위 또는 개인이 자신의 송사에 관한 증거 수집을 위하여 사진 촬영을 하는 경우 등은 업무를 목적으로 한 것이 아니다.

참고 ‘업무’의 개념

- 업무방해죄에 있어서의 업무란 직업 또는 사회생활상의 지위에 기하여 계속적으로 종사하는 사무나 사업의 일체를 의미하고, 그 업무가 주된 것이든 부수적인 것이든 가리지 아니하며, 일회적인 사무라 하더라도 그 자체가 어느 정도 계속하여 행해지는 것이거나 혹은 그것이 직업 또는 사회생활상의 지위에서 계속적으로 행하여 온 본래의 업무수행과 밀접불가분의 관계에서 이루어진 경우에도 이에 해당한다(대법원 2005. 4. 15. 선고 2004도8701 판결 등 참조).
- 업무상과실치사상죄에 있어서의 업무란 사람의 사회생활면에 있어서의 하나의 지위로서 계속적으로 종사하는 사무를 말하고, 여기에는 수행하는 직무 자체가 위험성을 갖기 때문에 안전배려를 의무의 내용으로 하는 경우는 물론 사람의 생명·신체의 위험을 방지하는 것을 의무내용으로 하는 업무도 포함된다 할 것이다(대법원 1988. 10. 11. 선고 88도1273 판결, 2002. 5. 31. 선고 2002도1342 판결 등 참조).
- 업무상 횡령죄에서 ‘업무’란 법령, 계약에 의한 것뿐만 아니라 관례를 좇거나 사실상의 것이거나를 묻지 않고 같은 행위를 반복할 지위에 따른 사무를 가리키는 것이다(대법원 2006. 4. 27. 선고 2003도135).

나 개인정보파일을 운용하기 위한 것이어야 한다.

개인정보를 수집·이용·제공하고 있다고 해서 모두가 개인정보처리자가 되는 것은 아니다. 「개인정보 보호법」상 개인정보처리자가 되기 위해서는 개인정보파일을 운용하기 위하여 개인정보를 처리하는 자만이 개인정보처리자가 된다.

EU의 「일반 개인정보 보호법」(GDPR, 2018)을 비롯하여 영국, 일본 등의 개인정보 보호 법령도 모든 개인정보가 아니라 특정한 파일체계의 일부를 구성하고 있거나, 구성하도록 예정되어 있거나, 그런 의도로 처리되는 개인정보에 한하여 해당 법령의 적용을 받도록 규정하고 있다.

일회성 메모나 문서작성 행위까지 개인정보 처리로 본다면 법이 개인의 사소한 행위에 까지 규제하게 되어 불합리한 결과를 초래하게 된다. 이에 따라 개인정보 수집·이용·제공 등에 대한 동의, 개인정보에 대한 보호조치 등의 의무를 부과하는 대상은 개인정보파일을 운용하는 자로 한정하여 규제의 합목적성과 실효성을 담보하고자 하였다.

다 스스로 또는 다른 사람을 통하여 개인정보를 처리해야 한다.

개인정보처리자는 스스로 개인정보를 처리할 수도 있지만 다른 사람을 통해서도 개인정보를 처리할 수 있다. 즉 자신이 직접 개인정보를 수집, 가공, 편집, 이용, 제공, 전송하지 아니하고 다른 사람 예컨대 수탁자, 대리인, 이행보조자 등을 통해서 처리하는 경우에도 개인정보처리자에 해당한다.

라 공공기관, 법인, 단체, 개인 등이어야 한다.

이 법은 개인정보 보호를 위한 일반법이므로 개인정보를 수집, 이용, 제공 등 처리하는 모든 자에게 적용될 수 있도록 ‘개인정보처리자’의 개념을 폭넓게 정의하였다. 적용 대상을 특정 목적이나 업종으로 한정하는 것은 개인정보 보호 사각지대 해소라는 법률 제정 취지에 부합하지 않기 때문이다.

개인정보처리자는 공공기관, 영리·비영리 법인, 영리·비영리 단체, 개인이 모두 포함된다. 기존 「공공기관 개인정보 보호법」, 「정보통신망법」 등과 달리 공공부문과 민간 부문이 모두 포함되며, 주식회사와 같은 영리기업은 물론 동창회·동호회와 같은 비영리 단체도 포함된다. 개인에는 1인 사업자, 개인활동가 등 본인의 업무를 목적으로 개인정보를 처리하는 경우가 포함된다.

그런데 여기서 ‘개인’은 ‘본인의 업무를 목적으로 개인정보를 처리하는 자’이므로 ‘공공기관, 영리·비영리 법인, 영리·비영리 단체, 개인’의 ‘대리인, 사용인, 그 밖의 종업원으로서의 지위에 있는 개인’은 개인정보처리자에 해당하지 않는다. 법 제28조제1항은 임직원, 파견근로자, 시간제근로자 등 개인정보처리자의 지휘·감독을 받아 개인정보를 처리하는 자를 ‘개인정보취급자’라고 정의하고 있다.

참고 한국의 개인정보처리자, 취급자 및 EU의 Controller, Processor 간 비교		
	한국(「개인정보 보호법」)	EU(「GDPR」)
	개인정보처리자(제2조제5호)	Controller(제4조제7항)
정의	업무를 목적으로 개인정보 파일을 운용하기 위하여 스스로 또는 다른 사람을 통하여 개인정보를 처리하는 공공기관, 법인, 단체 및 개인 등을 말한다.	단독으로 또는 제3자와 공동으로 개인정보 처리의 목적 및 방법을 결정하는 자연인 또는 법인, 공공기관, 기관, 기타 기구를 가리킨다.
	개인정보취급자(제28조제1항)	Processor(제4조제8항)
정의	개인정보처리자의 지휘·감독을 받아 개인정보를 처리하는 업무를 담당하는 자로서 임직원, 파견근로자, 시간제근로자 등을 말한다.	컨트롤러를 대신하여 개인정보를 처리하는 자연인이나 법인, 공공기관, 기관 또는 기타 기구를 가리킨다.

- 「개인정보 보호법」 상 처리자, 취급자의 개념과 GDPR의 컨트롤러, 프로세서의 개념이 동일한 것으로 이해되나 실제로는 개념적 차이 존재
- 「개인정보 보호법」은 처리자 중심으로 규율하는 반면, GDPR은 컨트롤러와 프로세서 양자 모두를 규율
 - 프로세서에게 법정 의무를 부여(제28조제3항)하면서 특정한 경우 벌칙 부과

※ 제82조(보상 권리 및 책임) / 제83조(행정 과태료 부과에 관한 일반 조건) / 제84조(처벌)

2. 관련 법률

「신용정보법」은 법 수범자로서 신용정보제공자와 이용자를 규정하고 있다. 이는 상거래를 위하여 신용정보를 타인에게 제공하거나 제공받아 본인의 영업에 이용하는 자 및 이에 준하는 자를 말하므로 「개인정보 보호법」상의 개인정보처리자와는 차이가 있다. 한편, 「개인정보 보호법」상 정보통신서비스 제공자등에 적용되는 특례 조항에서는 「정보통신망법」상 정보통신서비스 제공자등을 수범자로 하고 있다(제6장 정보통신서비스 제공자등의 개인정보 처리 등 특례규정 개관 부분 참조). 정보통신서비스 제공자는 「전기통신사업법」에 의한 전기통신사업자 및 영리를 목적으로 전기통신사업자의 전기통신역무를 이용하여 정보를 제공 또는 정보 제공을 매개하는 자를 말한다.

정보통신망법	제2조제3호 “정보통신서비스 제공자”란 「전기통신사업법」 제2조제8호에 따른 전기통신사업자와 영리를 목적으로 전기통신사업자의 전기통신역무를 이용하여 정보를 제공하거나 정보의 제공을 매개하는 자를 말한다.
신용정보법	제2조제7호 “신용정보제공·이용자”란 고객과의 금융거래 등 상거래를 위하여 본인의 영업과 관련하여 얻거나 만들어 낸 신용정보를 타인에게 제공하거나 타인으로부터 신용정보를 제공받아 본인의 영업에 이용하는 자와 그 밖에 이에 준하는 자로서 대통령령으로 정하는 자를 말한다.

3. 질의응답

- Q** | 개인정보처리자로부터 제공받은 개인정보를 처리(저장, 정정, 복구 등)하는 자는 개인정보처리자(해외소재 회사 포함)인지?
- A** | 다른 사람을 통하여 개인정보를 수집하는 자도 개인정보처리자에 해당되며, 개인정보처리자로부터 제공받은 개인정보를 처리하는 자도 개인정보처리자가 된다.

제6호 | 공공기관

법률	6. “공공기관”이란 다음 각 목의 기관을 말한다. 가. 국회, 법원, 헌법재판소, 중앙선거관리위원회의 행정사무를 처리하는 기관, 중앙행정기관(대통령 소속 기관과 국무총리 소속 기관을 포함한다) 및 그 소속 기관, 지방자치단체 나. 그 밖의 국가기관 및 공공단체 중 대통령령으로 정하는 기관
시행령	제2조(공공기관의 범위) 「개인정보 보호법」(이하 “법”이라 한다) 제2조제6호나목에서 “대통령령으로 정하는 기관”이란 다음 각 호의 기관을 말한다. 1. 「국가인권위원회법」 제3조에 따른 국가인권위원회 1의2. 「고위공직자범죄수사처 설치 및 운영에 관한 법률」 제3조제1항에 따른 고위공직자범죄수사처 2. 「공공기관의 운영에 관한 법률」 제4조에 따른 공공기관 3. 「지방공기업법」에 따른 지방공사와 지방공단 4. 특별법에 따라 설립된 특수법인 5. 「초·중등교육법」, 「고등교육법」, 그 밖의 다른 법률에 따라 설치된 각급 학교
표준지침	3. “공공기관”이란 법 제2조제6호 및 「개인정보 보호법 시행령」(이하 “영”이라 한다) 제2조에 따른 기관을 말한다.

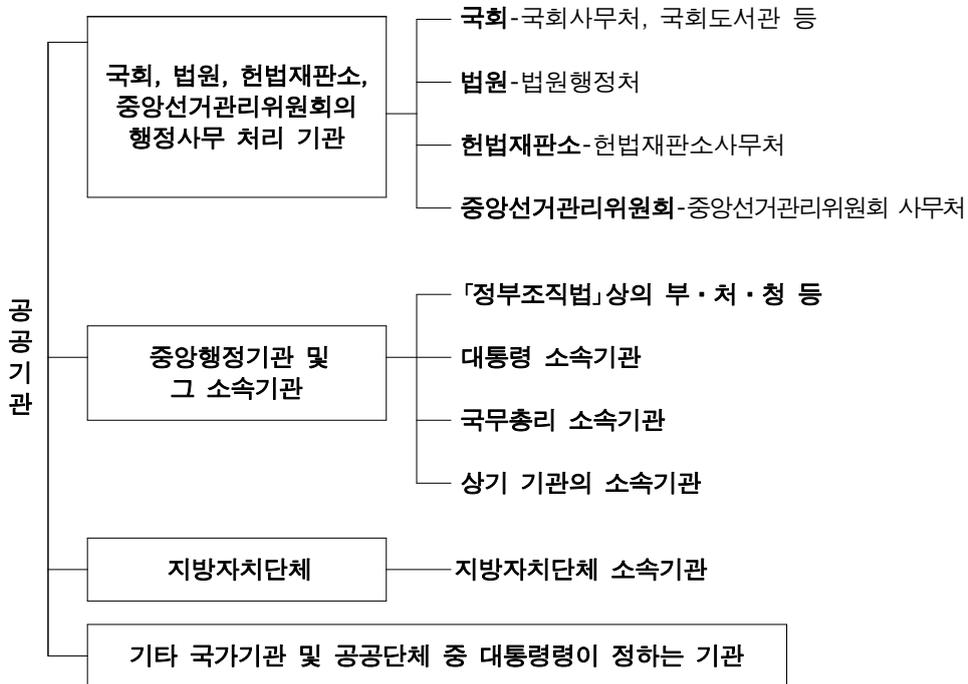
1. 공공기관

이 법은 공공부문과 민간부문을 구분하지 않고 하나의 법률에 의하여 동일한 개인정보 보호 원칙을 적용하는 단일법주의를 채택하고 있다. 하지만 공공기관에 대해서는 몇 가지 달리 정하는 바가 있다.

< 공공기관에 대하여 달리 정한 규정 >

의무가 강화된 조항	의무가 완화된 조항
<ul style="list-style-type: none"> ▪ 개인정보 목적 외 이용·제공의 법적근거, 목적 및 범위 등 공개의무 (제18조제4항) ▪ 영상정보처리기기 설치·운영시 공청회·설명회 등 의견수렴 의무(제25조제3항) ▪ 영상정보처리기기 설치·운영에 관한 업무위탁 절차·요건 강화(제25조제8항) ▪ 개인정보파일 등록·공개 의무(제32조) ▪ 개인정보 영향평가 실시의무(제33조) ▪ 개인정보열람 요구권 행사 편의를 위한 별도의 단일창구 마련(제35조제1항) ▪ 개인정보 분쟁조정에 응할 의무(제43조제3항) 	<ul style="list-style-type: none"> ▪ 정보주체 동의 없는 개인정보 수집·이용 사유 확대 (제15조제1항제3호) ▪ 개인정보 목적 외 이용·제공 사유의 확대 (제18조제2항단서) ▪ 개인정보처리방침 제정·공개 의무 완화 (제30조제1항) ▪ 개인정보 열람요구권 제한·거절 사유 확대 (제35조제4항제3호) ▪ 개인정보처리 정지요구 대상 개인정보의 범위 제한(제37조제1항 단서) ▪ 개인정보처리 정지요구권 거절 사유 확대 (제37조제2항제3호) ▪ 통계법에 따라 처리된 개인정보에 대한 법률 적용의 일부 제외(제58조제1항제1호)

< 공공기관의 분류 >



가 헌법기관

국회·법원·헌법재판소·중앙선거관리위원회의 행정사무를 처리하는 기관이라 함은 각각 국회사무처, 국회도서관, 국회입법조사처, 국회예산정책처, 법원행정처, 헌법재판소 사무처, 중앙선거관리위원회사무처 등을 말한다.

나 중앙행정기관 및 그 소속 기관

중앙행정기관에는 「정부조직법」 제2조제2항에 따른 중앙행정기관(부·처·청)과 동법 제5조의 합의제행정기관이 포함된다.

중앙행정기관에는 대통령 소속기관과 국무총리 소속기관도 포함된다. 대통령 소속기관으로는 감사원, 국가정보원, 방송통신위원회 등이 있고, 국무총리 소속기관으로는 법제처, 국가보훈처, 공정거래위원회, 금융위원회, 국민권익위원회 등이 있다.

중앙행정기관의 소속기관도 공공기관에 해당되므로 중앙행정기관이 그 소관 사무의 수행을 위하여 설치·운영하는 「정부조직법」 제3조의 특별지방행정기관(지방우정청, 지방국세청 등)과 제4조의 부속기관(시험연구기관, 교육훈련기관, 문화기관, 의료기관, 제조기관, 자문기관 등)도 공공기관에 포함된다.

「국가인권위원회법」 제3조에 따른 국가인권위원회는 시행령 제2조제1호에 따라 “그 밖의 국가기관 및 공공단체 중 대통령령으로 정하는 기관”에 포함된다.

다 지방자치단체

지방자치단체란 국가 아래에서 국가 영토의 일부를 구성요소로 하고 그 구역 안의 주민을 법률이 정하는 범위 안에서 지배할 수 있는 권한을 가진 단체를 말한다. 지방자치단체는 자치행정의 주체로서 국가로부터 행정권의 일부를 부여받은 공공단체이며 「지방자치법」 제3조제1항에 따라 공법인(公法人)이기도 하다.

지방자치단체의 종류로는 우선 「지방자치법」 제2조제1항에 따른 광역자치단체(특별시, 광역시, 특별자치시, 도, 특별자치도)와 기초자치단체(시, 군, 구)가 있으며, 동법 제2조제3항에 따른 특별지방자치단체(자치단체조합)가 있다.

또한 지방자치단체 소속 행정기관으로 자치경찰기관, 소방기관, 교육훈련기관, 보건진료기관, 시험연구기관 및 중소기업지도기관 등의 직속기관이 있고(「지방자치법」 제113조), 그 밖에 사업소(「지방자치법」 제114조), 출장소(「지방자치법」 제115조), 합의제

행정기관(「지방자치법」 제116조), 심의회·위원회 등의 자문기관(「지방자치법」 제116조의2) 등도 지방자치단체 소속 행정기관에 포함된다. 그 외에 지방자치단체 하부행정기관으로 자치구가 아닌 구, 읍, 면, 동이 있다(「지방자치법」 제117조).

한편, 지방자치단체의 교육·과학 및 체육에 관한 사무를 분장하기 위하여 「지방교육자치에 관한 법률」에 따라 교육감(제18조), 하급교육행정기관(제34조) 등의 별도기관이 있다.

라 「공공기관의 운영에 관한 법률」 제4조에 따른 공공기관

「공공기관의 운영에 관한 법률」 제4조에 따라 지정된 기관을 말하며, 공기업(시장형 공기업, 준시장형 공기업), 준정부기관(기금관리형 준정부기관, 위탁집행형 준정부기관), 기타 공공기관으로 구분된다. 동 법 제6조에 따라 기획재정부장관은 매 회계연도 개시 후 1개월 이내에 공공기관을 새로 지정하거나, 지정을 해제하거나, 구분을 변경하여 지정하고 이를 고시한다.¹⁾

마 지방공사 및 지방공단

지방자치단체가 수도사업, 공업용 수도사업, 궤도사업, 자동차운송사업, 지방유료도로사업, 하수도사업, 주택사업, 토지개발사업 등을 효율적으로 수행하기 위하여 「지방공기업법」에 따라 설립한 지방공사(제49조)와 지방공단(제76조)도 공공기관에 해당한다.

바 특별법에 따라 설립된 특수법인

특별법에 의하여 설립된 특수법인들도 공공기관에 포함된다. 특수법인이란 일반적으로 특정한 국가적 정책이나 공공의 이익을 달성하기 위한 사업의 수행을 위하여 「민법」·「상법」 이외의 특별법이나 특별규정에 의하여 설립되는 비영리법인을 말한다. 당해 법인의 설치 및 규율을 목적으로 특별히 제정된 법률에 의하여 설립된 법인뿐만 아니라 「민법」·「상법」에 대한 상대적 의미로서의 특별법 규정에 따라 설립된 법인도 포함될 수 있다.

당해 법인의 설치 및 규율을 목적으로 특별히 제정된 법률에 의하여 설립된 법인에 국한하지 않는다고 하더라도 직·간접적으로 국가나 지방자치단체의 재정지원을 받으며, 공익적인 사무를 수행함으로써 행정상의 권리와 의무의 귀속 주체가 되어야 하고, 정책 결정과 관련하여 사실상 국가 또는 지자체의 지배력 하에 있어야 한다.

1) 기획재정부가 운영하는 '공공기관 경영정보시스템-www.alio.go.kr'참조

이처럼 특별법에 근거해서 설립되었다고 해서 모든 법인이 특수법인이 되는 것은 아니며, 설립목적, 운영실태 등을 종합적으로 고려해서 개별적으로 평가되어야 한다. 특수법인이 되기 위해서는 최소한 특별법에 의한 설치, 국가·자자체 등으로부터의 재정지원, 국가 또는 지자체 사무의 수탁 처리, 사실상 국가 또는 지자체의 지배, 공공 또는 공익 기능 수행 등의 본질적 요소를 갖추어야 한다.

사 각급 학교

「초·중등교육법」, 「고등교육법」 및 그 밖의 다른 법률에 따라 설치된 각급 학교들도 공공기관으로 취급된다. 「초·중등교육법」에 따라 설치된 학교로는 초등학교, 중학교·고등공민학교, 고등학교·고등기술학교, 방송통신중학교, 방송통신고등학교, 특수학교, 각종학교, 대안학교, 외국인학교 등이 있고, 「고등교육법」에 따라 설치된 학교로는 대학, 산업대학, 교육대학, 전문대학, 원격대학(방송대학·통신대학·방송통신대학·사이버대학), 기술대학, 대학원대학, 각종학교 등이 있다.

다른 법률에 따라 설치된 각급 학교로는 공군항공과학고등학교(「공군항공과학고등학교 설치법」), 육군사관학교·해군사관학교·공군사관학교(「사관학교 설치법」), 국방대학교(「국방대학교 설치법」), 육군3사관학교(「육군3사관학교 설치법」), 국군간호사관학교(「국군간호사관학교 설치법」), 경찰대학(「경찰대학 설치법」), 울산과학기술원(「울산과학기술원법」) 한국농수산대학(「한국농수산대학 설치법」), 기능대학법, 국가정보대학원(「국가정보대학원 설치법」), 법학전문대학원(「법학전문대학원 설치·운영에 관한 법률」) 등이 있다.

한편, 「법학전문대학원 설치·운영에 관한 법률」에 따라 설립된 법학전문대학원은 「고등교육법」에 따른 대학 소속으로 되어있어 개인정보처리자가 법학전문대학원인지, 아니면 법학전문대학원이 설치된 대학인지 해석상 다툼이 있을 수 있다. 그런데 법학전문대학원은 입학생 선발, 교무행정, 졸업생 사정 및 학사업무 등이 대학의 통제를 받는 점 등을 고려하면 법학전문대학원은 비록 ‘다른 법률에 따라 설치된 학교’ 이지만 독립된 개인정보처리자가기 보다는 해당 대학이 개인정보처리자인 것으로 해석하는 것이 타당하다.

제7호 | 영상정보처리기기

법률	7. “영상정보처리기기”란 일정한 공간에 지속적으로 설치되어 사람 또는 사물의 영상 등을 촬영하거나 이를 유·무선망을 통하여 전송하는 장치로서 대통령령으로 정하는 장치를 말한다.
시행령	제3조(영상정보처리기기의 범위) 법 제2조제7호에서 “대통령령으로 정하는 장

	<p>치”란 다음 각 호의 장치를 말한다.</p> <ol style="list-style-type: none"> 1. 폐쇄회로 텔레비전 : 다음 각 목의 어느 하나에 해당하는 장치 <ul style="list-style-type: none"> 가. 일정한 공간에 지속적으로 설치된 카메라를 통하여 영상 등을 촬영하거나 촬영한 영상정보를 유무선 폐쇄회로 등의 전송로를 통하여 특정 장소에 전송하는 장치 나. 가목에 따라 촬영되거나 전송된 영상정보를 녹화·기록할 수 있도록 하는 장치 2. 네트워크 카메라 : 일정한 공간에 지속적으로 설치된 기기로 촬영한 영상정보를 그 기기를 설치·관리하는 자가 유무선 인터넷을 통하여 어느 곳에서나 수집·저장 등의 처리를 할 수 있도록 하는 장치
표준지침	<ol style="list-style-type: none"> 8. “영상정보처리기기”란 일정한 공간에 지속적으로 설치되어 사람 또는 사물의 영상 등을 촬영하거나 이를 유·무선망을 통하여 전송하는 일체의 장치로서 영 제3조에 따른 폐쇄회로 텔레비전 및 네트워크 카메라를 말한다. 9. “개인영상정보”란 영상정보처리기기에 의하여 촬영·처리되는 영상정보 중 개인의 초상, 행동 등과 관련된 영상으로서 해당 개인을 식별할 수 있는 정보를 말한다. 10. “영상정보처리기기운영자”란 법 제25조제1항 각 호에 따라 영상정보처리기기를 설치·운영하는 자를 말한다. 11. “공개된 장소”란 공원, 도로, 지하철, 상가 내부, 주차장 등 불특정 또는 다수가 접근하거나 통행하는 데에 제한을 받지 아니하는 장소를 말한다.

1. 영상정보처리기기

영상을 촬영하여 처리할 수 있는 기기의 용도와 종류는 매우 다양하므로 이 법은 개인 정보 보호의 필요성과 규제의 실익이 있는 경우로 영상정보처리기기의 범위를 한정하고 있다.

법 제2조제7호는 영상정보처리기기를 ‘일정한 공간에 지속적으로 설치되어 사람 또는 사물의 영상 등을 촬영하거나 이를 유·무선망을 통하여 전송하는 장치로서 대통령령으로 정하는 장치’로 정의하고 있다.

가 일정한 공간에 지속적으로 설치

이 법에 따른 영상정보처리기기는 ‘일정한 공간’에 설치되어 있어야 한다. 예컨대 건물 실내, 도로, 공원 등 일정한 공간에 기반하여 영상정보처리기기가 설치되어 있어야 함을 의미한다. 또한, 영상정보처리기기는 일정한 공간에 설치되어 있는 것만을 포함하므로,

그 촬영 범위도 일정한 공간이나 구역을 촬영하는 것으로 한정된다.

또한 이 법의 규제대상이 되는 영상정보처리기기는 ‘지속적’으로 설치되어 있는 영상정보처리기기만을 의미한다. 여기서 지속적 설치의 의미는 영상정보처리기기를 어느 정도 고정적·항구적(恒久的)으로 운영할 목적으로 설치된 것을 말한다.

예를 들어, 개인이 휴대하고 있는 캠코더, 디지털카메라 등으로 촬영 공간과 촬영 대상 범위를 바꾸어 가면서 영상을 촬영하는 것은 이 법에 따른 영상정보처리기기의 범주에 포함되지 않는다. 만약 개인용 영상기기를 일정한 공간에 설치해 두고 영상을 촬영한다고 하더라도, 그것이 고정적·항구적으로 운영할 목적이 아닌 이상은 역시 이 법에 따른 영상정보처리기기가 아니다.

다만, ‘일정한 공간’이라는 의미는 반드시 ‘고정된 장소’를 의미하는 것은 아니다. 만약 이동성이 있는 공간이라 하더라도 그 촬영기기의 설치 위치와 촬영 범위가 일정하게 한정되어 있다면 이 법에 따른 영상정보처리기기에 해당된다.

예를 들어 버스, 택시 등 영업용 차량 내부에 설치된 CCTV는 차량 내부라는 일정한 공간에 설치되어 일정한 승객 탑승공간을 촬영하고 있으므로 이 법에 따른 영상정보처리기기에 해당된다. 반면, 이른바 ‘차량 블랙박스’와 같이 차량 내부에 설치되어 있으면서도 차량 주행에 따라 외부를 촬영하는 기기의 경우에는 촬영 대상·범위가 수시로 변동되므로 이 법에 따른 영상정보처리기기에 해당되지 않는다.

한 가지 주의할 점은 이 법에 따른 영상정보처리기기가 아닌 장치를 통하여 개인을 촬영하는 행위는 제25조에 따른 영상정보처리기기 규제는 적용되지 않으나, 경우에 따라서 이 법의 다른 조항이나 다른 법이 적용될 수 있다는 것이다.

예를 들어, 업무를 목적으로 개인정보파일을 운용하기 위해 개인정보처리자가 개인(들)에 대한 영상을 촬영하는 경우에는 이 법에 따른 개인정보 수집·이용 규정 등이 적용될 수 있다. 또한 성적 욕망 또는 수치심을 유발할 수 있는 타인의 신체를 그 의사에 반하여 촬영하는 행위 등은 「성폭력범죄의 처벌 등에 관한 특례법」에 의하여 처벌될 수 있다.

제14조(카메라 등을 이용한 촬영) ① 카메라나 그 밖에 이와 유사한 기능을 갖춘 기계장치를 이용하여 성적 욕망 또는 수치심을 유발할 수 있는 사람의 신체를 촬영 대상자의 의사에 반하여 촬영한 자는 7년 이하의 징역 또는 5천만 원 이하의 벌금에 처한다.

② 제1항에 따른 촬영물 또는 복제물(복제물의 복제물을 포함한다. 이하 이 조에서 같다)을 반포·판매·임대·제공 또는 공공연하게 전시·상영(이하 “반포등”이라 한다)한 자 또는 제1항의 촬영이 촬영 당시에는 촬영 대상자의 의사에 반하지 아니한 경우(자신의 신체를 직접 촬영한 경우를 포함한다)에도 사후에 그 촬영물 또는 복제물을 촬영대상자의 의사에 반하여 반포등을 한 자는 7년 이하의 징역 또는 5천만 원 이하의 벌금에 처한다.

③ 영리를 목적으로 촬영 대상자의 의사에 반하여 「정보통신망 이용촉진 및 정보보호 등에 관한 법률」 제2조제1항제1호의 정보통신망(이하 “정보통신망”이라 한다)을 이용하여 제2항의 죄를 범한 자는 3년 이상의 유기징역에 처한다.

④ 제1항 또는 제2항의 촬영물 또는 복제물을 소지·구입·저장 또는 시청한 자는 3년 이하의 징역 또는 3천만 원 이하의 벌금에 처한다.

⑤ 상습으로 제1항부터 제3항까지의 죄를 범한 때에는 그 죄에 정한 형의 2분의 1까지 가중한다.

나 사람 또는 사물의 영상 등을 촬영

사회 통념상 ‘영상을 촬영’ 한다는 개념에는 음성·음향 녹음도 포함된다고 볼 수 있다. 그러나 CCTV와 같은 영상정보처리기는 일정한 장소에 지속적으로 설치되어 그 촬영 범위 안에 있는 것을 전부 촬영하므로, 만약 영상정보처리기에 음성·음향까지 녹음된다면 예기치 않게 타인 간의 대화 등이 녹음될 가능성이 있다.

그러나 공개되지 아니한 타인 간의 대화를 녹음·청취하는 행위는 「통신비밀보호법」 제3조를 위반하게 된다. 따라서 「개인정보 보호법」에 따른 영상정보처리기의 ‘촬영’은 순수하게 영상만을 촬영하는 것으로 한정되며, 음성·음향을 녹음하는 것은 포함되지 않는다.

한편, 여기에서 ‘사물’이란 「개인정보 보호법」의 입법 취지를 고려할 때 이 법의 보호 대상이 되는 사람과 일정한 관계가 있는 사물로 한정하여 해석해야 한다. 예를 들어 천문대에 설치된 망원경은 비록 일정한 공간에 지속 설치되어 우주 공간(사물)을 촬영하고는 있으나 그 촬영 대상이 사람과 일정한 생활 관계에 놓여 있다고 보기 어렵기 때문에, 이 법에 따른 영상정보처리기에 포함되지 않는다.

다 촬영된 정보를 유·무선망을 통하여 전송

사람·사물의 영상을 촬영하는 것뿐만 아니라, 촬영된 정보를 유·무선망을 통하여 전송하는 장치도 영상정보처리기의 개념에 포함된다. 사실상 영상정보처리기는 단순히 영상만

을 촬영하는 것이 아니라, 그 촬영 화면을 전송하여 그 설치 목적에 따라 열람·활용하는 방식이 널리 이용되고 있다. 여기에는 폐쇄회로 텔레비전(CCTV)과 같이 촬영 화면을 폐쇄망을 통해 전송하여 모니터링하는 경우, 네트워크카메라 등과 같이 인터넷망 등을 이용해 영상을 전송하고 열람하는 경우가 모두 포함된다.

라 대통령령이 정하는 장치

사람·사물을 촬영할 수 있는 영상정보처리기는 매우 다양하다. 이 같은 기기들의 사용을 모두 엄격하게 규제할 경우 사회생활이나 경제활동에 제약을 가져올 수 있기 때문에, 이 법에 따른 영상정보처리기의 종류는 대통령령으로 정하는 기기만을 인정하고 있다. 영 제3조에서는 영상정보처리기의 종류를 아래와 같이 규정하고 있다.

< 영상정보처리기의 종류 >

종 류	내 용
폐쇄회로 텔레비전	일정한 공간에 지속적으로 설치된 카메라를 통하여 영상 등을 촬영하거나 이를 유·무선 폐쇄회로 등의 전송로를 통해 전송 또는 저장매체에 녹화·기록할 수 있도록 하는 장치
네트워크 카메라	일정한 공간에 지속적으로 설치된 촬영기기로 수집한 영상정보를 유·무선 인터넷을 통하여 어느 곳에서나 수신·조작·저장 등의 처리를 할 수 있도록 하는 장치

제8호 | 과학적 연구

법률

8. “과학적 연구”란 기술의 개발과 실증, 기초연구, 응용연구 및 민간 투자 연구 등 과학적 방법을 적용하는 연구를 말한다.

1. 과학적 연구

개인정보처리자는 과학적 연구를 위하여 정보주체의 동의 없이 가명정보를 처리할 수 있다(제28조의2제1항). 과학적 연구는 과학적 방법을 적용하는 연구를 말하며 자연과학, 사회과학, 의료 등 다양한 분야에서 이루어질 수 있다. 여기서, 과학적 방법이란 체계적이고 객관적인 방법으로 검증 가능한 질문에 대해 연구하는 것을 말한다. 과학적 연구는 기술의 개발과 실증, 기초 연구, 응용 연구뿐만 아니라 새로운 기술·제품·서비스 개발 등 산업적 목적을 위해서도 수행이 가능하며, 민간 투자 연구도 가능하다.

참고로 「신용정보법」의 제32조제6항제9호의2는 통계작성, 연구, 공익적 기록보존 등을 위하여 가명정보를 제공할 수 있도록 규정하고 있으며, 여기에서의 연구에는 산업적 연구가 포함된다. 「신용정보법」과 「개인정보 보호법」상의 과학적 연구의 개념은 모두 산업적 연구를 포함하는 것으로 해석할 수 있다.

제3조 | 개인정보 보호 원칙

법률

제3조(개인정보 보호 원칙) ① 개인정보처리자는 개인정보의 처리 목적을 명확하게 하여야 하고 그 목적에 필요한 범위에서 최소한의 개인정보만을 적법하고 정당하게 수집하여야 한다.

② 개인정보처리자는 개인정보의 처리 목적에 필요한 범위에서 적법하게 개인정보를 처리하여야 하며, 그 목적 외의 용도로 활용하여서는 아니 된다.

③ 개인정보처리자는 개인정보의 처리 목적에 필요한 범위에서 개인정보의 정확성, 완전성 및 최신성이 보장되도록 하여야 한다.

④ 개인정보처리자는 개인정보의 처리 방법 및 종류 등에 따라 정보주체의 권리가 침해받을 가능성과 그 위험 정도를 고려하여 개인정보를 안전하게 관리하여야 한다.

⑤ 개인정보처리자는 개인정보 처리방침 등 개인정보의 처리에 관한 사항을 공개하여야 하며, 열람청구권 등 정보주체의 권리를 보장하여야 한다.

⑥ 개인정보처리자는 정보주체의 사생활 침해를 최소화하는 방법으로 개인정보를 처리하여야 한다.

⑦ 개인정보처리자는 개인정보를 익명 또는 가명으로 처리하여도 개인정보 수집목적 달성을 수 있는 경우 익명처리가 가능한 경우에는 익명에 의하여, 익명처리로 목적을 달성할 수 없는 경우에는 가명에 의하여 처리될 수 있도록 하여야 한다.

⑧ 개인정보처리자는 이 법 및 관계 법령에서 규정하고 있는 책임과 의무를 준수하고 실천함으로써 정보주체의 신뢰를 얻기 위하여 노력하여야 한다.

표준지침

제4조(개인정보 보호 원칙) ① 개인정보처리자는 개인정보 처리 목적을 명확하게 하여야 하고 그 목적에 필요한 범위에서 최소한의 개인정보만을 적법하고 정당하게 수집하여야 한다.

② 개인정보처리자는 개인정보의 처리 목적에 필요한 범위에서 적법하게 개인정보를 처리하여야 하며, 그 목적 외의 용도로 활용하여서는 아니 된다.

③ 개인정보처리자는 개인정보의 처리 목적에 필요한 범위에서 개인정보의 정확성과 최신성을 유지하도록 하여야 하고, 개인정보를 처리하는 과정에서 고의 또는 과실로 부당하게 변경 또는 훼손되지 않도록 하여야 한다.

- ④ 개인정보처리자는 개인정보의 처리 방법 및 종류 등에 따라 정보주체의 권리가 침해받을 가능성과 그 위험 정도를 고려하여 그에 상응하는 적절한 관리적·기술적 및 물리적 보호조치를 통하여 개인정보를 안전하게 관리하여야 한다.
- ⑤ 개인정보처리자는 개인정보 처리방침 등 개인정보의 처리에 관한 사항을 공개하여야 하며, 열람청구권 등 정보주체의 권리가 보장될 수 있도록 합리적인 절차와 방법 등을 마련하여야 한다.
- ⑥ 개인정보처리자는 개인정보의 처리 목적에 필요한 범위에서 적법하게 개인정보를 처리하는 경우에도 정보주체의 사생활 침해를 최소화하는 방법으로 개인정보를 처리하여야 한다.
- ⑦ 개인정보처리자는 개인정보를 적법하게 수집한 경우에도 익명에 의하여 업무 목적을 달성할 수 있으면 개인정보를 익명에 의하여 처리될 수 있도록 하여야 한다.
- ⑧ 개인정보처리자는 관계 법령에서 규정하고 있는 책임과 의무를 준수하고 실천함으로써 정보주체의 신뢰를 얻기 위하여 노력하여야 한다.

법 제3조는 개인정보 처리와 관련하여 국제적으로 통용되고 있는 원칙들을 반영하고 있다. 제3조의 개인정보 보호 원칙은 1980년 제정된 「OECD 사생활 가이드라인」 상의 개인정보 보호 8원칙과 EU 회원국의 입법기준이 되는 「개인정보보호지침」(95/46/EC, 1995) 이후 「일반 개인정보 보호법」(GDPR, 2018)을 참고하였고, 우리나라가 제정과정에서 결정적인 역할을 수행한 「APEC 사생활 원칙」(2004)도 고려하였다. 그 밖에 법률에서 개인정보 보호원칙을 상세하게 기술하고 있는 영국, 스웨덴, 캐나다, 홍콩, 호주, 뉴질랜드 등의 「개인정보 보호법」도 참고하였다.

< OECD, EU 및 한국의 개인정보 보호 원칙 비교 >

OECD 프라이버시 8원칙	GDPR 제5조	개인정보 보호 원칙
▪수집제한의 원칙 (1원칙)	▪데이터 최소화 (1.c항)	▪목적에 필요한 최소정보의 수집(제1항) ▪사생활 침해를 최소화하는 방법으로 처리(제6항) ▪익명처리의 원칙(제7항)
▪정보 정확성의 원칙 (2원칙)	▪정확성(1.d항)	▪처리목적 내에서 정확성·완전성·최신성 보장(제3항)
▪목적 명확화의 원칙 (3원칙)	▪목적 제한(1.b항)	▪처리목적의 명확화(제1항)
▪이용제한의 원칙 (4원칙)	▪저장기간 제한 (1.e항)	▪목적 범위 내에서 적법하게 처리, 목적 외 활용금지(제2항)
▪안전성 확보의 원칙 (5원칙)	▪무결성과 기밀성 (1.f항)	▪권리침해 가능성 등을 고려하여 안전하게 관리(제4항)
▪처리방침 공개의 원칙 (6원칙)	▪적법성 공정성 투명성 (1.a항)	▪개인정보 처리방침 등 공개(제5항)
▪정보주체 참여의 원칙 (7원칙)	-	▪열람청구권 등 정보주체의 권리보장(제5항)
▪책임의 원칙 (8원칙)	▪책임성(2항)	▪개인정보처리자의 책임준수·신뢰확보 노력(제8항)

개인정보 보호 원칙은 개인정보처리자에게는 행동의 지침을 제시해 주고, 정책담당자에게는 정책 수립 및 법 집행의 기준을 제시해 주며, 사법부에 대해서는 법 해석의 이론적 기초를 제시해 줌과 동시에 입법적 공백을 막아줄 수 있다. 뿐만 아니라 대법원은 제3조에 따른 개인정보 보호 원칙을 개인정보처리자 행위의 위법성을 판단하기 위한 고려사항으로 열거하기도 하였다(대법원 2017. 4. 7. 선고 2016도13263 판결 참고).

참고 경품 응모권 고지사항의 「개인정보 보호법」 제3조 원칙 위반 여부 판단

이 사건 경품행사에 응모한 고객들은 응모권 뒷면과 인터넷 응모화면에 기재되어 있는 ‘개인정보 수집 및 제3자 제공 동의’ 등 사항이 경품행사 진행을 위하여 필요한 것으로 받아들일 가능성이 크다. 그런데 응모권에 따라서는 경품추첨 사실을 알리는 데 필요한 개인정보와 관련 없는 ‘응모자의 성별, 자녀 수, 동거 여부’ 등 사생활의 비밀에 관한 정보와 심지어는 주민등록번호와 같은 고유식별정보까지 수집하면서 이에 관한 동의를 하지 않을 때에는 응모가 되지 아니하거나 경품 추첨에서 제외된다고 고지하고 있다. 이는 개인정보처리자가 정당한 목적으로 개인정보를 수집하는 경우라 하더라도 그 목적에 필요한 최소한의 개인정보 수집에 그쳐야 하고 이에 동의하지 아니한다는 이유로 정보주체에게 재화 또는 서비스의 제공을 거부하여서는 안 된다는 개인정보 보호 원칙(「개인정보 보호법」 제3조 제1항)과 「개인정보 보호법」 규정에 위반되는 것이다(대법원 2017. 4. 7. 선고 2016도13263 판결).

개인정보 보호 원칙에 따라 개인정보처리자는 구체적이고 명확한 수집 목적을 가지고 개인정보를 수집하여야 하며, 특정된 목적 달성에 직접적으로 필요하지 않은 개인정보는 처리하여서는 안 된다.

예를 들어 세탁서비스 제공자는 세탁 완료를 알리거나 세탁물을 배달하기 위한 목적으로 고객의 성명, 주소, 전화번호 등을 수집할 수 있으나, 그밖에 목적 달성을 위해 직접적으로 필요하지 않은 정보를 수집·이용해서는 안 된다는 원칙이다.

개인정보처리자는 개인정보의 정확성, 완전성 및 최신성을 확보하기 위하여 개인정보 입력 시 입력내용을 사전에 확인하는 절차, 개인정보에 대한 열람 및 정정 요구 등 필요한 절차나 방법 등을 마련하여야 하며, 오류정보를 발견한 경우 정정이나 삭제할 수 있는 절차도 마련하여야 한다. 또한 개인정보를 처리하는 과정에서 개인정보취급자 등이 고의 또는 과실로 개인정보를 변경·훼손하는 일이 없도록 주의의무를 다하여야 한다.

개인정보처리자는 정보주체의 개인정보가 분실, 도난, 유출, 변조 또는 훼손되지 않도록 안전성 확보를 위한 보안조치를 강구하여야 하며, 정보주체가 제공한 개인정보가 어떠한 용도와 방식으로 이용되고 있으며 개인정보 보호를 위하여 어떠한 조치를 취하고 있는지를 공개하여야 한다. 또한 정보주체가 제공한 개인정보를 열람, 정정 및 삭제를 요구할 수 있는 절차를 마련하여야 한다.

그밖에 개인정보처리자는 수집된 개인정보가 다른 사람에게 노출되거나 악용되는 것을 막고 사생활 침해를 최소화하는 방법으로 개인정보를 처리하여야 한다. 또한, 개인정보를 익명 또는 가명으로 처리하여도 수집 목적을 달성할 수 있는 경우 구체적인 업무의 특성을 반영하여 개인정보 데이터 기록에서 개인식별자를 제거하거나 대체하는 등 개인정보의 익명처리가 가능한 경우에는 특정 개인을 알아볼 수 없는 형태로 익명처리를 하여야 한다. 다만, 익명처리로 목적을 달성할 수 없는 경우에는 가명처리 하여야 한다.

제4조 | 정보주체의 권리

법률

제4조(정보주체의 권리) 정보주체는 자신의 개인정보 처리와 관련하여 다음 각 호의 권리를 가진다.

1. 개인정보의 처리에 관한 정보를 제공받을 권리
2. 개인정보의 처리에 관한 동의 여부, 동의 범위 등을 선택하고 결정할 권리
3. 개인정보의 처리 여부를 확인하고 개인정보에 대하여 열람(사본의 발급을 포함한다. 이하 같다)을 요구할 권리
4. 개인정보의 처리 정지, 정정·삭제 및 파기를 요구할 권리
5. 개인정보의 처리로 인하여 발생한 피해를 신속하고 공정한 절차에 따라 구제받을 권리

1. 연혁

제4조가 규정하고 있는 정보주체의 권리는 각국의 판례와 입법례를 통해서 확립된 것이다.

EU의 「개인정보 보호지침」(95/46/EC, 1995) 이후, 「일반 개인정보 보호법」(GDPR, 2018) 상 정보주체는 정보를 제공받을 권리, 자신의 개인정보에 대한 접근권, 부정확한 정보의 수정·삭제·파기요구권, 개인정보의 처리를 거부할 권리, 개인정보가 직접 판매에 이용되는 것을 거부할 권리, 자동처리정보만으로 불이익을 받지 않을 권리를 인정하고 있다. 우리나라의 경우에도 2011년 「개인정보 보호법」 제정 당시 시행 중이던 「정보통신망법」은 동의철회권, 열람요구권, 정정요구권 등을 규정하고 있었으며, 구(舊) 「공공기관 개인정보 보호법」은 정보주체의 열람청구권과 정정 및 삭제청구권을 인정하고 있었다.

우리나라 헌법재판소는 이른바 ‘개인정보자기결정권’ 또는 ‘개인정보자기통제권’을 「헌법」상 보장되는 기본권으로 인정하고 있다. 헌법재판소는 개인정보자기결정권을 「헌법」 제10조 제1문에서 도출되는 일반적 인격권 및 「헌법」 제17조의 사생활의 비밀과 자유에 의하여 보장되는 권리로서 자신에 관한 정보가 언제 누구에게 어느 범위까지 알려지고 또 이용되도록 할 것인지를 그 정보주체가 스스로 결정할 수 있는 권리라고 판시하였다(헌법재판소 2005. 7. 21. 2003헌마282, 425 결정 참고).

2. 권리의 내용

제4조에 따른 정보주체의 권리의 세부 내용은 다음 각 호와 같고, 각 호는 이 법의 개별 조항을 통하여 구체화되어 있다.

가 개인정보 처리에 관한 정보를 제공받을 권리

정보주체는 개인정보 수집, 이용, 제공 등의 처리 목적과 범위 등에 관한 정보를 개인정보처리자로부터 제공받을 권리가 있다. 이에 따라 개인정보처리자는 개인정보 수집·이용·제공 목적·범위 등의 고지, 개인정보처리방침의 수립·공개 등의 의무를 진다(제15조제2항, 제17조제2항, 제30조, 제39조의3제1항 등 참고). 이 외에도 정보통신서비스 제공자등은 개인정보 이용내역의 통지 의무를 진다(제39조의8 참고).

나 동의 여부, 동의범위 등을 선택하고 결정할 권리

개인정보자기결정권의 핵심은 정보주체가 개인정보처리자의 개인정보 처리에 대하여 실질적인 통제권을 갖는 것이다. 정보주체에게 개인정보 처리 여부 및 동의 범위 등을 선택할 수 있는 권리를 부여한다고 하더라도 개인정보처리자가 사실상 동의를 강요하면 정보주체의 권리가 형식화하기 때문에 포괄적인 동의를 금지하고 있다(제22조 등 참고).

다 개인정보의 처리 유무를 확인하고 열람을 요구할 권리

정보주체가 자신의 개인정보를 누가 얼마나 가지고 있고 어떻게 이용·제공·관리하고 있는지를 확인할 수 있도록 자신의 개인정보에 접근권을 보장하고 있다(제35조 참고). 열람요구권은 개인정보처리자의 무분별한 개인정보 수집·이용·제공을 방지하는 기능도 수행한다.

라 개인정보의 처리정지·정정·삭제 및 파기를 요구할 권리

개인정보처리자의 잘못된 개인정보 처리로 인한 피해를 방지하기 위하여 정보주체에게 불완전하거나 부정확한 정보에 대한 처리정지·정정·삭제를 요구할 권리를 보장하고 있다(제36조, 제37조 참고). 이 외에도 이용자에게는 정보통신서비스 제공자등에 대하여 개인정보 수집·이용·제공 등에 관한 동의를 철회할 권리를 보장하고 있다(제39조의7제1항 참고). 또한 정보주체는 개인정보 유출 등의 피해를 방지하고 오남용이 발생하지 않도록 개인정보의 처리목적이 달성되는 등 개인정보를 계속해서 보관할 필요성이 없어진 경우에는 자신의 개인정보를 파기해 달라고 요구할 수도 있다.

마 피해를 신속하고 공정한 절차에 따라 구제받을 권리

정보주체는 개인정보의 수집·이용·제공 등으로 피해가 발생한 경우, 신속하고 공정한 절차에 따라 피해의 심각성에 비례하여 적절한 보상을 받을 권리를 가진다. 이 같은 권리를 보장하기 위해 이 법은 입증책임의 전환(제39조제1항 단서 참고), 분쟁조정제도(제40조~제50조 참고) 및 권리침해 중지 단체소송제도(제51조~제57조 참고), 법정·징벌적 손해배상제도(제39조의2 및 제39조제3항 참고), 정보통신서비스 제공자등의 손해배상책임 보장 조치 의무(제39조의9 참고) 등을 도입하고 있다.

제5조 | 국가 등의 책무

법률

- 제5조(국가 등의 책무)** ① 국가와 지방자치단체는 개인정보의 목적 외 수집, 오용·남용 및 무분별한 감시·추적 등에 따른 피해를 방지하여 인간의 존엄과 개인의 사생활 보호를 도모하기 위한 시책을 강구하여야 한다.
- ② 국가와 지방자치단체는 제4조에 따른 정보주체의 권리를 보호하기 위하여 법령의 개선 등 필요한 시책을 마련하여야 한다.
- ③ 국가와 지방자치단체는 개인정보의 처리에 관한 불합리한 사회적 관행을 개선하기 위하여 개인정보처리자의 자율적인 개인정보 보호활동을 존중하고 촉진·지원하여야 한다.
- ④ 국가와 지방자치단체는 개인정보의 처리에 관한 법령 또는 조례를 제정하거나 개정하는 경우에는 이 법의 목적에 부합되도록 하여야 한다.

1. 인간존엄 및 사생활 보호를 위한 시책 강구

국가 및 지방자치단체는 개인정보의 오·남용 등으로부터 인간의 존엄과 개인의 사생활을 보호할 수 있도록 개인정보 처리 실태를 점검하고 필요한 시책을 수립·시행하여야 한다.

2. 법령의 개선 등 필요한 시책 마련

국가와 지방자치단체는 정보주체의 권리를 보호하기 위해 필요한 법령을 정비하는 등 필요한 시책을 마련하여 시행하여야 한다.

3. 개인정보 보호 자율규제 촉진·지원

사회 전반에 개인정보 보호 제도와 관행이 정착되기 위해서는 개인정보처리자의 자율규제가 활성화되어야 한다. 이를 위해 국가와 지방자치단체는 개인정보처리자의 자발적인 개인정보 보호 활동을 존중하고 촉진·지원하여 개인정보 처리에 관한 불합리한 사회적 관행을 개선하고 개인정보가 안전하게 처리될 수 있는 사회적 환경을 조성할 책무가 있다.

4. 이 법 목적에 부합하도록 법령·조례 제·개정

국가 및 지방자치단체는 개인정보 처리에 관한 법령 또는 조례, 소관 부처 지침·고시 등을 제·개정할 때 개인의 자유와 권리를 보호하고 나아가 개인의 존엄과 가치의 구현이라 하는 이 법의 목적에 부합할 수 있도록 하여야 한다.

제6조 | 다른 법률과의 관계

법률	제6조(다른 법률과의 관계) 개인정보 보호에 관하여는 다른 법률에 특별한 규정이 있는 경우를 제외하고는 이 법에서 정하는 바에 따른다.
표준지침	제5조(다른 지침과의 관계) 중앙행정기관의 장이 소관 분야의 개인정보 처리와 관련한 개인정보 보호지침을 정하는 경우에는 이 지침에 부합되도록 하여야 한다.

1. 「개인정보 보호법」의 성격

개인정보 보호에 관하여 이 법 이외에 다른 개별법이 있는 경우 이 법과 그 개별법 사이의 관계를 규정한 것이다. 이 법은 개인정보 보호에 관한 일반법적 성격을 가지므로 다른 법률에 특별한 규정이 있는 경우에는 그 법률의 규정이 우선하여 적용된다. 이는 해당 분야의 특수성을 고려한 것이다.

현재 「신용정보법」, 「위치정보의 보호 및 이용 등에 관한 법률」, 「전자상거래 등에서의 소비자보호에 관한 법률」 등 다수의 개별법에서 개인정보의 처리 및 보호에 관한 규정을 두고 있다. 따라서 조문별로 이 법에 우선하여 적용해야 하는지를 검토하여야 한다.

2. 법률의 적용기준

「신용정보법」 등 개별법을 적용받는 자라고 해서 이 법의 적용이 면제되는 것은 아니다. 개인정보를 처리하는 자는 누구든지 이 법의 규정을 적용받는다. 다만, 해당 개별법이 이 법의 내용과 다른 특별한 규정이 있는 경우 해당 법률의 규정이 우선 적용된다.

그러나 개별법에서 이 법의 내용과 다른 규정을 두고 있다고 해서 무조건 해당 개별법의 규정이 우선 적용되는 것은 아니다. 개별법의 목적, 취지, 내용 등을 전반적으로 고려해서 이 법의 적용을 배제할 의도가 분명하다고 인정되는 경우 또는 이 법의 규정을 그대로 적용할 경우 이 법과 개별법 사이에 모순이 발생하거나 불합리한 상황 또는 왜곡된 결과가 발생하는 경우만 개별법 규정이 우선 적용된다.

판례 특별법 우선 원칙이 적용되는 경우 법률이 상호 모순·저촉되는지 판단하는 기준

일반적으로 특별법이 일반법에 우선하고 신법이 구법에 우선한다는 원칙은 동일한 형식의 성문법 규인 법률이 상호 모순·저촉되는 경우에 적용된다. 이때 법률이 상호 모순·저촉되는지는 법률의 입법목적, 규정사항 및 적용범위 등을 종합적으로 검토하여 판단하여야 한다(대법원 2016. 11. 25. 선고 2014도14166 판결).

결정례 제6조 ‘특별한 규정’ 판단 기준

판례 등의 의견을 종합하면 정보통신망법(2020. 2. 4. 법률 제16955호로 개정되기 전의 것)의 규정을 보호법 제6조의 ‘특별한 규정’으로 판단할 수 있는 기준은 ① 상호 모순·저촉되는 규정의 존재 여부 ② 보호법 관련 조항을 배제하고자 하는 내용의 포함 여부라고 판단됨(보호위원회 결정 제2018-02-006호).

이 법은 일반법으로서 개인정보 처리에 관한 경제·사회의 공통적이고 평균적인 요구 수준을 반영하고 있으므로 다른 법률의 규정이 이 법의 규정보다 보호 수준을 더 강화하고 있는 경우는 물론 이 법의 규정보다 더 보호 수준을 완화하고 있는 경우에도 해당 개별법의 규정이 우선하여 적용된다.

다른 ‘법률’에 특별한 규정이 있는 경우에만 그 법률의 규정이 이 법에 우선하여 적용되므로 법률이 아닌 시행령이나 시행규칙 고시, 조례 등에 이 법과 다른 특별한 규정이 있다고 하여도 그 시행령 등은 우선 적용되지 않는다. 그런 경우에는 당연히 이 법이 우선하여 적용된다. 다만, 그 시행령 등이 법률의 위임을 받은 것일 경우에 한하여 그 시행령 등이 우선하여 적용될 수 있다.

사례 「상법」 우선 적용

「개인정보 보호법」에서는 정보주체로부터 별도의 동의를 받거나, 다른 법률의 특별한 규정이 있는 경우 등에 한하여 개인정보를 제3자에게 제공할 수 있다(제15조제1항 및 제18조제2항). 근로자의 복리후생을 위해 회사가 근로자를 일괄하여 피보험자로 하는 단체보험을 체결하는 경우, 회사는 직원의 개인정보를 제3자인 보험자에게 제공해야 하는데, 「개인정보 보호법」에 따라 직원의 별도의 동의를 받아야 한다.

그러나 「상법」은 타인의 생명보험과 관련하여 제731조제1항에서 “타인의 사망을 보험사고로 하는 보험계약에는 보험계약 체결 시에 그 타인의 서면에 의한 동의를 얻어야 한다.”고 규정하고 있고, 단체의 대표자가 그 단체의 구성원의 전부 또는 일부를 피보험자로 하여 보험자와 1개의 보험계약을 체결함으로써 성립하는 단체보험의 경우 「상법」 제735조의3제1항에 따라 “단체의 규약에 따라 구성원의 전부 또는 일부를 피보험자로 하는 생명보험계약을 체결하는 경우에는 제731조를 적용하지 아니한다.”고 규정하고 있다. 상해보험의 경우에도 「상법」 제739조에 따라 생명보험에 관한 규정이 준용되므로 단체상해보험계약을 체결하기 위해서는 보험계약체결에 대한 근로자의 동의를 갈음하는 규약이 있는 경우 근로자의 서면동의가 없어도 된다.

따라서 단체보험계약체결에 관한 사항을 포함하고 있는 규약이 있는 경우에는 근로자의 동의 없이 회사가 수집한 개인정보를 보험회사인 제3자에게 제공할 수 있도록 규정하고 있는 「상법」이 적용된다.

「상법」 제735조의3에서 말하는 규약의 의미는 단체협약, 취업규칙, 정관 등 그 형식을 막론하고 단체보험의 가입에 관한 단체내부의 협정에 해당하는 것이고, 당해 보험가입과 관련하여 상세한 사항까지 규정할 것을 요하지 않지만 대표자가 구성원을 위하여 일괄하여 계약을 체결할 수 있다는 취지는 담겨 있어야 할 것이다(대법원 2006.4.27. 선고2003다60259판결). 예를 들어 취업규칙 등에 생명보험가입에 관한 조항을 두고, 보험금의 지급은 사망직금이나 사망위로금의 지급에 충당하는 규정을 두고 있고

근로자가 서명날인 하였다면 피보험자의 동의에 갈음할 수 있을 것이다. 그러나 규약에 단체보험계약 체결에 관한 사항을 포함하지 않고 단순히 퇴직금, 사망위로금 등만 규정하고 있는 경우에는 근로자의 서면동의가 필요하다.

3. 다른 법률과의 관계

이 법은 일반법으로서 모든 개인정보처리자와 정보주체와의 관계에 적용된다. 다만, 「신용정보법」에 따른 신용정보사업자와 신용정보주체와의 관계에 있어서 해당 법에 특별한 규정이 있다면 그 규정을 따른다. 종래 정보통신서비스 제공자와 정보통신서비스 이용자 사이의 관계에서는 「정보통신망법」에 특별한 규정이 있는 경우 해당 규정이 우선 적용되었으나, 2020년 2월 4일의 「개인정보 보호법」 개정으로 「정보통신망법」의 개인정보 보호 규정은 「개인정보 보호법」상 정보통신서비스 제공자 등의 특례로 이관되었다(이와 관련한 자세한 내용은 제6장 정보통신서비스 제공자 등의 개인정보 처리 등 특례 개관 부분 해설 참고).

일반 상거래기업이 상거래정보를 처리함에 있어 「개인정보 보호법」 및 「신용정보법」 간 적용 우선 순위에 대한 법률 해석상 이견이 존재한다. 개인의 상거래정보 중 특정 개인을 식별할 수 있으면 「개인정보 보호법」상 개인정보에 해당하고, 거래 상대방의 신용을 판단할 때 필요한 정보인 경우에만 「신용정보법」 제2조제1호의 신용정보라 볼 수 있다.²⁾

그러나 신용정보의 범위를 넓게 설정하면 모든 상거래정보는 「신용정보법」의 규율을 받아야 하는 결론에 도달하게 되며, 이 경우 개인정보에 대한 일반법으로서 「개인정보 보호법」의 지위가 사라지고, 신용정보의 보호 및 활용에 관한 특별법인 「신용정보법」이 오히려 일반법적 지위를 획득하게 되는 결과를 초래하게 된다.³⁾

따라서, 상거래정보는 통상적으로 일반법인 「개인정보 보호법」을 적용하고, 상거래정보를 “신용정보주체의 신용을 판단하는 경우”에만 특별법인 「신용정보법」을 우선 적용하는 것이 타당하다.

이런 맥락에서 「개인정보 보호법」이 적용되는 경우를 온라인과 오프라인으로 나누어 볼 수 있는데, 온라인 거래에는 제6장 정보통신서비스 제공자등에 대한 특례규정을 적용하고, 오프라인 거래에는 일반규정을 적용하면 된다.

2) “거래 상대방의 신용을 판단할 때 필요한 정보”의 범위를 넓게 보아 “상대방의 신용을 판단할 가능성이 있는 경우”까지 확장함으로써 모든 상거래정보를 신용정보로 보아야 한다는 다른 해석도 있음

3) 금융위원회는 「신용정보법」이 제정된 1995년 당시에는 개인정보에 대한 규제가 전혀 존재하지 않아 가급적 신용정보를 두텁게 보호하자는 취지에서 금융분야가 아니었음에도 “신용정보”를 넓게 해석하여 “상거래정보”까지 포함되는 것으로 해석

이 외에, 영상정보처리기기, 영향평가, 고유식별정보 및 민감정보 처리 제한, 집단분쟁 조정제도, 권리침해행위 단체소송, 정보주체 이외로부터 수집한 개인정보의 출처 고지 등 「개인정보 보호법」에만 규정되어 있는 내용은 당연히 「개인정보 보호법」이 적용된다.

한편, 다른 법에서 「개인정보 보호법」 제31조의 개인정보 보호책임자와 그 취지상 유사한 제도를 두고 있는 경우에는 해당 법률에 따라 지정하면 되고 「개인정보 보호법」에 따라 개인정보 보호책임자를 별도로 지정할 필요는 없다. 예컨대, 「신용정보법」에 따라 신용정보 관리책임자를 지정하였을 경우에는 별도로 개인정보 보호책임자를 지정하지 않아도 된다. 다만 「개인정보 보호법」에서 규정한 개인정보 보호책임자의 업무를 동시에 수행하여야 한다.

제2장 개인정보 보호정책의 수립 등

제7조	개인정보 보호위원회
제7조의2	보호위원회의 구성 등
제7조의3	위원장
제7조의4	위원의 임기
제7조의5	위원의 신분보장
제7조의6	겸직금지 등
제7조의7	결격사유
제7조의8	보호위원회의 소관 사무
제7조의9	보호위원회의 심의·의결 사항 등
제7조의10	회의
제7조의11	위원의 제적·기피·회피
제7조의12	소위원회
제7조의13	사무처
제7조의14	운영 등
제8조의2	개인정보 침해요인 평가
제9조	기본계획
제10조	시행계획
제11조	자료제출 요구 등
제12조	개인정보 보호지침
제13조	자율규제의 촉진 및 지원
제14조	국제협력



제7조 | 개인정보 보호위원회

법률

제7조(개인정보 보호위원회) ① 개인정보 보호에 관한 사무를 독립적으로 수행하기 위하여 국무총리 소속으로 개인정보 보호위원회(이하 “보호위원회”라 한다)를 둔다.

② 보호위원회는 「정부조직법」 제2조에 따른 중앙행정기관으로 본다. 다만, 다음 각 호의 사항에 대하여는 「정부조직법」 제18조를 적용하지 아니한다.

1. 제7조의8제3호 및 제4호의 사무
2. 제7조의9제1항의 심의·의결 사항 중 제1호에 해당하는 사항

1. 보호위원회의 설치 배경

개인정보 보호 제도의 운영에 있어서 독립적이고 전문적인 개인정보 감독기구의 설치는 가장 핵심적인 요소이자 안전장치이다. 이에 개인정보 보호에 관한 사무를 독립적으로 체계적으로 수행할 수 있도록 하기 위하여 보호위원회를 두고 있다.

2020. 2. 4. 「개인정보 보호법」 개정으로 보호위원회가 중앙행정기관으로 격상되고, 과거 행정안전부와 방송통신위원회가 수행하던 개인정보 보호 기능이 보호위원회로 이관됨에 따라 개인정보 보호정책·집행 기능이 일원화되었다. 그간 분산된 개인정보 규제체계에 의해 필연적으로 발생할 수밖에 없었던 사업자의 혼란 및 중복규제 부담이 해소되었고, 수범자와 정보주체를 보다 체계적으로 보호할 수 있는 기반이 마련되었다.

또한 보호위원회는 EU의 「일반 개인정보 보호법」(GDPR, 2018) 등 해외 법제가 요구하는 개인정보 보호 감독기구의 독립성과 권한을 충족하는 등 선진국 수준의 감독체계를 갖추게 되어 향후 외국과의 개인정보 국외이전 논의 시 안전한 보호체계를 갖춘 것으로 평가받을 수 있게 되었다.

2. 보호위원회의 소속과 지위

보호위원회는 행정 각부를 통괄하는 국무총리 소속으로 하고(제7조제1항), 보호위원회를 중앙행정기관으로서 인사·예산권 및 조사·처분 등 집행권을 갖도록 하고 있다(제7조제2항 본문). 이를 통해 보호위원회가 개인정보를 대량으로 처리하는 정부기관이나 대기업들의 개인정보 처리 활동을 전문적으로 평가하고 효과적으로 견제할 수 있도록 하였다.

3. 보호위원회의 독립성

보호위원회가 조직상으로는 국무총리 소속의 중앙행정기관이지만, 업무상 독립적인 감독기구로서 역할도 수행한다. 「개인정보 보호법」은 보호위원회의 독립성을 보장하기 위해 정보주체의 권리침해에 대한 조사·처분, 개인정보의 처리와 관련한 고충처리·권리구제 및 개인정보에 관한 분쟁의 조정, 보호위원회의 심의·의결에 대해서는 「정부조직법」 제18조(국무총리의 행정감독권)의 적용을 배제하고 있다(제7조제2항 단서)⁴⁾. 이는 개인정보 보호의 핵심적 기능에 대해 보호위원회의 업무상 독립성을 보장하기 위한 최소한의 법적 장치이다.

4) 다른 국무총리 산하 원자력안전위원회 역시 위원회의 독립성을 보장하기 위해 국무총리의 행정 감독권을 배제하고 있음(「원자력안전위원회의 설치 및 운영에 관한 법률」 제3조제2항)

제7조의2(보호위원회의 구성 등) ① 보호위원회는 상임위원 2명(위원장 1명, 부위원장 1명)을 포함한 9명의 위원으로 구성한다.

② 보호위원회의 위원은 개인정보 보호에 관한 경력과 전문지식이 풍부한 다음 각 호의 사람 중에서 위원장과 부위원장은 국무총리의 제청으로, 그 외 위원 중 2명은 위원장의 제청으로, 2명은 대통령이 소속되거나 소속되었던 정당의 교섭단체 추천으로, 3명은 그 외의 교섭단체 추천으로 대통령이 임명 또는 위촉한다.

1. 개인정보 보호 업무를 담당하는 3급 이상 공무원(고위공무원단에 속하는 공무원을 포함한다)의 직에 있거나 있었던 사람
2. 판사·검사·변호사의 직에 10년 이상 있거나 있었던 사람
3. 공공기관 또는 단체(개인정보처리자로 구성된 단체를 포함한다)에 3년 이상 임원으로 재직하였거나 이들 기관 또는 단체로부터 추천받은 사람으로서 개인정보 보호 업무를 3년 이상 담당하였던 사람
4. 개인정보 관련 분야에 전문지식이 있고 「고등교육법」 제2조제1호에 따른 학교에서 부교수 이상으로 5년 이상 재직하고 있거나 재직하였던 사람

③ 위원장과 부위원장은 정무직 공무원으로 임명한다.

④ 위원장, 부위원장, 제7조의13에 따른 사무처의 장은 「정부조직법」 제10조에도 불구하고 정부위원이 된다.

제7조의3(위원장) ① 위원장은 보호위원회를 대표하고, 보호위원회의 회의를 주재하며, 소관 사무를 총괄한다.

② 위원장이 부득이한 사유로 직무를 수행할 수 없을 때에는 부위원장이 그 직무를 대행하고, 위원장·부위원장이 모두 부득이한 사유로 직무를 수행할 수 없을 때에는 위원회가 미리 정하는 위원이 위원장의 직무를 대행한다.

③ 위원장은 국회에 출석하여 보호위원회의 소관 사무에 관하여 의견을 진술할 수 있으며, 국회에서 요구하면 출석하여 보고하거나 답변하여야 한다.

④ 위원장은 국무회의에 출석하여 발언할 수 있으며, 그 소관 사무에 관하여 국무총리에게 의안 제출을 건의할 수 있다.

제7조의4(위원의 임기) ① 위원의 임기는 3년으로 하되, 한 차례만 연임할 수 있다.

② 위원이 궐위된 때에는 지체 없이 새로운 위원을 임명 또는 위촉하여야 한다. 이 경우 후임으로 임명 또는 위촉된 위원의 임기는 새로이 개시된다.

제7조의5(위원의 신분 보장) ① 위원은 다음 각 호의 어느 하나에 해당하는 경우를 제외하고는 그 의사에 반하여 면직 또는 해촉되지 아니한다.

1. 장기간 심신장애로 인하여 직무를 수행할 수 없게 된 경우

	<p>2. 제7조의7의 결격사유에 해당하는 경우</p> <p>3. 이 법 또는 그 밖의 다른 법률에 따른 직무상의 의무를 위반한 경우</p> <p>② 위원은 법률과 양심에 따라 독립적으로 직무를 수행한다.</p> <p>제7조의6(결직금지 등) ① 위원은 재직 중 다음 각 호의 직(職)을 겸하거나 직무와 관련된 영리업무에 종사하여서는 아니 된다.</p> <ol style="list-style-type: none"> 1. 국회의원 또는 지방의회의원 2. 국가공무원 또는 지방공무원 3. 그 밖에 대통령령으로 정하는 직 <p>② 제1항에 따른 영리업무에 관한 사항은 대통령령으로 정한다.</p> <p>③ 위원은 정치활동에 관여할 수 없다.</p> <p>제7조의7(결격사유) ① 다음 각 호의 어느 하나에 해당하는 사람은 위원이 될 수 없다.</p> <ol style="list-style-type: none"> 1. 대한민국 국민이 아닌 사람 2. 「국가공무원법」 제33조 각 호의 어느 하나에 해당하는 사람 3. 「정당법」 제22조에 따른 당원 <p>② 위원이 제1항 각 호의 어느 하나에 해당하게 된 때에는 그 직에서 당연 퇴직한다. 다만, 「국가공무원법」 제33조제2호는 파산선고를 받은 사람으로서 「채무자 회생 및 파산에 관한 법률」에 따라 신청기한 내에 면책신청을 하지 아니하였거나 면책불허가 결정 또는 면책 취소가 확정된 경우만 해당하고, 같은 법 제33조제5호는 「형법」 제129조부터 제132조까지, 「성폭력범죄의 처벌 등에 관한 특례법」 제2조, 「아동·청소년의 성보호에 관한 법률」 제2조제2호 및 직무와 관련하여 「형법」 제355조 또는 제356조에 규정된 죄를 범한 사람으로서 금고 이상의 형의 선고유예를 받은 경우만 해당한다.</p>
시행령	<p>제4조의2(영리업무의 금지) 법 제7조제1항에 따른 개인정보 보호위원회(이하 “보호위원회” 라 한다)의 위원은 법 제7조의6제1항에 따라 영리를 목적으로 다음 각 호의 어느 하나에 해당하는 업무에 종사해서는 안 된다.</p> <ol style="list-style-type: none"> 1. 법 제7조의9제1항에 따라 보호위원회가 심의·의결하는 사항과 관련된 업무 2. 법 제40조제1항에 따른 개인정보 분쟁조정위원회(이하 “분쟁조정위원회” 라 한다)가 조정하는 사항과 관련된 업무

1. 보호위원회의 구성

보호위원회는 상임위원 2명(위원장 1명, 부위원장 1명)을 포함한 9명의 위원으로 구성한다(제7조의2제1항).

가 위원장

위원장은 국무총리의 제청으로 대통령이 임명한다(제7조의2제2항). 위원장은 정무직 공무원으로 보하며(제7조의2제3항), 정부위원이 된다(제7조의2제4항). 위원장은 보호위원회를 대표하고 보호위원회의 회의를 주재하며 소관 사무를 총괄한다(제7조의3제1항). 국회에 출석하여 보호위원회의 소관 사무에 관하여 의견을 진술할 수 있으며, 국회에서 요구하면 출석하여 보고하거나 답변하여야 한다(제7조의3제3항). 그리고 국무회의에 출석하여 발언할 수 있으며, 그 소관 사무에 관하여 국무총리에게 의안 제출을 건의할 수 있다(제7조의3제4항).

나 부위원장

부위원장은 국무총리의 제청으로 대통령이 임명한다(제7조의2제2항). 부위원장은 정무직 공무원으로 보하며(제7조의2제3항), 정부위원이 된다(제7조의2제4항). 부위원장은 보호위원회의 업무에 관하여 위원장을 보좌한다. 또한 위원장이 부득이한 사유로 직무를 수행할 수 없을 때에는 부위원장이 그 직무를 대행한다(제7조의3제2항 전단).

다 위원

위원장과 부위원장을 제외한 위원 중 2명은 위원장의 제청으로, 2명은 대통령이 소속되거나 소속되었던 정당의 교섭단체 추천으로, 3명은 그 외의 교섭단체 추천으로 대통령이 임명 또는 위촉한다(제7조의2제2항). 위원장·부위원장이 모두 부득이한 사유로 직무를 수행할 수 없을 때에는 위원회가 미리 정하는 위원이 위원장의 직무를 대행한다(제7조의3제2항 후단).

라 위원의 자격

보호위원회의 위원은 개인정보 보호에 관한 경력과 전문지식이 풍부한 다음 각 호의 사람 중에서 임명 또는 위촉된다.

위원의 자격 (제7조의2제2항)

1. 개인정보 보호 업무를 담당하는 3급 이상 공무원(고위공무원단에 속하는 공무원을 포함한다)의 직에 있거나 있었던 사람
2. 판사·검사·변호사의 직에 10년 이상 있거나 있었던 사람
3. 공공기관 또는 단체(개인정보처리자로 구성된 단체를 포함한다)에 3년 이상 임원으로 재직하였거나 이들 기관 또는 단체로부터 추천받은 사람으로서 개인정보 보호 업무를 3년 이상 담당하였던 사람
4. 개인정보 관련 분야에 전문지식이 있고 「고등교육법」 제2조제1호에 따른 학교에서 부교수 이상으로 5년 이상 재직하고 있거나 재직하였던 사람

마 위원의 임기

위원의 임기는 3년으로 하되, 한 차례만 연임할 수 있다(제7조의4제1항). 위원이 꺾워된 때에는 지체 없이 새로운 위원을 임명 또는 위촉하여야 한다. 이 경우 후임으로 임명 또는 위촉된 위원의 임기는 새로 개시된다(제7조의4제2항).

2. 위원의 직무상 독립성과 공정성 보장

이 법은 위원의 직무상 독립성과 공정성 보장을 위하여 위원의 신분 보장, 직무상 독립성 보장, 겸직금지과 영리업무 종사 금지, 정치활동 관여 금지를 규정하고 있다.

가 위원의 신분보장

위원은 장기간 심신장애로 인하여 직무를 수행할 수 없게 된 경우, 결격사유에 해당하는 경우 또는 법률에 따른 직무상의 의무를 위반한 경우에 해당하지 않는 한 원칙적으로 그 의사에 반하여 면직 또는 해촉되지 않는다(제7조의5제1항).

나 직무상 독립성 보장

위원은 법률과 양심에 따라 독립적으로 직무를 수행한다(제7조의5제2항).

다 겸직금지과 영리업무 종사 금지

위원은 재직 중 국회의원 또는 지방의회의원, 국가공무원 또는 지방공무원을 겸하는 것이 금지된다(제7조의6제1항).

나아가 위원은 직무와 관련된 영리업무에 종사하는 것이 금지된다(제7조의6제1항 후단). 여기서 “영리업무에 종사”란 위원이 영리를 목적으로 법 제7조의9제1항에 따라 심의·결정하는 사항과 관련된 업무 또는 법 제40조에 따른 개인정보 분쟁조정위원회(이하 “분쟁조정위원회”라 한다)가 조정하는 사항과 관련된 업무에 종사하는 것을 말한다(영 제4조의2제2항).

라 정치활동 관여 금지

위원은 정치활동에 관여하는 것이 금지된다(제7조의6제3항).

3. 위원의 결격사유

다음 결격사유 중 어느 하나에 해당하는 사람은 위원이 될 수 없다.

결격 사유(제7조의7제1항)

1. 대한민국 국민이 아닌 사람
2. 「국가공무원법」 제33조 각 호의 어느 하나에 해당하는 사람
3. 「정당법」 제22조에 따른 당원

위원이 위의 결격사유 중 어느 하나에 해당하게 된 때에는 그 직에서 당연 퇴직한다(제7조의7제2항 본문). 하지만 「국가공무원법」 제33조제2호는 파산선고를 받은 사람으로서 「채무자 회생 및 파산에 관한 법률」에 따라 신청기한 내에 면책신청을 하지 아니하였거나 면책불허가 결정 또는 면책 취소가 확정된 경우만 해당하고, 같은 법 제33조제5호는 「형법」 제129조부터 제132조까지, 「성폭력범죄의 처벌 등에 관한 특례법」 제2조, 「아동·청소년의 성보호에 관한 법률」 제2조제2호 및 직무와 관련하여 「형법」 제355조 또는 제356조에 규정된 죄를 범한 사람으로서 금고 이상의 형의 선고유예를 받은 경우만 해당한다(제7조의7제2항 단서).

제7조의8(보호위원회의 소관 사무) 보호위원회는 다음 각 호의 소관 사무를 수행한다.

1. 개인정보의 보호와 관련된 법령의 개선에 관한 사항
2. 개인정보 보호와 관련된 정책·제도·계획 수립·집행에 관한 사항
3. 정보주체의 권리침해에 대한 조사 및 이에 따른 처분에 관한 사항
4. 개인정보의 처리와 관련한 고충처리·권리구제 및 개인정보에 관한 분쟁의 조정
5. 개인정보 보호를 위한 국제기구 및 외국의 개인정보 보호기구와의 교류·협력
6. 개인정보 보호에 관한 법령·정책·제도·실태 등의 조사·연구, 교육 및 홍보에 관한 사항
7. 개인정보 보호에 관한 기술개발의 지원·보급 및 전문인력의 양성에 관한 사항
8. 이 법 및 다른 법령에 따라 보호위원회의 사무로 규정된 사항

제7조의9(보호위원회의 심의·의결 사항 등) ① 보호위원회는 다음 각 호의 사항을 심의·의결한다.

1. 제8조의2에 따른 개인정보 침해요인 평가에 관한 사항
 2. 제9조에 따른 기본계획 및 제10조에 따른 시행계획에 관한 사항
 3. 개인정보 보호와 관련된 정책, 제도 및 법령의 개선에 관한 사항
 4. 개인정보의 처리에 관한 공공기관 간의 의견조정에 관한 사항
 5. 개인정보 보호에 관한 법령의 해석·운용에 관한 사항
 6. 제18조제2항제5호에 따른 개인정보의 이용·제공에 관한 사항
 7. 제33조제3항에 따른 영향평가 결과에 관한 사항
 8. 제28조의6, 제34조의2, 제39조의15에 따른 과징금 부과에 관한 사항
 9. 제61조에 따른 의견제시 및 개선권고에 관한 사항
 10. 제64조에 따른 시정조치 등에 관한 사항
 11. 제65조에 따른 고발 및 징계권고에 관한 사항
 12. 제66조에 따른 처리 결과의 공표에 관한 사항
 13. 제75조에 따른 과태료 부과에 관한 사항
 14. 소관 법령 및 보호위원회 규칙의 제정·개정 및 폐지에 관한 사항
 15. 개인정보 보호와 관련하여 보호위원회의 위원장 또는 위원 2명 이상이 회의에 부치는 사항
 16. 그 밖에 이 법 또는 다른 법령에 따라 보호위원회가 심의·의결하는 사항
- ② 보호위원회는 제1항 각 호의 사항을 심의·의결하기 위하여 필요한 경우

	<p>다음 각 호의 조치를 할 수 있다.</p> <ol style="list-style-type: none"> 1. 관계 공무원, 개인정보 보호에 관한 전문 지식이 있는 사람이나 시민사회 단체 및 관련 사업자로부터의 의견 청취 2. 관계 기관 등에 대한 자료제출이나 사실조회 요구 ③ 제2항제2호에 따른 요구를 받은 관계 기관 등은 특별한 사정이 없으면 이에 따라야 한다. ④ 보호위원회는 제1항제3호의 사항을 심의·의결한 경우에는 관계 기관에 그 개선을 권고할 수 있다. ⑤ 보호위원회는 제4항에 따른 권고 내용의 이행 여부를 점검할 수 있다.
시행령	<p>제9조의2(정책·제도·법령 개선 권고의 절차 등) ① 보호위원회는 법 제7조의 9제4항에 따라 관계 기관에 정책·제도 및 법령의 개선을 권고하는 경우에는 그 내용과 사유 등을 함께 통보해야 한다.</p> <p>② 보호위원회는 법 제7조의9제5항에 따른 권고내용의 이행여부를 점검하기 위하여 관계 기관에 권고사항의 이행결과에 대한 자료 제출을 요청할 수 있다.</p>

1. 보호위원회의 소관 사무

보호위원회는 다음의 소관사무를 수행한다(제7조의8).

보호위원회 소관 사무(제7조의8)

1. 개인정보의 보호와 관련된 법령의 개선에 관한 사항
2. 개인정보 보호와 관련된 정책·제도·계획 수립·집행에 관한 사항
3. 정보주체의 권리침해에 대한 조사 및 이에 따른 처분에 관한 사항
4. 개인정보의 처리와 관련한 고충처리·권리구제 및 개인정보에 관한 분쟁의 조정
5. 개인정보 보호를 위한 국제기구 및 외국의 개인정보 보호기구와의 교류·협력
6. 개인정보 보호에 관한 법령·정책·제도·실태 등의 조사·연구, 교육 및 홍보에 관한 사항
7. 개인정보 보호에 관한 기술개발의 지원·보급 및 전문인력의 양성에 관한 사항
8. 이 법 및 다른 법령에 따라 보호위원회의 사무로 규정된 사항

2. 보호위원회의 심의·의결 사항 등

가 심의·의결 사항

보호위원회는 다음 각 호의 사항을 심의·의결한다(제7조의9제1항).

보호위원회 심의·의결 사항(제7조의9제1항)

1. 제8조의2에 따른 개인정보 침해요인 평가에 관한 사항
2. 제9조에 따른 기본계획 및 제10조에 따른 시행계획에 관한 사항
3. 개인정보 보호와 관련된 정책, 제도 및 법령의 개선에 관한 사항
4. 개인정보의 처리에 관한 공공기관 간의 의견조정에 관한 사항
5. 개인정보 보호에 관한 법령의 해석·운용에 관한 사항
6. 제18조제2항제5호에 따른 개인정보의 이용·제공에 관한 사항
7. 제33조제3항에 따른 영향평가 결과에 관한 사항
8. 제28조의6, 제34조의2, 제39조의15에 따른 과징금 부과에 관한 사항
9. 제61조에 따른 의견제시 및 개선권고에 관한 사항
10. 제64조에 따른 시정조치 등에 관한 사항
11. 제65조에 따른 고발 및 징계권고에 관한 사항
12. 제66조에 따른 처리 결과의 공표에 관한 사항
13. 제75조에 따른 과태료 부과에 관한 사항
14. 소관 법령 및 보호위원회 규칙의 제정·개정 및 폐지에 관한 사항
15. 개인정보 보호와 관련하여 보호위원회의 위원장 또는 위원 2명 이상이 회의에 부치는 사항
16. 그 밖에 이 법 또는 다른 법령에 따라 보호위원회가 심의·의결하는 사항

보호위원회의 심의·의결은 해당 사안의 당사자가 아닌 제3자에게도 그 효력이 확장되는 경우가 있다. 가령 개인정보 보호에 관한 법령의 해석·운용에 관한 심의·의결의 경우 보호위원회가 신청기관 및 대상기관을 명시하여 심의·의결하였다 하더라도, 사실관계 및 적용 법령이 동일한 건에 대해서는 의결 신청기관이 아닌 제3의 개인정보처리자도 해당 의결의 내용을 준용하여 업무에 적용된다.

나 의견청취 및 자료제출 요구 등

보호위원회는 심의·의결을 위하여 필요한 경우 관계 공무원, 전문가, 시민사회단체, 관련 사업자 등으로부터 의견을 들을 수 있고, 관계기관 등에 대하여 자료제출이나 사실조회를 요구할 수 있다(제7조의9제2항). 이러한 자료제출이나 사실조회의 요청을 받은 관계기관의 장은 특별한 사정이 없으면 이에 따라야 한다(제7조의9제3항).

다 정책·제도 개선권고 및 이행점검권

보호위원회는 개인정보 보호와 관련된 정책, 제도 및 법령의 개선에 관한 사항(제7조의9제1항제3호)을 심의·의결한 경우에는 관계 기관에 그 개선을 권고할 수 있다(제7조의9제4항). 이러한 경우에는 그 내용과 사유 등을 함께 통보하여야 한다(영 제9조의2제1항).

그리고 이러한 권고 내용의 이행 여부를 점검할 수 있으며(제7조의9제5항), 이를 위하여 관계 기관에 권고사항의 이행결과에 대한 자료 제출을 요청할 수 있다(영 제9조의2제2항).

제7조의10(회의) ① 보호위원회의 회의는 위원장이 필요하다고 인정하거나 재적위원 4분의 1 이상의 요구가 있는 경우에 위원장이 소집한다.

② 위원장 또는 2명 이상의 위원은 보호위원회에 의안을 제의할 수 있다.

③ 보호위원회의 회의는 재적위원 과반수의 출석으로 개의하고, 출석위원 과반수의 찬성으로 의결한다.

제7조의11(위원의 제척·기피·회피) ① 위원은 다음 각 호의 어느 하나에 해당하는 경우에는 심의·의결에서 제척된다.

1. 위원 또는 그 배우자나 배우자였던 자가 해당 사안의 당사자가 되거나 그 사건에 관하여 공동의 권리자 또는 의무자의 관계에 있는 경우
2. 위원이 해당 사안의 당사자와 친족이거나 친족이었던 경우
3. 위원이 해당 사안에 관하여 증언, 감정, 법률자문을 한 경우
4. 위원이 해당 사안에 관하여 당사자의 대리인으로서 관여하거나 관여하였던 경우
5. 위원이나 위원이 속한 공공기관·법인 또는 단체 등이 조인 등 지원을 하고 있는 자와 이해관계가 있는 경우

② 위원에게 심의·의결의 공정을 기대하기 어려운 사정이 있는 경우 당사자는 기피 신청을 할 수 있고, 보호위원회는 의결로 이를 결정한다.

③ 위원이 제1항 또는 제2항의 사유가 있는 경우에는 해당 사안에 대하여 회피할 수 있다.

제7조의12(소위원회) ① 보호위원회는 효율적인 업무 수행을 위하여 개인정보 침해 정도가 경미하거나 유사·반복되는 사항 등을 심의·의결할 소위원회를 둘 수 있다.

② 소위원회는 3명의 위원으로 구성한다.

③ 소위원회가 제1항에 따라 심의·의결한 것은 보호위원회가 심의·의결한 것으로 본다.

④ 소위원회의 회의는 구성위원 전원의 출석과 출석위원 전원의 찬성으로 의결한다.

제7조의13(사무처) 보호위원회의 사무를 처리하기 위하여 보호위원회에 사무처를 두며, 이 법에 규정된 것 외에 보호위원회의 조직에 관한 사항은 대통령령으로 정한다.

제7조의14(운영 등) 이 법과 다른 법령에 규정된 것 외에 보호위원회의 운영 등에 필요한 사항은 보호위원회의 규칙으로 정한다.

제5조(전문위원회) ① 보호위원회는 법 제7조의9제1항에 따른 심의·의결 사항에 대하여 사전에 전문적으로 검토하기 위하여 보호위원회에 분야별 전문위

위원회(이하 “전문위원회”라 한다)를 둘 수 있다.

② 제1항에 따라 전문위원회를 두는 경우 각 전문위원회는 위원장 1명을 포함한 20명 이내의 위원으로 성별을 고려하여 구성하되, 전문위원회 위원은 다음 각 호의 사람 중에서 보호위원회 위원장이 임명하거나 위촉하고, 전문위원회 위원장은 보호위원회 위원장이 전문위원회 위원 중에서 지명한다.

1. 보호위원회 위원
2. 개인정보 보호 관련 업무를 담당하는 중앙행정기관의 관계 공무원
3. 개인정보 보호에 관한 전문지식과 경험이 풍부한 사람
4. 개인정보 보호와 관련된 단체 또는 사업자단체에 속하거나 그 단체의 추천을 받은 사람

③ 삭제 <2020. 8. 4.>

제5조의2(개인정보 보호 정책협의회) ① 개인정보 보호 정책의 일관성 있는 추진과 개인정보 보호 관련 사안에 대한 관계 중앙행정기관 간 협의를 위하여 보호위원회에 개인정보 보호 정책협의회(이하 “정책협의회”라 한다)를 둘 수 있다.

② 정책협의회는 다음 각 호의 사항을 협의한다.

1. 법 제9조에 따른 개인정보 보호 기본계획 및 법 제10조에 따른 시행계획 등 개인정보 보호와 관련된 주요 정책
2. 개인정보 보호와 관련된 주요 법령의 제·개정
3. 개인정보 보호와 관련된 주요 정책의 협력 및 의견조정
4. 개인정보 침해사고 예방 및 대응
5. 개인정보 보호 기술개발 및 전문인력의 양성
6. 그 밖에 개인정보 보호와 관련하여 관계 중앙행정기관 간 협이가 필요한 사항

③ 정책협의회는 관계 중앙행정기관의 고위공무원단에 속하는 공무원 또는 그에 상당하는 공무원으로서 개인정보 보호와 관련된 업무를 담당하는 사람 중 소속 기관의 장이 지명하는 사람으로 구성하되, 정책협의회의 의장(이하 이 조에서 “의장”이라 한다)은 보호위원회의 부위원장으로 한다.

④ 정책협의회는 업무를 수행하기 위하여 필요한 경우에는 실무협의회 또는 분야별 협의회를 둘 수 있다.

⑤ 실무협의회 및 분야별 협의회는 의장은 보호위원회 소속 공무원 중에서 의장이 임명한다.

⑥ 정책협의회, 실무협의회 및 분야별 협의회는 업무를 수행하기 위하여 필요한 경우에는 관계 기관·단체 및 전문가 등에게 출석, 자료 또는 의견의 제출 등 필요한 협조를 요청할 수 있다.

⑦ 제1항부터 제6항까지에서 규정한 사항 외에 정책협의회의 운영 등에 필요한 사항은 정책협의회의 의결을 거쳐 의장이 정한다.

제5조의3(시·도 개인정보 보호 관계 기관 협의회) ① 개인정보 보호 정책의 효율적인 추진과 자율적인 개인정보 보호 강화를 위하여 특별시, 광역시, 특별자치시, 도, 특별자치도(이하 “시·도” 라 한다)에 시·도 개인정보 보호 관계 기관 협의회(이하 “시·도협의회” 라 한다)를 둘 수 있다. [시행일 : 2021.2.5.]

② 시·도협의회는 다음 각 호의 사항을 협의한다.

1. 시·도 개인정보 보호 정책
2. 관계 기관·단체 등의 의견 수렴 및 전달
3. 개인정보 보호 우수사례 공유
4. 그 밖에 개인정보 보호와 관련하여 시·도협의회의 협이가 필요한 사항

③ 제1항 및 제2항에서 규정한 사항 외에 시·도협의회의 구성 및 운영 등에 필요한 사항은 시·도의 조례로 정한다.

제6조(의사의 공개) 보호위원회의 의사(議事)는 공개한다. 다만, 보호위원회 위원장이 필요하다고 인정하는 경우에는 공개하지 아니할 수 있다.

제7조(공무원 등의 파견) 보호위원회는 그 업무 수행을 위하여 필요하다고 인정하는 경우에는 공공기관에 그 소속 공무원 또는 임직원의 파견을 요청할 수 있다.

제9조(출석수당 등) 보호위원회, 전문위원회 또는 정책협의회에 출석한 위원, 법 제7조의9제2항에 따라 보호위원회에 출석한 사람, 전문위원회에 출석한 사람 또는 정책협의회에 출석한 사람에게는 예산의 범위에서 수당·여비, 그 밖에 필요한 경비를 지급할 수 있다. 다만, 공무원이 그 소관 업무와 직접 관련되어 출석하는 경우에는 그렇지 않다.

1. 보호위원회 소집 및 의결

가 회의 소집 및 의안 제의

보호위원회의 회의는 위원장이 필요하다고 인정하거나 재적위원 4분의 1 이상의 요구가 있는 경우에 위원장이 소집한다(제7조의10제1항).

그리고 위원장 또는 2명 이상의 위원은 보호위원회에 의안을 제의할 수 있다(제7조의10제2항).

나 위원회 의결

보호위원회의 회의는 재적위원 과반수의 출석으로 개의하고, 출석위원 과반수의 찬성으로 의결한다(제7조의10제3항). 여기서 재적위원이란 법정 위원정수(9명)가 아니라 위원정수에서 사망·사직·퇴직 등에 의하여 결원된 위원 수를 제외한 현재 위원 신분을 가진 사람의 수를 의미한다(법제처 법령해석 07-0324호, 08-0220호 참고).

다 의사의 공개

보호위원회의 의사는 공개함을 원칙으로 한다. 다만, 보호위원회가 필요하다고 인정하는 경우에는 공개하지 아니할 수 있다(영 제6조).

라 위원의 제척·기피·회피

이 법은 위원회의 심의·의결에 있어서 위원의 공정성을 확보하기 위하여 다음과 같은 제척사유 중의 하나에 해당하는 위원을 심의·의결에서 제척되도록 하고 있다(제7조의11 제1항).

위원의 제척사유(제7조의11제1항)

1. 위원 또는 그 배우자나 배우자였던 자가 해당 사안의 당사자가 되거나 그 사건에 관하여 공동의 권리자 또는 의무자의 관계에 있는 경우
2. 위원이 해당 사안의 당사자와 친족이거나 친족이었던 경우
3. 위원이 해당 사안에 관하여 증언, 감정, 법률자문을 한 경우
4. 위원이 해당 사안에 관하여 당사자의 대리인으로서 관여하거나 관여하였던 경우
5. 위원이나 위원이 속한 공공기관·법인 또는 단체 등이 조언 등 지원을 하고 있는 자와 이해관계가 있는 경우

또한 위원에게 심의·의결의 공정성을 기대하기 어려운 사정이 있는 경우 당사자는 기피 신청을 할 수 있고, 보호위원회는 의결로 이를 결정한다(제7조의11제2항).

그리고 위원이 위의 제척사유 또는 기피사유가 있는 경우에는 해당 사안에 대하여 회피할 수 있다(제7조의11제3항).

2. 소위원회

가 소위원회의 설치와 구성

보호위원회는 효율적인 업무 수행을 위하여 개인정보 침해 정도가 경미하거나 유사·반복되는 사항 등을 심의·의결할 소위원회를 둘 수 있다(제7조의12제1항). 소위원회는 3명의 위원으로 구성한다(제7조의12제2항).

나 소위원회의 심의·의결

소위원회가 제1항에 따라 심의·의결한 것은 보호위원회가 심의·의결한 것으로 본다(제7조의12제3항).

소위원회의 회의는 구성위원 전원의 출석과 출석위원 전원의 찬성으로 의결한다(제7조의12제4항).

3. 사무처

보호위원회의 사무를 처리하기 위하여 보호위원회에 사무처를 두며(제7조의13), 보호위원회 사무처의 장은 정부위원이 된다(제7조의2제4항).

4. 전문위원회

보호위원회는 제7조의9제1항에 따른 심의·의결 사항에 대하여 사전에 전문적으로 검토하기 위하여 보호위원회에 분야별 전문위원회(이하 “전문위원회”라 한다)를 둘 수 있다(영 제5조제1항).

각 전문위원회는 위원장 1명을 포함한 20명 이내의 위원으로 성별을 고려하여 구성하되, 전문위원회 위원은 보호위원회 위원, 개인정보 보호 관련 업무를 담당하는 중앙행정기관의 관계 공무원, 개인정보 보호에 관한 전문지식과 경험이 풍부한 사람, 개인정보 보호와 관련된 단체 또는 사업자단체에 속하거나 그 단체의 추천을 받은 사람 중에서 보호위원회 위원장이 임명하거나 위촉하고, 전문위원회 위원장은 보호위원회 위원장이 전문위원회 위원 중에서 지명한다(영 제5조제2항).

5. 개인정보 보호 정책협의회 등

가 개인정보 보호 정책협의회

개인정보 보호 정책의 효율적인 추진과 개인정보 유출사고 예방 및 효과적인 대응 등을 위한 범정부 협업체계로서 개인정보 보호 정책협의회를 둘 수 있도록 하고, 실무협의회 또는 분야별 협의회를 통해 정책협의회의 업무를 지원할 수 있도록 하고 있다(영 제5조의2).

다 시·도 개인정보 보호 관계기관 협의회(2021. 2. 5. 시행 예정)

지방자치단체의 자율적인 개인정보 보호 강화를 위하여 시·도 협의회를 둘 수 있으며(영 제5조의3), 이는 정책 협업, 현장의견 수렴 및 전달, 정책·기술 등 우수사례 공유 및 협력을 통해 지방자치단체의 자율적인 개인정보 보호 강화를 촉진하는 의미를 가진다.

제8조의2 | 개인정보 침해요인 평가

법률

- 제8조의2(개인정보 침해요인 평가)** ① 중앙행정기관의 장은 소관 법령의 제정 또는 개정을 통하여 개인정보 처리를 수반하는 정책이나 제도를 도입·변경하는 경우에는 보호위원회에 개인정보 침해요인 평가를 요청하여야 한다.
- ② 보호위원회가 제1항에 따른 요청을 받은 때에는 해당 법령의 개인정보 침해요인을 분석·검토하여 그 법령의 소관기관의 장에게 그 개선을 위하여 필요한 사항을 권고할 수 있다.
- ③ 제1항에 따른 개인정보 침해요인 평가의 절차와 방법에 관하여 필요한 사항은 대통령령으로 정한다.

시행령

- 제9조의3(개인정보 침해요인 평가 절차 등)** ① 중앙행정기관의 장은 법 제8조의2제1항에 따라 개인정보 침해요인 평가(이하 “침해요인 평가”라 한다)를 요청하는 경우 다음 각 호의 사항을 포함하는 개인정보 침해요인 평가 요청서(전자문서를 포함한다)를 보호위원회에 제출하여야 한다.
1. 법령(법령안을 포함한다)을 통하여 도입되거나 변경되는 개인정보 처리를 수반하는 정책·제도의 목적과 주요 내용
 2. 개인정보 처리를 수반하는 정책·제도의 도입·변경에 따른 제2항 각 호의 사항에 대한 개인정보 침해요인 자체 분석
 3. 개인정보 처리를 수반하는 정책·제도의 도입·변경에 따른 개인정보 보호 대책
- ② 보호위원회는 제1항에 따른 요청서를 받은 경우에는 다음 각 호의 사항을 고려하여 침해요인 평가를 하고, 그 결과를 해당 중앙행정기관의 장에게 통보하여야 한다.
1. 개인정보 처리의 필요성
 2. 개인정보 주체의 권리보장의 적정성
 3. 개인정보 관리의 안전성
 4. 그 밖에 침해요인 평가에 필요한 사항
- ③ 중앙행정기관의 장은 법 제8조의2제2항에 따른 권고를 받은 경우에는 그 내용을 해당 법령안에 반영하는 등 권고내용을 이행하도록 노력하여야 한다. 다만, 보호위원회의 권고대로 이행하기 곤란한 경우에는 그 사유를 보호위원회에 통보하여야 한다.
- ④ 보호위원회는 침해요인 평가를 하는 경우에는 침해요인 평가에 필요한 자료 등을 해당 중앙행정기관의 장에게 요청할 수 있다.
- ⑤ 보호위원회는 침해요인 평가의 세부기준 및 방법 등 침해요인 평가에 필요한 지침을 수립하여 중앙행정기관의 장에게 통보할 수 있다.
- ⑥ 보호위원회는 침해요인 평가를 실시하기 위하여 필요하면 관계 전문가에게 자문 등을 할 수 있다.

중앙행정기관의 장은 소관 법령의 제정 또는 개정을 통하여 개인정보 처리를 수반하는 정책이나 제도를 도입·변경하는 경우에는 보호위원회에 개인정보 침해요인 평가를 요청하여야 한다.

평가대상은 개인정보 처리를 수반하는 정책이나 제도를 도입·변경하는 법령의 제·개정안이다. 여기서 ‘처리’란 개인정보의 수집, 생성, 연계, 연동, 기록, 저장, 보유, 가공, 편집, 검색, 출력, 정정, 복구, 이용, 제공, 공개, 파기, 그 밖에 이와 유사한 행위를 말한다. ‘수반’이란 특정 법령 조항의 운영이나 법 집행 과정에서 개인정보 처리가 주로 또는 부수적으로 발생하는 경우 등이다. 한편, 국회에서 의원 입법 형식으로 발의되는 법률 제·개정안은 평가대상에 해당하지 않는다.

보호위원회가 이러한 요청을 받은 때에는 ① 개인정보 처리의 필요성 ② 개인정보 주체의 권리보장의 적정성 ③ 개인정보 관리의 안전성 ④ 그 밖에 침해요인 평가에 필요한 사항을 고려하여 침해요인 평가를 하고, 그 결과를 해당 중앙행정기관의 장에게 통보하여야 한다. 중앙행정기관의 장은 이러한 권고 통보를 받은 경우에는 그 내용을 해당 법령안에 반영하는 등 권고내용을 이행하도록 노력하여야 한다. 다만, 보호위원회의 권고대로 이행하기 곤란한 경우에는 그 사유를 보호위원회에 통보하여야 한다.

한편, 보호위원회는 침해요인 평가를 하는 경우에는 침해요인 평가에 필요한 자료 등을 해당 중앙행정기관의 장에게 요청할 수 있으며 침해요인 평가를 실시하기 위하여 필요하면 관계 전문가에게 자문 등을 구할 수 있다.

제9조 | 기본계획

법률	<p>제9조(기본계획) ① 보호위원회는 개인정보의 보호와 정보주체의 권익 보장을 위하여 3년마다 개인정보 보호 기본계획(이하 “기본계획” 이라 한다)을 관계 중앙행정기관의 장과 협의하여 수립한다.</p> <p>② 기본계획에는 다음 각 호의 사항이 포함되어야 한다.</p> <ol style="list-style-type: none"> 1. 개인정보 보호의 기본목표와 추진방향 2. 개인정보 보호와 관련된 제도 및 법령의 개선 3. 개인정보 침해 방지를 위한 대책 4. 개인정보 보호 자율규제의 활성화 5. 개인정보 보호 교육·홍보의 활성화 6. 개인정보 보호를 위한 전문인력의 양성 7. 그 밖에 개인정보 보호를 위하여 필요한 사항 <p>③ 국회, 법원, 헌법재판소, 중앙선거관리위원회는 해당 기관(그 소속 기관을 포함한다)의 개인정보 보호를 위한 기본계획을 수립·시행할 수 있다.</p>
시행령	<p>제11조(기본계획의 수립절차 등) ① 보호위원회는 3년마다 법 제9조에 따른 개인정보 보호 기본계획(이하 “기본계획” 이라 한다)을 그 3년이 시작되는 해의 전년도 6월 30일까지 수립해야 한다.</p> <p>② 보호위원회는 제1항에 따라 기본계획을 작성하는 경우에는 관계 중앙행정기관의 장으로부터 개인정보 보호 관련 중장기 계획과 시책 등을 반영한 부문별 계획을 제출받아 기본계획에 반영할 수 있다. 이 경우 보호위원회는 기본계획의 목표, 추진 방향 및 부문별 계획의 작성 지침 등에 관하여 관계 중앙행정기관의 장과 협의하여야 한다.</p> <p>③ 보호위원회는 기본계획이 확정되면 지체 없이 관계 중앙행정기관의 장에게 통보하여야 한다.</p>

개인정보 보호 시책을 범정부 차원에서 종합적이고 체계적으로 추진하기 위하여 중기적 관점의 개인정보 보호 기본계획을 3년마다 수립·시행하고 기본계획을 바탕으로 매년 연도별 시행계획을 수립·시행하도록 하고 있다.

1. 기본계획의 작성주체

보호위원회는 관계 중앙행정기관의 장과 협의하여 사회 전 분야에 걸쳐 개인정보 보호의 기본목표와 추진방향, 법제도 개선, 침해방지 대책 등이 포함된 기본계획을 수립한다.

한편, 국회, 법원, 헌법재판소, 중앙선거관리위원회 등 헌법기관들은 권력분립의 원칙에

따라 해당기관(그 소속 기관을 포함한다)의 개인정보 보호를 위한 기본계획을 자체적으로 수립·시행할 수 있도록 하고 있다.

2. 기본계획의 작성절차

보호위원회는 기본계획을 작성하는 경우에는 관계 중앙행정기관의 장으로부터 개인정보 보호 관련 중장기 계획과 시책 등을 반영한 부문별 계획을 제출받아 기본계획에 반영할 수 있다. 이 경우 보호위원회는 기본계획의 목표, 추진방향 및 부문별 계획의 작성 지침 등에 관하여 관계 중앙행정기관의 장과 협의하여야 한다.

한편, 보호위원회는 기본계획이 시작되는 해의 전년도 6월 30일까지 수립하여야 하므로 해당 일까지 심의·의결을 마쳐야 한다. 아울러 보호위원회는 기본계획이 확정되면 지체 없이 관계 중앙행정기관의 장에게 통보하여야 한다.

3. 기본계획의 내용

기본계획은 개인정보 보호의 기본목표와 추진방향을 큰 틀에서 제시하고, 이를 달성하기 위한 법·제도의 개선방안, 개인정보 침해방지대책, 개인정보 보호 자율규제의 활성화 방안, 개인정보 보호 교육·홍보방안, 전문인력 양성 및 기타 개인정보 보호를 위하여 필요한 사항 등에 관한 중기적 관점의 계획을 포함하여야 한다.

제10조 | 시행계획

법률	제10조(시행계획) ① 중앙행정기관의 장은 기본계획에 따라 매년 개인정보보호를 위한 시행계획을 작성하여 보호위원회에 제출하고, 보호위원회의 심의·의결을 거쳐 시행하여야 한다. ② 시행계획의 수립·시행에 필요한 사항은 대통령령으로 정한다.
시행령	제12조(시행계획의 수립절차 등) ① 보호위원회는 매년 6월 30일까지 다음 해 시행계획의 작성방법 등에 관한 지침을 마련하여 관계 중앙행정기관의 장에게 통보해야 한다. ② 관계 중앙행정기관의 장은 제1항의 지침에 따라 기본계획 중 다음 해에 시행할 소관 분야의 시행계획을 작성하여 매년 9월 30일까지 보호위원회에 제출해야 한다. ③ 보호위원회는 제2항에 따라 제출된 시행계획을 그 해 12월 31일까지 심의·의결해야 한다.

1. 시행계획의 작성주체

관계 중앙행정기관의 장이 개인정보 보호 기본계획과 연계되도록 매년 소관 분야에 관한 다음 연도의 시행계획을 작성한다.

2. 시행계획의 작성절차

가 작성지침의 제정·배포

보호위원회는 매년 6월 30일까지 다음해 시행계획의 작성방법 등에 관한 지침을 마련하여 관계 중앙행정기관의 장에게 통보하여야 한다. 관계 중앙행정기관의 장은 매년 9월 30일까지 소관 분야에 관한 다음 연도의 시행계획을 작성해 보호위원회에 제출하여야 한다.

나 보호위원회의 심의·의결

시행계획이 보호위원회에 제출되면 보호위원회는 회의를 소집하고 그 해 12월 31일까지 심의·의결 절차를 밟아야 한다. 시행계획은 보호위원회의 심의·의결을 거쳐야 확정된다.

제11조 | 자료제출 요구 등

법률

제11조(자료제출 요구 등) ① 보호위원회는 기본계획을 효율적으로 수립하기 위하여 개인정보처리자, 관계 중앙행정기관의 장, 지방자치단체의 장 및 관계 기관·단체 등에 개인정보처리자의 법규 준수 현황과 개인정보 관리 실태 등에 관한 자료의 제출이나 의견의 진술 등을 요구할 수 있다.

② 보호위원회는 개인정보 보호 정책 추진, 성과평가 등을 위하여 필요한 경우 개인정보처리자, 관계 중앙행정기관의 장, 지방자치단체의 장 및 관계 기관·단체 등을 대상으로 개인정보 관리 수준 및 실태파악 등을 위한 조사를 실시할 수 있다.

③ 중앙행정기관의 장은 시행계획을 효율적으로 수립·추진하기 위하여 소관 분야의 개인정보처리자에게 제1항에 따른 자료제출 등을 요구할 수 있다.

④ 제1항부터 제3항까지에 따른 자료제출 등을 요구받은 자는 특별한 사정이 없으면 이에 따라야 한다.

⑤ 제1항부터 제3항까지에 따른 자료제출 등의 범위와 방법 등 필요한 사항은 대통령령으로 정한다.

시행령

제13조(자료제출 요구 등의 범위와 방법) ① 보호위원회는 법 제11조제1항에 따라 개인정보처리자에게 다음 각 호의 사항에 관한 자료의 제출이나 의견의 진술 등을 요구할 수 있다.

1. 해당 개인정보처리자가 처리하는 개인정보 및 개인정보파일의 관리와 영상정보처리기기의 설치·운영에 관한 사항
2. 법 제31조에 따른 개인정보 보호책임자의 지정 여부에 관한 사항
3. 개인정보의 안전성 확보를 위한 기술적·관리적·물리적 조치에 관한 사항
4. 정보주체의 열람, 개인정보의 정정·삭제·처리정지의 요구 및 조치 현황에 관한 사항
5. 그 밖에 법 및 이 영의 준수에 관한 사항 등 기본계획의 수립·추진을 위하여 필요한 사항

② 보호위원회는 제1항에 따라 자료의 제출이나 의견의 진술 등을 요구할 때에는 기본계획을 효율적으로 수립·추진하기 위하여 필요한 최소한의 범위로 한정하여 요구하여야 한다.

③ 법 제11조제3항에 따라 중앙행정기관의 장이 소관 분야의 개인정보처리자에게 자료의 제출 등을 요구하는 경우에는 제1항과 제2항을 준용한다. 이 경우 “보호위원회”는 “중앙행정기관의 장”으로, “법 제11조제1항”은 “법 제11조제3항”으로 본다.

제11조는 개인정보 보호 기본계획 및 시행계획의 효율적 수립·추진 및 개인정보 보호 정책 추진, 성과평가 등을 위하여 보호위원회가 개인정보처리자의 개인정보 보호 법규 준수 현황, 개인정보 관리실태 등에 관한 자료제출, 의견진술 등을 요구할 수 있도록 하고 있다.

1. 자료제출·의견진술 등의 대상

가 기본계획 수립·추진에 필요한 자료 등의 요구

보호위원회는 기본계획을 효율적으로 수립하기 위하여 개인정보처리자의 법규 준수 현황과 개인정보 관리 실태 등에 관한 자료의 제출이나 의견의 진술 등을 요구할 수 있다. 이러한 요구는 ① 개인정보처리자 ② 관계 중앙행정기관의 장 ③ 지방자치단체의 장 ④ 관계 기관·단체 등에 대하여 한다. 관계 단체란 사업의 일부 또는 전부가 개인정보 처리 또는 보호에 관련된 사업을 수행하고 있는 사업자협회나 소비자단체 등을 말한다. 이러한 자료제출이나 의견진술 등을 요구받은 자는 특별한 사정이 없으면 이에 따라야 한다.

나 시행계획 수립·추진에 필요한 자료 등의 요구

중앙행정기관의 장은 시행계획을 효율적으로 수립·추진하기 위하여 소관 분야의 개인정보처리자에게 개인정보처리자의 법령 등의 준수현황과 개인정보 관련 실태 등에 관한 자료의 제출이나 의견의 진술을 요구할 수 있다. 이러한 자료제출이나 의견진술 등을 요구받은 자는 특별한 사정이 없으면 이에 따라야 한다.

다 보호위원회의 정책추진·성과평가 등을 위한 조사 실시

보호위원회는 개인정보 보호 정책 추진, 성과평가 등을 위하여 필요한 경우 개인정보관리 수준 및 실태파악 등을 위한 조사를 실시할 수 있다. 이러한 조사는 ① 개인정보처리자 ② 관계 중앙행정기관의 장 ③ 지방자치단체의 장 ④ 관계 기관·단체 등에 대하여 한다. 이러한 조사를 요구받은 자는 특별한 사정이 없으면 이에 따라야 한다.

2. 제출자료 등의 범위와 방법

보호위원회 및 중앙행정기관의 장이 기본계획·시행계획의 수립을 위하여 요구할 수 있는 자료·진술 등의 범위 및 방법 등에 관한 세부사항은 대통령령에 위임하고 있다. 제63조

에 따른 위법행위 조사 등과의 구별을 명확히 하고, 지나치게 자의적으로 자료제출, 의견진술 등의 요구가 행사되지 않도록 요구할 수 있는 자료, 진술 등의 범위를 시행령에서 구체화하고 있다. 자료제출, 의견진술 등의 요구에 관한 구체적인 절차와 방법은 「행정조사기본법」에 따른다.

기본계획 수립을 위한 자료의 요청은 ① 해당 개인정보처리자가 처리하는 개인정보 및 개인정보파일의 관리와 영상정보처리기의 설치·운영에 관한 사항 ② 법 제31조에 따른 개인정보 보호책임자의 지정 여부에 관한 사항 ③ 개인정보의 안전성 확보를 위한 기술적·관리적·물리적 조치에 관한 사항 ④ 정보주체의 열람, 개인정보의 정정·삭제·처리정지의 요구 및 조치 현황에 관한 사항 ⑤ 그 밖에 법 및 이 영의 준수에 관한 사항 등 기본계획의 수립·추진을 위하여 필요한 사항이다. 이러한 자료의 제출이나 의견의 진술 등을 요구할 때에는 기본계획을 효율적으로 수립·추진하기 위하여 필요한 최소한의 범위로 한정하여 요구하여야 한다. 이는 시행계획 수립 시의 자료제출 등에 있어서도 동일하다.

❖ 제11조와 제63조의 구별 ❖

- **법 제11조(자료제출 요구 등)** : 개인정보 보호 기본계획·시행계획의 정책 수립이나 제도개선을 위하여 개인정보의 수집·이용, 제공 실태 및 개인정보의 기술적·관리적 보호조치 현황 등 개인정보처리자의 위법여부와 관계없이 요구할 수 있는 처리실태 및 관리현황 등에 관한 자료 및 통계 등의 조사를 말함
- **법 제63조(자료제출요구 및 검사 등)** : 위법사실이 발견되었거나 혐의가 있는 경우 등과 같이 사후적 집행·감독을 위하여 필요한 행정조사를 의미한다.
 - ※ 침해신고, 언론보도, 실태조사 등을 통해 위법사실을 인지한 경우 시정명령이나 과태료 부과 등의 행정규제를 위한 조사를 말함

제12조 | 개인정보 보호지침

법률

- 제12조(개인정보 보호지침)** ① 보호위원회는 개인정보의 처리에 관한 기준, 개인정보 침해의 유형 및 예방조치 등에 관한 표준 개인정보 보호지침(이하 “표준지침”이라 한다)을 정하여 개인정보처리자에게 그 준수를 권장할 수 있다.
- ② 중앙행정기관의 장은 표준지침에 따라 소관 분야의 개인정보 처리와 관련한 개인정보 보호지침을 정하여 개인정보처리자에게 그 준수를 권장할 수 있다.
- ③ 국회, 법원, 헌법재판소 및 중앙선거관리위원회는 해당 기관(그 소속 기관을 포함한다)의 개인정보 보호지침을 정하여 시행할 수 있다.

이 법에 의한 개인정보 보호지침은 보호위원회가 정하는 표준 개인정보 보호지침, 중앙행정기관의 장 등이 정하는 소관 분야별 개인정보 보호지침을 말한다.

개인정보 보호지침은 보호위원회, 중앙행정기관, 헌법기관 등에게 입법 보충권을 부여하기 위한 것이다. 이 법은 개인정보 보호에 관한 일반법이기 때문에 모든 분야, 모든 산업을 세세하게 규율할 수는 없다. 또한 개인정보처리자가 종사하는 업무의 환경이나 위험도에 따라 개인정보의 처리 범위·방법, 요구되는 보호수준 등이 각기 다를 수 있지만, 이 법은 경제·사회의 공통적 요소와 요구들을 중심으로 일반적이고 추상적인 내용들로 규정되어 있다.

따라서 개인정보 보호를 위한 구체적인 처리기준, 보호조치 등은 분야별·산업별 특성을 고려해서 개별적으로 보충되어야 한다. 일반법주의를 채택하고 있는 나라들은 대부분 제12조와 마찬가지로 개인정보 감독기구에게 지침, 가이드라인 등의 제정·배포를 통한 입법 보충권을 부여하고 있다. 개인정보 처리기술과 환경을 모두 법률로 규율할 경우 현실을 반영하기 어렵고 현실을 외면하거나 현실과 동떨어진 규제가 될 수 있기 때문이다.

1. 표준 개인정보 보호지침의 제정

개인정보처리자가 이 법과 개별법에 의해서 부여된 제반 의무를 성실하게 준수하고 개인정보를 안전하게 이용·보호하도록 하기 위하여 어떤 처리 절차와 방법에 따라 무슨 보호조치를 취해야 하는지를 표준적으로 제시한 것이 표준 개인정보 보호지침(이하 “표준지침”이라 한다)이다. 표준지침은 전 분야에 걸쳐서 공통적으로 적용되기 때문에 일반지침 또는 공통지침이라고 할 수 있다.

2. 소관 분야별 개인정보 보호지침

가 개인정보 보호지침의 제정

분야별 지침은 중앙행정기관의 장 또는 헌법기관이 소관 분야별로 정해서 시행한다. 중앙행정기관의 장이 분야별 지침을 정할 때에는 보호위원회가 제정한 표준지침을 따르되, 개별법의 규정들도 고려해서 중복규제가 발생하지 않도록 하여 보다 명확하고 분야별 특성에 충실해야 한다. 정부조직법 또는 개별 조직법의 업무분장에 의거, 소관 분야가 2개 이상의 부처에 걸쳐 있는 경우에는 해당 부처가 공동으로 지침을 정할 수도 있다.

분야별 지침은 구체적 타당성을 확보한 실천적 행동규범을 개인정보처리자에게 제시함으로써 자발적인 법규준수를 유도·장려하고 법 집행의 형평성을 확보하기 위한 것이므로 그 자체 위법성을 해석·심사하는 기준이 되어야 하지 또다시 해석의 여지를 남기는 추상적·다의적 내용이어서는 안 된다.

한편, 국회, 법원, 헌법재판소, 중앙선거관리위원회 등 헌법기관들은 권력분립의 정신에 따라 해당 기관(그 소속 기관을 포함한다)의 분야별 지침을 자체적으로 정하여 시행하도록 규정하고 있다. 이 경우 보호위원회가 제정한 표준지침을 참고해서 정할 수 있다.

나 개인정보 보호지침의 내용

개인정보 보호지침에는 개인정보처리 기준, 개인정보 침해유형, 개인정보 침해 예방 등에 관하여 구체적인 지침이 포함되어 있어야 한다.

첫째, 개인정보처리자가 개인정보를 수집·이용·제공 및 파기하는 경우에 법률에서 정한 요건에 적합한지 여부를 판단할 수 있는 기준과 사례가 제시되어야 한다.

둘째, 구체적 조건과 상황에서 개인정보처리자의 작위 또는 부작위가 개인정보 침해에 해당되는지 여부를 판단할 수 있는 기준과 사례가 제시되어야 한다.

셋째, 개인정보 권리 침해를 예방하기 위하여 개인정보처리자가 지켜야 할 보호조치나 이행조치의 내용이 개인정보의 처리 단계별, 개인정보의 처리 규모, 개인정보의 활용빈도, 처리되는 개인정보의 용도, 개인정보의 보유 기간, 처리되는 개인정보의 위험도, 개인정보를 처리하기 위해 도입된 기술별로 구체적으로 제시되어야 한다.

제13조 | 자율규제의 촉진 및 지원

<p>법률</p>	<p>제13조(자율규제의 촉진 및 지원) 보호위원회는 개인정보처리자의 자율적인 개인정보 보호활동을 촉진하고 지원하기 위하여 다음 각 호의 필요한 시책을 마련하여야 한다.</p> <ol style="list-style-type: none"> 1. 개인정보 보호에 관한 교육·홍보 2. 개인정보보호와 관련된 기관·단체의 육성 및 지원 3. 개인정보보호 인증마크의 도입·시행 지원 4. 개인정보처리자의 자율적인 규약의 제정·시행 지원 5. 그 밖에 개인정보처리자의 자율적 개인정보 보호활동을 지원하기 위하여 필요한 사항
<p>시행령</p>	<p>제14조(자율규제의 촉진 및 지원) 보호위원회는 법 제13조제2호에 따라 개인정보처리자의 자율적인 개인정보 보호활동을 촉진하기 위하여 예산의 범위에서 개인정보 보호와 관련된 기관 또는 단체에 필요한 지원을 할 수 있다.</p>
<p>고시</p>	<p>개인정보 보호 자율규제단체 지정 등에 관한 규정(보호위원회 고시 제2020-3호)</p> <p>제1조(목적) 이 규정은 「개인정보 보호법」(이하 “법”이라 한다)제5조제3항, 제13조제2호, 제4호 및 제5호와 같은 법 시행령 제14조에 따라 개인정보 보호와 관련하여 자율규제를 수행하는 단체(이하 “자율규제단체”라 한다)의 지정 등에 관한 사항을 정함으로써 개인정보처리자의 자율적인 개인정보 보호활동을 촉진하고 이를 지원하고자 함을 목적으로 한다.</p> <p>제2조(적용범위) 다음 각 호의 자는 자율규제단체의 지정·지정취소, 자율규제협의회 구성 등에 관하여 다른 법령에 특별히 정한 경우를 제외하고는 이 규정에서 정하는 바에 따른다.</p> <ol style="list-style-type: none"> 1. 제7조에 따라 자율규제단체로 지정된 협회, 단체, 자율규제단체에 소속된 개인정보처리자(이하 “소속 개인정보처리자”라 한다) 2. 제15조에 따라 지정된 전문기관 <p>제3조(자율규제단체 등의 책무) 자율규제단체와 소속 개인정보처리자는 자율적인 개인정보 보호 활동을 함에 있어서 다음 각 호 사항을 준수하여야 한다.</p> <ol style="list-style-type: none"> 1. 자율규제단체와 그 소속 개인정보처리자는 상호 신뢰와 합의에 기초하여 자율규제 규약을 마련하여 준수한다. 2. 자율규제단체는 그 소속 개인정보처리자가 개인정보 보호 활동에 자발적으로 참여할 수 있도록 노력한다. 3. 자율규제단체는 개인정보 보호 활동의 전문성을 확보하기 위하여 필요한 인력과 예산을 확보하도록 노력하여야 한다. 4. 자율규제단체는 소속 개인정보처리자가 개인정보 보호 관련 법령에 따라

안전하게 개인정보의 처리를 할 수 있도록 필요한 지원과 노력을 하여야 한다.

5. 자율규제단체와 그 소속 개인정보처리자는 법 제3조의 개인정보 보호 원칙을 준수하여야 한다.

제4조(자율규제 협의회) 개인정보 보호위원회(이하 “보호위원회”라 한다)는 자율규제단체 지정 등에 관한 다음 각 호의 업무를 위하여 개인정보보호 자율규제 협의회(이하 “협의회”라 한다)를 둘 수 있다.

1. 자율규제단체의 지정 및 지정 취소에 대한 심사
2. 제10조의 자율규제 규약에 대한 검토
3. 제13조의 연간 개인정보 보호 수행계획 및 결과에 대한 검토
4. 제14조의 개인정보 보호 수행계획에 따른 결과의 평가에 대한 검토
5. 그 밖에 자율규제단체의 개인정보 보호 활동에 관하여 필요한 사항

제5조(협의회의 구성 등) ① 협의회는 보호위원회, 자율규제단체 소관 행정기관, 전문기관 및 해당 분야 전문가로 구성하며 위원은 다음 각 호에 해당하는 자로 한다.

1. 보호위원회, 자율규제단체 소관 행정기관 소속 개인정보 보호 업무를 담당하는 국장급 공무원
 2. 제15조에 따라 전문기관으로 지정된 기관의 개인정보 보호 업무를 담당하는 임직원
 3. 개인정보 보호와 자율규제에 관하여 학식과 경험이 풍부한 전문가 5인 이내
- ② 위원장은 협의회의 업무를 총괄하며 제1항제3호 민간 전문가 1인으로 정한다.
- ③ 간사는 제15조제2항에 따라 지정된 한국인터넷진흥원 개인정보 보호 자율규제 업무를 담당하는 자로 한다.
- ④ 제1항제3호 위원 임기는 2년으로 하되, 연임할 수 있다.
- ⑤ 협의회의 회의는 위원장이 필요하다고 인정하거나 재적 위원 3분의 1 이상의 요구가 있는 경우에 위원장이 소집한다.

제6조(행정기관 등에 대한 협조요청) ① 협의회는 제4조 각 호의 업무를 위하여 필요한 경우 행정기관이나 전문기관 또는 전문가의 의견 청취, 자율규제단체에 자료 및 의견 제출 등의 협조를 요청할 수 있다.

- ② 행정기관이나 자율규제단체는 제1항에 따른 요청을 받은 경우 이에 적극 응하여야 한다.

제7조(자율규제단체의 지정) ① 자율규제단체로 지정받고자 하는 협회, 단체는 별지 제1호 서식의 자율규제단체 지정신청서와 제13조에 따른 연간 수행계획을 협의회에 제출하여야 한다.

- ② 협의회는 제1항의 신청서를 제출한 협회, 단체가 자율적 개인정보 보호할

등 역량이 있는지 여부에 대하여 별표에 따라 심사한다.

③ 보호위원회는 제2항의 심사 결과에 따라 자율규제단체를 지정 확인한 후 별지 제2호의 자율규제단체 지정서를 발급한다.

제8조(자율규제단체의 지정 취소) ① 협의회는 자율규제단체가 다음 각 호의 어느 하나에 해당하는 경우 자율규제단체 지정 취소를 심사할 수 있다.

1. 허위 또는 부정방법으로 제7조의 지정을 받은 경우
2. 자율규제단체의 수행실적 관련 보고 및 제출을 하지 않은 경우
3. 자율규제단체 운영을 통해 알게 된 정보를 부당하게 이용한 경우
4. 권한 오남용, 직무상 의무 위반 등 자격유지가 부적합하다고 인정되는 경우
5. 자율규제단체가 제9조에 따른 업무를 허위 또는 불성실하게 수행하였음이 인정되는 경우

② 자율규제단체는 자율규제단체 지정의 취소를 원하는 경우 지정의 취소를 보호위원회에 신청할 수 있다.

③ 보호위원회는 제1항의 심사 결과나 제2항의 지정의 취소 신청에 따라 자율규제단체를 지정 취소할 수 있다.

제9조(자율규제단체의 업무) 자율규제단체는 소속 개인정보처리자의 자율적인 개인정보 보호 활동을 지원하기 위하여 다음 각 호의 업무를 수행하도록 노력하여야 한다.

1. 연간 개인정보 보호 자율규제 수행계획 수립
2. 개인정보 보호 교육 및 홍보 활동
3. 개인정보 보호 자율규제 규약 제정·개정
4. 개인정보 자율점검 및 컨설팅
5. 그 밖의 소속 개인정보처리자의 개인정보 보호 활동에 관하여 필요한 업무

제10조(자율규제 규약) ① 자율규제단체는 소속 개인정보처리자의 개인정보 처리 특성을 고려하여 개인정보 보호에 필요한 규약(이하 “자율규제 규약”이라 한다)을 작성하고 공표하여야 한다.

② 자율규제단체는 소속 개인정보처리자가 자율규제 규약을 준수하도록 지도, 권고 등 필요한 조치를 할 수 있다.

③ 소속 개인정보처리자는 자율규제 규약을 준수하도록 노력하여야 한다.

제11조(자율점검) ① 자율규제단체는 자율규제 규약에 따라 소속 개인정보처리자의 개인정보 처리 실태를 점검하고 미흡한 점을 개선하도록 지도할 수 있다.

② 자율규제단체는 제1항의 실태 점검 최소 1개월 전에 소속 개인정보처리자가 스스로 개인정보 처리 실태를 점검할 수 있도록 표준 자율점검표를 마련하여 배포하여야 한다.

제12조(소속 개인정보처리자) 소속 개인정보처리자는 개인정보 보호 자율규제 활동에 대하여 자율적으로 참여 여부를 선택할 수 있다. 다만, 제12조의2에

따른 자율규제활동 제한 기간에는 참여할 수 없다.

제12조의2(자율규제단체 소속 개인정보처리자의 참여 제한) ① 자율규제단체는 소속 개인정보처리자가 다음 각 호의 어느 하나에 해당하는 경우에는 자율규제 활동의 전부 또는 일부를 일정기간 제한할 수 있다.

1. 법 위반으로 인해 형벌 또는 행정처분을 받은 경우
2. 제11조제1항의 개인정보 처리실태에 따른 개선을 지도받았음에도 불구하고 이를 이행하지 아니한 경우
3. 소속 개인정보처리자가 자율점검을 허위 또는 불성실하게 이행한 경우

② 제1항에도 불구하고 협의회는 자율규제단체가 소속 개인정보처리자의 참여 제한을 정당한 이유 없이 이행하지 아니하는 경우에는 그 자율규제단체에게 소속 개인정보처리자의 참여 제한 이행을 권고하거나 심사를 통하여 해당 자율규제단체의 지정을 취소할 수 있다.

③ 제1항에 따른 제한기간은 최소 1년으로 하고, 구체적인 기간은 자율규제단체 자율규약으로 정한다.

제13조(연간 수행계획 및 결과 보고의무 등) ① 자율규제단체는 다음 각 호의 내용을 포함하는 연간 개인정보 보호 자율규제 수행계획 및 그 결과를 협의회에 보고하여야 한다.

1. 연간 교육·컨설팅 계획 및 수행결과
2. 자율규약 체결 목표 및 수행결과
3. 자율규약 및 점검표 제.개정 계획 및 수행결과
4. 자율점검 이행목표 및 수행결과

② 자율규제단체는 보호위원회 및 협의회의 자율규제 수행 관련 의견 및 자료 요청에 적극적으로 응하여야 한다.

제14조(수행계획에 따른 결과의 평가 등) ① 협의회는 자율규제단체의 개인정보 보호 자율규제 수행계획에 따른 결과를 평가할 수 있다.

② 보호위원회는 제1항에 따른 평가 결과가 우수한 자율규제단체 및 소속 개인정보처리자에 대하여 포상할 수 있다.

제14조의2(자료제출 및 감사의 면제 등) ① 보호위원회는 자율규제단체의 자율규제 활동에 참여하는 소속 개인정보처리자가 자율규제 규약을 충실히 준수하고 자율점검을 성실히 수행하여 수행결과가 우수하다고 인정되는 경우에는 자료제출 요구 및 감사를 1년간 면제할 수 있다.

② 제1항에 따른 자료제출 요구 및 감사의 면제는 해당 소속 개인정보처리자가 법 제63조제1항의 어느 하나에 해당하는 경우에는 적용하지 아니한다.

제15조(전문기관 지정 등) ① 보호위원회는 자율규제단체 지정, 자율규제단체의 개인정보 보호 활동의 확인 등 관련 업무의 지원을 위하여 총괄 전문기관을 지정하고 해당 업무를 위탁할 수 있다.

- ② 제1항에 따른 전문기관은 한국인터넷진흥원으로 한다.
- ③ 보호위원회는 협회·단체의 자율규제 업무를 지원하기 위해 특별한 전문성이 필요로 하는 경우 분야별 전문기관을 추가하여 지정할 수 있다.
- ④ 보호위원회는 제3의 전문기관을 지정한 경우 이를 공고하여야 한다.

제16조(업무의 지원) 보호위원회는 자율규제단체의 업무 수행에 필요한 다음 각 호의 사항을 지원할 수 있다.

1. 개인정보 보호 전문인력 파견, 자율점검 지원
2. 개인정보 보호 전문교육, 인식제고 교육 실시
3. 웹 취약점 점검, 보안도구의 제공 등의 기술지원(단, 보안도구 제공 등 일부 기술지원은 ‘중소기업기본법 제2조’에 따른 중소기업에만 해당)
4. 개인정보 보호 관련 정보 제공 등

제17조(재검토 기한) 보호위원회는 「훈령·예규 등의 발령 및 관리에 관한 규정」에 따라 이 고시에 대하여 2020년 8월 11일을 기준으로 매 3년이 되는 시점(매 3년째의 8월 10일까지를 말한다)마다 그 타당성을 검토하여 개선 등의 조치를 하여야 한다.

제5조는 국가 등의 책무로서 개인정보 처리에 관한 불합리한 사회적 관행을 개선하기 위한 개인정보처리자의 자율적 개인정보 보호활동을 존중하고 촉진·지원할 것을 규정하고 있는데, 제13조는 제5조의 책무를 구체화한 것이다. 개인정보 처리는 어느 한 분야만의 일이 아니고 모든 경제·사회 영역에서 매일 이루어지기 때문에 법적인 강제만으로 이 법의 목적을 달성할 수 없으며, 개인정보처리자와 정보주체들의 자발적인 노력이 없이는 불가능하기 때문이다.

이 법의 목적을 보다 효율적으로 달성하기 위해서는 강제적인 규제조치와 함께 개인정보처리자와 정보주체가 자발적으로 개인정보를 보호할 수 있는 환경 조성이 필요하다. 개인정보처리자가 스스로 개인정보 보호에 대한 필요성을 인식하고 자신의 책무를 다할 때, 또한 정보주체들이 스스로의 권리를 인식하고 자신의 권리 보호에 앞장설 때 개인정보는 보다 안전하게 이용되고 보호될 수 있을 것이다.

이를 위해 보호위원회는 다음의 시책을 마련하여야 한다.

1. 개인정보 보호에 관한 교육·홍보

자발적인 개인정보 보호 활동이 이루어지기 위해서는 개인정보의 보호 필요성, 피해사례, 이용 관행 및 환경 등에 대한 인식과 함께 개인정보 보호 법제 및 기술에 대한 깊은 이해가 필요하다. 이와 관련하여 보호위원회는 개인정보처리자의 자발적인 개인정보 보호 활동이 이루어질 수 있도록 필요한 교육과 홍보 및 관련 지원을 할 수 있도록 하였다.

2. 개인정보 보호와 관련된 기관·단체 등의 육성·지원

개인정보의 안전한 이용을 위해서는 정보주체 스스로의 권리보호 노력도 필요하다. 개인정보 보호 관련 기관·단체를 육성하기 위하여 보호위원회는 예산의 범위 내에서 단체를 육성·지원 할 수 있다.

이와 관련하여 보호위원회는 개인정보처리자의 자율적인 개인정보 보호활동을 촉진하고 이를 지원하고자 「개인정보 보호 자율규제단체 지정 등에 관한 규정(개인정보 보호위원회고시 제2020-3호)」을 마련하였다. 동 규정은 개인정보 보호와 관련하여 자율규제를 수행하는 단체의 지정, 자율규제 협의회 설치, 자율규제단체의 업무, 자율규제단체에 대한 지원 등에 대한 사항을 담고 있으며 그 주요내용은 다음과 같다.

첫째, 자율규제 협의회 설치 및 운영에 대하여 규정하고 있다. 보호위원회는 ① 자율규제단체의 지정 및 지정 취소에 대한 심사 ② 자율규제 규약에 대한 검토 ③ 개인정보 보호 자율규제 계획 및 활동에 대한 검토 ④ 기타 자율규제단체의 개인정보 보호 활동에 관하여 필요한 사항 등에 관한 업무를 위하여 개인정보 보호 자율규제 협의회를 둘 수 있다. 협의회는 보호위원회, 보건복지부, 문화체육관광부 등 자율규제단체 소속 국장급 공무원, 전문기관 및 전문가로 구성한다.

둘째, 자율규제단체의 지정, 지정취소, 지정추가 등에 대하여 규정하고 있다. 자율규제단체는 자율규제협회의 심사를 거쳐 보호위원회가 지정, 확정한다. 자율규제단체는 소속 개인정보처리자를 대상으로 ‘개인정보 보호 교육 및 홍보 활동’ 과 ‘개인정보 보호 자율규제 규약 제정’ 을 반드시 수행하여야 하며, 그밖에 개인정보 자율점검 및 컨설팅, 소속 개인정보처리자의 개인정보 보호 활동에 관하여 필요한 업무를 수행하도록 노력하여야 한다.

셋째, 자율규제단체에 대한 지원을 규정하고 있다. 보호위원회는 ① 개인정보 보호 전문인력 파견, 자율점검 지원 ② 개인정보 보호 전문교육, 인식제고 교육 실시 ③ 웹 취약점 점검, 보안도구의 제공 등의 기술지원 ④ 개인정보 보호 관련 정보 제공 등과 관련하여 자율규제단체의 업무 수행에 필요한 사항을 지원할 수 있다.

3. 개인정보 보호 인증마크의 도입·시행

개인정보 보호 인증마크는 개인정보를 적법하고 안전하게 처리하는 개인정보처리자에게 부여되는 안전마크의 일종이다. 인증마크를 획득한 개인정보처리자에 대해서는 개인정보의 안전한 처리를 신뢰할 수 있기 때문에 인증마크는 기업이나 기관의 개인정보 보호활동을 촉진할 수 있다.

4. 자율규제 규약의 제정·시행 지원

개인정보처리자는 자신의 개인정보 처리에 대해서 가장 잘 알고 있다. 해당 업무처리를 위해서 어느 정도의 개인정보 수집·이용이 가장 적절한지, 이에 따른 위험은 무엇인지, 보다 안전한 처리를 위해서는 어떤 조치가 필요한지 등에 대해서 잘 알고 있기 때문에 개인정보처리자가 스스로 규약이나 행동강령을 정해 지키도록 한 것이다.

자율규제 규약은 개인정보처리자가 혼자 또는 협회 차원에서 마련할 수도 있고, 개인정보 보호단체 또는 소관 정부부처와 공동으로 제정할 수도 있다. 일본의 경우 「개인정보 보호법」 제47조에 근거하여 인정개인정보 보호단체(認定個人情報保護團體)를 지정하고, 지정된 단체에서 개인정보 보호지침을 제정하도록 지도하여 자율규제를 활성화하고 있다. 유럽연합은 「일반 개인정보 보호법」(GDPR) 제40조, 제41조를 통해 사업 분야를 대표할 수 있는 협·단체에 자율규약의 입안을 장려하고 이에 대한 공인 절차 및 모니터링 사항 등을 규정하여 자율규제의 기반을 마련하였다.

5. 그 밖의 자율규제 활동 지원

보호위원회는 앞에서 열거한 사항 이외에 개인정보 침해정보공유, 개인정보 유출 점검시스템 개발·보급, 개인정보 보호 솔루션 개발 보급 지원 등 개인정보처리자의 자율적인 개인정보 보호활동을 지원하기 위하여 필요한 시책을 마련하여야 한다. 이와 관련하여 투자여력이 부족한 중소기업자를 위해 ‘개인정보 보호 기술지원센터’를 설치하여 운영하고 있다.

6. 유사 입법례

「가맹사업거래의 공정화에 관한 법률」 등 다수의 법에서 자율규제를 강조하는 규정을 두는 유사 입법례가 있다.

< 현행법상 자율규제 관련 규정 >

법 명	조문 내용
가맹사업거래의 공정화에 관한 법률	<p>제15조(자율규약) ① 가맹본부 또는 가맹본부를 구성원으로 하는 사업 자단체는 가맹사업의 공정한 거래질서를 유지하기 위하여 자율적으로 규약을 정할 수 있다.</p> <p>② 가맹본부 또는 가맹본부를 구성원으로 하는 사업자단체는 제1항의 규정에 의하여 자율규약을 정하고자 하는 경우 그 규약이 제12조제1항의 규정에 위반하는 지에 대한 심사를 공정거래위원회에 요청할 수 있다.</p>

법 명	조문 내용
표시·광고의 공정화에 관한 법률	<p>제14조(표시·광고의 자율규약) ① 사업자등은 제3조제1항을 위반하는 행위를 방지하기 위하여 자율적으로 표시·광고에 관한 규약이나 기준 등(이하 “자율규약”이라 한다)을 정할 수 있다.</p> <p>② 자율규약은 제3조제1항을 위반하는 행위를 방지하기에 적합하여야 하며, 정당한 사유 없이 사업자등의 표시·광고 또는 소비자에 대한 정보 제공을 제한하여서는 아니 된다.</p> <p>제14조의2(표시·광고의 자율심의기구등) ① 사업자등의 표시·광고가 제3조제1항 또는 자율규약에 위반되는지 등을 심의(그 명칭에 관계없이 표시·광고가 법령 또는 자율규약에 위반되는지를 판단하는 행위를 말한다. 이하 같다)하는 등 부당한 표시·광고를 방지하기 위한 조직(이하 “자율심의기구등”이라 한다)을 운영하는 자는 대통령령으로 정하는 바에 따라 공정거래위원회에 신고할 수 있다. 사업자 등이 자율심의기구등이 심의하여 처리한 결과에 따라 시정된 경우라도 이 법을 위반하는 행위를 반복하는 등 자율심의기구등의 시정만으로는 소비자나 경쟁사업자의 피해를 방지하기 곤란하다고 판단하는 경우에는 그러하지 아니하다.</p>
청소년보호법	<p>제11조(청소년유해매체물의 자율 규제) ① 매체물의 제작자·발행자, 유통행위자 또는 매체물과 관련된 단체는 자율적으로 청소년 유해 여부를 결정하고 결정한 내용의 확인을 청소년보호위원회나 각 심의기관에 요청할 수 있다.</p>
자율관리어업법	<p>제9조(공동체의 구성 등) ① 다음 각 호의 어느 하나에 해당하는 자격을 가진 어업인은 자율적으로 공동체를 구성할 수 있다.</p> <p>제10조(공동체 자체규약) ① 공동체는 다음 각 호의 사항을 고려하여 공동체 자체규약(이하 “자체규약”이라 한다)을 제정하여야 한다.</p> <ol style="list-style-type: none"> 1. 해중림(海中林)의 조성, 어장환경 개선, 어장면적 조정, 어장휴식 등 어장관리에 관한 사항 2. 어구사용량의 축소, 그물코 크기의 확대, 휴어제(休漁制)의 운영 등 수산자원관리에 관한 사항 3. 공동 생산·판매, 체험어장의 운영 등을 통한 어업 외의 소득증대 등 경영개선에 관한 사항 4. 불법어업 근절대책, 수산 관계 법령의 준수, 공동체 간 분쟁 해결 등 질서유지에 관한 사항 <p>② 자체규약의 세부기준 및 변경 등에 필요한 사항은 해양수산부령으로 정한다.</p>
상호저축은행법	<p>제18조의6 (광고의 자율심의) ① 상호저축은행이 예금등, 대출, 후순위채권 등 자신이 취급하는 상품에 관하여 광고를 하려는 경우에는 광고계획신고서와 광고안을 제25조에 따른 상호저축은행중앙회(이하 이 조에서 “중앙회”라 한다)에 제출하여 심의를 받아야 한다.</p> <p>② 중앙회는 제1항에 따른 심의 결과 광고의 내용이 사실과 다르거나 「금융소비자 보호에 관한 법률」 제22조를 위반하여 광고하려는 경우에는 해당 상호저축은행에 대하여 광고의 시정이나 사용중단을 요구할 수 있다. 이 경우 해당 상호저축은행은 정당한 사유가 없으면 중앙회의 요구에 성실히 응하여야 한다.</p>

제14조 | 국제협력

법률

- 제14조(국제협력)** ① 정부는 국제적 환경에서의 개인정보 보호 수준을 향상시키기 위하여 필요한 시책을 마련하여야 한다.
- ② 정부는 개인정보 국외 이전으로 인하여 정보주체의 권리가 침해되지 아니하도록 관련 시책을 마련하여야 한다.

이 조는 국가 간 무역 확대 및 인적자원의 교류 증가로 개인정보의 국제적 이전이 다반사로 발생하는 현실에서 우리나라의 개인정보 보호 수준을 국제적 흐름에 맞추어 선진국 수준으로 향상시키고 국제적인 협력관계를 증진시킴으로써 해외에서 처리되고 있거나 해외로 이전된 내국인의 개인정보를 보호하기 위한 정부의 노력 의무를 규정한 것이다.

이를 위해 정부는 ① 국제기구, 외국정부, 외국기관 등과의 협력관계 증진 ② 개인정보 보호 국제규범의 제·개정 추진 ③ 신규이슈의 발굴 및 공동 조사·연구 수행 ④ 개인정보 보호를 위한 국제표준화의 추진지원 ⑤ 국제적인 개인정보 보호 문제에 대응하기 위한 정보공유 ⑥ 국제적인 개인정보 보호를 위한 협력창구 또는 협의체의 구성·운영 등의 사업을 적극적으로 추진할 필요가 있다.

< 개인정보 보호 관련 국제 기구 및 단체 >

기구·단체명	성격
국제 개인정보보호 감독기구 협의체(GPA, Global Privacy Assembly*) (기존 International Conference of Data Protection and Privacy Commission에서 명칭 변경)	국제협의회
국제 정보통신 개인정보보호 작업반(IWGDP, International Working Group on Data Protection in Telecommunication)	국제협의회
유럽의회 개인정보보호 조약(CoE 108, Council of Europe 108)	국제협의회
경제협력 개발기구(OECD) 데이터 거버넌스·프라이버시 작업반 (WPDGP, Working Party on Data Governance and Privacy)	국제기구
국제프라이버시 네트워크(GPEN, Global Privacy Enforcement Network)	국제기구
아시아태평양 경제협력체(APEC) 전자상거래운영그룹(DESIG-DPS, Digital Economy Steering Group-Data Privacy Subgroup)	국제기구
EU 정보보호 감독기구(EDPS, European Data Protection Supervisor)	국제기구
EU 개인정보보호 이사회(EDPB, European Data Protection Board)	지역협의회(EU)
아시아·태평양 프라이버시 감독기관 포럼(APPA, Asia Pacific Privacy Authorities)	지역협의회(아·태)
전자개인정보센터(EPIC, Electronic Privacy Information Center)	민간단체
국제 프라이버시 전문가 협회 (IAPP, International Association of Privacy Professionals)	민간단체

제3장 개인정보의 처리

제1절 개인정보의 수집, 이용, 제공 등

- 제15조 개인정보의 수집·이용
- 제16조 개인정보의 수집 제한
- 제17조 개인정보의 제공
- 제18조 개인정보의 목적 외 이용·제공 제한
- 제19조 개인정보를 제공받은 자의 이용·제공 제한
- 제20조 정보주체 이외로부터 수집한 개인정보의 수집 출처 등 고지
- 제21조 개인정보의 파기
- 제22조 동의를 받는 방법

제2절 개인정보의 처리 제한

- 제23조 민감정보의 처리 제한
- 제24조 고유식별정보의 처리 제한
- 제24조의2 주민등록번호 처리의 제한
- 제25조 영상정보처리기기의 설치·운영 제한
- 제26조 업무위탁에 따른 개인정보의 처리 제한
- 제27조 영업양도 등에 따른 개인정보의 이전 제한
- 제28조 개인정보취급자에 대한 감독

제3절 가명정보 처리에 관한 특례

- 제28조의2 가명정보의 처리 등
- 제28조의3 가명정보의 결합 제한
- 제28조의4 가명정보에 대한 안전조치의무 등
- 제28조의5 가명정보 처리 시 금지의무 등
- 제28조의6 가명정보 처리에 대한 과징금 부과 등
- 제28조의7 적용범위



제1절 개인정보의 수집, 이용, 제공 등

제15조 | 개인정보의 수집·이용

법률

제15조(개인정보의 수집·이용) ① 개인정보처리자는 다음 각 호의 어느 하나에 해당하는 경우에는 개인정보를 수집할 수 있으며 그 수집 목적의 범위에서 이용할 수 있다.

1. 정보주체의 동의를 받은 경우
2. 법률에 특별한 규정이 있거나 법령상 의무를 준수하기 위하여 불가피한 경우
3. 공공기관이 법령 등에서 정하는 소관 업무의 수행을 위하여 불가피한 경우
4. 정보주체와의 계약의 체결 및 이행을 위하여 불가피하게 필요한 경우
5. 정보주체 또는 그 법정대리인이 의사표시를 할 수 없는 상태에 있거나 주소 불명 등으로 사전 동의를 받을 수 없는 경우로서 명백히 정보주체 또는 제3자의 급박한 생명, 신체, 재산의 이익을 위하여 필요하다고 인정되는 경우
6. 개인정보처리자의 정당한 이익을 달성하기 위하여 필요한 경우로서 명백하게 정보주체의 권리보다 우선하는 경우. 이 경우 개인정보처리자의 정당한 이익과 상당한 관련이 있고 합리적인 범위를 초과하지 아니하는 경우에 한한다.

② 개인정보처리자는 제1항제1호에 따른 동의를 받을 때에는 다음 각 호의 사항을 정보주체에게 알려야 한다. 다음 각 호의 어느 하나의 사항을 변경하는 경우에도 이를 알리고 동의를 받아야 한다.

1. 개인정보의 수집·이용 목적
2. 수집하려는 개인정보의 항목
3. 개인정보의 보유 및 이용 기간
4. 동의를 거부할 권리가 있다는 사실 및 동의 거부에 따른 불이익이 있는 경우에는 그 불이익의 내용

③ 개인정보처리자는 당초 수집 목적과 합리적으로 관련된 범위에서 정보주체에게 불이익이 발생하는지 여부, 암호화 등 안전성 확보에 필요한 조치를 하였는지 여부 등을 고려하여 대통령령으로 정하는 바에 따라 정보주체의 동의 없이 개인정보를 이용할 수 있다.

시행령

제14조의2(개인정보의 추가적인 이용·제공의 기준 등) ① 개인정보처리자는 법 제15조제3항 또는 17조제4항에 따라 정보주체의 동의 없이 개인정보를 이용 또는 제공(이하 “개인정보의 추가적인 이용 또는 제공”이라 한다)하려는 경우에는 다음 각 호의 사항을 고려해야 한다.

	<ol style="list-style-type: none"> 1. 당초 수집 목적과 관련성이 있는지 여부 2. 개인정보를 수집한 정황 또는 처리 관행에 비추어 볼 때 개인정보의 추가적인 이용 또는 제공에 대한 예측 가능성이 있는지 여부 3. 정보주체의 이익을 부당하게 침해하는지 여부 4. 가명처리 또는 암호화 등 안전성 확보에 필요한 조치를 하였는지 여부 <p>② 개인정보처리자는 제1항 각 호의 고려사항에 대한 판단 기준을 법 제30조 제1항에 따른 개인정보 처리방침에 미리 공개하고, 법 제31조제1항에 따른 개인정보 보호책임자가 해당 기준에 따라 개인정보의 추가적인 이용 또는 제공을 하고 있는지 여부를 점검해야 한다.</p>
표준지침	<p>제6조(개인정보의 수집·이용) ① 개인정보의 “수집”이란 정보주체로부터 직접 이름, 주소, 전화번호 등의 개인정보를 제공받는 것뿐만 아니라 정보주체에 관한 모든 형태의 개인정보를 취득하는 것을 말한다.</p> <p>② 개인정보처리자는 다음 각 호의 경우에 개인정보를 수집할 수 있으며, 그 수집 목적의 범위에서 이용할 수 있다.</p> <ol style="list-style-type: none"> 1. 정보주체로부터 사전에 동의를 받은 경우 2. 법률에서 개인정보를 수집·이용할 수 있음을 구체적으로 명시하거나 허용하고 있는 경우 3. 법령에서 개인정보처리자에게 구체적인 의무를 부과하고 있고, 개인정보처리자가 개인정보를 수집·이용하지 않고는 그 의무를 이행하는 것이 불가능하거나 현저히 곤란한 경우 4. 공공기관이 개인정보를 수집·이용하지 않고는 법령 등에서 정한 소관 업무를 수행하는 것이 불가능하거나 현저히 곤란한 경우 5. 개인정보를 수집·이용하지 않고는 정보주체와 계약을 체결하고, 체결된 계약의 내용에 따른 의무를 이행하는 것이 불가능하거나 현저히 곤란한 경우 6. 정보주체 또는 그 법정대리인이 의사표시를 할 수 없는 상태에 있거나 주소 불명 등으로 사전 동의를 받을 수 없는 경우로서 명백히 정보주체 또는 제3자(정보주체를 제외한 그 밖의 모든 자를 말한다)의 급박한 생명, 신체, 재산의 이익을 위하여 필요하다고 인정되는 경우 7. 개인정보처리자가 법령 또는 정보주체와의 계약 등에 따른 정당한 이익을 달성하기 위하여 필요한 경우로서 명백하게 정보주체의 권리보다 우선하는 경우. 다만, 이 경우 개인정보의 수집·이용은 개인정보처리자의 정당한 이익과 상당한 관련이 있고 합리적인 범위를 초과하지 아니한 경우에 한한다. <p>③ 개인정보처리자는 정보주체로부터 직접 명함 또는 그와 유사한 매체(이하 “명함등”이라 함)를 제공받음으로써 개인정보를 수집하는 경우 명함등을 제공하는 정황 등에 비추어 사회통념상 동의 의사가 있었다고 인정되는 범</p>

위 내에서만 이용할 수 있다.

④ 개인정보처리자는 인터넷 홈페이지 등 공개된 매체 또는 장소(이하 “인터넷 홈페이지등”이라 함)에서 개인정보를 수집하는 경우 정보주체의 동의 의사가 명확히 표시되거나 인터넷 홈페이지등의 표시 내용에 비추어 사회통념상 동의 의사가 있었다고 인정되는 범위 내에서만 이용할 수 있다.

⑤ 개인정보처리자는 계약 등의 상대방인 정보주체가 대리인을 통하여 법률 행위 또는 의사표시를 하는 경우 대리인의 대리권 확인을 위한 목적으로만 대리인의 개인정보를 수집·이용할 수 있다.

⑥ 근로자와 사용자가 근로계약을 체결하는 경우 「근로기준법」에 따른 임금지급, 교육, 증명서 발급, 근로자 복지제공을 위하여 근로자의 동의 없이 개인정보를 수집·이용할 수 있다.

제14조(정보주체의 사전 동의를 받을 수 없는 경우) 개인정보처리자가 법 제15조제1항제5호 및 법 제18조제2항제3호에 따라 정보주체의 사전 동의 없이 개인정보를 수집·이용 또는 제공한 경우 당해 사유가 해소된 때에는 개인정보의 처리를 즉시 중단하여야 하며, 정보주체에게 사전 동의 없이 개인정보를 수집·이용 또는 제공한 사실과 그 사유 및 이용내역을 알려야 한다.

개인정보 ‘수집’이란 정보주체로부터 직접 이름, 주소, 전화번호 등의 정보를 제공받는 것뿐만 아니라 정보주체에 관한 모든 형태의 개인정보를 취득하는 것을 말한다(표준지침 제6조). 개인정보는 정보주체로부터 직접 수집하는 것이 원칙이나 필요한 경우에는 국가기관, 신용평가기관 등 제3자로부터 수집하거나 인터넷, 신문·잡지, 전화번호부, 인명록 등과 같은 공개된 자료원으로부터 수집할 수도 있다. 또한, 개인정보처리자가 직접 수집하지 않아도 업무처리 과정에서 개인정보가 생산되거나 생성된 경우도 적지 않다.

참고 개인정보 수집·이용 예시

- 명함을 받음으로써 부수적으로 개인정보를 취득하는 행위
- 본인 이외 제3자로부터 정보주체의 개인정보를 취득하는 행위
- 인터넷 검색이나 인명부, 전화번호부, 잡지, 신문기사 등 공개된 정보에서 개인정보를 취득하는 행위
- 정보주체 본인이나 제3자 또는 그 밖의 출처로부터 취득한 개인정보 이외에 개인정보처리자가 직접 정보를 생성하는 경우

개인정보의 수집·이용을 너무 어렵게 할 경우 외관상으로는 사생활 보호에 도움이 되는 것처럼 보이지만 실질적으로는 사생활 보호에 도움이 되지 않으면서 경제활동 위축과 비용 증가만 초래하고 공공서비스 제공에 지장을 가져올 수도 있다. 반면, 개인정보의 수집·이용을 지나치게 완화할 경우 개인정보 보호제도가 무의미해지게 된다. 따라서 정보주체의 사생활이 가장 잘 보호하기 위해서는 개인정보의 보호와 이용이 균형·조화를 이루어야 한다.

1. 개인정보를 수집·이용할 수 있는 경우

개인정보처리자는 다음의 어느 하나에 해당하는 경우에는 개인정보를 수집할 수 있으며, 그 수집 목적의 범위에서 이용할 수 있다(제15조제1항).

가 정보주체의 동의를 받은 경우

개인정보처리자는 정보주체의 동의를 받은 경우에 개인정보를 수집할 수 있는데, ‘동의’는 개인정보처리자가 개인정보를 수집·이용하는 것에 대한 정보주체의 자발적인 승낙의 의사표시로서(서명날인, 구두, 홈페이지 동의 등) 동의 여부를 명확하게 확인할 수 있어야 한다.

정보주체는 서비스를 제공받기 위하여 가입신청서 등의 서면에 직접 자신의 성명을 기재하고 인장을 찍는 방법 또는 자필 서명하거나, 인터넷 웹사이트 화면에서 ‘동의’ 버튼을 클릭하는 등으로 동의의 의사표시를 할 수 있다. 개인정보처리자는 전화상으로 개인정보 수집에 대한 정보주체의 동의를 받을 수 있다. 다만 향후 입증책임 문제가 발생할 수 있으므로 정보주체가 개인정보 수집·이용에 동의한다는 통화내용을 녹취할 수 있다.

정보주체에게 동의를 받을 때에는 어떤 개인정보를 왜 수집하는지를 정보주체가 쉽고 명확하게 인지할 수 있도록 알려야 하고, 제22조에서 규정한 방식에 따라 동의를 받아야 하기 때문에 이 법에서 정보주체의 동의는 명시적 동의를 의미한다.

※ 동의의 사례

- 영화관 멤버십카드 발급 시 「개인정보 활용동의서」에 기명날인하는 경우
- 공공기관의 인터넷홈페이지 회원가입시 개인정보 수집·이용 동의에 체크하는 경우

개인정보처리자가 정보주체의 동의를 받을 때에는 정보주체가 동의의 내용과 의미를 명확히 알 수 있도록 미리 ① 개인정보의 수집·이용목적 ② 수집하고자 하는 개인정보의 항목 ③ 개인정보의 보유 및 이용기간 ④ 동의를 거부할 권리가 있다는 사실 및 동의 거부에 따른 불이익이 있는 경우 그 불이익의 내용을 알려야 한다(제2항). 보유 및 이용 기간은 구체적으로 기간을 정해서 알려야 하나, 보유 및 이용 기간을 특정할 수 없는 경우에는 보유 및 이용 기간을 결정하는데 사용되는 기준을 알려도 된다. 이 경우 보유 및 이용 기간을 알릴 수 없는 사유는 개인정보처리자가 입증하여야 한다. 이는 정보주체가 자유의지에 따라 동의 여부를 판단·결정할 수 있도록 보장하기 위한 것이다.

한편, 명함을 주고받는 행위와 관련하여 정보주체로부터 직접 명함 또는 그와 유사한 매체(이하 “명함등”이라 함)를 제공받음으로써 개인정보를 수집하는 경우 명함 등을 제공하는 정황 등에 비추어 사회통념상 동의 의사가 있었다고 인정되는 범위 내에서만 이용할

수 있다(표준지침 제6조제3항). 예를 들어 정보주체가 자동차 구매를 위해 자동차판매점을 방문하고 담당직원에게 명함을 준 경우, 그 직원은 정보주체의 동의가 없었지만 자동차 구매와 관련한 정보의 제공 등을 위해 명함에 기재된 연락처를 이용할 수 있다.

다만, 이 경우에도 정보주체의 개인정보를 제3자에게 제공하거나 다른 목적을 위해 이용하기 위해서는 정보주체의 동의를 받아야 한다. 즉 위의 예시에서 자동차판매점의 직원은 자동차 판매와 관련하지 않은 목적으로 고객의 정보를 이용하기 위해서는 고객의 동의를 받아야 한다.

인터넷 홈페이지 등 공개된 매체, 장소 등에 정보주체가 자신의 개인정보를 수집·이용해도 된다는 명시적인 동의의사를 표시하거나, 홈페이지의 성격, 게시물 내용 등에 비추어 사회통념상 동의의사가 있었다고 인정되면, 해당 정보주체의 개인정보는 동의 없이 수집·이용할 수 있다(표준지침 제6조제4항). 대법원 또한 이미 공개된 개인정보를 수집·이용·제공 등 처리를 할 때는 정보주체의 동의가 있었다고 객관적으로 인정되는 범위 내에서 정보주체의 별도의 동의는 불필요하다고 보아야 한다고 판시하였다(대법원 2016. 8. 17. 선고 2014다235080 판결 참고).

판례 공개된 개인정보를 정보주체의 동의 없이 수집·제공 등 처리할 수 있는지 여부

이와 같이 이미 공개된 개인정보를 객관적으로 보아 정보주체가 동의한 범위 내에서 처리하는 것으로 평가할 수 있는 경우에도 그 동의의 범위가 외부에 표시되지 아니하였다는 이유만으로 또다시 정보주체의 별도 동의를 받을 것을 요구한다면 이는 정보주체의 공개의사에도 부합하지 아니하거나 정보주체나 개인정보처리자에게 무의미한 동의절차를 밟기 위한 비용만을 부담시키는 결과가 된다. (중략) 이미 공개된 개인정보를 정보주체의 동의가 있었다고 객관적으로 인정되는 범위 내에서 수집·이용·제공 등 처리를 할 때는 정보주체의 별도의 동의는 불필요하다고 보아야 하고, 별도의 동의를 받지 아니하였다고 하여 「개인정보 보호법」 제15조나 제17조를 위반한 것으로 볼 수 없다. 그리고 정보주체의 동의가 있었다고 인정되는 범위 내인지는 공개된 개인정보의 성격, 공개의 형태와 대상 범위, 그로부터 추단되는 정보주체의 공개 의도 내지 목적 뿐 만 아니라, 정보처리자의 정보제공 등 처리의 형태와 정보 제공으로 공개의 대상 범위가 원래의 것과 달라졌는지, 정보 제공이 정보주체의 원래의 공개 목적과 상당한 관련성이 있는지 등을 검토하여 객관적으로 판단하여야 한다. (대법원 2016. 8. 17. 선고 2014다235080 판결)

예컨대, 인터넷 중고거래사이트에서 상품을 팔기 위해서 정보주체가 판매물품에 대한 설명과 자신의 전화번호를 기재한 경우, 이는 해당 상품의 거래목적으로 전화번호를 이용해도 된다는 동의의 의사표시를 한 것으로 볼 수 있다.

또한 공공기관의 홈페이지에서 담당직원의 회사전화번호나 이메일이 기재된 경우, 이는 담당직원이 담당하고 있는 업무와 관련한 목적을 위해서는 직원의 전화번호와 이메일을 수집·이용할 수 있다.

그러나 홈페이지에 게시된 전화번호 또는 이메일을 통해 직원들에게 직장인 우대대출, 홍보성 이벤트 안내 등을 해서는 안되며, 이를 위해서는 정보주체의 동의를 받아야 한다.

<공개된 개인정보의 처리 관련 사례>

결정예1 서울특별시 민생사법경찰단의 온라인에 공개된 개인정보 수집·분석 행위

서울특별시 민생사법경찰단이 범죄 수사 및 내사의 전단계에서 이루어지는 조사활동을 목적으로 인공지능 기반 시스템을 개발하여 인터넷·SNS 등 온라인에 공개된 게시물을 광범위하게 수집하고, 범죄 관련성이 높다고 판단되는 게시물을 분석하여 해당 게시물에 포함된 성명, 아이디, (휴대)전화번호, 주소, 업체명 등을 이용하는 것은 「개인정보 보호법」 제15조 제1항 제1호, 제2호 및 제3호에 위반된다(보호위원회 결정 제2019-09-130호).

결정예2 차량 외부에 부착된 자동차등록번호판에 기재된 자동차등록번호 수집·제공 행위

신청인 회사의 본건 서비스의 경우 정보주체가 자동차를 운전하는 모든 국민이므로 공적인 존재라고 할 수 없고, 자동차등록번호판을 차량 외부에 부착하는 것은 정보주체의 의사가 아닌 「자동차관리법」 제10조에 따른 의무사항으로 도로교통 질서의 확보, 차량방법 등 공익적 목적을 위해 필요한 경우 자동차를 효율적으로 식별하기 위한 것임을 고려할 때, 자동차등록번호가 자동차 외부에 기재되어 누구나 알 수 있다는 이유만으로 정보주체인 차량소유자가 자신의 자동차등록번호를 신청인 회사의 본 건 서비스를 목적으로 수집·제공하는 것에 대하여 암묵적으로 동의한 것으로 보기는 어려운 것으로 판단된다(보호위원회 결정 제2019-16-260호).

나 법률에 특별한 규정이 있거나 법령상 의무를 준수하기 위해 불가피한 경우 —

1) 법률에 특별한 규정이 있는 경우

법률에서 개인정보의 수집·이용을 구체적으로 요구하거나 허용하고 있어야 한다. 수집·이용할 수 있는 개인정보의 대상·범위가 막연한 경우는 특별한 규정이라고 할 수 없다. 법률에 특별한 규정이 있어야 하므로 법률에 위임근거가 없는 한 시행령이나 시행규칙에 규정하는 것은 안 된다.

일반적으로 법률의 규정에 의한 수집·이용은 정보주체로부터 보다는 제3자로부터의 수집·이용을 의미하는 경우가 많다. 이 경우 법률에서 수집·이용을 요구하거나 허용하기만 하고 상대방(제3자)에게 제공 의무를 규정하고 있지 않아도 제3자는 정보주체의 동의 없이 개인정보를 제공할 수 있다(대법원 2012다105482 판결, 2016.3.10. 선고). 그러나 이러한 경우 개인정보를 제공하는 제3자는 다른 법률에 특별한 규정이 있어 정보주체의 개인정보를 제공하더라도 정보주체 또는 제3자의 이익을 부당하게 침해할 우려가 있을 때에는 제공 요청을 거부할 수 있다(제18조제2항 참고).

구 「전기통신사업법」 제54조(현행 제83조) 제3항, 제4항은 이용자의 인적사항에 관한 정보에 해당하는 통신자료에 대하여는 수사기관의 서면요청만으로도 전기통신사업자가 이를 제공할 수 있도록 하고 있는데, 이는 수사상 신속과 다른 범죄의 예방 등을 위하여 해당 개인정보의 내용과 성격 등에 따라 통신자료에 대해서는 법원의 허가나 법관의 영장 없이도 일정한 사항을 기재한 수사기관의 자료제공요청서라는 서면요청에 의해 통신자료를 제공하여 수사에 협조할 수 있도록 한 것으로 보아야 한다. (대법원 2016.3.10. 선고 2012다105482 판결)

<‘법률의 특별한 규정이 있는 경우’의 예시>

법률명	조문 내용
신용정보법	<p>제40조(신용정보회사등의 금지사항) 신용정보회사등은 다음 각 호의 행위를 하여서는 아니 되며, 신용정보회사등이 아니면 제4호 본문의 행위를 업으로 하거나 제5호의 행위를 하여서는 아니 된다.</p> <p>4. 특정인의 소재 및 연락처(이하 “소재등” 이라 한다)를 알아내거나 금융거래 등 상거래관계 외의 사생활 등을 조사하는 일. 다만, 채권추심업을 허가받은 신용정보회사가 그 업무를 하기 위하여 특정인의 소재등을 알아내는 경우 또는 다른 법령에 따라 특정인의 소재등을 알아내는 것이 허용되는 경우에는 그러하지 아니하다.</p>
보험업법	<p>제176조(보험요율산출기관) ⑩ 보험요율 산출기관은 순보험요율을 산출하기 위하여 필요한 경우 또는 보험회사의 보험금 지급업무에 필요한 경우에는 음주운전 등 교통법규 위반 또는 운전면허(「건설기계관리법」 제26조제1항 본문에 따른 건설기계조종사면허를 포함한다. 이하 제177조에서 같다)의 효력에 관한 개인정보를 보유하고 있는 기관의 장으로부터 그 정보를 제공받아 보험회사가 보험계약자에게 적용할 순보험료의 산출 또는 보험금 지급업무에 이용하게 할 수 있다.</p>
자동차손해배상보장법	<p>제14조(진료기록의 열람 등) ① 보험회사등은 의료기관으로부터 제12조제2항에 따라 자동차보험진료수가를 청구받으면 그 의료기관에 대하여 관계 진료기록의 열람을 청구할 수 있다.</p> <p>② 제12조의2에 따라 심사 등을 위탁받은 전문심사기관은 심사 등에 필요한 자료를 의료기관에 요청할 수 있다.</p> <p>③ 제1항 또는 제2항의 경우 의료기관은 정당한 사유가 없는 한 이에 응하여야 한다.</p> <p>④ 보험회사등은 보험금 지급 청구를 받은 경우 대통령령으로 정하는 바에 따라 경찰청 등 교통사고 조사기관에 대하여 교통사고 관련 조사기록의 열람을 청구할 수 있다. 이 경우 경찰청 등 교통사고 조사기관은 특별한 사정이 없는 한 열람하게 하여야 한다.</p> <p>⑤ 보험회사등 또는 전문심사기관에 종사하거나 종사한 자는 제1항부터 제4항까지에 따른 진료기록 또는 교통사고 관련 조사기록의 열람으로 알게 된 다른 사람의 비밀을 누설하여서는 아니 된다.</p>
병역법	<p>제11조의2(자료의 제출 요구 등) ① 지방병무청장은 병역판정검사와 관련하여 병역판정검사전담의사, 병역판정검사전문지사 또는 제12조의2에 따라 신체검사를 위하여 파견된 군의관(軍醫官) 등이 질병이나 심신장애의 확인을</p>

법률명	조문 내용
	<p>위하여 필요하다고 인정하는 경우 「의료법」에 따른 의료기관의 장, 「국민건강보험법」에 따른 국민건강보험공단의 장, 「초·중등교육법」에 따른 학교의 장 등에 대하여 병역판정검사 대상자의 진료기록·치료 관련 기록 내역, 학교생활기록부 등의 제출을 요구할 수 있다. 이 경우 자료 제출을 요구받은 사람은 특별한 사유가 없으면 요구에 따라야 한다.</p> <p>② 누구든지 제1항에 따라 취득한 병역판정검사 대상자에 대한 정보·자료를 공개 또는 누설하거나 다른 사람에게 제공하는 등 병역판정검사 외의 목적으로 사용하여서는 아니 된다.</p>
의료법	<p>제21조의2(진료기록의 송부 등) ① 의료인 또는 의료기관의 장은 다른 의료인 또는 의료기관의 장으로부터 제22조 또는 제23조에 따른 진료기록의 내용 확인이나 진료기록의 사본 및 환자의 진료경과에 대한 소견 등을 송부 또는 전송할 것을 요청받은 경우 해당 환자나 환자 보호자의 동의를 받아 그 요청에 응하여야 한다. 다만, 해당 환자의 의식이 없거나 응급환자인 경우 또는 환자의 보호자가 없어 동의를 받을 수 없는 경우에는 환자나 환자 보호자의 동의 없이 송부 또는 전송할 수 있다.</p> <p>제22조(진료기록부 등) ① 의료인은 각각 진료기록부, 조산기록부, 간호기록부, 그 밖의 진료에 관한 기록(이하 “진료기록부등”이라 한다)을 갖추어 두고 환자의 주된 증상, 진단 및 치료 내용 등 보건복지부령으로 정하는 의료행위에 관한 사항과 의견을 상세히 기록하고 서명하여야 한다.</p> <p>② 의료인이나 의료기관 개설자는 진료기록부등[제23조제1항에 따른 전자 의무기록(電子醫務記錄)을 포함하며, 추가 기재·수정된 경우 추가 기재·수정된 진료기록부등 및 추가 기재·수정 전의 원본을 모두 포함한다. 이하 같다]을 보건복지부령으로 정하는 바에 따라 보존하여야 한다.</p> <p>③ 의료인은 진료기록부등을 거짓으로 작성하거나 고의로 사실과 다르게 추가 기재·수정하여서는 아니 된다.</p>

2) 법령상 의무를 준수하기 위해 불가피한 경우

법령에서 개인정보처리자에게 일정한 의무를 부과하고 있는 경우로서 해당 개인정보처리자가 그 의무 이행을 위해서는 불가피하게 개인정보를 수집·이용할 수밖에 없는 경우를 말한다. 법률에 의한 의무뿐만 아니라 시행령, 시행규칙에 따른 의무도 포함된다.

‘불가피한 경우’란 개인정보를 수집하지 않고는 법령에서 부과하는 의무를 이행하는 것이 불가능하거나 개인정보처리자가 다른 방법을 사용하여 의무를 이행하는 것이 현저히 곤란한 경우를 의미한다.

사업자들에게 부과된 결함상품 리콜의무(「소비자기본법」), 각종 법령에 따른 본인확인 또는 연령확인 의무(「정보통신망법」, 「청소년보호법」, 「공직선거법」, 「금융실명거래 및 비밀보장에 관한 법률」, 「선원법」, 「법원경비관리대의 설치·조직 및 분장사무 등에 관한 규칙」) 등을 이행하기 위한 개인정보의 수집·이용이 법령상 의무 준수의 사례에 해당한다.

이와 관련하여, 손해배상을 부당하게 수취할 목적으로 고의로 교통사고를 조작하거나 과장하여 사고를 일으킨 후 가해운전자와 직접협상을 요구하면서 가해운전자가 가입한 손해배상보험회사에 자신의 개인정보를 주지 않는 경우가 발생할 수 있다.

이때 보험회사는 제15조제1항제2호에 따라 피해자의 동의 없이 피해자의 개인정보를 수집·이용할 수 있는데, 이는 「상법」 제719조에서 책임보험계약의 보험자는 피보험자가 보험기간 중의 사고로 인하여 제삼자에 배상할 책임을 진 경우에 이를 보상할 책임이 있으므로, 이러한 법령상 의무를 준수하기 위해 불가피한 경우 보험회사는 피해자가 개인정보 수집·이용에 대한 동의를 거부하여도 피해자의 동의 없이 피해자의 개인정보를 수집·이용할 수 있도록 하고 있기 때문이다.

참고 1 법령에 따라 본인확인이 필요한 경우

- 「정보통신망법」 제44조의5 : 게시판이용자의 본인확인
- 「공직선거법」 제82조의6 : 인터넷언론사 게시판·대화방 등의 실명확인
- 「금융실명거래 및 비밀보장에 관한 법률」 제3조 : 금융실명거래를 위한 실명확인
- 「법원경비관리대의 설치, 조직 및 분장사무 등에 관한 규칙」 제5조 : 법원경비관리대원은 주민등록증 또는 그 밖의 신분을 확인할 수 있는 자료에 의하여 청사출입자의 신분을 확인하여야 함
- 「선원법」에 따른 선원조사
- 그 밖에 공공기관이 접수된 민원을 처리하기 위하여 신고자를 확인하는 경우

참고 2 법령에 따라 연령확인이 필요한 경우

- 「청소년보호법」 제16조 : 청소년유해매체물 판매·대여·배포 등을 하고자 하는 경우 그 상대방의 연령을 확인하여야 함
- 「청소년보호법」 제26조 : 인터넷게임(정보통신망을 통하여 실시간으로 제공되는 게임물)의 제공자는 16세 미만 청소년에게 오전0시~오전6시까지 인터넷게임을 제공해서는 안 됨
- 「청소년보호법」 제29조 : 청소년유해업소 업주는 종업원을 고용하고자 하는 때 그 연령을 확인해야 하며, 출입자의 연령을 확인하여 청소년이 당해 업소에 출입·이용하지 못하게 해야 함
- 「민법」상 미성년자 보호제도 : 우리나라 법원은 미성년자의 적극적인 기망행위만을 「사술」로 인정하고 사술의 존재에 대하여 이를 주장하는 상대방이 입증하여야 한다고 판시하고 있음, 따라서 미성년자와 거래를 하는 사업자는 미성년자인지 여부를 신분증 확인과 같은 보다 적극적인 수단에 따라 확인하여야 할 필요가 있음

다 공공기관이 법령 등에서 정하는 소관업무 수행을 위해 불가피한 경우 ——

공공기관의 경우에는 개인정보를 수집할 수 있도록 명시적으로 허용하는 법률 규정이 없더라도 법령 등에서 소관 업무를 정하고 있고 그 소관 업무의 수행을 위하여 불가피하게 개인정보를 수집할 수밖에 없는 경우에는 정보주체의 동의 없이 개인정보 수집이 허용된다.

사실 ‘법령 등에서 정하는 소관업무 수행’은 제2호에서 규정하고 있는 ‘법령상 의무

준수'에 포함된다고 볼 수도 있으나, 법령상 의무준수와 소관업무 수행의 차이를 좀 더 명확하게 하기 위하여 별도로 규정한 것이다.

‘법령 등에서 정하는 소관업무’란 「정부조직법」 및 각 기관별 직제령·직제규칙, 개별 조직법 등에서 정하고 있는 소관 사무 이외에, 「주민등록법」, 「국세기본법」, 「의료법」, 「국민건강보험법」 등 법령에 의해서 부여된 권한과 의무, 지방자치단체의 경우 조례에서 정하고 있는 업무 등을 의미한다.

‘불가피한 경우’란 개인정보를 수집하지 아니하고는 법령 등에서 해당 공공기관에 부여하고 있는 권한의 행사나 의무의 이행이 불가능하거나 다른 방법을 사용하여 소관 업무를 수행하는 것이 현저히 곤란한 경우를 의미한다.

판례 법률의 위임 없이 주민의 의무부과에 관한 사항을 정한 조례의 ‘법령 등’ 해당 여부

「개인정보 보호법」 제15조제1항제3호는 공공기관이 법령 등에서 정하는 소관 업무의 수행을 위하여 불가피한 경우 개인정보처리자는 개인정보를 수집할 수 있도록 규정하고 있는데, 위 ‘법령 등’은 적법한 법령 등이어야 함은 당연하다.

그런데 앞서 본 바와 같이, 이 사건 조례안 제8조제1항, 제3항이 법률의 위임 없이 주민의 의무부과에 관한 사항을 규정한 것이어서 허용될 수 없는 이상, 이러한 규정에 근거하여 인사검증 대상자의 형사처벌, 행정제재 및 도덕성 등에 관한 개인정보자료를 제출하게 하는 이 사건 조례안 제9조제3호, 제4호(이하 ‘이 사건 개인정보제출 조례규정’이라 한다)는 「개인정보 보호법」 제15조제1항제3호에 위반된다(대법원 2017. 12. 13. 선고 2014추664 판결).

참고 공공기관의 소관업무 인용 예시

- 인사혁신처가 「정부조직법」 제22조의3, 「인사혁신처와 그 소속기관 직제」 및 「인사혁신처와 그 소속기관 직제 시행규칙」에 따라 공무원의 인사·윤리·복무·연금 등 관리를 위해 공무원인사 관련 파일을 수집·이용하거나 국가인재데이터베이스 시스템을 구축·운영하는 경우
- 국민건강보험공단이 「국민건강보험법」 제14조에 따라 보험급여관리 등을 위하여 진료내역 등을 수집·이용하는 경우
- 대학교 행정실이 「고등교육법」 제15조제3항에 따른 학교의 행정사무(학교 시설 유지·관리 업무) 수행을 위하여 잘못된 주차 행위를 한 차주의 휴대전화번호를 교내 재학정보시스템에서 조회하여 교내 주차민원 해결에 이용하는 경우(2017년 개인정보 분쟁조정 사례 22면)

라 정보주체와의 계약 체결·이행을 위해 불가피하게 필요한 경우

정보주체와 계약 체결 및 이행을 위하여 개인정보의 수집이 불가피하게 수반되는 경우 까지 정보주체의 동의를 받도록 하면 경제활동에 막대한 지장을 초래하고 동의 획득에 소요되는 비용만 증가시키게 되므로, 계약 체결이나 이행을 위해 불가피하게 필요한 개인정보는 정보주체에 대한 고지·동의 없이도 개인정보를 수집할 수 있도록 한 것이다.

‘계약체결’에는 계약체결을 위한 준비단계도 포함된다. 예컨대 부동산거래에 있어서 계약체결 전에 해당 부동산의 소유자, 권리관계 등을 미리 조사·확인하는 경우가 이에 해당한다. 단, 계약 미체결시에는 수집한 개인정보는 즉시 파기하여야 한다.

참고 1 계약체결의 사례

- 보험회사가 계약체결을 위해 청약자의 자동차사고 이력, 다른 유사보험의 가입여부 등에 관한 정보를 수집하는 경우
- 거래 체결 전에 거래상대방의 신용도 평가를 위해 정보를 수집·이용하는 경우
- 회사가 취업지원자와 근로계약 체결 전에 지원자의 이력서, 졸업증명서, 성적증명서 등 정보를 수집·이용하는 경우

‘계약이행’은 물건의 배송·전달이나 서비스의 이행과 같은 주된 의무의 이행뿐만 아니라 부수의무 즉 경품배달, 포인트(마일리지) 관리, 애프터서비스 의무 등의 이행도 포함된다.

참고 2 계약이행 사례

- 고객이 주문한 상품을 배송하기 위하여 주소, 연락처 정보를 수집하는 경우
- 경품행사시 당첨자에게 경품을 발송하기 위해 주소와 연락처 정보를 요구하는 경우
- 쇼핑몰이 주문시 포인트를 지급하기로 약정하고 주문정보를 수집하는 경우

대리인을 통한 계약체결의 경우 정당한 대리권을 부여받았는지의 여부는 반드시 필요한 사항으로 대리권 확인을 위한 목적으로 대리인의 개인정보를 수집·이용할 수 있다(표준지침 제6조제5항). 일반적으로 위임장에는 대리인의 성함, 주소, 전화번호 등이 기재되어 있는데, 대리권 확인을 위한 대리인의 개인정보를 수집·이용하는 것은 계약체결 등 법률행위를 위해 불가피한 사항이므로 단순히 대리인 여부를 확인하기 위해서는 대리인의 개인정보를 수집·이용할 수 있다. 다만 주민등록번호 등의 고유식별번호는 「개인정보 보호법」 제24조, 제24조의2에 따라 수집이 제한된다.

근로자가 사용자에게 근로를 제공하고 사용자는 이에 대하여 임금을 지급하는 것을 목적으로 근로계약을 체결한 경우, 근로계약을 이행하기 위해서 직원의 개인정보를 수집·이용하는 것은 반드시 필요한 사항이므로 사용자는 근로자의 임금지급, 계약서에 명시된 복지 제공 등 근로계약을 이행하기 위하여 근로자의 동의 없이 개인정보를 수집·이용할 수 있다.

그러나 근로관계에서 근로자는 사용자보다 약자의 지위에 처하게 되므로 근로자의 개인정보는 더욱 중요하게 보호될 필요가 있다. 따라서 근로자의 동의를 받지 않는다고 하더라도, 법 제4조제1호에서 정보주체의 권리로서 개인정보의 처리에 관한 정보를 제공받을 권리를 명시하고 있는 점 등에 비추어 근로계약 체결 시 근로계약서, 별도의 개인정보 처리방침

등을 통해 직원의 개인정보 수집·이용에 관한 사항을 알리는 것이 바람직하다(직원 개인정보의 수집목적, 수집항목, 직원의 열람·처리정지·정정·삭제 등에 관한 사항, 보유기간, 퇴직 후 직원정보의 처리절차 등).

마 급박한 생명·신체·재산상 이익을 위하여 필요한 경우

정보주체 또는 그 법정대리인이 의사표시를 할 수 없는 상태에 있거나 주소불명 등으로 사전 동의를 받을 수 없는 경우로서 명백히 정보주체 또는 제3자의 급박한 생명·신체·재산상 이익을 위하여 필요하다고 인정되는 경우에도 정보주체의 동의 없이 개인정보를 수집할 수 있다.

1) 의사표시를 할 수 없는 상태

정신미약, 교통사고, 수술(의사표시를 하기 어려운 의료행위 포함) 등으로 정보주체가 자신의 의사표시를 할 수 없거나, 태풍·홍수·화재 등 재난상태에 고립되어 있거나 납치·감금 등 범죄자들의 수중에 구금되어 있어 정보주체의 의사를 물어볼 수 없는 경우를 말한다.

2) 사전 동의를 받을 수 없는 경우

주소불명, 전화불통, 이메일 차단 등 불가피한 사유로 사전에 동의를 받을 수 없는 경우에만 해당한다. 수차례 전화를 걸었으나 정보주체 또는 법정대리인이 전화를 받지 아니한 경우에도 전화를 기다릴 시간적 여유가 없다면 사전 동의를 받을 수 없는 경우에 해당한다. 그러나 정보주체 또는 법정대리인이 멀리 떨어져 있어 동의를 받기 어렵다거나 단순히 동의를 거부하고 있다는 사실만으로는 사전 동의를 받을 수 없는 경우에 해당하지 않는다.

개인정보처리자는 정보주체의 사전 동의 없이 개인정보를 수집 또는 이용한 경우에도 당해 사유가 해소된 때에는 개인정보의 처리를 즉시 중단하여야 하며, 정보주체에게 사전 동의 없이 개인정보를 수집 또는 이용한 사실, 그 사유와 이용내역을 알려야 한다(표준지침 제14조). 급박한 사유가 해소된 이후 계속해서 정보주체의 개인정보를 이용하려는 경우에는 정보주체의 동의를 받아야 한다.

3) 명백히 정보주체 등의 이익을 위한 경우

개인정보의 수집·이용 목적이 명백하게 정보주체 또는 제3자의 생명·신체·재산상의 이익을 위한 것이어야 한다. 이익이 되지만 동시에 손해가 될 수도 있는 경우에는 정보주체의 동의 없이 개인정보를 수집할 수 없다.

문제는 제3자에게는 명백히 이익이 되지만 정보주체에게는 손해가 되는 경우이다. 이 경우에는 제3자의 이익이 정보주체의 이익보다 월등한 경우에만 동의 없는 개인정보 수집이

가능하다고 하여야 할 것이다. 특히 제3자의 재산상 이익은 정보주체의 생명·신체상 이익을 앞설 수는 없다고 보아야 한다.

4) 급박한 생명·신체·재산상 이익

생명·신체·재산상 이익이 급박해야 한다. 정보주체 또는 법정대리인의 동의를 받을 수 있는 충분한 시간적 여유가 있거나 다른 수단에 의해서도 생명·신체·재산상의 이익을 보호할 수 있다면 급박한 상태에 있다고 할 수 없다.

참고 급박한 이익의 사례

- 조난·홍수 등으로 실종되거나 고립된 사람을 구조하기 위하여 연락처, 주소, 위치정보 등 개인정보를 수집하는 경우
- 아파트에 화재가 발생한 경우, 집안에 있는 자녀를 구하기 위해 해당 자녀 또는 부모의 이동전화번호를 수집하는 경우
- 의식불명이나 중태에 빠진 환자의 수술 등 의료조치를 위하여 개인정보를 수집하는 경우
- 고객이 전화사기(보이스피싱)에 걸린 것으로 보여 은행이 임시로 자금이체를 중단시키고 고객에게 사실 확인을 하고자 하는 경우

바 개인정보처리자의 정당한 이익 달성을 위해 필요한 경우

개인정보처리자의 정당한 이익을 달성하기 위하여 필요한 경우로서 명백하게 정보주체의 권리보다 우선하는 경우에도 정보주체의 동의 없이 개인정보를 수집할 수 있다. 이 경우 수집하고자 하는 개인정보가 개인정보처리자의 정당한 이익과 상당한 관련이 있어야 하며 합리적인 범위를 초과해서는 안 된다.

1) 개인정보처리자의 정당한 이익

요금 징수 및 정산, 채권추심, 소 제기 및 진행 등을 위하여 증빙자료를 조사·확보하는 경우, 영업비밀 유출 및 도난방지, 출입이 통제되고 있는 사업장 내 시설안전을 목적으로 한 CCTV 설치 등 법률상 개인정보처리자의 정당한 이익이 존재해야 한다.

< 개인정보처리자의 정당한 이익달성 사례 >

- 사업자가 요금정산·채권추심 등을 위하여 고객의 서비스 이용내역, 과금내역 등의 개인정보를 생성·관리하는 경우
⇒ 요금정산을 위해서는 고객의 물품 주문내역, 서비스 이용내역, 통신사실확인자료 등과 같이 요금을 산출하고 과금하기 위한 자료를 생성하게 되며, 계약이행에 따른 정당한 대가를 받기 위한 것이므로 수집이 가능하다고 보아야 함
※ 정보주체로부터 직접 제공받은 성명·주민등록번호 등의 정보가 아니더라도 사업자가 생성한 정보도 개인정보의 '수집'행위에 해당됨

- 사업자가 고객과의 소송이나 분쟁에 대비하여 요금 정산자료, 고객의 민원제기 내용 및 대응자료 등을 수집·관리하는 경우
 - ⇒ 이미 해결된 민원인데도 계속해서 민원을 제기하는 경우 기존의 민원제기 내역 및 대처기록 등의 자료를 기록·보관할 때, 요금정산 및 과금에 대한 불만 발생시 이를 증빙할 수 있는 서비스 이용내역에 대한 증빙자료를 생성·관리할 때, 사전에 동의를 받도록 한다면 사업자의 영업활동에 과도한 부담이 됨
- 도난방지, 시설안전 등을 위해서 회사 출입구(현관), 엘리베이터, 복도 등에 CCTV를 설치·운영하는 경우
 - ⇒ 근로자의 사생활침해 가능성이 낮은 반면, 도난방지, 시설안전 등의 효과가 크므로 필요성도 있고 정당성도 있다고 할 수 있음

2) 명백하게 정보주체의 권리보다 우선

개인정보처리자의 정당한 이익을 위한 것이라고 하더라도 정보주체의 사생활을 과도하게 침해하거나 다른 이익을 침해하는 경우에는 정보주체의 동의 없이 개인정보를 수집할 수 없다.

또한 정보주체의 권리와 개인정보처리자의 이익을 형량한 결과 명백하게 개인정보처리자의 이익이 월등해야 한다. EU에서는 정보주체의 이익과 개인정보처리자의 이익을 비교형량하여 ‘정보주체의 권리가 개인정보처리자 기타 제3자의 이익에 우선하지 않는 경우’에 정당한 이익에 기하여 처리를 정당화할 수 있도록 하고 있으나(EU 「일반 개인정보 보호법」 제6조제1항f호), 우리나라에서는 개인정보처리자의 이익이 명백히 우선하는 경우에만 개인정보 수집이 허용된다고 규정하고 있다.

참고 명백성 판단 (예시)

회사가 업무효율성 및 영업비밀 보호 등을 이유로 직원의 업무처리 내역 및 인터넷 접속내역 등을 모니터링하는 시스템을 설치하는 것은 정보주체 권리보다 명백히 우선한다고 보기는 어려우므로, 이 경우는 노사 협의에 따라 처리하거나 직원에 대한 고지 또는 동의절차를 거치는 것이 바람직하다.

3) 상당한 관련성과 합리적 범위 내의 수집

개인정보처리자의 정당한 이익이 존재하고, 그것이 명백하게 정보주체의 권리보다 우선한다고 하더라도 해당 개인정보가 개인정보처리자의 정당한 이익과 관련성이 낮거나 합리적인 범위를 초과해서는 안된다.

<제15조제1항제6호 관련 사례>

사례 1

철도차량 운전실에 폐쇄회로 텔레비전을 설치하여 운전제어대와 기관사의 두 손을 촬영한 경우

한국철도공사가 철도사고시 사고원인 규명을 위하여 폐쇄된 공간인 철도차량 운전실에 폐쇄회로 텔레비전을 설치하여 각종 계기판과 안전운행장치 등으로 구성된 운전제어대와 그 위에 위치한 기관사의 두 손을 촬영하고, 촬영된 영상정보를 최장 7일간 각 철도차량 운전실 저장장치에 저장하고 철도사고 시에만 사고원인 규명을 위하여 열람·이용한 사안에서 ① 철도사고 원인규명과 승객의 안전 확보가 한국철도공사의 정당한 이익에 해당하며 ② 본건 영상정보의 수집 및 이용이 그러한 목적 달성에 필요하며 ③ 목적 달성을 위하여 합리적인 범위를 초과하지 않고 ④ 본건 영상정보의 촬영 대상, 보관 기간 등을 감안하면 한국철도공사의 정당한 이익이 본건 영상정보의 위와 같은 촬영으로 인하여 제한되는 정보주체(기관사)의 개인정보자기결정권보다 명백히 우선한다는 이유로 법 제15조 제1항 제6호 사유가 있다고 판단됨(보호위원회 결정 제2015-12-22호)

사례 2

분리과금 해지를 목적으로 이동통신사를 통하여 퇴사한 직원의 휴대전화번호를 조회한 경우

회사(피신청인)가 직원 복리후생 제도의 일환으로 이동전화요금 일부를 대납하여 주는 '분리과금'을 제공하고 있었는데, 퇴사한 직원(신청인)이 '분리과금'을 해지하지 않은 채 휴대전화번호를 변경하여 회사가 이를 해지하기 위해 이동통신사를 통하여 직원의 변경된 휴대전화번호를 조회한 사안에서 ① 복리후생 제도의 일환으로 이동전화요금 일부를 대납하여 주는 '분리과금'은 재직 중인 직원에게만 제공되는 혜택으로, 신청인 또한 이를 인지하고 퇴사 이후에는 '분리과금' 혜택이 해지될 것을 충분히 예상할 수 있었으며 ② 피신청인 입장에서 퇴사한 신청인에 대한 '분리과금'을 피신청인이 해지하지 아니할 경우 신청인에게 부과되는 이동전화 요금 중 일부를 계속하여 부담하여야 하고, '분리과금'의 해지를 위해서는 해당 회선의 이동전화 번호가 확인되어야 하는 점을 고려할 때 불가피하게 변경된 신청인의 이동전화번호를 조회할 수밖에 없었다는 점이 인정되므로 제15조 제1항 제6호에 해당한다고 보임 (2016년 개인정보 분쟁조정 사례집, 55-57면)

사례 3

야간에는 경비원의 휴식공간으로도 사용되는 관리사무소 사무실 내에 CCTV를 설치하여 상시 운영한 경우

피신청인이 시설안전과 범죄예방 목적으로 주상목합건을 관리사무소 사무실에 CCTV를 설치하여 상시 운영한 사안에서 해당 공간이 주간에는 일반에게 공개되지만 야간에는 일반에게 공개되지 않고 신청인 등 경비원이 취침 등 휴식공간으로도 사용하고 있는 점 등을 고려할 때 비록 건물관리에 필요한 시설물의 안전을 위하여 CCTV를 설치하였더라도 야간 근무자의 취침공간까지 지속적으로 촬영할 필요까지는 인정하기 어렵고, 나아가 사생활 보호를 위한 최소한의 조치 없이 사무실 전체를 모두 촬영하는 데 따른 피신청인의 이익이 정보주체인 신청인의 권리보다 명백하게 우선한대거나 사생활이나 다른 이익을 과도하게 침해하는 것이 아니라고 단정하기 어렵다고 판단됨(제15조 제1항 제6호에 해당하지 않음) (2015년 개인정보 분쟁조정 사례집, 101-106면)

사 친목단체의 운영을 위한 경우

친목단체는 친목단체의 운영을 위하여 회원의 개인정보를 수집·이용하는 경우 정보주체의 동의를 받을 필요가 없다(제58조제3항). 친목단체란 온라인 및 오프라인을 막론하고, 자

원봉사, 취미, 정치, 종교 등 공통의 관심사나 목표를 전제로 단체를 이루는 구성원 상호 간 친교하면서 화합을 조성하는 것을 목적으로 하는 모임을 말한다.

친목단체는 내부구성원간의 친교를 목적으로 하는 점에서 외부적 단체의사표시 내지 외부적 영향력 행사를 전제로 하는 정당, 종교단체 및 언론 등과는 구별된다. 친목단체의 운영을 위한 사항이란 ① 친목단체의 가입을 위한 성명, 연락처 및 친목단체의 회칙으로 정한 공통의 관심사나 목표와 관련된 인적 사항 ② 친목단체의 회비 등 친목유지를 위해 필요한 비용의 납부현황에 관한 사항 ③ 친목단체의 활동에 대한 구성원의 참석 여부 및 활동내용에 관한 사항 ④ 기타 친목단체의 구성원 상호 간의 친교와 화합을 위해 구성원이 다른 구성원에게 알리기를 원하는 생일, 취향 및 가족의 애경사 등에 관한 사항을 말한다.

2. 개인정보의 추가적인 이용

「개인정보 보호법」은 개인정보 보호의 주요 원칙으로서 개인정보 처리 목적을 명확하게 하고, 그 목적에 필요한 범위 내에서 개인정보를 수집하며, 그 목적 외로 활용하지 않아야 한다는 점을 선언하고 있다. 그런데 지나치게 경직적으로 수집 목적 내에서만 이용하도록 하는 경우, 오히려 정보주체의 개인정보자기결정권 보호에는 기여하지 못하면서 사회적 비용이나 비효율만을 초래하는 결과가 발생할 수 있다.

이에 따라 제15조제3항은 개인정보처리자가 당초 수집 목적과 합리적으로 관련된 범위 내에서 대통령령으로 정하는 바에 따라 정보주체의 동의 없이 개인정보를 이용할 수 있도록 하였다. 합리적 관련성의 기준이 되는 ‘당초 개인정보가 수집된 목적’은 개인정보를 적법하게 수집한 경우 해당 수집 목적을 의미하는 바, 제15조제1항에 따라 적법하게 개인정보를 수집한 경우에는 같은 조 제3항에 따라 추가적으로 이용할 수 있는 대상이 된다.

한편, 개인정보처리자는 제15조제3항에 따라 정보주체의 동의 없이 개인정보를 이용하는 경우에는 다음 사항을 종합적으로 고려하여야 한다.

가 당초 수집 목적과 관련성이 있는지 여부

개인정보처리자가 적법하게 수집하여 보관 중인 개인정보를 추가적인 목적으로 이용하려면, 당초 수집 목적과 추가적 이용·제공의 목적 사이에 관련성을 고려하여야 한다. 여기서 관련성이 있다는 것은 당초 수집 목적과 추가적 이용·제공의 목적이 서로 그 성질이나 경향 등에 있어서 연관이 있다는 것을 의미한다.

< 법률요건으로서 ‘관련성’ 관련 판례 >

판례	내용
대법원 2020. 2. 13. 선고 2019도14341, 2019전도130(병합) 판결	객관적 관련성은 압수·수색영장에 기재된 혐의사실의 내용과 수사의 대상, 수사 경위 등을 종합하여 구체적·개별적 연관관계가 있는 경우에만 인정된다고 보아야 하고, 혐의사실과 단순히 동종 또는 유사 범행이라는 사유만으로 객관적 관련성이 있다고 할 것은 아니다.
대법원 2012. 7. 26. 선고 2010두12552 판결	사업 관련성의 유무는 지출의 목적과 경위, 사업의 내용 등에 비추어 그 지출이 사업의 수행에 필요한 것이었는지를 살펴 개별적으로 판단하여야 한다.
대법원 2013. 11. 28. 선고 2011도17163 판결	위 규정들에서 “후보자로 추천하는 일과 관련하여”라 함은 정치자금의 제공이 후보자 추천의 대가 또는 사례에 해당하거나, 그렇지 아니더라도 후보자 추천에 있어서 어떠한 형태로든 영향을 미칠 수 있는 경우에 해당하여야 한다.

나 개인정보를 수집한 정황 또는 처리 관행에 비추어 볼 때 개인정보의 추가적인 이용 또는 제공에 대한 예측 가능성이 있는지 여부

개인정보의 추가적인 이용이 수집 정황이나 처리 관행에 비추어 합리적으로 예측 가능한지 고려하여야 한다. 여기서 정황은 개인정보의 수집 목적·내용, 추가적 처리를 하는 개인정보처리자와 정보주체 간의 관계, 현재의 기술 수준과 그 기술의 발전 속도 등 비교적 구체적 사정을 의미하고, 관행은 개인정보 처리가 비교적 오랜 기간 정립된 일반적 사정을 의미한다. 이와 같은 구체적 사정이나 일반적 사정을 고려할 때 개인정보를 추가적으로 이용할 수 있다고 예측 가능한지를 고려하여야 한다.

다 정보주체의 이익을 부당하게 침해하는지 여부

정보주체의 이익을 부당하게 침해하는 경우에는 추가적 이용의 정당성이 인정되기 어렵다. 정보주체의 이익을 부당하게 침해하는지 여부는 정보주체의 이익을 실질적으로 침해하는지와 해당 이익 침해가 부당한지를 고려하여야 한다. 또한, 이는 추가적인 이용의 목적이나 의도와의 관계에서 판단되어야 한다.

예를 들어, 정보주체가 구매한 재화나 용역과 관련하여, 구매 시 알려주지 못한 사항을 알릴 목적으로 연락을 한 것이 다소 정보주체가 불편함을 느낄 수 있다고 하여 언제나 부당한 침해라고 단정할 수 없다. 반면에 해당 침해 내용이 사회통념상 허용되기 어려운 정도라면 이는 당연히 부당한 침해로 보아야 한다.

한편, 침해여부가 불확실한 경우에는 개인정보의 침해 가능성을 보다 적극적으로 검토하여야 하며, 정보주체가 예측할 가능성이 높고 동시에 안전조치를 충분히 할 수 있는 경우가 아니라면 추가적인 이용이 가능하지 못한 것으로 고려되어야 할 필요성이 크다.

라 가명처리 또는 암호화 등 안전성 확보에 필요한 조치를 하였는지 여부

동의 없는 개인정보 이용에 따른 개인정보 침해 우려를 최소화하기 위하여, 가명처리 또는 암호화 등 안전성 확보에 필요한 조치를 하여야 한다. 또한, 안전조치의 내용은 가명처리나 암호화 등의 조치에 그치지 않는 바, 다양한 행위자에 의한 침해 가능성을 적극적으로 고려하여 그에 맞는 안전조치를 하여야 한다. 가명처리, 개인정보 암호화 조치와 관련한 자세한 사항은 각각 「가명처리 가이드라인」, 「개인정보의 암호화 조치 안내서」를 참고할 수 있다.

마 개인정보의 추가적인 이용 시 고려하여야 할 사항

개인정보처리자는 영 제14조의2제1항 각 호의 고려사항에 대한 구체적 기준을 스스로 정하여 개인정보 처리방침에 미리 공개하여야 한다. 이 경우 구체적 기준은 각 개인정보 처리자가 처한 상황이나 개인정보의 처리 목적 등에 따라 달라질 수 있다. 아울러, 개인정보 보호책임자는 해당 기준에 따라 개인정보의 추가적인 이용을 하고 있는지 여부를 스스로 점검하여야 한다.

참고 EU의 당초 수집 목적과 합리적으로 관련된 범위의 개인정보 이용·제공 사례

- LP음반을 판매하는 회사가 고객의 동의를 받아 정기적으로 LP음반의 카탈로그를 보내오다가, 오디오테이프, CD, DVD 형태의 음악 카탈로그도 보내는 경우
- 약국에서 다른 고객의 의약품을 잘못 가져간 경우, 약국이 고객에게 위 사실을 알리기 위하여 처방 병원으로부터 휴대전화번호를 제공받아 전화하는 경우

3. 다른 법률과의 관계

「신용정보법」상 개인신용정보 수집과 관련해서는 신용정보에 대한 수집·조사의 원칙(제15조), 공공기관에 대한 신용정보의 열람 및 제공 요청 등(제23조) 등이 적용된다. 한편, 개인신용정보의 추가적인 이용에 관해서는 제32조제6항제9호의4, 제33조제1항제4호에 따라 당초 수집한 목적과 상충되지 아니하는 목적으로 개인신용정보를 동의 없이 이용하도록 하고 있다.

제15조(수집·조사 및 처리의 원칙) ① 신용정보회사, 본인신용정보관리회사, 채권추심회사, 신용정보집중기관 및 신용정보제공·이용자(이하 “신용정보회사등”이라 한다)는 신용정보를 수집하고 처리할 수 있다. 이 경우 이 법 또는 정관으로 정한 업무 범위에서 수집·조사 및 처리의 목적을 명확히 하여야 하며, 이 법 및 「개인정보 보호법」 제3조제1항 및 제2항에 따라 그 목적 달성에 필요한 최소한의 범위에서 합리적이고 공정한 수단을 사용하여 신용정보를 수집·조사 및 처리하여야 한다.

② 신용정보회사등이 개인신용정보를 수집하는 때에는 해당 신용정보주체의 동의를 받아야 한다. 다만, 다음 각 호의 어느 하나에 해당하는 경우에는 그러하지 아니하다.

1. 「개인정보 보호법」 제15조 제1항 제2호로부터 제6호까지의 어느 하나에 해당하는 경우
2. 다음 각 목의 어느 하나에 해당하는 정보를 수집하는 경우
 - 가. 법령에 따라 공시되거나 공개된 정보
 - 나. 출판물이나 방송매체 또는 「공공기관의 정보공개에 관한 법률」 제2조 제3호에 따른 공공기관의 인터넷 홈페이지 등의 매체를 통하여 공시 또는 공개된 정보
 - 다. 신용정보주체가 스스로 사회관계망서비스 등에 직접 또는 제3자를 통하여 공개한 정보. 이 경우 대통령령으로 정하는 바에 따라 신용정보주체의 동의가 있었다고 객관적으로 인정하는 범위 내로 한정한다.
3. 제1호 및 제2호에 준하는 경우로서 대통령령으로 정하는 경우

제22조의2(신용정보 등의 보고) 개인신용평가회사, 개인사업자신용평가회사, 기업신용조회회사 및 본인신용정보관리회사는 신용정보의 이용범위, 이용기간, 제공 대상자를 대통령령으로 정하는 바에 따라 금융위원회에 보고하여야 한다.

제23조(공공기관에 대한 신용정보의 제공 요청 등) ① 삭제

② 신용정보집중기관이 국가·지방자치단체 또는 대통령령으로 정하는 공공단체(이하 “공공기관”이라 한다)의 장에게 신용정보주체의 신용도·신용거래능력 등의 판단에 필요한 신용정보로서 대통령령으로 정하는 신용정보의 제공을 요청하면 그 요청을 받은 공공기관의 장은 다음 각 호의 법률에도 불구하고 해당 신용정보집중기관에 정보를 제공할 수 있다. 이 경우 정보를 제공하는 기준과 절차 등은 대통령령으로 정한다.

1. 「공공기관의 정보공개에 관한 법률」
2. 「개인정보 보호법」
3. 「국민건강보험법」
4. 「국민연금법」
5. 「한국전력공사법」
6. 「주민등록법」

③ 신용정보집중기관은 제2항에 따라 공공기관으로부터 제공받은 신용정보를 대통령령으로 정하는 신용정보의 이용자에게 제공할 수 있다.

④ 신용정보집중기관 또는 제3항에 따른 신용정보의 이용자가 제2항 및 제3항에 따라 공공기관으로부터 제공받은 개인신용정보를 제공하는 경우에는 제32조제3항에서 정하는 바에 따라 제공받으려는 자가 해당 개인으로부터 신용정보 제공·이용에 대한 동의를 받았는지를 확인하여야 한다.

⑤ 제4항에 따라 개인신용정보를 제공받은 자는 그 정보를 타인에게 제공하여서는 아니 된다.

⑥ 제2항에 따라 신용정보의 제공을 요청하는 자는 관계 법령에 따라 열람료 또는 수수료 등을 내야 한다.

⑦ 신용정보회사등은 공공기관의 장이 관계 법령에서 정하는 공무상 목적으로 이용하기 위하여 신용정보의 제공을 문서로 요청한 경우에는 그 신용정보를 제공할 수 있다.

제24조(주민등록전산정보자료의 이용) ① 신용정보집중기관 및 대통령령으로 정하는 신용정보제공·이용자는 다음 각 호의 어느 하나에 해당하는 경우에는 행정자치부장관에게 「주민등록법」 제30조제1항에 따른 주민등록전산정보자료의 제공을 요청할 수 있다. 이 경우 요청을 받은 행정자치부장관은 특별한 사유가 없으면 그 요청에 따라야 한다.

1. 「상법」 제64조 등 다른 법률에 따라 소멸시효가 완성된 예금 및 보험금 등의 지급을 위한 경우로서 해당 예금 및 보험금 등의 원권리자에게 관련 사항을 알리기 위한 경우
2. 금융거래계약의 만기 도래, 실효(失効), 해지 등 계약의 변경사유 발생 등 거래 상대방의 권리·의무에 영향을 미치는 사항을 알리기 위한 경우

② 제1항에 따라 주민등록전산정보자료를 요청하는 경우에는 금융위원회 위원장의 심사를 받아야 한다.

③ 제2항에 따라 금융위원회위원장의 심사를 받은 경우에는 「주민등록법」 제30조제1항에 따른 관계 중앙행정기관의 장의 심사를 거친 것으로 본다. 처리절차, 사용료 또는 수수료 등에 관한 사항은 「주민등록법」에 따른다.

제32조(개인신용정보의 제공·활용에 대한 동의) ① 신용정보제공·이용자가 개인신용정보를 타인에게 제공하려는 경우에는 대통령령으로 정하는 바에 따라 해당 신용정보주체로부터 다음 각 호의 어느 하나에 해당하는 방식으로 개인신용정보를 제공할 때마다 미리 개별적으로 동의를 받아야 한다. 다만, 기존에 동의한 목적 또는 이용 범위에서 개인신용정보의 정확성·최신성을 유지하기 위한 경우에는 그러하지 아니하다.

⑥ 신용정보회사등(제9호의3을 적용하는 경우에는 데이터전문기관을 포함한다)이 개인신용정보를 제공하는 경우로서 다음 각 호의 어느 하나에 해당하는 경우에는 제1항부터 제5항까지를 적용하지 아니한다.

9의4. 다음 각 목의 요소를 고려하여 당초 수집한 목적과 상충되지 아니하는 목적으로 개인신용정보를 제공하는 경우

- 가. 양 목적 간의 관련성
- 나. 신용정보회사등이 신용정보주체로부터 개인신용정보를 수집한 경위다. 해당 개인신용정보의 제공이 신용정보주체에게 미치는 영향
- 라. 해당 개인신용정보에 대하여 가명처리를 하는 등 신용정보의 보안대책을 적절히 시행하였는지 여부

제33조(개인신용정보의 이용) ① 개인신용정보는 다음 각 호의 어느 하나에 해당하는 경우에만 이용하여야 한다.

1. ~ 3. (생략)
4. 제32조제6항 각 호의 경우
5. (생략)

4. 벌칙규정

위반행위	벌칙
수집·이용기준을 위반하여 개인정보를 수집한 자 (제15조제1항 위반)	5천만원 이하 과태료 (제75조제1항제1호)
정보주체에 대한 고지의무 위반 (제15조제2항 위반)	3천만원 이하 과태료 (제75조제2항제1호)

한편, 제15조제3항은 그 자체로 별도의 벌칙 규정이 없다. 그러나 제15조제3항의 요건에 해당하지 않는데도 개인정보를 추가적으로 이용하려는 경우에는 제18조제2항에서 정하는 바에 따라 정보주체로부터 별도의 동의를 받거나 다른 법률에 특별한 규정이 있는 경우 등에 해당하여야 한다. 따라서 이 경우는 제18조제2항 각 호의 어느 하나에 해당하는지 여부에 따라 제18조제1항 위반에 관한 벌칙조항의 적용을 받을 수 있다.

5. 질의 응답

Q | 이전에 경품 이벤트에 응모했던 고객 리스트를 활용해 신상품 출시를 안내하는 홍보 이메일을 보내도 문제가 없는지?

A | 경품 이벤트를 통해 이벤트 활용 목적으로만 동의를 받고 '상품광고'에 대해서는 동의를 받지 않았다면, 해당 개인정보는 상품출시 안내 이메일 발송 등의 광고 목적으로 이용할 수 없다. 다만 홍보 목적에 대해 별도의 동의를 받으면 가능하다.

Q | 정보주체로부터 제공받은 명함이나, 전화번호부, 공개된 인터넷 홈페이지를 통해 개인정보를 수집하는 경우에도 법 제15조제1항제1호에 따라 정보주체의 동의를 받아야 하는지?

A | 정보주체로부터 직접 명함 또는 그와 유사한 매체를 제공받음으로써 개인정보를 수집하는 경우, 정보주체가 동의의사를 명확히 표시하거나 그렇지 않은 경우 명함 등을 제공하는 정황 등에 비추어 사회통념상 동의 의사가 있었다고 인정되는 범위 내에서만 이용할 수 있다.

또한 전화번호부, 공개된 인터넷 홈페이지를 통해 개인정보를 수집하는 경우에도 본인의 개인정보를 인터넷 홈페이지 등에 게시하거나 게시하도록 허용한 정보주체의 동의 의사가 명확히 표시되거나 인터넷 홈페이지 등의 표시 내용에 비추어 사회통념상 동의 의사가 있었다고 인정되는 범위 내에서 이용하여야 한다.

Q 정보주체의 동의가 필요한 개인정보는 장래에 변경이 가능하다는 점에서 정보주체가 동의할 시점에서 확정된 동의를 받아야 할 항목을 모두 열거하고 그 외 이에 준하거나 유사한 항목을 포섭하는 의미로 '등'의 용어를 사용하는 것이 허용되는지?

A 「개인정보 보호법」은 개인정보 수집 시 필요 최소한의 개인정보만을 수집하도록 하고 있으며, '등'의 용어를 써서 추가적인 개인정보를 받을 수 있도록 한다면 무분별한 개인정보 수집으로 이어질 소지가 있으므로 정보주체 동의 시 수집할 구체적인 개인정보 항목을 나열하면서 '등'을 써서는 안 되며, 추후 업무상 새로운 개인정보가 필요한 경우 별도로 동의를 얻어야 한다.

Q 직원 채용 시 이력서 등을 통하여 얻게 되는 직원 개인정보는 “정보주체와의 계약의 체결 및 이행을 위하여 불가피하게 필요한 경우”에 해당하는 것으로 보아 그 수집·이용에 대하여 동의가 면제되는 것으로 볼 수 있는지

A 「근로기준법 시행령」 제27조에 의하면 사업자는 직원의 성명, 주민등록번호, 가족수당의 계산기초가 되는 사항과 기타 근로조건에 관한 사항을 임금 대장에 기록하여야 하는 바, 이는 법령이 정한 경우에 해당한다. 기타 정보의 경우에도 구직예정자의 개인정보 또한 그 수집, 이용과 관련하여 법 제15조제1항제4호(계약의 체결 및 이행에 필요한 경우)에 의하여 구직예정자의 동의가 면제될 수 있을 것이다.

다만 기본적으로 직원에 관한 정보는 계약체결 목적뿐만 아니라 복지, 노조관리, 위탁 등의 목적으로 활용 여지가 높고 민감정보를 수집할 여지가 있기 때문에, 채용 시에는 입사서류에 채용을 포함한 회사의 개인정보 이용목적, 기간 등을 명확히 기재하여 대상자에게 알리는 것이 바람직하다.

Q 임차인이 전세대출을 위해 은행에 전세계약서를 제출하는 경우 전세계약서에는 임차인의 정보뿐만 아니라 임대인의 개인정보도 포함하고 있는데, 이때 은행은 임대인의 개인정보 수집·이용에 대한 동의를 받아야 하는지?

A 은행이 임대인의 동의 없이 계약서에 기재된 임대인의 개인정보를 수집할 수 있는 경우는

- ① 법률의 특별한 규정 또는 법령상 의무준수를 위해 불가피한 경우
- ② 정보주체의 사전 동의가 어려운 경우로서 제3자의 급박한 생명, 신체, 재산의 이익을 위해 필요한 경우
- ③ 개인정보처리자의 정당한 이익 달성에 필요한 경우(정보주체의 권리보다 우선하는 경우)로 한정된다.

은행은 전세대출계약을 함에 있어 임대차계약이 진정하게 성립되었는지 여부를 확인할 필요가 있으며, 이를 위하여 전세계약서를 통해 임대인의 개인정보를 확인하는 것은 개인정보처리자(은행)의 정당한 이익에 해당된다. 즉 전세자금대출은 임대차계약상의 임차보증금에 담보를 설정하는 것으로, 임대차계약의 허위여부를 판단하기 위하여 임대인의 개인정보를 수집하는 것은 은행의 정당한 이익(대출금 회수 등)과 상당한 관련이 있고 합리적인 범위를 초과하였다고 볼 수 없다. 또한 은행의 전세자금대출은 임대인에게 미치는 피해가 없으며, 임대인의 개인정보 역시 단순히 임대차계약의 진위여부를 확인하기 위한 목적으로만 처리되므로 임대인의 개인정보에 관한 권리가 침해될 소지가 적다.

따라서 은행은 「개인정보 보호법」 제15조제1항제6호에 의하여 동의 없이 임대인의 개인정보를 수집 이용할 수 있으며, 다만 이 경우에도 「개인정보 보호법」 제24조의2에 따라 주민등록번호의 수집은 제한된다.

Q | 가명정보를 과학적 연구 등의 목적으로 이용하려는 경우, 영 제14조의2에 따라 당초 수집 목적과 합리적 관련성이 있어야 하는지?

A | 영 제14조의2는 법 제15조에 따라 개인정보를 추가적으로 이용할 수 있도록 하는 규정으로서 법 제28조의2에 따라 가명정보를 과학적 연구 등의 목적으로 이용하도록 하는 규정과 구별된다. 가명정보이면 당초 수집 목적과 관련성이 없더라도 과학적 연구 등의 목적으로 이용할 수 있다.

Q | 민감정보 또는 고유식별정보를 영 제14조의2에 따라 추가적으로 이용할 수 있는지?

A | 민감정보 또는 고유식별정보의 경우 다른 개인정보와 달리 법 제23조 또는 제24조에 따라 정보주체로부터 별도의 동의를 받거나 법령에 근거가 있는 경우에 한하여 처리할 수 있는 바, 법 제15조를 근거로 추가적 이용을 할 수 없다.

제16조 | 개인정보의 수집 제한

법률

제16조(개인정보의 수집 제한) ① 개인정보처리자는 제15조제1항 각 호의 어느 하나에 해당하여 개인정보를 수집하는 경우에는 그 목적에 필요한 최소한의 개인정보를 수집하여야 한다. 이 경우 최소한의 개인정보 수집이라는 입증책임은 개인정보처리자가 부담한다.

② 개인정보처리자는 정보주체의 동의를 받아 개인정보를 수집하는 경우 필요한 최소한의 정보 외의 개인정보 수집에는 동의하지 아니할 수 있다는 사실을 구체적으로 알리고 개인정보를 수집하여야 한다.

③ 개인정보처리자는 정보주체가 필요한 최소한의 정보 외의 개인정보 수집에 동의하지 아니한다는 이유로 정보주체에게 재화 또는 서비스의 제공을 거부하여서는 아니 된다.

1. 최소 수집 원칙

제15조제1항 각 호의 목적을 위해서 정보주체의 개인정보를 수집할 때에는 그 목적에 필요한 범위 내에서 최소한의 개인정보만을 수집하여야 한다. 개인정보를 필요 이상으로 수집·저장하고 있으면 해킹 등에 의하여 언제든지 개인정보가 유출될 위험이 있고 개인정보처리자에 의하여 남용될 우려가 있기 때문이다.

정보주체의 자발적인 동의를 받으면 필요 최소한의 정보 이외의 것도 수집·이용할 수 있다. 그러나 이를 위해 필요 최소한의 정보라고 하여 정보주체의 동의를 의무화하거나 강요해서는 안 된다.

참고 최소정보의 예

- 쇼핑업체가 고객에게 상품을 배송하기 위해 수집한 이름, 주소, 전화번호(자택 및 휴대전화번호) 등은 필요 최소한의 개인정보라고 할 수 있으나, 직업, 생년월일 등 배송과 관련 없는 개인정보를 요구하는 것은 최소정보의 범위를 벗어난 것임
- 경품 행사에 응모한 고객에게 경품추첨 사실을 알리는데 필요한 개인정보 외에 응모자의 성별, 자녀 수, 동거 여부 등 사생활의 비밀에 관한 정보, 주민등록번호 등 고유식별정보를 요구하는 것은 최소정보의 범위를 벗어난 것임
- 취업 희망자의 경력, 전공, 자격증 등에 관한 정보는 업무능력을 판단하기 위한 최소한의 정보라고 할 수 있으나 가족관계, 결혼유무, 본적(원적) 등에 관한 정보는 최소정보의 범위를 벗어난 것임

2. 입증책임의 부담

최소한의 개인정보라는 입증책임은 개인정보처리자가 부담한다. 즉 개인정보처리자가 수집한 개인정보가 정당한 목적을 위해 수집한 개인정보라고 하더라도 정보주체가 최소수집 원칙을 위배하여 처리한 것이라고 주장하여 손해배상청구소송을 제기하는 경우 개인정보처리자가 그 목적 달성을 위해 필요한 최소한의 개인정보라는 것을 입증하지 못하면 패소하게 된다.

3. 동의 거부권의 고지

개인정보처리자는 정보주체의 동의를 받아 개인정보를 수집하는 경우 그 목적에 필요한 최소한의 정보 외의 개인정보 수집에는 동의하지 아니할 수 있다는 사실을 구체적으로 알리고 개인정보를 수집하여야 한다. 구체적으로 알린다는 것은 어떤 정보가 필요 최소한의 정보이고 아닌지를 정보주체가 쉽게 알아볼 수 있게 구분해서 고지해야 하고, 필요 최소한의 정보가 아닌 정보에 대해서는 재화 또는 서비스의 이용에 방해가 없음을 자유롭게 동의를 거부할 수 있음을 알려야 한다는 것을 의미한다.

예를 들어, 개인정보처리자는 재화 또는 서비스 제공을 위하여 필요한 최소한의 개인정보와 홍보, 마케팅 등의 목적으로 필요한 개인정보를 구분하여 정보주체에게 알리고 후자에 대하여는 정보주체에게 동의를 거부할 수 있음을 알리고 동의를 받아야 한다.

4. 재화 등 제공 거부 금지

필요 최소한의 정보 외의 개인정보 수집에 동의하지 아니한다는 이유로 정보주체에게 재화 또는 서비스 제공을 거부해서는 안 된다. 서비스 제공에는 회원 가입도 포함된다. 유료의 경우는 물론이고 무료의 경우도 마찬가지이다. 이는 개인정보 수집·이용에 대해 강요된 동의를 막기 위한 것이다. 따라서 정보주체의 동의를 받으면서 선택정보에 대한 동의를 거부할 경우 그 선택정보의 수집을 통해 제공되는 재화 또는 서비스의 이용이 제한될 수 있다고 알리는 것은 가능하다.

5. 벌칙규정

위반행위	벌칙
필수정보 이외의 정보 수집에 동의하지 않는다는 이유로 재화 또는 서비스의 제공을 거부한 자 (제16조제3항 위반)	3천만원 이하 과태료 (제75조제2항제2호)

6. 다른 법률과의 관계

「신용정보법」은 신용정보의 필요 최소한의 신용정보 수집·조사 및 처리에 관한 원칙을 규정하고, 선택적 동의사항의 경우 신용정보회사등의 서비스 제공 거부 금지를 명시하고 있으므로, 이에 대해서는 「신용정보법」이 적용된다.

신용정보법	<p>제15조(수집·조사 및 처리의 원칙) ① 신용정보회사, 본인신용정보관리회사, 채권추심회사, 신용정보집중기관 및 신용정보제공·이용자(이하 “신용정보회사등”이라 한다)는 신용정보를 수집·조사 및 처리할 수 있다. 이 경우 이 법 또는 정관으로 정한 업무 범위에서 수집·조사 및 처리의 목적을 명확히 하여야 하며, 이 법 및 「개인정보 보호법」에 따라 그 목적 달성에 필요한 최소한의 범위에서 합리적이고 공정한 수단을 사용하여 신용정보를 수집·조사 및 처리하여야 한다.</p> <p>제32조(개인신용정보 제공·활용에 대한동의) ⑤ 신용정보회사등은 신용정보주체가 선택적 동의사항에 동의하지 아니한다는 이유로 신용정보주체에게 서비스의 제공을 거부하여서는 아니된다.</p>
-------	---

7. 질의 응답

Q | 수집목적에 필요한 최소한의 개인정보의 범위란?

A | 서비스제공자가 수집하는 “필요한 최소한의 개인정보”는 서비스의 특성을 고려하여 서비스 제공을 위해 반드시 필요한 정보에 한한다.

예컨대, 인터넷 쇼핑물의 경우 계약의 성립과 상품 배송 및 대금결제를 위하여 필요한 성명, 전화번호, 주소 및 통장계좌번호 또는 신용카드번호 등이 이에 해당할 수 있다.

필요한 최소한의 개인정보 수집이라는 입증책임은 개인정보처리자가 부담한다.

Q | 정보주체의 동의를 받는 경우에는 목적에 필요한 최소한의 범위를 벗어난 개인정보 수집이 허용될 수 있는지?

A | 목적에 필요한 최소한의 범위를 벗어난 개인정보는 선택정보로서 필수정보와 구분하여 동의를 얻어야 하며 정보주체가 동의를 하는 경우에는 수집이 가능하다. 다만, 필요한 최소한의 정보 외의 개인정보 수집에 동의하지 아니한다는 이유로 정보주체에게 재화 또는 서비스의 제공을 거부 위반하는 경우에는 3천만원 이하의 과태료가 부과된다.

필요한 최소한의 개인정보 수집이라는 입증책임은 개인정보처리자가 부담한다.

제17조 | 개인정보의 제공

법률

제17조(개인정보의 제공) ① 개인정보처리자는 다음 각 호의 어느 하나에 해당되는 경우에는 정보주체의 개인정보를 제3자에게 제공(공유를 포함한다. 이하 같다)할 수 있다.

1. 정보주체의 동의를 받은 경우
2. 제15조제1항제2호·제3호·제5호 및 제39조의3제2항제2호·제3호에 따라 개인정보를 수집한 목적 범위에서 개인정보를 제공하는 경우

② 개인정보처리자는 제1항제1호에 따른 동의를 받을 때에는 다음 각 호의 사항을 정보주체에게 알려야 한다. 다음 각 호의 어느 하나의 사항을 변경하는 경우에도 이를 알리고 동의를 받아야 한다.

1. 개인정보를 제공받는 자
2. 개인정보를 제공받는 자의 개인정보 이용 목적
3. 제공하는 개인정보의 항목
4. 개인정보를 제공받는 자의 개인정보 보유 및 이용 기간
5. 동의를 거부할 권리가 있다는 사실 및 동의 거부에 따른 불이익이 있는 경우에는 그 불이익의 내용

③ 개인정보처리자가 개인정보를 국외의 제3자에게 제공할 때에는 제2항 각 호에 따른 사항을 정보주체에게 알리고 동의를 받아야 하며, 이 법을 위반하는 내용으로 개인정보의 국외 이전에 관한 계약을 체결하여서는 아니 된다.

④ 개인정보처리자는 당초 수집 목적과 합리적으로 관련된 범위에서 정보주체에게 불이익이 발생하는지 여부, 암호화 등 안전성 확보에 필요한 조치를 하였는지 여부 등을 고려하여 대통령령으로 정하는 바에 따라 정보주체의 동의 없이 개인정보를 제공할 수 있다.

시행령

제14조의2(개인정보의 추가적인 이용·제공의 기준 등) ① 개인정보처리자는 법 제15조제3항 또는 제17조제4항에 따라 정보주체의 동의 없이 개인정보를 이용 또는 제공(이하 “개인정보의 추가적인 이용 또는 제공”이라 한다)하려는 경우에는 다음 각 호의 사항을 고려해야 한다.

1. 당초 수집 목적과 관련성이 있는지 여부
2. 개인정보를 수집한 정황 또는 처리 관행에 비추어 볼 때 개인정보의 추가적인 이용 또는 제공에 대한 예측 가능성이 있는지 여부
3. 정보주체의 이익을 부당하게 침해하는지 여부
4. 가명처리 또는 암호화 등 안전성 확보에 필요한 조치를 하였는지 여부

② 개인정보처리자는 제1항 각 호의 고려사항에 대한 판단 기준을 법 제30조제1항에 따른 개인정보 처리방침에 미리 공개하고, 법 제31조제1항에 따른 개인정보 보호책임자가 해당 기준에 따라 개인정보의 추가적인 이용 또는 제공을 하고 있는지 여부를 점검해야 한다.

제7조(개인정보의 제공) ① 개인정보의 “제공”이란 개인정보의 저장 매체나 개인정보가 담긴 출력물·책자 등을 물리적으로 이전하거나 네트워크를 통한 개인정보의 전송, 개인정보에 대한 제3자의 접근권한 부여, 개인정보처리자와 제3자의 개인정보 공유 등 개인정보의 이전 또는 공동 이용 상태를 초래하는 모든 행위를 말한다.

② 법 제17조의 “제3자”란 정보주체와 정보주체에 관한 개인정보를 수집·보유하고 있는 개인정보처리자를 제외한 모든 자를 의미하며, 정보주체의 대리인(명백히 대리의 범위 내에 있는 것에 한한다)과 법 제26조제2항에 따른 수탁자는 제외한다(이하 같다).

③ 개인정보처리자가 법 제17조제2항제1호에 따라 정보주체에게 개인정보를 제공받는 자를 알리는 경우에는 그 성명(법인 또는 단체인 경우에는 그 명칭)과 연락처를 함께 알려야 한다.

1. 개인정보 제3자 제공의 의미

개인정보의 제공이란 개인정보처리자 외의 제3자에게 개인정보의 지배·관리권이 이전되는 것을 의미한다. 즉 개인정보를 저장한 매체나 수기문서를 전달하는 경우뿐만 아니라, DB 시스템에 대한 접속권한을 허용하여 열람·복사가 가능하게 하여 개인정보를 공유하는 경우 등도 ‘제공’에 포함된다.

한편, 민감정보 및 고유식별정보를 제3자에게 제공하는 경우에는 제23조, 제24조 및 제24조의2를 따라야 한다.

2. 이용, 처리업무 위탁 및 영업양도와의 차이

가 이용과의 차이

개인정보의 이용이란 개인정보처리자(기관·단체·법인 등) 내에서 개인정보의 지배·관리권 이전 없이 스스로의 목적으로 쓰는 것을 의미하는 반면, 개인정보의 제공이란 개인정보처리자(개인정보 처리업무 수탁자 포함) 및 정보주체(정보주체의 대리인 포함) 외의 제3자에게 개인정보의 지배·관리권이 이전되는 것을 말한다. 따라서 같은 개인정보처리자 내의 다른 부서가 당초 수집 목적과 달리 이용하는 경우라면 제공이 아니라 목적 외 이용에 해당한다.

나 처리업무 위탁과의 차이

업무위탁과 개인정보 제3자 제공 모두 개인정보가 다른 사람(제3자)에게 이전되거나 공동으로 처리하게 된다는 측면에서는 동일하다. 그러나 ‘업무위탁’의 경우에는 개인정보처리자의 업무를 처리할 목적으로 개인정보가 제3자(수탁자)에게 이전되지만, ‘제공’은 제공받는 자의 업무를 처리할 목적 및 이익을 위해서 개인정보가 이전된다는 점이 다르다. 또한 위탁의 경우에는 개인정보처리자의 관리·감독을 받지만, 제3자 제공은 개인정보가 제공된 이후에는 제3자가 자신의 책임 하에 개인정보를 처리하게 되며, 개인정보처리자의 관리·감독권이 미치지 못한다.

판례 개인정보 처리위탁에 있어 ‘수탁자’가 제3자 제공의 ‘제3자’에 해당하는지 여부

「개인정보 보호법」 제17조에서 말하는 개인정보의 ‘제3자 제공’은 본래의 개인정보 수집·이용 목적의 범위를 넘어 정보를 제공받는 자의 업무처리와 이익을 위하여 개인정보가 이전되는 경우인 반면, 「개인정보 보호법」 제26조에서 말하는 개인정보의 ‘처리위탁’은 본래의 개인정보 수집·이용 목적과 관련된 위탁자 본인의 업무 처리와 이익을 위하여 개인정보가 이전되는 경우를 의미한다. 개인정보 처리위탁에 있어 수탁자는 위탁자로부터 위탁사무 처리에 따른 대가를 지급받는 것 외에는 개인정보 처리에 관하여 독자적인 이익을 가지지 않고, 정보제공자의 관리·감독 아래 위탁받은 범위 내에서만 개인정보를 처리하게 되므로, 「개인정보 보호법」 제17조에 정한 ‘제3자’에 해당하지 않는다(대법원 2017. 4. 7 선고 2016도13263 판결).

다 영업양도 등과의 차이

영업의 양도·합병(제27조)은 비록 개인정보가 제3자에게 이전된다는 점에서는 ‘제공’과 유사하다. 그러나 영업의 양도·합병은 그 개인정보를 이용한 업무의 형태는 변하지 않고 단지 개인정보의 관리주체만 변한다는 점에서 ‘제공’과는 차이가 있다. 이에 따라 영업의 양도·합병에 대해서는 제27조에서 별도의 규정을 두고 있으며, 제공과 관련한 규정은 적용되지 않는다.

3. 개인정보처리자의 제3자 제공이 가능한 경우

개인정보처리자는 정보주체의 동의를 받아 개인정보를 제3자에게 제공하거나 제15조제1항제2호(법률 규정 또는 법령 상 의무 준수), 제3호(공공기관 소관업무 수행) 및 제5호(급박한 생명·신체·재산상 이익)에 따라 개인정보를 수집한 목적 범위 내에서 동의 없이 제3자에게 제공할 수 있다.

가 정보주체의 동의를 받은 경우

개인정보처리자가 제3자 제공에 대한 동의를 받을 때에는 정보주체가 제공의 내용과 의미를 명확히 알 수 있도록 미리 ① 개인정보를 제공받는 자의 성명(법인 또는 단체인 경우에는 그 명칭) ② 제공받는 자의 개인정보 이용 목적 ③ 제공하는 개인정보의 항목 ④ 제공받는 자의 개인정보 보유 및 이용 기간 ⑤ 동의 거부권이 존재하다는 사실 및 동의 거부에 따른 불이익이 있는 경우에는 그 내용을 알려주어야 한다. 알려야 할 사항 중 어느 하나에 변경이 있는 경우에도 정보주체에게 변경 사실을 다시 알리고 동의를 받아야 한다.

‘개인정보를 제공받는 자’란 제공받는 자의 이름 또는 상호를 의미하므로, 금융기관, 정부기관 등과 같이 정보주체가 제공받는 자를 알기 어렵도록 포괄적으로 알려서는 아니 되며, 제공받는 자가 여러 명일 경우에는 각각의 이름 또는 상호를 알리고 제공되는 목적, 항목, 기간 등이 다를 경우에는 제공받는 자별로 그 목적, 항목, 기간 등을 각각 알려야 한다. 이 경우 개인정보처리자는 제공받는 자의 연락처도 함께 알리는 것이 바람직하다.

이와 같이 제공받는 자가 특정되어 있어야 하기 때문에 우리나라에서는 사실상 데이터베이스 마케팅(정보주체들의 동의를 받아 대량의 개인정보를 수집하여 저장해 두고, 다른 사람들에게 개인정보를 판매·대여하거나, 다른 사람이 보유하고 있는 개인정보 데이터베이스를 최신의 상태로 업데이트시켜 주거나, 다른 사람의 상품 광고를 대행해 주는 서비스)은 금지되어 있다고 할 수 있다.

< 관련 위반 사례 >

- XX서점은 영업의 특성상 제휴업체가 빈번히 변경된다는 이유로 회원가입신청서 상에 “개인정보를 제공받는 자(제휴업체명) 및 개인정보의 제공목적”을 고지하지 않고 개인정보를 여러 제휴업체와 제공·공유함
- XX마트는 “개장 기념 경품이벤트”를 실시하면서, 경품행사에 응모한 고객의 정보가 제휴 생명보험사에 제공되어 「휴일 무료 상해보험」에 가입된다는 사실에 대한 동의를 받지 않고 제휴업체에 제공함

나 법률에 특별한 규정이 있거나 법령상 의무준수를 위해 불가피하여 수집한 경우로서 그 수집 목적 범위 내에서 개인정보를 제공하는 경우

1) 법률의 특별한 규정

‘법률의 특별한 규정이 있는 경우’란 법률에서 개인정보의 활용에 대하여 구체적으로 요구하거나 허용하고 있는 경우를 말한다. 따라서 시·군·구의 장의 공직선거 입후보자에 대한 선거인명부 교부(「공직선거법」 제46조), 보험요율산출기관의 보험회사에 대한 보험계약자 교통법규위반 개인정보 제공(「보험업법」 제176조) 등의 경우 개인정보처리자는 정보주체의 동의 없이 개인정보를 관계 당사자에게 제공할 수 있다.

제46조(명부사본의 교부) ① 구·시·군의 장은 후보자[비례대표국회의원후보자 및 비례대표 지방의회의원(비례대표시·도의원 및 비례대표자치구·시·군의원을 말한다. 이하 같다)후보자를 제외한다]·선거사무장(비례대표국회의원선거 및 비례대표지방의회의원선거의 선거사무장을 제외한다) 또는 선거연락소장의 신청이 있는 때에는 작성된 선거인명부 또는 부재자신고인명부의 사본이나 전산자료복사본을 후보자별로 1통씩 24시간 이내에 신청인에게 교부하여야 한다.

② 제1항에 따른 선거인명부 또는 부재자신고인명부의 사본이나 전산자료복사본의 교부신청은 선거기간개시일까지 해당 구·시·군의 장에게 서면으로 하여야 한다.

2) 법령상 의무 준수

법령에서 개인정보처리자에게 일정한 의무를 부과하고 있는 경우로서 해당 개인정보처리자가 그 의무 이행을 위해서 개인정보를 불가피하게 수집·이용할 수밖에 없는 경우를 말한다. 법률에 의한 의무뿐만 아니라 시행령, 시행규칙에 따른 의무도 포함된다.

‘불가피한 경우’란 개인정보를 수집하지 않고는 법령에서 부과하는 의무를 이행하는 것이 불가능하거나 개인정보처리자가 다른 방법을 사용하여 의무를 이행하는 것이 현저히 곤란한 경우를 의미한다.

법령상 의무준수를 위하여 불가피한 경우에 해당하여 개인정보를 수집·이용한 경우에는 그 목적 범위 내에서 개인정보를 제공할 수 있다. 학원을 설립·운영하려는 자의 강사명단 등을 교육감에게 등록하여야 하는 의무(「학원의 설립·운영 및 과외교습에 관한 법률」 제6조), 소득지급자의 소득귀속자에 대한 원천징수의무 및 원천징수이행상황신고 의무(「소득세법」 제127조 및 제128조) 등을 이행하기 위한 개인정보의 제공이 법령상 의무 준수의 예에 속한다.

제127조(원천징수의무) ① 국내에서 거주자나 비거주자에게 다음 각 호의 어느 하나에 해당하는 소득을 지급하는 자(제3호의 소득을 지급하는 자의 경우에는 사업자 등 대통령령으로 정하는 자로 한정한다)는 이 절의 규정에 따라 그 거주자나 비거주자에 대한 소득세를 원천징수하여야 한다.

1. 이자소득
2. 배당소득
3. 대통령령으로 정하는 사업소득(이하 “원천징수대상 사업소득”이라 한다)
4. 근로소득. 다만, 다음 각 목의 어느 하나에 해당하는 소득은 제외한다.
 - 가. 외국기관 또는 우리나라에 주둔하는 국제연합군(미군은 제외한다)으로부터 받는 근로소득
 - 나. 국외에 있는 비거주자 또는 외국법인(국내지점 또는 국내영업소는 제외한다)으로부터 받는 근로소득. 다만, 다음의 어느 하나에 해당하는 소득은 제외한다.
 - 1) 제120조제1항 및 제2항에 따른 비거주자의 국내사업장과 「법인세법」 제94조제1항

및 제2항에 따른 외국법인의 국내사업장의 국내원천소득금액을 계산할 때 필요경비 또는 손금으로 계상되는 소득

2) 국외에 있는 외국법인(국내지점 또는 국내영업소는 제외한다)으로부터 받는 근로소득 중 제156조의7에 따라 소득세가 원천징수되는 파견근로자의 소득

5. 연금소득

6. 기타소득. 다만, 다음 각 목의 어느 하나에 해당하는 소득은 제외한다.

가. 제8호에 따른 소득

나. 제21조제1항제10호에 따른 위약금·배상금(계약금이 위약금·배상금으로 대체되는 경우만 해당한다)

다. 제21조제1항제23호 또는 제24호에 따른 소득

7. 퇴직소득. 다만, 제4호 각 목의 어느 하나에 해당하는 근로소득이 있는 사람이 퇴직함으로써 받는 소득은 제외한다.

8. 대통령령으로 정하는 봉사료

제128조(원천징수세액의 납부) ① 원천징수의무자는 원천징수한 소득세를 그 징수일이 속하는 달의 다음 달 10일까지 대통령령으로 정하는 바에 따라 원천징수 관할 세무서, 한국은행 또는 체신관서에 납부하여야 한다.

다 공공기관이 법령 등에서 정하는 소관업무 수행을 위해 불가피하여 수집한 경우로서 그 수집 목적 범위 내에서 개인정보를 제공하는 경우

공공기관의 경우에는 법령 등에서 정해진 소관업무를 수행하기 위하여 수시로 개인정보를 제3자에게 제공해야 할 필요가 있다. 공공기관의 경우에는 개인정보를 수집할 수 있도록 명시적으로 허용하는 법률 규정이 없더라도 법령 등에서 소관 업무를 정하고 있고 그 소관 업무의 수행을 위하여 불가피하게 개인정보를 수집할 수밖에 없는 경우에는 정보주체의 동의 없이 개인정보의 수집이 허용된다.

‘법령 등에서 정하는 소관업무’란 「정부조직법」 및 각 기관별 직제·직제규칙, 개별 조직법 등에서 정하고 있는 소관 사무 이외에, 「주민등록법」, 「국세기본법」, 「의료법」, 「국민건강보험법」 등 소관법령에 의해서 부여된 권한과 의무, 지방자치단체의 경우 조례에서 정하고 있는 업무 등을 의미한다. 지방자치단체의 경우 다양한 인허가사무, 신고수리, 복지업무, 관리·감독 등의 업무를 수행해야 하기 때문에 실무적으로 개인정보를 제3자에게 제공해야 하는 경우가 자주 발생할 수 있다.

공공기관이 소관 업무를 수행하기 위하여 개인정보를 제3자에게 제공함에 있어서는 정말로 불가피한 사유가 있는지 여부를 신중하게 검토해야 한다. ‘불가피한 경우’란 개인정보를 제공하지 아니하고는 법령 등에서 해당 공공기관에 부여하고 있는 권한의 행사나 의무의 이행이 불가능하거나 다른 방법을 사용하여 소관 업무를 수행하는 것이 현저히 곤란한 경우를 의미한다. 특히 공공기관이 내부고발, 민원업무 등을 처리하기 위하여 민원인의

개인정보를 제3자에게 제공할 때에는 주의해야 한다. 민원업무를 쉽게 해결하기 위하여 민원인의 개인정보를 피민원인이나 피민원기관에 제공하는 것은 불가피한 필요가 있는 경우라고 보기 어렵다.

라 급박한 생명·신체·재산상 이익을 위하여 필요한 경우

정보주체 또는 그 법정대리인이 의사표시를 할 수 없는 상태에 있거나 주소불명 등으로 사전 동의를 받을 수 없는 경우로서 명백히 제3자의 급박한 생명·신체·재산상의 이익을 위하여 필요하다고 인정되어 개인정보를 수집하였다면 그 수집 목적 범위에서 정보주체의 동의 없이 개인정보를 제3자에게 제공할 수 있다. 동사무소나 경찰관서가 시급히 수술 등의 의료 조치가 필요한 교통사고 환자의 연락처를 의료기관에 알려주는 행위가 이에 속한다.

< 개인정보의 수집·이용기준과 제공기준의 비교 >

기준	수집·이용(제15조)	제공(제17조)
• 정보주체의 동의를 받은 경우	가능	제공 가능
• 법률에 특별한 규정이 있거나 법령상 의무를 준수하기 위하여 불가피한 경우	가능	수집목적 범위 안에서 제공 가능
• 공공기관이 법령 등에서 정하는 소관 업무의 수행을 위하여 불가피한 경우	가능	수집목적 범위 안에서 제공 가능
• 정보주체와의 계약의 체결 및 이행을 위하여 불가피하게 수반되는 경우	가능	제공 불가 (정보주체 동의 필요)
• 정보주체 또는 그 법정대리인이 의사표시를 할 수 없는 상태에 있거나 주소불명 등으로 사전 동의를 받을 수 없는 경우로서 명백히 정보주체 또는 제3자의 급박한 생명, 신체, 재산의 이익을 위하여 필요하다고 인정되는 경우	가능	수집목적 범위 안에서 제공 가능
• 개인정보처리자의 정당한 이익을 달성하기 위하여 필요한 경우로서 명백히 정보주체의 권리보다 우선하는 경우	가능	제공 불가 (정보주체 동의 필요)

4. 정보통신서비스 제공자가 제3자 제공을 할 수 있는 경우

정보통신서비스 제공자도 정보주체의 동의를 받은 경우에 개인정보를 제3자에게 제공할 수 있다. 한편, 정보통신서비스 제공자의 개인정보 수집·이용에 대해서는 제15조가 아닌 제39조의3제1항이 적용되므로 정보통신서비스 제공자는 같은 조 제2항제2호 및 제3호에서 정한 경우에 한하여 개인정보를 수집한 목적 범위 내에서 동의 없이 제3자에게 제공할 수 있다.

가 정보주체의 동의를 받은 경우

정보통신서비스 제공자도 정보주체의 동의를 받은 경우에는 개인정보를 제3자에게 제공할 수 있다. 정보통신서비스 제공자가 제3자 제공에 대한 동의를 받을 때에는 정보주체가 제공의 내용과 의미를 명확히 알 수 있도록 미리 ① 개인정보를 제공받는 자의 성명(법인 또는 단체인 경우에는 그 명칭) ② 제공받는 자의 개인정보 이용 목적 ③ 제공하는 개인정보의 항목 ④ 제공받는 자의 개인정보 보유 및 이용 기간 ⑤ 동의 거부권이 존재하다는 사실 및 동의 거부에 따른 불이익이 있는 경우에는 그 내용을 알려주어야 한다.

나 정보통신서비스의 제공에 따른 요금정산을 위하여 필요하여 수집한 경우로서 그 수집 목적 범위 내에서 개인정보를 제공하는 경우

정보통신서비스 제공자는 정보통신서비스의 제공에 따른 요금정산을 위하여 필요하여 개인정보를 수집하였다면 그 수집 목적 범위 내에서 동의 없이 개인정보를 제3자에게 제공할 수 있다. 예컨대, 이용자의 정보통신서비스 이용에 따른 서비스별 요금액, 납부 또는 미납한 사실, 미납액 등에 관한 정보들은 요금 정산이 완료될 때까지 이용자의 동의 여부와 관계없이 수집할 수 있고, 요금 정산의 목적 범위 내에서 제3자에게 제공할 수 있다.

다 다른 법률에 특별한 규정이 있어 수집한 경우로서 그 수집 목적 범위 내에서 개인정보를 제공하는 경우

다른 법률에서 해당 개인정보를 특정 목적으로 이용하도록 규정하고 있어 개인정보를 수집하였다면 그 목적의 범위 내에서 동의 없이 제3자에게 제공할 수 있다.

참고 「전자상거래 등에서의 소비자보호에 관한 법률」

제21조(금지행위) ① 전자상거래를 하는 사업자 또는 통신판매업자는 다음 각 호의 어느 하나에 해당하는 행위를 하여서는 아니 된다.

6. 본인의 허락을 받지 아니하거나 허락받은 범위를 넘어 소비자에 관한 정보를 이용하는 행위. 다만, 다음 각 목의 어느 하나에 해당하는 경우는 제외한다.

가. 재화등의 배송 등 소비자와의 계약을 이행하기 위하여 불가피한 경우로서 대통령령으로 정하는 경우

나. 재화등의 거래에 따른 대금정산을 위하여 필요한 경우

다. 도용방지를 위하여 본인 확인에 필요한 경우로서 대통령령으로 정하는 경우

라. 법률의 규정 또는 법률에 따라 필요한 불가피한 사유가 있는 경우

5. 국외 제공 및 이전 제한

가 개인정보의 국외 제3자 제공

개인정보처리자가 개인정보를 국외의 제3자에게 ‘제공’ 하고자 할 때에는 ① 개인정보를 제공받는 자의 성명(법인 또는 단체인 경우에는 그 명칭) ② 제공받는 자의 개인정보 이용 목적 ③ 제공하는 개인정보의 항목 ④ 제공받는 자의 개인정보 보유 및 이용 기간 ⑤ 동의 거부권이 존재한다는 사실 및 동의 거부에 따른 불이익의 내용(불이익이 있는 경우에 한함)을 모두 정보주체에게 알리고 동의를 받아야 한다(제3항 전단).

개인정보처리자는 동의 받은 범위를 초과하여 국외 제3자에게 제공하여서는 아니 된다. 그러나 제18조제2항 각 호의 어느 하나에 해당하는 경우에는 정보주체 또는 제3자의 이익을 부당하게 침해할 우려가 있을 때를 제외하고는 동의 받은 범위를 초과하여 국외 제3자에게 제공할 수 있다. 다만, 공공기관은 제5호부터 제9호까지의 경우에 해당하는 경우에만 동의 받은 범위를 초과하여 국외 제3자에게 제공할 수 있다.

한편, 정보통신서비스 제공자등이 국외 제3자 제공을 포함하여 개인정보를 국외로 이전하는 경우에는 제17조제3항이 아닌 제39조의12에 따라 동의를 받아야 하며, 제18조제1항제1호 및 제2호에 해당하는 경우에만 동의 받은 범위를 초과하여 국외로 이전할 수 있다.

나 개인정보 국외 이전

이 법을 위반하는 내용으로 개인정보의 국외 이전에 관한 계약을 체결하여서는 아니 된다. 개인정보를 국외에 이전하여 이 법의 적용을 회피하려는 것을 막기 위한 최소한의 조치라고 할 수 있다.

국외 이전은 국외 제공보다 개념이 넓다. 국외의 제3자에게 개인정보를 제공하는 것은 물론이고, 개인정보처리를 국외의 제3자에게 위탁하기 위해 국외로 옮겨지는 경우도 국외 이전에 포함된다. 위탁의 경우 정보주체의 동의를 받을 필요는 없지만 처리위탁에 관한 규정(제26조)에 따라야 한다.

6. 개인정보의 추가적 제공

개인정보의 추가적인 제공에 대한 해설은 제15조(개인정보의 수집·이용) “개인정보의 추가적인 이용” 부분을 참고하도록 한다. 이 경우 ‘이용’을 ‘제공’으로 하여 준용한다.

7. 벌칙규정

위반행위	벌칙
정보주체의 동의를 받지 않고 개인정보를 제3자에게 제공한 자 및 그 사정을 알고 제공받은 자 (제17조제1항제1호 위반)	5년 이하의 징역 또는 5천만원 이하 벌금 (제71조제1호)
정보주체에 대한 고지의무 위반 (제17조제2항 위반)	3천만원 이하의 과태료 (제75조제2항제1호)
개인정보 제3자 제공기준을 위반하여 개인정보를 제공한 정보통신서비스 제공자등 (제17조제1항 및 제2항 위반)	위반행위 관련 매출액의 100분의 3이하 과징금 (제39조의15제1항제1호)

제17조제4항은 그 자체로 별도의 벌칙 규정이 없다. 그러나 제17조제4항의 요건에 해당하지 않는데도 개인정보를 추가적으로 제공하려는 경우에는 제18조제2항에서 정하는 바에 따라 정보주체로부터 별도의 동의를 받거나 다른 법률에 특별한 규정이 있는 경우 등에 해당하여야 한다. 따라서 이 경우는 제18조제2항 각 호의 어느 하나에 해당하는지 여부에 따라 제18조제1항 위반에 관한 벌칙조항의 적용을 받을 수 있다.

8. 다른 법률과의 관계

「신용정보법」에는 개인신용정보의 제공에 관하여 규정하고 있으며, 이에 관하여 신용정보이용·제공자 등은 「신용정보법」에 따라야 한다.

신용정보법	<p>제32조(개인신용정보의 제공·활용에 대한 동의) ① 신용정보제공·이용자가 개인신용정보를 타인에게 제공하려는 경우에는 대통령령으로 정하는 바에 따라 해당 신용정보주체로부터 다음 각 호의 어느 하나에 해당하는 방식으로 개인신용정보를 제공할 때마다 미리 개별적으로 동의를 받아야 한다. 다만, 기존에 동의한 목적 또는 이용 범위에서 개인신용정보의 정확성·최신성을 유지하기 위한 경우에는 그러하지 아니하다.</p> <ol style="list-style-type: none"> 1. 서면 2. 「전자서명법」 제2조제3호에 따른 공인전자서명이 있는 전자문서(「전자거래기본법」 제2조제1호에 따른 전자문서를 말한다) 3. 개인신용정보의 제공 내용 및 제공 목적 등을 고려하여 정보 제공 동意的 안정성과 신뢰성이 확보될 수 있는 유무선 통신으로 개인비밀번호를 입력하는 방식 4. 유무선 통신으로 동의 내용을 해당 개인에게 알리고 동의를 받는 방법. 이 경우 본인 여부 및 동의 내용, 그에 대한 해당 개인의 답변을 음성녹음하는 등 증거자료를 확보·유지하여야 하며, 대통령령으로 정하는 바에 따른 사후 고지절차를 거친다.
-------	---

5. 그 밖에 대통령령으로 정하는 방식

② 개인신용평가회사, 개인사업자신용평가회사, 기업신용조회회사 또는 신용정보집중기관으로부터 개인신용정보를 제공받으려는 자는 대통령령으로 정하는 바에 따라 해당 신용정보주체로부터 제1항 각 호의 어느 하나에 해당하는 방식으로 개인신용정보를 제공받을 때마다 개별적으로 동의(기준에 동의한 목적 또는 이용 범위에서 개인신용정보의 정확성·최신성을 유지하기 위한 경우는 제외한다)를 받아야 한다. 이 경우 개인신용정보를 제공받으려는 자는 개인신용정보의 조회 시 개인신용평점이 하락할 수 있는 때에는 해당 신용정보주체에게 이를 고지하여야 한다.

③ 개인신용평가회사, 개인사업자신용평가회사, 기업신용조회회사 또는 신용정보집중기관이 개인신용정보를 제2항에 따라 제공하는 경우에는 해당 개인신용정보를 제공받으려는 자가 제2항에 따른 동의를 받았는지를 대통령령으로 정하는 바에 따라 확인하여야 한다.

④ 신용정보회사등은 개인신용정보의 제공 및 활용과 관련하여 동의를 받을 때에는 대통령령으로 정하는 바에 따라 서비스 제공을 위하여 필수적 동의사항과 그 밖의 선택적 동의사항을 구분하여 설명한 후 각각 동의를 받아야 한다. 이 경우 필수적 동의사항은 서비스 제공과의 관련성을 설명하여야 하며, 선택적 동의사항은 정보제공에 동의하지 아니할 수 있다는 사실을 고지하여야 한다.

⑤ 신용정보회사등은 신용정보주체가 선택적 동의사항에 동의하지 아니한다는 이유로 신용정보주체에게 서비스의 제공을 거부하여서는 아니 된다.

⑥ 신용정보회사등이 개인신용정보를 제공하는 경우로서 다음 각 호의 어느 하나에 해당하는 경우에는 제1항부터 제5항까지를 적용하지 아니한다.

1. 신용정보회사 및 채권추심회사가 다른 신용정보회사 및 채권추심회사 또는 신용정보집중기관과 서로 집중관리·활용하기 위하여 제공하는 경우
2. 제17조제2항에 따라 신용정보의 처리를 위탁하기 위하여 제공하는 경우
3. 영업양도·분할·합병 등의 이유로 권리·의무의 전부 또는 일부를 이전하면서 그와 관련된 개인신용정보를 제공하는 경우
4. 채권추심(추심채권을 추심하는 경우만 해당한다), 인가·허가의 목적, 기업의 신용도 판단, 유가증권의 양수 등 대통령령으로 정하는 목적으로 사용하는 자에게 제공하는 경우
5. 법원의 제출명령 또는 법관이 발부한 영장에 따라 제공하는 경우
6. 범죄 때문에 피해자의 생명이나 신체에 심각한 위협 발생이 예상되는 등 긴급한 상황에서 제5호에 따른 법관의 영장을 발부받을 시간적 여유가 없는 경우로서 검사 또는 사법경찰관의 요구에 따라 제공하는 경우. 이 경우 개인신용정보를 제공받은 검사는 지체 없이 법관에게 영장을 청구하여야 하고, 사법경찰관은 검사에게 신청하여 검사의 청구로 영장을 청구하여야 하며, 개인신용정보를 제공받은 때부터 36시간 이내에 영장을 발부받지 못하면 지체 없이 제공받은 개인신용정보를 폐기하여야 한다.
7. 조세에 관한 법률에 따른 질문·검사 또는 조사를 위하여 관할 관서의 장이 서면으로 요구하거나 조세에 관한 법률에 따라 제출의무가 있는 과세자료의 제공을 요구함에 따라 제공하는 경우
8. 국제협약 등에 따라 외국의 금융감독기구에 금융회사가 가지고 있는 개인신용정보를 제공하는 경우
9. 제2조제1호의4나목 및 다목의 정보를 개인신용평가회사, 개인사업자신용평가회사, 기업신용등급제공업무·기술신용평가업무를 하는 기업신용조회회

	<p>사 및 신용정보집중기관에 제공하거나 그로부터 제공받는 경우</p> <p>9의2. 통계작성, 연구, 공익적 기록보존 등을 위하여 가명정보를 제공하는 경우. 이 경우 통계작성에는 시장조사 등 상업적 목적의 통계작성을 포함하며, 연구에는 산업적 연구를 포함한다.</p> <p>9의3. 제17조의2제1항에 따른 정보집합물의 결합 목적으로 데이터전문기관에 개인신용정보를 제공하는 경우</p> <p>9의4. 다음 각 목의 요소를 고려하여 당초 수집한 목적과 상충되지 아니하는 목적으로 개인신용정보를 제공하는 경우</p> <p>가. 양 목적 간의 관련성</p> <p>나. 신용정보회사등이 신용정보주체로부터 개인신용정보를 수집한 경위</p> <p>다. 해당 개인신용정보의 제공이 신용정보주체에게 미치는 영향</p> <p>라. 해당 개인신용정보에 대하여 가명처리를 하는 등 신용정보의 보안대책을 적절히 시행하였는지 여부</p> <p>10. 이 법 및 다른 법률에 따라 제공하는 경우</p> <p>11. 제1호부터 제10호까지의 규정에 준하는 경우로서 대통령령으로 정하는 경우</p> <p>⑦ 제6항 각 호에 따라 개인신용정보를 타인에게 제공하려는 자 또는 제공받은 자는 대통령령으로 정하는 바에 따라 개인신용정보의 제공 사실 및 이유 등을 사전에 해당 신용정보주체에게 알려야 한다. 다만, 대통령령으로 정하는 불가피한 사유가 있는 경우에는 인터넷 홈페이지 게재 또는 그 밖에 유사한 방법을 통하여 사후에 알리거나 공시할 수 있다.</p> <p>⑧ 제6항제3호에 따라 개인신용정보를 타인에게 제공하는 신용정보제공·이용자로서 대통령령으로 정하는 자는 제공하는 신용정보의 범위 등 대통령령으로 정하는 사항에 관하여 금융위원회의 승인을 받아야 한다.</p> <p>⑨ 제8항에 따른 승인을 받아 개인신용정보를 제공받은 자는 해당 개인신용정보를 금융위원회가 정하는 바에 따라 현재 거래 중인 신용정보주체의 개인신용정보와 분리하여 관리하여야 한다.</p> <p>⑩ 신용정보회사등이 개인신용정보를 제공하는 경우에는 금융위원회가 정하여 고시하는 바에 따라 개인신용정보를 제공받는 자의 신원(身元)과 이용 목적을 확인하여야 한다.</p> <p>⑪ 개인신용정보를 제공한 신용정보제공·이용자는 제1항에 따라 미리 개별적 동의를 받았는지 여부 등에 대한 다툼이 있는 경우 이를 증명하여야 한다.</p>
--	---

9. 질의 응답

Q | 같은 그룹 내의 호텔, 여행, 쇼핑몰 사이트 등 회원정보 DB를 통합하고 1개의 ID로 로그인이 가능하게 하는 이른바 '패밀리 사이트'제도를 도입하려 한다. 같은 그룹 내부의 계열사이기 때문에 고객들의 별도 동의는 필요 없는지?

A |

- 제3자는 고객으로부터 개인정보를 수집한 해당 사업자를 제외한 모든 법인, 단체 등을 의미하므로, 같은 그룹 내부의 계열사라 하더라도 개인정보의 수집·이용 목적이 다른 별도의 법인에 해당한다면 제3자에 해당한다.
- 따라서 그룹 계열사 간이라도 패밀리 사이트라는 명목으로 개인정보를 제공·공유하기 위해서는 제3자 제공에 따른 사항을 알리고 동의를 얻어야 한다.

제18조 | 개인정보의 목적 외 이용·제공 제한

법률

제18조(개인정보의 목적 외 이용·제공 제한) ① 개인정보처리자는 개인정보를 제15조제1항 및 제39조의3제1항 및 제2항에 따른 범위를 초과하여 이용하거나 제17조제1항 및 제3항에 따른 범위를 초과하여 제3자에게 제공하여서는 아니 된다.

② 제1항에도 불구하고 개인정보처리자는 다음 각 호의 어느 하나에 해당하는 경우에는 정보주체 또는 제3자의 이익을 부당하게 침해할 우려가 있을 때를 제외하고는 개인정보를 목적 외의 용도로 이용하거나 이를 제3자에게 제공할 수 있다. 다만, 이용자(「정보통신망 이용촉진 및 정보보호 등에 관한 법률」 제2조제1항제4호에 해당하는 자를 말한다. 이하 같다)의 개인정보를 처리하는 정보통신서비스 제공자(「정보통신망 이용촉진 및 정보보호 등에 관한 법률」 제2조제1항제3호에 해당하는 자를 말한다. 이하 같다)의 경우 제1호·제2호의 경우로 한정하고, 제5호부터 제9호까지의 경우는 공공기관의 경우로 한정한다.

1. 정보주체로부터 별도의 동의를 받은 경우
2. 다른 법률에 특별한 규정이 있는 경우
3. 정보주체 또는 그 법정대리인이 의사표시를 할 수 없는 상태에 있거나 주소불명 등으로 사전 동의를 받을 수 없는 경우로서 명백히 정보주체 또는 제3자의 급박한 생명, 신체, 재산의 이익을 위하여 필요하다고 인정되는 경우
4. 삭제 <2020. 2. 4.>
5. 개인정보를 목적 외의 용도로 이용하거나 이를 제3자에게 제공하지 아니하면 다른 법률에서 정하는 소관 업무를 수행할 수 없는 경우로서 보호위원회 심의·의결을 거친 경우
6. 조약, 그 밖의 국제협정의 이행을 위하여 외국정부 또는 국제기구에 제공하기 위하여 필요한 경우
7. 범죄의 수사와 공소의 제기 및 유지를 위하여 필요한 경우
8. 법원의 재판업무 수행을 위하여 필요한 경우
9. 형(刑) 및 감호, 보호처분의 집행을 위하여 필요한 경우

③ 개인정보처리자는 제2항제1호에 따른 동의를 받을 때에는 다음 각 호의 사항을 정보주체에게 알려야 한다. 다음 각 호의 어느 하나의 사항을 변경하는 경우에도 이를 알리고 동의를 받아야 한다.

1. 개인정보를 제공받는 자
2. 개인정보의 이용 목적(제공 시에는 제공받는 자의 이용 목적을 말한다)
3. 이용 또는 제공하는 개인정보의 항목
4. 개인정보의 보유 및 이용 기간(제공 시에는 제공받는 자의 보유 및 이용

	<p>기간을 말한다)</p> <p>5. 동의를 거부할 권리가 있다는 사실 및 동의 거부에 따른 불이익이 있는 경우에는 그 불이익의 내용</p> <p>④ 공공기관은 제2항제2호부터 제6호까지, 제8호 및 제9호에 따라 개인정보를 목적 외의 용도로 이용하거나 이를 제3자에게 제공하는 경우에는 그 이용 또는 제공의 법적 근거, 목적 및 범위 등에 관하여 필요한 사항을 보호위원회가 고시로 정하는 바에 따라 관보 또는 인터넷 홈페이지 등에 게재하여야 한다.</p> <p>⑤ 개인정보처리자는 제2항 각 호의 어느 하나의 경우에 해당하여 개인정보를 목적 외의 용도로 제3자에게 제공하는 경우에는 개인정보를 제공받는 자에게 이용 목적, 이용 방법, 그 밖에 필요한 사항에 대하여 제한을 하거나, 개인정보의 안전성 확보를 위하여 필요한 조치를 마련하도록 요청하여야 한다. 이 경우 요청을 받은 자는 개인정보의 안전성 확보를 위하여 필요한 조치를 하여야 한다.</p>
시행령	<p>제15조(개인정보의 목적 외 이용 또는 제3자 제공의 관리) 공공기관은 법 제18조제2항에 따라 개인정보를 목적 외의 용도로 이용하거나 이를 제3자에게 제공하는 경우에는 다음 각 호의 사항을 보호위원회가 정하여 고시하는 개인정보의 목적 외 이용 및 제3자 제공 대장에 기록하고 관리해야 한다.</p> <ol style="list-style-type: none"> 1. 이용하거나 제공하는 개인정보 또는 개인정보파일의 명칭 2. 이용기관 또는 제공받는 기관의 명칭 3. 이용 목적 또는 제공받는 목적 4. 이용 또는 제공의 법적 근거 5. 이용하거나 제공하는 개인정보의 항목 6. 이용 또는 제공의 날짜, 주기 또는 기간 7. 이용하거나 제공하는 형태 8. 법 제18조제5항에 따라 제한을 하거나 필요한 조치를 마련할 것을 요청한 경우에는 그 내용
고시	<p>개인정보 처리 방법에 관한 고시(보호위원회고시 제2020-7호)</p> <p>제2조(공공기관에 의한 개인정보의 목적 외 이용 또는 제3자 제공의 공고) 제2조(공공기관에 의한 개인정보의 목적 외 이용 또는 제3자 제공의 공고) 공공기관은 개인정보를 목적 외의 용도로 이용하거나 제3자에게 제공(이하 “목적외이용등”이라 한다)하는 경우에는 「개인정보 보호법」(이하 “법”이라 한다) 제18조제4항에 따라 개인정보를 목적외이용등을 한 날부터 30일 이내에 다음 각 호의 사항을 관보 또는 인터넷 홈페이지에 게재하여야 한다. 이 경우 인터넷 홈페이지에 게재할 때에는 10일 이상 계속 게재하되, 게재를 시작하는 날은 목적외이용등을 한 날부터 30일 이내여야 한다.</p> <ol style="list-style-type: none"> 1. 목적외이용등을 한 날짜

	<p>2. 목적외이용등의 법적 근거</p> <p>3. 목적외이용등의 목적</p> <p>4. 목적외이용등을 한 개인정보의 항목(구성)</p> <p>제3조(개인정보보호 업무 관련 장부 및 문서 서식) ① 법 제18조제2항과 「개인정보 보호법 시행령」(이하 “영”이라 한다) 제15조에 따른 개인정보의 목적 외 이용 및 제3자 제공 대장은 별지 제1호서식과 같다.</p>
표준지침	<p>제8조(개인정보의 목적 외 이용·제공) ① 개인정보처리자가 법 제18조제2항에 따라 개인정보를 목적 외의 용도로 제3자에게 제공하는 경우에는 개인정보를 제공받는 자에게 이용 목적, 이용 방법, 이용 기간, 이용 형태 등을 제한하거나, 개인정보의 안전성 확보를 위하여 필요한 구체적인 조치를 마련하도록 문서(전자문서를 포함한다. 이하 같다)로 요청하여야 한다. 이 경우 요청을 받은 자는 그에 따른 조치를 취하고 그 사실을 개인정보를 제공한 개인정보처리자에게 문서로 알려야 한다.</p> <p>② 법 제18조제2항에 따라 개인정보를 목적 외의 용도로 제3자에게 제공하는 자는 해당 개인정보를 제공받는 자와 개인정보의 안전성 확보 조치에 관한 책임관계를 명확히 하여야 한다.</p> <p>③ 개인정보처리자가 법 제18조제3항제1호에 따라 정보주체에게 개인정보를 제공받는 자를 알리는 경우에는 그 성명(법인 또는 단체인 경우에는 그 명칭)과 연락처를 함께 알려야 한다.</p>

1. 개인정보의 목적 외 이용·제공 금지

개인정보처리자는 정보주체에게 이용·제공의 목적을 고지하고 동의를 받은 범위나 이 법 또는 다른 법령에 의하여 이용·제공이 허용된 범위를 벗어나서 개인정보를 이용하거나 제공해서는 안 된다.

참고 1 목적 외 이용사례

- 공무원들에게 업무용으로 발급한 이메일 계정 주소로 사전 동의절차 없이 교육 등 마케팅 홍보자료를 발송한 경우
- 조세 담당 공무원이 자신과 채권·채무 관계로 소송 중인 사람에 관한 납세정보를 조회하여 소송에 이용한 경우
- 상품배송을 목적으로 수집한 개인정보를 사전에 동의 받지 않은 자사의 별도 상품·서비스의 홍보에 이용
- 고객 만족도 조사, 판촉행사, 경품행사에 응모하기 위하여 입력한 개인정보를 사전에 동의 받지 않고 자사의 할인판매행사 안내용 광고물 발송에 이용
- A/S센터에서 고객 불만 및 불편 사항을 처리하기 위해 수집한 개인정보를 자사의 신상품 광고에 이용
- 공개된 개인정보의 성격과 공개 취지 등에 비추어 그 공개된 목적을 넘어 DB마케팅을 위하여 수집한 후 이용하는 행위

참고 2 목적 외 제공 사례

- 주민센터 복지카드 담당 공무원이 복지카드 신청자의 개인정보(홍보 마케팅 등으로 개인정보 제공을 동의하지 않은 경우)를 정보주체의 동의 없이 사설학습지 회사에 제공
- 홈쇼핑 회사가 주문 상품을 배달하기 위해 수집한 고객정보를 정보주체의 동의 없이 계열 콘도미니엄사에 제공하여 콘도미니엄 판매용 홍보자료 발송에 활용

2. 목적 외 이용·제공 금지 예외 사유

제18조제2항 각 호는 개인정보를 목적 외의 용도로 이용하거나 제3자에게 제공할 수 있는 예외적인 사유를 규정하고 있다. 이 경우에도 정보주체 또는 제3자의 이익을 부당하게 침해할 우려가 있을 때에는 개인정보를 목적 외의 용도로 이용하거나 제3자에게 제공할 수 없다.

다만, 이용자의 개인정보를 처리하는 정보통신서비스 제공자의 경우 제1호 및 제2호의 예외 사유만 적용된다. 한편, 제5호부터 제9호까지의 사유는 공공기관이 처리하는 개인정보를 목적 외로 이용하거나 제3자에게 제공하는 경우에 한정되므로 개인정보처리자가 공공기관인 경우에만 해당 조항에 따라 개인정보를 제3자에게 제공할 수 있다(헌법재판소 2018. 8. 30. 2016헌마483 결정 참고). 목적 외로 제공받는 제3자는 공공기관이 아니어도 무방하다(보호위원회 결정 2019. 1. 28. 제2019-02-014호).

가 정보주체의 별도의 동의가 있는 경우

개인정보를 수집 목적을 넘어 이용하거나, 제공하는 경우 다른 개인정보의 처리에 대한 동의와 분리해서 목적 외 이용·제공에 대한 별도의 동의를 받아야 한다.

나 다른 법률에 특별한 규정이 있는 경우

다른 법률에 개인정보의 목적 외 이용·제공에 대한 특별한 규정이 있는 경우에는 그에 따른 목적 외 이용·제공이 허용된다.

‘법률’로 한정되어 있으므로 시행령·시행규칙에만 관련 규정이 있는 경우에는 제2호에 따른 목적 외 이용·제공이 허용되지 않는다. 다만 법률에 위임근거가 있고 이에 따라 시행령·시행규칙에 제공 관련 규정이 있는 경우는 허용된다.

또한 목적 외 이용·제공과 관련하여 ‘특별한 규정이 있는 경우’에 한하므로, 법률에서 개인정보의 목적 외 이용·제공을 구체적으로 허용하고 있어야 하며, ‘법령상 의무이행’과 같이 포괄적으로 규정된 경우에는 허용되지 않는다. 다만, 해당 법률에 목적 외 이용·제공되

는 개인정보의 항목이 구체적으로 열거되어 있지 않더라도 당해 업무의 목적, 성격 등을 고려 하였을 때 목적 외 이용·제공 대상에 개인정보가 포함될 것이 합리적으로 예견되는 경우에는 허용될 수 있다(보호위원회 결정 제2018-14-133호 참고).

참고 다른 법률의 특별한 규정 사례

- 소득세법 제170조에 따른 세무공무원의 조사, 질문
- 감사원법 제27조에 따른 감사원의 자료 요구
- 국가유공자 등 예우 및 지원에 관한 법률 제77조에 따른 국가보훈처장의 자료제공 요구
- 병역법 제81조제2항에 따른 병무청장의 자료제공 요구
- 부패방지 및 국민권익위원회 설치와 운영에 관한 법률 제42조제1항 및 제3항에 따른 국민권익위원회의 자료제출 요청 등
- 질서행위위반규제법 제22조 제1항에 따른 관계인에 대한 자료제출 요구 및 참고인 진술 청취
- 국회법 제128조 제1항, 국정감사 및 조사에 관한 법률 제10조 제1항의 보고 또는 서류제출 요구
- 공공기관의 정보공개에 관한 법률 제5조 제1항에 의한 정보공개청구의 대상이 되는 정보(공공기관이 보유·관리하는 정보)로서 동법 제9조 제1항 제6호 단서 각 목에 정한 비공개대상정보 제외 사유에 해당하는 경우

다 급박한 생명·신체·재산상 이익을 위하여 필요한 경우

정보주체 또는 그 법정대리인이 의사표시를 할 수 없는 상태에 있거나 주소불명 등으로 사전 동의를 받을 수 없는 경우로서 명백히 제3자의 급박한 생명·신체·재산상의 이익을 위하여 필요하다고 인정되는 경우에는 그에 따른 목적 외 이용·제공이 허용된다.

라 개인정보를 목적 외의 용도로 이용하거나 이를 제3자에게 제공하지 아니하면 다른 법률에서 정하는 소관 업무를 수행할 수 없는 경우로서 보호위원회의 심의·의결을 거친 경우

공공기관이 다른 법률에서 정하는 소관 업무를 수행하기 위하여 목적 외 이용 또는 제공이 불가피하게 필요한 경우가 있다. 소관 업무 수행이라는 목적 하에 개인정보 이용·제공을 무조건 허용하게 되면 남용의 소지가 많기 때문에 보호위원회의 심의·의결을 거치도록 하고 있다. 시행령·시행규칙에서 정하고 있는 소관업무로는 안 되고 반드시 ‘법률’에서 정하고 있는 업무이어야 한다. 다만 법률에 위임근거가 있고 이에 따라 시행령·시행규칙에 소관 업무가 규정된 경우는 허용된다.

마 조약, 그 밖의 국제협정의 이행

「헌법」 제6조는 헌법에 의하여 체결, 공포된 조약과 일반적으로 승인된 국제법규는

국내법과 같은 효력을 가진다고 규정하고 있다. 조약이란 국가 간의 문서에 의한 합의를 뜻하는데, 그 명칭이 조약이든, 조약 이외의 “협약, 협정, 규약, 선언, 의정서” 이든 그 명칭 여하를 불문하고 ‘국가 간의 문서에 의한 합의’ 이면 조약이 된다. 조약이 국내법과 동일한 효력을 가지면서 관련 규정이 상충할 때에는 특별법 우선적용의 원칙이 적용된다는 것이 일반적인 견해이다. 특별법은 일정한 사람·시간·장소에 대하여 그 효력이 미치는 것이므로, 조약의 체결 시에는 조약의 체결 당사국이 조약규정을 그대로 적용하겠다는 의사 함치가 있는 것으로 보아야 할 것이므로 조약에 대해 특별법적 지위를 인정할 수 있다. 따라서 법률의 효력을 가지는 조약이나 국제협정에서 개인정보의 목적 외 이용 또는 제공을 규정하고 있다면, 이러한 조약 등의 이행을 위해서는 정보주체의 동의 없이도 개인정보를 목적 외 이용 또는 제공할 수 있다.

바 범죄 수사와 공소의 제기 및 유지

개인정보처리자는 보유하고 있는 개인정보를 수집·이용 목적 이외의 용도로 제공하기 위해서는 다른 법률의 특별한 규정이 있거나 정보주체의 동의를 받아야 한다. 즉 공공기관 외의 개인정보처리자에 대해서는 비록 범죄 수사 목적이라 하더라도 원칙적으로 형사소송법 등의 규정에 따라서만 개인정보 제공을 요구할 수 있다.

그러나 공공기관의 경우 수사기관이 범죄 수사, 공소 제기 및 유지를 위해서 필요하다고 요청하는 경우 해당 개인정보를 정보주체의 별도의 동의 없이 제공할 수 있다. 이는 범죄수사 편의를 위해 공공기관이 보유하고 있는 개인정보에 대해서는 정보주체의 동의 없이 목적 외로 이용 또는 제공할 수 있게 하기 위한 것이다.

< 범죄수사, 공소제기 및 유지를 위한 경우의 예외 및 한계 필요성 >

- 범죄수사, 공소제기·유지, 형집행 등의 형사절차에 「개인정보 보호법」을 그대로 적용할 경우, 수사기밀이 유출되거나 정보주체의 정보공개·정정요구 등으로 수사에 장애를 초래하여 범죄예방과 처단이 불가능해 질 우려가 있다.
- 수사가 종결되어 공소가 제기되면 정보주체는 법원에서 자유롭게 수사기록을 열람하여 자신의 정보를 확인하는 것이 가능하고, 불기소처분된 경우는 정보공개청구를 통해 정보주체가 자신의 정보를 열람할 수 있으므로, 형사절차와 관련하여서는 「개인정보 보호법」을 적용하지 아니하더라도 정보주체의 정보보호에 소홀한 점이 없다고 보아야 할 것이다.
- 다만, 수사기관이 공공기관 이외의 기관으로부터도 개인정보를 무제한적으로 제공받을 수 있게 할 경우 오히려 정보주체의 보호가 약화될 수 있는 만큼 법 제18조제2항제7호는 공공기관으로부터만 개인정보를 제공받을 수 있도록 하여 정보주체의 개인정보를 두텁게 보호하고자 하였다.
- 이 경우에도 정보주체 또는 제3자의 이익을 부당하게 침해할 우려가 있는 경우에는 개인정보를 목적 외의 용도로 이용하거나 제3자에게 제공할 수 없다.

수사란 범죄의 혐의 유무를 명백히 하여 공소의 제기과 유지 여부를 결정하기 위하여 범인을 발견·확보하고 증거를 수집·보전하는 수사기관(검사, 사법경찰관리)의 활동을 말한다. 수사는 주로 공소 제기 전에 하는 것이 일반적이나 공소제기 후에도 공소유지를 위하여 또는 공소 유지 여부를 결정하기 위한 수사도 허용된다.

결정례 제18조 제2항 제7호에 따른 피내사자 개인정보 제공 가능 여부

내사는 범죄혐의의 유무를 확인하기 위하여 범죄 인지 전에 행해지는 수사기관 내부의 조사활동으로서 수사와 구분되는 개념이기 때문에, 법 제18조제2항제7호에 원칙적으로 해당하지 않는다. 그러나 범죄의 수사를 위하여 피내사자의 개인정보 제공이 불가피하다면 법 제18조제2항제7호에 해당할 수 있으며, 이 경우 정보주체 또는 제3자의 이익을 부당하게 침해할 우려가 없어야 하고, 범죄의 수사 목적에 필요한 최소한의 범위 내에서 개인정보가 제공되어야 할 것이다(보호위원회 결정 제2016-07-15호).

「형사소송법」에 따라 검사는 범죄의 혐의가 있다고 사료되는 때에는 범인, 범죄사실과 증거를 수사하여야 하고(제195조), 검사의 지휘를 받아 사법경찰관리는 범죄의 혐의가 있다고 인식하는 때에는 범인, 범죄사실과 증거에 관하여 수사를 개시·진행한다(제196조). 수사는 수사기관의 주관적 혐의에 의해 개시되는데, 수사개시의 원인인 수사의 단서는 고소, 고발, 자수, 진정, 범죄신고, 현행범인의 체포, 변사자의 검시, 불심검문, 기사, 소문 등이 있다.

수사는 임의수사에 의하고 강제수사는 법률에 규정된 경우에 한하여 예외적으로 허용된다(「형사소송법」 제199조). 임의수사에는 공무소 등에 대한 조회(「형사소송법」 제199조제2항), 피의자신문(「형사소송법」 제200조 및 제241조 이하), 피의자 이외의 제3자에 대한 조사(「형사소송법」 제221조제1항제1문), 감정·통역·번역의 위촉(「형사소송법」 제221조제2항) 등이 있으며, 이러한 임의수사의 원칙은 임의수사 자유의 원칙을 의미하는 것은 아니므로, 임의수사도 수사의 필요성과 상당성이 인정되어야만 적법한 수사라고 할 수 있다.

특히 임의수사를 위해 공무소 등에 조회를 하거나 공공기관에게 요청하는 자료에 개인정보가 포함되어 있다면 “범죄수사에 필요한 때”를 더욱 엄격히 해석함으로써 가능한 개인정보자기결정권에 대한 침해가 되지 않도록 해야 한다.

영장에 의하지 않는 경우에는 피의자가 죄를 범하였다고 의심할 만한 정황이 있고 해당 사건과 관계가 있다고 인정할 수 있는 경우에 한하여 극히 제한적으로 개인정보를 제공하여야 할 것이며, 범죄의 형태나 경중, 정보주체가 받을 불이익의 정도 등 제반 사정을 종합적으로 고려하여 개인정보 이용이 없이는 수사의 목적을 달성할 수 없는 경우에 한하여 극히 제한적으로 개인정보를 제공하여야 할 것이다.

이와 관련하여 「신용정보법」은 개인신용정보 제공의 근거를 법원이 발부한 영장에 두고 있으며(「신용정보법」 제32조제6항제5호), 영장을 발부받을 시간적 여유가 없을 급박한 경우에는 개인정보를 제공 받은 이후에 검사는 영장을 청구하고, 36시간 안에 영장을 받지 못한 경우에는 제공받은 개인신용정보를 폐기하도록 하고 있다(「신용정보법」 제32조제6항제6호). 따라서 수사기관이 「개인정보 보호법」상의 공공기관에 해당하는 신용정보회사등에 대해서 개인신용정보의 제공을 요청할 때에는 원칙적으로 영장에 의하여야 한다.

사 법원의 재판업무 수행

법원은 판결, 화해, 조정 등 재판 업무의 원활한 수행을 위해 공공기관이 보유하고 있는 개인정보에 대해 보정명령, 자료제출명령 등을 통해 정보주체의 동의 없이 목적 외로 이용 또는 제공할 수 있게 하고 있다.

아 형(刑) 및 감호, 보호처분의 집행

형, 보호·치료감호, 보호처분의 원활한 집행을 위하여 공공기관이 보유하고 있는 개인정보의 목적 외 이용 또는 제공을 허용하고 있다.

3. 목적 외 이용·제공 동의를 방법

가 별도의 동의

목적 외 이용·제공에 대하여 정보주체의 동의를 받을 때에는 당초 동의와 별도로 정보주체에게 동의를 받아야 한다. 목적 외 이용 또는 제공 동의는 당초의 동의 범위를 벗어난 이용 또는 제공에 대한 동의이므로 통상 당초 동의 이후에 발생한 새로운 필요에 따라 이루어지는 것이므로 개인정보처리에 대한 최초 동의 시에 함께 받을 수 없다고 보아야 할 것이다.

나 동의 획득 시 고지사항

수집한 개인정보를 수집목적의 범위를 벗어나 이용하기 위해서는 정보주체의 동의를 받아야 하며, 이 때 ① 개인정보의 이용목적 ② 이용하는 개인정보의 항목 ③ 개인정보의 보유 및 이용기간 ④ 동의거부권이 있다는 사실 및 동의거부에 따른 불이익에 관한 사항을 알려야 한다. 알려할 사항에 변경이 있는 때에도 이를 다시 알리고 동의를 받아야 한다.

수집·이용하고 있는 개인정보를 수집·이용 목적의 범위를 벗어나 제3자에게 제공하기 위해서는 정보주체의 별도의 동의가 필요하며, 이때 ① 개인정보를 제공받는 자의 성명(법인 또는 단체인 경우에는 그 명칭) ② 제공받는 자의 이용목적 ③ 제공하는 개인정보의 항목 ④ 제공받는 자의 개인정보 보유 및 이용 기간 ⑤ 동의거부권이 있다는 사실 및 동의거부에 따른 불이익을 정보주체에게 알려야 한다. 알려야 할 사항에 변경이 있는 때에도 이를 다시 알리고 동의를 받아야 한다.

4. 목적 외 이용·제공의 공개

공공기관이 개인정보를 목적 외로 이용하거나 제3자에게 제공하는 경우에는 목적 외 이용·제공을 한 날로부터 30일 이내에 목적 외 이용·제공의 법적 근거, 이용 또는 제공 일자·목적·항목에 관하여 관보 또는 인터넷 홈페이지에 게재하여야 한다. 다만, 정보주체의 동의를 받거나 범죄수사와 공소제기 및 유지를 위해 개인정보를 목적 외로 이용하거나 제공하는 경우에는 그러하지 아니하다.

5. 목적 외 제공 시 보호조치

개인정보처리자는 제2항 각 호의 어느 하나의 경우에 해당하여 개인정보를 목적 외의 용도로 제3자에게 제공하는 경우에는 개인정보를 제공받는 자에게 이용 목적, 이용 방법, 그 밖에 필요한 사항에 대하여 제한을 하거나, 개인정보의 안전성 확보를 위하여 필요한 조치를 마련하도록 요청하여야 한다. 이 경우 요청을 받은 자는 개인정보의 안전성 확보를 위하여 필요한 조치를 하여야 한다. 개인정보를 제공하는 자와 개인정보를 제공받는 자 사이에 개인정보의 안전성에 관한 책임관계를 명확히 하기 위해서이다.

개인정보처리자가 개인정보를 목적 외로 제3자에게 제공할 때에는 개인정보를 제공받는 자가 개인정보를 안전하게 처리하도록 이용 목적, 이용방법 등에 일정한 제한을 가하거나 제29조에 따른 안전성 확보조치를 강구하도록 요청하여야 한다. 개인정보처리자는 제공과 동시에 또는 필요한 경우 제공한 이후에 개인정보를 제공받는 자에게 이용 목적, 이용 방법, 이용 기간, 이용 형태 등을 제한하거나, 개인정보의 안전성 확보를 위하여 필요한 구체적인 조치를 마련하도록 문서(전자문서를 포함한다. 이하 같다)로 요청하여야 한다. 이 경우 요청을 받은 자는 그에 따른 조치를 취하고 그 사실을 개인정보를 제공한 개인정보처리자에게 문서로 알려야 한다(표준지침 제8조제1항).

< 개인정보의 단계별 규제수준 비교 >

구분	수집·이용 및 제공기준	목적 외 이용·제공 기준
공통기준		· 정보주체 또는 제3자의 이익을 부당하게 침해할 우려가 없는 범위 안에서만 목적 외 이용·제공이 가능함
동의	· 정보주체의 동의를 받은 경우 ⇒ 수집·이용 및 제공 가능	· 정보주체로부터 별도의 동의를 받은 경우 (모든 개인정보처리자)
법률규정	· 법률에 특별한 규정이 있거나 법령상 의무를 준수하기 위하여 불가피한 경우 ⇒ 수집 및 해당 목적범위 안에서 이용·제공 가능	· 다른 법률에 특별한 규정이 있는 경우 (모든 개인정보처리자)
공공기관 소관업무 수행	· 공공기관이 소관 업무의 수행을 위하여 불가피한 경우 ⇒ 수집 및 해당 목적범위 안에서 이용·제공 가능	· 개인정보를 목적 외로 이용하거나 제공하지 아니하면 다른 법률에서 정하는 소관 업무를 수행할 수 없는 경우로서 보호위원회의 심의를 거친 경우(공공기관만 적용)
계약이행	· 계약의 이행을 위하여 불가피하게 수반되는 경우 ⇒ 수집 및 해당 목적범위 안에서 이용 가능(제공 불가)	
정보주체 또는 제3자의 이익	· 정보주체 또는 제3자의 생명, 신체, 재산의 이익을 위하여 필요하다고 인정되는 경우로서 정보주체의 사전 동의를 받기 곤란한 경우 ⇒ 수집 및 해당 목적범위 안에서 이용·제공 가능	· 정보주체 또는 그 법정대리인이 의사표시를 할 수 없는 상태에 있거나 주소불명 등으로 사전 동의를 받을 수 없는 경우로서 명백히 정보주체 또는 제3자의 급박한 생명, 신체, 재산의 이익을 위하여 필요하다고 인정되는 경우 (정보통신서비스 제공자를 제외한 개인정보처리자)
개인정보처리자의 이익	· 개인정보처리자의 정당한 이익을 달성하기 위하여 필요한 경우로서 명백히 정보주체의 권리보다 우선하는 경우 ⇒ 수집 및 해당 목적범위 안에서 이용 가능(제공 불가)	
국제협정 이행		· 조약 그 밖의 국제협정의 이행을 위하여 외국정부 또는 국제기구에 제공하기 위하여 필요한 경우 (공공기관만 적용)
범죄수사 등		· 범죄의 수사 및 공소제기 및 유지를 위하여 필요한 경우(공공기관만 적용)
재판		· 법원의 재판업무 수행을 위하여 필요한 경우 (공공기관만 적용)

구분	수집·이용 및 제공기준	목적 외 이용·제공 기준
형·감호 집행		· 형 및 감호의 집행을 위하여 필요한 경우 (공공기관만 적용)

※ 정보통신서비스 제공자 등 특례 규정 내용은 미포함

한편, 민감정보 및 고유식별정보를 처리하는 경우에는 이에 관한 규정인 제23조, 제24조 및 제24조의2가 특별한 규정으로 적용되므로, 민감정보 및 고유식별정보의 처리에 대한 별도의 동의 또는 법령의 명시적 근거가 필요하다.

6. 다른 법률과의 관계

「신용정보법」은 각각 개인정보의 이용과 관련하여 수집한 목적을 넘어서 이용하지 못하도록 규정하고 있으므로, 신용정보이용·제공자 등은 개인정보를 목적 외 이용·제공하는 경우 이에 따라 처리하여야 한다. 다만, 「신용정보법」상 개인신용정보가 아닌 개인정보에 관하여는 「개인정보 보호법」의 적용을 받는다.

신용정보법	<p>제32조(개인신용정보의 제공·활용에 대한 동의) ① 신용정보제공·이용자가 개인 신용정보를 타인에게 제공하려는 경우에는 대통령령으로 정하는 바에 따라 해당 신용정보주체로부터 다음 각 호의 어느 하나에 해당하는 방식으로 개인신용정보를 제공할 때마다 미리 개별적으로 동의를 받아야 한다. 다만, 기존에 동의한 목적 또는 이용 범위에서 개인신용정보의 정확성·최신성을 유지하기 위한 경우에는 그러하지 아니하다.</p> <ol style="list-style-type: none"> 1. 서면 2. 「전자서명법」 제2조제3호에 따른 공인전자서명이 있는 전자문서(「전자거래기본법」 제2조제1호에 따른 전자문서를 말한다) 3. 개인신용정보의 제공 내용 및 제공 목적 등을 고려하여 정보 제공 동의의 안정성과 신뢰성이 확보될 수 있는 유무선 통신으로 개인비밀번호를 입력하는 방식 4. 유무선 통신으로 동의 내용을 해당 개인에게 알리고 동의를 받는 방법. 이 경우 본인 여부 및 동의 내용, 그에 대한 해당 개인의 답변을 음성녹음하는 등 증거자료를 확보·유지하여야 하며, 대통령령으로 정하는 바에 따른 사후 고지절차를 거친다. 5. 그 밖에 대통령령으로 정하는 방식 <p>② 개인신용평가회사, 개인사업자신용평가회사, 기업신용조사회회사 또는 신용정보집중기관으로부터 개인신용정보를 제공받으려는 자는 대통령령으로 정하는 바에 따라 해당 신용정보주체로부터 제1항 각 호의 어느 하나에 해당하는 방식으로 개인신용정보를 제공받을 때마다 개별적으로 동의(기존에 동의한 목적 또는 이용 범위에서 개인신용정보의 정확성·최신성을 유지하기 위한 경우는 제외한다)를 받아야 한다. 이 경우 개인신용정보를 제공받으려는 자는 개인신용정보의 조회 시 개인신용평점이 하락할 수 있는 때에는 해당 신용정보주체에게 이를</p>
-------	---

고지하여야 한다.

③ 개인신용평가회사, 개인사업자신용평가회사, 기업신용조회회사 또는 신용정보집중기관이 개인신용정보를 제2항에 따라 제공하는 경우에는 해당 개인신용정보를 제공받으려는 자가 제2항에 따른 동의를 받았는지를 대통령령으로 정하는 바에 따라 확인하여야 한다.

④ 신용정보회사등은 개인신용정보의 제공 및 활용과 관련하여 동의를 받을 때에는 대통령령으로 정하는 바에 따라 서비스 제공을 위하여 필수적 동의사항과 그 밖의 선택적 동의사항을 구분하여 설명한 후 각각 동의를 받아야 한다. 이 경우 필수적 동의사항은 서비스 제공과의 관련성을 설명하여야 하며, 선택적 동의사항은 정보제공에 동의하지 아니할 수 있다는 사실을 고지하여야 한다.

⑤ 신용정보회사등은 신용정보주체가 선택적 동의사항에 동의하지 아니한다는 이유로 신용정보주체에게 서비스의 제공을 거부하여서는 아니 된다.

⑥ 신용정보회사등(제9호의3을 적용하는 경우에는 데이터전문기관을 포함한다)이 개인신용정보를 제공하는 경우로서 다음 각 호의 어느 하나에 해당하는 경우에는 제1항부터 제5항까지를 적용하지 아니한다.

1. 신용정보회사 및 채권추심회사가 다른 신용정보회사 및 채권추심회사 또는 신용정보집중기관과 서로 집중관리·활용하기 위하여 제공하는 경우
2. 제17조제2항에 따라 신용정보의 처리를 위탁하기 위하여 제공하는 경우
3. 영업양도·분할·합병 등의 이유로 권리·의무의 전부 또는 일부를 이전하면서 그와 관련된 개인신용정보를 제공하는 경우
4. 채권추심(추심채권을 추심하는 경우만 해당한다), 인가·허가의 목적, 기업의 신용도 판단, 유가증권의 양수 등 대통령령으로 정하는 목적으로 사용하는 자에게 제공하는 경우
5. 법원의 제출명령 또는 법관이 발부한 영장에 따라 제공하는 경우
6. 범죄 때문에 피해자의 생명이나 신체에 심각한 위험 발생이 예상되는 등 긴급한 상황에서 제5호에 따른 법관의 영장을 발부받을 시간적 여유가 없는 경우로서 검사 또는 사법경찰관의 요구에 따라 제공하는 경우. 이 경우 개인신용정보를 제공받은 검사는 지체 없이 법관에게 영장을 청구하여야 하고, 사법경찰관은 검사에게 신청하여 검사의 청구로 영장을 청구하여야 하며, 개인신용정보를 제공받은 때부터 36시간 이내에 영장을 발부받지 못하면 지체 없이 제공받은 개인신용정보를 폐기하여야 한다.
7. 조세에 관한 법률에 따른 질문·검사 또는 조사를 위하여 관할 관서의 장이 서면으로 요구하거나 조세에 관한 법률에 따라 제출의무가 있는 과세자료의 제공을 요구함에 따라 제공하는 경우
8. 국제협약 등에 따라 외국의 금융감독기구에 금융회사가 가지고 있는 개인신용정보를 제공하는 경우
9. 제2조제1호의4나목 및 다목의 정보를 개인신용평가회사, 개인사업자신용평가회사, 기업신용등급제공업무·기술신용평가업무를 하는 기업신용조회회사 및 신용정보집중기관에 제공하거나 그로부터 제공받는 경우
- 9의2. 통계작성, 연구, 공익적 기록보존 등을 위하여 가명정보를 제공하는 경우. 이 경우 통계작성에는 시장조사 등 상업적 목적의 통계작성을 포함하며, 연구에는 산업적 연구를 포함한다.
- 9의3. 제17조의2제1항에 따른 정보집합물의 결합 목적으로 데이터전문기관에 개인신용정보를 제공하는 경우

9의4. 다음 각 목의 요소를 고려하여 당초 수집한 목적과 상충되지 아니하는 목적으로 개인신용정보를 제공하는 경우

가. 양 목적 간의 관련성

나. 신용정보회사등이 신용정보주체로부터 개인신용정보를 수집한 경우

다. 해당 개인신용정보의 제공이 신용정보주체에게 미치는 영향

라. 해당 개인신용정보에 대하여 가명처리를 하는 등 신용정보의 보안대책을 적절히 시행하였는지 여부

10. 이 법 및 다른 법률에 따라 제공하는 경우

11. 제1호부터 제10호까지의 규정에 준하는 경우로서 대통령령으로 정하는 경우

⑦ 제6항 각 호에 따라 개인신용정보를 타인에게 제공하려는 자 또는 제공받은 자는 대통령령으로 정하는 바에 따라 개인신용정보의 제공 사실 및 이유 등을 사전에 해당 신용정보주체에게 알려야 한다. 다만, 대통령령으로 정하는 불가피한 사유가 있는 경우에는 인터넷 홈페이지 게재 또는 그 밖에 유사한 방법을 통하여 사후에 알리거나 공시할 수 있다.

⑧ 제6항제3호에 따라 개인신용정보를 타인에게 제공하는 신용정보제공·이용자로서 대통령령으로 정하는 자는 제공하는 신용정보의 범위 등 대통령령으로 정하는 사항에 관하여 금융위원회의 승인을 받아야 한다.

⑨ 제8항에 따른 승인을 받아 개인신용정보를 제공받은 자는 해당 개인신용정보를 금융위원회가 정하는 바에 따라 현재 거래 중인 신용정보주체의 개인신용정보와 분리하여 관리하여야 한다.

⑩ 신용정보회사등이 개인신용정보를 제공하는 경우에는 금융위원회가 정하여 고시하는 바에 따라 개인신용정보를 제공받는 자의 신원(身元)과 이용 목적을 확인하여야 한다.

⑪ 개인신용정보를 제공한 신용정보제공·이용자는 제1항에 따라 미리 개별적 동의를 받았는지 여부 등에 대한 다름이 있는 경우 이를 증명하여야 한다.

제33조(개인신용정보의 이용) ① 개인신용정보는 다음 각 호의 어느 하나에 해당하는 경우에만 이용하여야 한다.

1. 해당 신용정보주체가 신청한 금융거래 등 상거래관계의 설정 및 유지 여부 등을 판단하기 위한 목적으로 이용하는 경우

2. 제2호의 목적 외의 다른 목적으로 이용하는 것에 대하여 신용정보주체로부터 동의를 받은 경우

3. 개인이 직접 제공한 개인신용정보(그 개인과의 상거래에서 생긴 신용정보를 포함한다)를 제공받은 목적으로 이용하는 경우(상품과 서비스를 소개하거나 그 구매를 권유할 목적으로 이용하는 경우는 제외한다)

4. 제32조제6항 각 호의 경우

5. 그 밖에 제1호부터 제4호까지의 규정에 준하는 경우로서 대통령령으로 정하는 경우

② 신용정보회사등이 개인의 질병, 상해 또는 그 밖에 이와 유사한 정보를 수집·조사하거나 제3자에게 제공하려면 미리 제32조 제1항 각 호의 방식으로 해당 개인의 동의를 받아야 하며, 대통령령으로 정하는 목적으로만 그 정보를 이용하여야 한다.

제34조(개인식별정보의 수집·이용 및 제공) 신용정보제공회사등이 개인을 식별하기 위하여 필요로 하는 정보로서 대통령령으로 정하는 정보를 수집·이용 및 제공하는 경우에는 제15조, 제32조 및 제33조를 준용한다.

7. 벌칙규정

위반행위	벌칙
개인정보를 목적 외로 이용하거나 제3자에게 제공한 자 및 그 사정을 알면서도 영리 또는 부정한 목적으로 개인정보를 제공받은 자(제18조제1항·제2항 위반)	5년 이하의 징역 또는 5천만원 이하의 벌금 (제71조제2호)
개인정보를 목적 외로 이용하거나 제3자에게 제공한 정보통신서비스 제공자등(제18조제1항·제2항 위반)	위반행위 관련 매출액의 100분의 3 이하 과징금 (제39조의15제1항제1호)
정보주체에 대한 고지의무 위반 (제18조제3항 위반)	3천만원 이하의 과태료 (제75조제2항제1호)

8. 질의응답

Q | 성형외과에서 성형 환자들의 성형 결과를 사진으로 촬영해 병원 홈페이지의 '성형 성공 사례'에 게시하는 경우에 문제가 없는지?

A | 병원에서 환자의 성형수술결과 사진을 홍보 목적으로 활용하기 위해서는 '촬영한 사진을 병원의 홍보 목적'으로 게재한다는 사실을 정보주체(환자)에게 명확히 알리고 동의를 얻어야 한다.
만일 수집한 개인정보를 별도의 고지·동의 절차 없이 홍보 목적으로 임의로 사용한다면 이는 '개인정보의 목적 외 이용 행위'에 해당한다.

Q | 학교 졸업앨범, 동창회 명부 등 공개 정보를 이용한 마케팅은 문제가 없는지?

A | 이른바 '공개된 개인정보'는 당초 공개된 목적 내에서만 이용할 수 있다. 예컨대 동창회 명부라면 원칙적으로 해당 회원들의 상호 연락 및 친목 도모 등을 위해 이용될 수 있지만, 회원의 동의를 얻지 않은 마케팅 행위 등에는 이용할 수 없다.

Q | 경찰서로부터 수사를 위하여 회원의 개인정보를 제출하여 달라는 요청을 받았다. 본인의 동의 없이 회원정보를 수사기관에 제공하여도 되는지?

A | · 사업자가 고객의 개인정보를 제3자에게 제공하기 위해서는 원칙적으로 고객의 동의를 얻어야 하나, 법률에 특별한 규정이 있는 경우에는 동의 없이 개인정보를 제공할 수 있다.
· 「형사소송법」, 「통신비밀보호법」, 「전기통신사업법」 등은 검찰·경찰 등 수사기관에서 수사목적에 위해 해당 법률이 정한 절차를 거쳐 요구하는 경우 관련 자료를 제출할 수 있도록 규정하고 있으므로, 고객 본인의 동의 없이 개인정보 제공이 허용된다(예: 「형사소송법」 제215조(압수, 수색, 검증)에 따른 절차).
· 그러나 범죄수사를 위해 관련 법률에 따라 개인정보를 제공하는 경우에도 수사에 필요한 최소한의 범위의 개인정보를 제공해야 한다.

제19조 | 개인정보를 제공받은 자의 이용·제공 제한

법률

제19조(개인정보를 제공받은 자의 이용·제공 제한) 개인정보처리자로부터 개인정보를 제공받은 자는 다음 각 호의 어느 하나에 해당하는 경우를 제외하고는 개인정보를 제공받은 목적 외의 용도로 이용하거나 이를 제3자에게 제공하여서는 아니 된다.

1. 정보주체로부터 별도의 동의를 받은 경우
2. 다른 법률에 특별한 규정이 있는 경우

1. 입법 취지

개인정보를 제공받은 자가 그 개인정보를 제한 없이 처리할 수 있다면 이는 개인정보 유출 또는 불법유통 등 정보주체에 관한 권리를 침해할 우려가 높아진다. 따라서 개인정보를 제공받는 자의 이용·제공에 대해서도 제한을 둘 필요가 있다.

2. 제공받는 자

개인정보처리자로부터 개인정보를 제공받은 자에 한정된다. 따라서 개인정보처리 업무를 위탁받은 수탁자에게는 본 조항이 적용되지 않는다.

3. 개인정보를 제공받은 자의 목적 외 이용·제공 금지

개인정보를 제공받은 자는 해당 개인정보를 제공하거나 제공받은 목적과 다른 용도로 이용하거나 제3자에게 제공하여서는 안 된다. 개인정보를 제공하는 자와 개인정보를 제공받는 자는 문서를 통해 개인정보를 제공하는 목적과 제공받는 목적을 구체화하는 것이 바람직하며, ① 개인정보를 제공받는 자의 성명(법인 또는 단체인 경우에는 그 명칭) ② 제공받는 자의 이용목적 ③ 제공하는 개인정보의 항목 ④ 제공받는 자의 개인정보 보유 및 이용기간 ⑤ 동의거부권이 있다는 사실 및 동의거부에 따른 불이익을 정보주체에게 알려야 한다.

한편, 제19조는 개인정보를 제공받은 자의 목적 외 이용·제공을 금지하는 규정일 뿐 개인정보를 제공받은 자의 목적 내 이용·제공을 금지하는 규정은 아니다. 따라서 개인정보를 제공받은 자는 제17조제1항제2호의 사유가 있는 경우 수집한 정보를 해당 수집 목적의 범위 내에서 정보주체의 동의 없이 제3자에게 제공할 수 있다.

4. 예외사유

개인정보처리자로부터 개인정보를 제공받은 자가 그 개인정보를 목적 외로 이용하거나 제공하는 경우에는 제18조가 적용되지 않고 제19조가 적용된다. 따라서 개인정보처리자로부터 개인정보를 제공받은 자는 제19조 각 호에 따라 정보주체로부터 별도의 동의를 받았거나 다른 법률에 특별한 규정이 있는 경우에는 예외적으로 개인정보를 제공받은 목적 외의 용도로 이용하거나 수집·이용 목적 범위를 벗어나 이를 제3자에게 제공할 수 있다.

5. 다른 법률과의 관계

다른 법률에서는 ‘개인정보를 제공받은 자의 이용·제공 제한’ 과 관련한 규정을 두고 있지 않으므로, 신용정보이용·제공자 등은 이 법에 따라 개인정보처리자로부터 개인정보를 제공받은 경우, 정보주체의 별도의 동의 또는 다른 법률에 특별한 규정이 있지 않는 한 개인정보를 제공받은 목적 외의 용도로 이용하거나 이를 제3자에게 제공하여서는 안 된다.

6. 벌칙규정

위반행위	벌칙
제공받은 개인정보를 목적 외로 이용하거나 제3자에게 제공한 자 및 그 사정을 알면서도 영리 또는 부정한 목적으로 개인정보를 제공받은 자 (제19조 위반)	5년 이하의 징역 또는 5천만원 이하의 벌금 (제71조제2호)
제공받은 개인정보를 목적 외의 용도로 이용하거나 제3자에게 제공한 정보통신서비스 제공자등 (제19조 위반)	위반행위 관련 매출액의 100분의 3이하 과징금 (제39조의15제1항제1호)

제20조 | 정보주체 이외로부터 수집한 개인정보의 수집 출처 등 고지

법률

제20조(정보주체 이외로부터 수집한 개인정보의 수집 출처 등 고지) ① 개인정보처리자가 정보주체 이외로부터 수집한 개인정보를 처리하는 때에는 정보주체의 요구가 있으면 즉시 다음 각 호의 모든 사항을 정보주체에게 알려야 한다.

1. 개인정보의 수집 출처
 2. 개인정보의 처리 목적
 3. 제37조에 따른 개인정보 처리의 정지를 요구할 권리가 있다는 사실
- ② 제1항에도 불구하고 처리하는 개인정보의 종류·규모, 종업원 수 및 매출액 규모 등을 고려하여 대통령령으로 정하는 기준에 해당하는 개인정보처리자가 제17조제1항제1호에 따라 정보주체 이외로부터 개인정보를 수집하여 처리하는 때에는 제1항 각 호의 모든 사항을 정보주체에게 알려야 한다. 다만, 개인정보처리자가 수집한 정보에 연락처 등 정보주체에게 알릴 수 있는 개인정보가 포함되지 아니한 경우에는 그러하지 아니하다.
- ③ 제2항 본문에 따라 알리는 경우 정보주체에게 알리는 시기·방법 및 절차 등 필요한 사항은 대통령령으로 정한다.
- ④ 제1항과 제2항 본문은 다음 각 호의 어느 하나에 해당하는 경우에는 적용하지 아니한다. 다만, 이 법에 따른 정보주체의 권리보다 명백히 우선하는 경우에 한한다.
1. 고지를 요구하는 대상이 되는 개인정보가 제32조제2항 각 호의 어느 하나에 해당하는 개인정보파일에 포함되어 있는 경우
 2. 고지로 인하여 다른 사람의 생명·신체를 해할 우려가 있거나 다른 사람의 재산과 그 밖의 이익을 부당하게 침해할 우려가 있는 경우

시행령

제15조의2(개인정보 수집 출처 등 고지 대상·방법·절차) ① 법 제20조제2항 본문에서 “대통령령으로 정하는 기준에 해당하는 개인정보처리자”란 다음 각 호의 어느 하나에 해당하는 개인정보처리자를 말한다.

1. 5만명 이상의 정보주체에 관하여 법 제23조에 따른 민감정보(이하 “민감정보”라 한다) 또는 법 제24조제1항에 따른 고유식별정보(이하 “고유식별정보”라 한다)를 처리하는 자
 2. 100만명 이상의 정보주체에 관하여 개인정보를 처리하는 자
- ② 제1항 각 호의 어느 하나에 해당하는 개인정보처리자는 법 제20조제1항 각 호의 사항을 서면·전화·문자전송·전자우편 등 정보주체가 쉽게 알 수 있는 방법으로 개인정보를 제공받은 날부터 3개월 이내에 정보주체에게 알려야 한다. 다만, 법 제17조제2항제1호부터 제4호까지의 사항에 대하여 같은 조 제1항제1호에 따라 정보주체의 동의를 받은 범위에서 연 2회 이상 주기적으로 개인정보를 제공받아 처리하는 경우에는 개인정보를 제공받은 날부터 3개월 이내에 정보주체에게 알리거나 그 동의를 받은 날부터 기산하

	<p>여 연 1회 이상 정보주체에게 알려야 한다.</p> <p>③ 제1항 각 호의 어느 하나에 해당하는 개인정보처리자는 제2항에 따라 알린 경우 다음 각 호의 사항을 법 제21조 또는 제37조제4항에 따라 해당 개인정보를 파기할 때까지 보관·관리하여야 한다.</p> <ol style="list-style-type: none"> 1. 정보주체에게 알린 사실 2. 알린 시기 3. 알린 방법
표준지침	<p>제9조(개인정보 수집 출처 등 고지) ① 개인정보처리자가 정보주체 이외로부터 수집한 개인정보를 처리하는 때에는 정당한 사유가 없는 한 정보주체의 요구가 있는 날로부터 3일 이내에 법 제20조제1항 각 호의 모든 사항을 정보주체에게 알려야 한다. 다만, 다음 각 호의 어느 하나에 해당하는 경우에는 그러하지 아니 하다.</p> <ol style="list-style-type: none"> 1. 고지를 요구하는 대상이 되는 개인정보가 법 제32조제2항 각 호의 어느 하나에 해당하는 개인정보파일에 포함되어 있는 경우 2. 고지로 인하여 다른 사람의 생명·신체를 해할 우려가 있거나 다른 사람의 재산과 그 밖의 이익을 부당하게 침해할 우려가 있는 경우 <p>② 개인정보처리자는 제1항 단서에 따라 제1항 전문에 따른 정보주체의 요구를 거부하는 경우에는 정당한 사유가 없는 한 정보주체의 요구가 있는 날로부터 3일 이내에 그 거부의 근거와 사유를 정보주체에게 알려야 한다.</p>

1. 입법취지

제20조제1항의 입법취지는 개인정보를 공개된 출처로부터 수집하거나 본인이 아닌 제3자로부터 수집하여 처리하는 경우에 당해 정보주체에게 수집·이용 목적 등을 알리는 것이 불가능한 경우가 많으므로 정보주체의 요구가 있는 때 출처 등을 고지하도록 한 것이다. 그러나 정보주체의 입장에서 보면 본인의 개인정보가 공개된 출처로부터 수집되거나 본인이 아닌 제3자로부터 수집된 경우 이러한 사실을 아는 것이 현실적으로 어려운 측면이 있다. 따라서 동조 제2항은 대통령이 정하는 기준에 해당하는 대량의 개인정보처리자에게 정보주체 이외로부터 수집한 개인정보의 출처, 처리 목적 및 개인정보 처리정지를 요구할 수 있는 권리가 있다는 사실을 정보주체에게 알리도록 한 것이다.

2. 정보주체 이외의 의미

정보주체 이외로부터 수집한 개인정보에는 제3자로부터 제공받은 정보, 신문·잡지·인터넷 등에 공개되어 있어 수집한 정보 등이 해당된다. 예를 들어, 인물DB 사업자가 학교·

기관 홈페이지 등에 공개된 자료를 통하여 개인정보를 수집하는 경우가 이에 해당한다. 그러나 자체적으로 생산하거나 생성된 정보는 제외한다.

3. 고지시기 및 고지사항

가 정보주체의 요구가 있는 경우

수집출처 등의 고지는 정보주체의 요구가 있는 때에 하면 된다. 정보주체의 요구가 있으면 개인정보의 ① 수집 출처 ② 처리 목적 ③ 제37조에 따른 개인정보 처리의 정지를 요구할 권리가 있다는 사실을 요구를 받은 날부터 3일 이내에 알려야 한다. 따라서 개인정보 처리자는 개인정보의 수집출처를 관리하고 있어야 한다.

나 대량의 개인정보처리자인 경우

개인정보처리자가 ① 5만명 이상의 정보주체에 관하여 법 제23조에 따른 민감정보 또는 법 제24조제1항에 따른 고유식별정보를 처리하는 자 또는 ② 100만 명 이상의 정보주체에 관하여 개인정보를 처리하는 자 중 어느 하나에 해당하는 경우에는 정보주체의 요구가 없더라도 ① 수집 출처 ② 처리 목적 ③ 제37조에 따른 개인정보 처리의 정지를 요구할 권리가 있다는 사실을 개인정보를 제공받은 후 3개월 이내에 정보주체에게 알려야 한다. 이 경우, 서면·전화·문자전송·전자우편 등 정보주체가 쉽게 알 수 있는 방법으로 알려야 하고, 정보주체에게 알린 사실을(시기 및 방법을 포함한다) 해당 정보를 파기할 때까지 관리하여야 한다.

다만, 제20조제2항은 법 제17조제1항제1호에 따라 정보주체의 동의를 받아 개인정보를 제공한 개인정보처리자로부터 수집한 개인정보에 대해서만 적용되므로 「신용정보법」에 따라 동의를 받아 개인정보를 제공한 자로부터 수집한 개인정보 또는 법령에 따라 제공한 개인정보에 대해서는 적용되지 아니한다.

한편, 정보통신서비스 제공자등은 「개인정보 보호법」 상 개인정보처리자에 해당한다. 따라서 정보통신서비스 제공자등이 다른 개인정보처리자(정보통신서비스 제공자를 포함한다)로부터 제17조제1항제1호에 따라 제공받은 개인정보에 대해서는 제20조제2항에 따라 해당 개인정보의 주체에게 수집 출처 등을 고지하여야 한다.

또한 개인정보처리자가 수집한 정보에 연락처 등 정보주체에게 알릴 수 있는 개인정보가 포함되지 아니한 경우에는 알리지 않아도 된다.

4. 고지거부 사유

고지 대상이 되는 개인정보가 제32조제2항 각 호의 어느 하나에 해당하는 개인정보파일 에 포함되어 있는 경우 개인정보처리자는 고지하지 않을 수 있다. 다만 제20조제1항에 따른 정보주체의 요구를 거부할 경우 개인정보처리자는 거부의 근거와 사유를 정보주체의 요구가 있는 날로부터 3일 이내에 알려야 한다(표준지침 제9조제2항). 이 법에 따른 정보주체의 권리보다 명백히 우선하는 경우에 한한다.

또한 고지로 인하여 다른 사람의 생명·신체를 해할 우려가 있거나 다른 사람의 재산과 그 밖의 이익을 부당하게 침해할 우려가 있는 때에도 개인정보처리자는 정보주체의 고지 요구를 거부할 수 있다. 예컨대 수사기관이 제보자 또는 참고인의 신분을 피의자에게 알릴 경우 생명·신체의 위험이 따를 수도 있으므로 개인정보의 출처 고지를 거부할 수 있다. 다만, 이 법에 따른 정보주체의 권리보다 명백히 우선하는 경우에 한한다. 이 경우에도 개인정보처리자는 거부의 근거와 사유를 정보주체의 요구가 있는 날로부터 3일 이내에 알려야 한다(표준지침 제9조제2항).

5. 다른 법률과의 관계

「신용정보법」은 정보주체 이외로부터 개인정보를 수집하는 경우 정보주체에 대한 수집출처 등의 고지의무를 규정하고 있지 않으므로, 이에 관하여 「개인정보 보호법」의 적용을 받는다.

6. 가명정보의 적용 제외

제20조는 가명정보의 처리에는 적용되지 않는다(제28조의7).

7. 벌칙규정

위반행위	벌칙
정보주체에게 개인정보의 수집 출처 및 목적, 개인정보 처리의 정지를 요구할 권리가 있다는 사실을 알리지 아니한 자 (제20조제1항, 제2항 위반)	3천만원 이하 과태료 (제75조제2항제3호)

제21조 | 개인정보의 파기

<p>법률</p>	<p>제21조(개인정보의 파기) ① 개인정보처리자는 보유기간의 경과, 개인정보의 처리 목적 달성 등 그 개인정보가 불필요하게 되었을 때에는 지체 없이 그 개인정보를 파기하여야 한다. 다만, 다른 법령에 따라 보존하여야 하는 경우에는 그러하지 아니하다.</p> <p>② 개인정보처리자가 제1항에 따라 개인정보를 파기할 때에는 복구 또는 재생되지 아니하도록 조치하여야 한다.</p> <p>③ 개인정보처리자가 제1항 단서에 따라 개인정보를 파기하지 아니하고 보존하여야 하는 경우에는 해당 개인정보 또는 개인정보파일을 다른 개인정보와 분리하여서 저장·관리하여야 한다.</p> <p>④ 개인정보의 파기방법 및 절차 등에 필요한 사항은 대통령령으로 정한다.</p>
<p>시행령</p>	<p>제16조(개인정보의 파기방법) ① 개인정보처리자는 법 제21조에 따라 개인정보를 파기할 때에는 다음 각 호의 구분에 따른 방법으로 하여야 한다.</p> <ol style="list-style-type: none"> 1. 전자적 파일 형태인 경우: 복원이 불가능한 방법으로 영구 삭제 2. 제1호 외의 기록물, 인쇄물, 서면, 그 밖의 기록매체인 경우: 파쇄 또는 소각 <p>② 제1항에 따른 개인정보의 안전한 파기에 관한 세부 사항은 보호위원회가 정하여 고시한다.</p>
<p>표준지침</p>	<p>제10조(개인정보의 파기방법 및 절차) ① 개인정보처리자는 개인정보의 보유 기간이 경과하거나 개인정보의 처리 목적 달성, 해당 서비스의 폐지, 사업의 종료 등 그 개인정보가 불필요하게 되었을 때에는 정당한 사유가 없는 한 그로부터 5일 이내에 그 개인정보를 파기하여야 한다.</p> <p>② 영 제16조제1항제1호의 ‘복원이 불가능한 방법’이란 현재의 기술 수준에서 사회통념상 적정한 비용으로 파기한 개인정보의 복원이 불가능하도록 조치하는 방법을 말한다.</p> <p>③ 개인정보처리자는 개인정보의 파기에 관한 사항을 기록·관리하여야 한다.</p> <p>④ 개인정보 보호책임자는 개인정보 파기 시행 후 파기 결과를 확인하여야 한다.</p> <p>⑤ 개인정보처리자 중 공공기관의 개인정보파일 파기에 관하여는 제55조 및 제56조를 적용한다.</p> <p>제11조(법령에 따른 개인정보의 보존) ① 개인정보처리자가 법 제21조제1항 단서에 따라 법령에 근거하여 개인정보를 파기하지 아니하고 보존하여야 하는 경우에는 물리적 또는 기술적 방법으로 분리하여서 저장·관리하여야 한다.</p> <p>② 제1항에 따라 개인정보를 분리하여 저장·관리하는 경우에는 개인정보 처리방침 등을 통하여 법령에 근거하여 해당 개인정보 또는 개인정보파일을 저장·관리한다는 점을 정보주체가 알 수 있도록 하여야 한다.</p>

개인정보를 수집한 목적이 달성된 경우에도 계속해서 보유할 경우 개인정보의 유출과 오용 가능성이 높아지므로 더 이상 개인정보가 불필요하게 된 때에는 이를 파기하도록 함으로써 개인정보를 안전하게 보호하려는 것이다.

개인정보처리자가 개인정보 보유기간을 고지하고 동의 받는 경우 그 보유기간을 정할 때에는 필요 최소한으로 정해야 한다. 이 경우 필요한 기간이라는 입증책임은 개인정보처리자가 부담한다(제16조).

1. 파기시기

개인정보처리자는 개인정보가 불필요하게 되었을 때에는 지체 없이 해당 개인정보를 파기해야 한다. “개인정보가 불필요하게 되었을 때”란 개인정보의 처리 목적이 달성되었거나, 해당 서비스의 폐지, 사업이 종료된 경우 등이 포함된다. 따라서 개인정보처리자는 처리목적이 달성되거나, 해당 서비스 및 사업이 종료된 경우, 정당한 사유가 없는 한 필요 없게 된 날로부터 근무일 기준 5일 이내에 개인정보를 파기하여야 한다(표준지침 제10조제1항). 개인정보의 보존 필요성이 있는지 여부는 객관적으로 판단하여야 하며 자의적으로 해석해서는 안 된다.

참고 불필요하게 된 때

- 개인정보처리자가 당초 고지하고 동의를 받았던 보유기간의 경과
- 동의를 받거나 법령 등에서 인정된 수집·이용·제공 목적의 달성
- 회원탈퇴, 제명, 계약관계 종료, 동의철회 등에 따른 개인정보처리의 법적 근거 소멸
- 개인정보처리자의 폐업·청산
- 대금 완제일이나 채권소멸시효기간의 만료

2. 파기방법

개인정보를 파기할 때에는 다시 복원하거나 재생할 수 없는 형태로 완벽하게 파기하여야 한다. 그런데 예를 들어 전자기적으로 기록된 개인정보는 비록 삭제하였다고 하더라도 복원기술을 적용할 경우에는 그 정보가 복구될 가능성도 있다. 따라서 말 그대로 ‘복원이 불가능한 방법’을 적용하기 위해서는 상당한 비용이 소요될 수도 있다. 이를 위하여 표준지침은 ‘복원이 불가능한 방법’이란 사회 통념상 현재의 기술 수준에서 적절한 비용이 소요되는 방법을 말하고 있다(표준지침 제10조제2항).

구체적으로, 하드디스크, CD/DVD, USB메모리 등의 매체에 전자기(電磁氣)적으로 기록

된 개인정보는 복원이 불가능한 방법으로 영구 삭제하여야 하며, 전용 소자장비를 이용하여 삭제하거나 데이터가 복원되지 않도록 덮어쓰기를 수행하는 등 다시 재생시킬 수 없는 기술적 방법으로 삭제하거나 물리적인 방법으로 매체를 파괴하여 복구할 수 없도록 하는 것이 이에 해당한다(영 제16조제1항제1호, 개인정보의 안전성 확보조치 기준 제13조제1항). 또한, 기록물, 인쇄물, 서면, 그 밖의 기록매체의 형태로 되어 있는 경우에는 물리적으로 파쇄하거나 소각하는 방법으로 해당 개인정보를 완전히 파괴하여야 한다(영 제16조제1항제2호, 개인정보의 안전성 확보조치 기준 제13조제1항).

한편, 개인정보처리자가 저장 중인 개인정보 중 보유기관이 경과한 일부 개인정보를 파기하는 경우와 같이 개인정보의 일부만 파기하는 경우 위의 방법으로 개인정보를 파기하는 것이 어려울 때에는 전자적 파일 형태인 경우 파기대상 개인정보를 삭제한 후 해당 정보가 복구 및 재생되지 않도록 관리 및 감독하여야 하고, 전자적 파일 외의 기록물, 인쇄물, 서면 및 기타 기록물인 경우 해당 부분을 마스킹, 천공 등으로 삭제하여야 한다(개인정보의 안전성 확보조치 기준 제13조제2항).

3. 파기절차

개인정보처리자는 개인정보의 파기에 관한 사항을 기록하고 관리하여야 한다. 보유목적 달성한 개인정보의 파기는 법적 의무사항이며 위반 시 벌칙이 부과되는 사항이므로 파기는 반드시 개인정보 보호책임자의 책임 하에 수행되어야 하며, 개인정보 보호책임자는 파기 결과를 확인하여야 한다(표준지침 제10조제4항).

4. 파기의무의 예외

개인정보처리자는 ‘다른 법령에 따라 보존해야 하는 경우’ 에는 예외적으로 개인정보를 파기하지 않아도 된다. 개인정보처리자가 개인정보를 파기하지 않고 보존하려고 하는 경우에는 그 법적 근거를 명확히 해야 한다.

채권소멸기간까지 개인정보를 보존할 수 있다고 하여 이미 요금정산이 끝난 소비자의 개인정보까지 보존하여서는 안 된다. 신용카드 이용고객의 신용관리를 이유로 회원의 동의 없이 탈퇴회원의 개인정보를 일정기간 보존하는 것도 파기의무 위반이다. 다른 법령에서 보존기간으로 정한 기간이 만료한 경우에는 지체 없이 파기하여야 한다.

개인정보처리자가 개인정보 보유기간을 고지하고 동의를 받는 경우 그 보유기간을 정할 때에는 필요 최소한으로 보유기간을 정해야 하며 이에 대한 입증책임은 개인정보처리자가 부담한다.

< 보존의무를 규정하고 있는 입법례 >

<p>전자상거래 등에서의 소비자보호에 관한 법률 제6조 및 같은 법 시행령 제6조</p>	<p>① 표시·광고에 관한 기록 : 6개월 ② 계약 또는 청약철회 등에 관한 기록 : 5년 ③ 대금결제 및 재화등의 공급에 관한 기록 : 5년 ④ 소비자의 불만 또는 분쟁처리에 관한 기록 : 3년</p>
<p>통신비밀보호법 제15조의2 및 같은 법 시행령 제41조</p>	<p>① 법 제2조제11호가목부터 라목까지 및 바목에 따른 통신사실확인자료 : 12개월 ② 위의 자료 중 시외·시내전화역무와 관련된 자료인 통신사실확인자료 : 6개월 ③ 법 제2조제11호마목 및 사목에 따른 통신사실확인자료(컴퓨터통신 또는 인터넷의 로그기록자료, 정보통신기기의 위치를 확인할 수 있는 접속지 추적자료) : 3개월</p>
<p>의료법 시행규칙 제15조</p>	<p>① 환자 명부 : 5년 ② 진료기록부 : 10년 ③ 처방전 : 2년 ④ 수술기록 : 10년 ⑤ 검사소견기록 : 5년 ⑥ 방사선사진 및 그 소견서 : 5년 ⑦ 간호기록부 : 5년 ⑧ 조산기록부 : 5년 ⑨ 진단서 등의 부분 (진단서·사망진단서 및 시체검안서 등을 따로 구분하여 보존할 것) : 3년</p>

5. 법령상 보관 의무가 있는 개인정보의 보존방법

개인정보처리자는 법령에 따라 개인정보를 파기하지 않고 보존하는 경우에는 물리적 또는 기술적 방법으로 해당 개인정보 또는 개인정보파일을 다른 개인정보와 분리해서 저장·관리하여야 한다(제21조제3항, 표준지침 제11조제1항). 미파기정보가 기존 개인정보와 혼재되어 있으면(예시 : 회원들을 대상으로 한 메일 발송시에 탈퇴 회원에게도 같이 발송) 개인정보의 목적 외 이용이나 유출, 오·남용의 위험성이 커지므로 이를 방지하기 위한 규정이다. 미파기 정보는 오로지 다른 법령에서 보존하도록 한 목적 범위 내에서만 처리 가능하도록 관리되어야 한다.

또한, 개인정보처리자는 법령에 근거하여 개인정보 또는 개인정보파일을 분리 저장·관리한다는 점을 개인정보 처리방침 등을 통하여 정보주체가 알 수 있도록 하여야 한다(표준지침 제11조제2항).

6. 다른 법률과의 관계

「신용정보법」은 신용정보제공·이용자에 대하여 금융거래 등 상거래관계가 종료된 날부터 최장 5년 이내(해당 기간 이전에 정보 수집·제공 등의 목적이 달성된 경우에는 그 목적이 달성된 날부터 3개월 이내)에 해당 신용정보주체의 개인신용정보를 관리대상에서 삭제하도록 규정하고 있으므로, 이에 관하여는 「신용정보법」 및 금융위원회의 관련 고시에서 정하는 바에 따른다.

신용정보법	<p>제21조(폐업 시 보유정보의 처리) 신용정보회사나 신용정보집중기관이 폐업하려는 경우에는 금융위원회가 정하여 고시하는 바에 따라 보유정보를 처분하거나 폐기하여야 한다.</p> <p>제20조의2(개인신용정보의 보유기간 등) ① 신용정보제공·이용자는 금융거래 등 상거래관계(고용관계는 제외한다. 이하 같다)가 종료된 날부터 금융위원회가 정하여 고시하는 기한까지 해당 신용정보주체의 개인신용정보가 안전하게 보호될 수 있도록 접근권한을 강화하는 등 대통령령으로 정하는 바에 따라 관리하여야 한다.</p> <p>② 신용정보제공·이용자는 금융거래 등 상거래관계가 종료된 날부터 최장 5년 이내(해당 기간 이전에 정보 수집·제공 등의 목적이 달성된 경우에는 그 목적이 달성된 날부터 3개월 이내)에 해당 신용정보주체의 개인신용정보를 관리대상에서 삭제하여야 한다. 다만, 다음 각 호의 경우에는 그러하지 아니하다.</p> <ol style="list-style-type: none"> 1. 다른 법률에 따른 의무를 이행하기 위하여 불가피한 경우 2. 개인의 급박한 생명·신체·재산의 이익을 위하여 필요하다고 인정되는 경우 3. 그 밖에 예금·보험금의 지급, 보험사기자의 재가입 방지를 위한 경우 등 개인신용정보를 보존할 필요가 있는 경우로서 대통령령으로 정하는 경우 <p>③ 신용정보제공·이용자가 제2항 단서에 따라 개인신용정보를 삭제하지 아니하고 보존하는 경우에는 현재 거래 중인 신용정보주체의 개인신용정보와 분리하는 등 대통령령으로 정하는 바에 따라 관리하여야 한다.</p> <p>④ 신용정보제공·이용자가 제3항에 따라 분리하여 보존하는 개인신용정보를 활용하는 경우에는 신용정보주체에게 통지하여야 한다.</p> <p>⑤ 제1항 및 제2항에 따른 개인신용정보의 종류, 관리기간, 삭제의 방법·절차 및 금융거래 등 상거래관계가 종료된 날의 기준 등은 대통령령으로 정한다.</p>
-------	--

7. 가명정보의 적용 제외

제21조는 가명정보를 파기하는 경우에는 적용되지 않는다(제28조의7).

8. 벌칙규정

위반행위	벌칙
개인정보 미파기 등 필요조치 위반 정보통신서비스 제공자등 (제21조제1항 위반)	2년 이하의 징역 또는 2천만원 이하의 벌금 (제73조 제1호의2)
개인정보 미파기 (제21조제1항 위반)	3천만원 이하 과태료 (제75조제2항제4호)
개인정보를 분리하여 저장·관리하지 아니한 경우 (제21조제3항 위반)	1천만원 이하 과태료 (제75조제4항제1호)

9. 질의 응답

Q | 고객이 TV홈쇼핑, 온라인 쇼핑몰을 통해 여행 상품에 대해 상담하였으나, 실제로 계약이 체결되지 않은 경우, 고객이 예약 후 취소한 경우 개인정보의 파기는 어떻게 해야 하는가?

A | TV홈쇼핑, 온라인 쇼핑몰로부터 제공받은 고객정보를 바탕으로 여행 상담 이후 계약 체결이 되지 않고 상담으로만 끝나는 경우라면 제공받은 고객정보는 지체 없이(5일 이내) 파기하여야 한다.
다만, 고객이 예약 후 취소한 경우라면 고객이 여행상품에 대한 비용결제는 하지 않았다면 지체 없이 파기하는 것이 바람직하고 고객이 여행상품에 대한 비용결제를 완료하였다면 환불 등 과정을 거쳐야 하므로 법적근거에 따라 그 기간 동안 보유해야 한다.

Q | 쇼핑몰에서 탈퇴한 회원들의 개인정보를 파기하려고 하는데, 일부 회원들은 할부 요금 아직 미납되었거나 제품 A/S 기간이 남아있다. 이러한 경우에는 어떻게 해야 하는가?

A | 사업자는 개인정보의 수집·이용 목적이 달성된 경우 등에는 5일 이내에 개인정보를 파기하여야 하나, 예외적으로 “다른 법률에 따라 개인정보를 보존하여야 하는 경우”에는 개인정보를 파기하지 않고 보존할 수 있다.
예를 들어, 전자상거래 등에서의 소비자 보호에 관한 법률 및 시행령에서는 대금결제 및 재화 공급에 관한 기록을 5년간 보관하도록 하고 있으므로, 질의와 같이 요금 미납, A/S 등에 해당하는 경우에는 동법에 의거 5년간 개인정보 보관이 가능하다.

Q | 할인마트의 고객들을 대상으로 경품추첨 이벤트를 실시하였는데, 이벤트 종료 후 이벤트 응모신청서는 어떻게 처리하면 되는가?

A | 경품추첨 이벤트가 종료되고 당첨자발표 및 경품배송까지 모두 종료되었다면, 그 이후에는 개인정보의 보유·이용기간에 대해 별도의 동의를 얻지 않은 한 5일 이내에 개인정보가 기재된 응모신청서를 파기하여야 한다.

Q | 학원에서 학생들의 개인정보 수집 동의서 징구 시, 개인정보 보유기간을 '학원을 폐쇄할 때까지'라고 정해도 되는지?

A | 학원은 원칙적으로 학습자가 퇴원 후, 수강목적 달성했으므로 지체 없이 해당 학습자의 개인정보를 모두 파기하여야 한다.
다만, 학원법에 따른 비치서류의 보관기간 준수와, 법인세 등의 증빙을 위하여 필요한 자료(전표, 영수증)는 별도로 분리하여 해당 법령에서 보관하도록 한 기간 동안 (국세기본법 5년) 정보주체의 동의 없이 보관할 수 있다.

제22조 | 동의를 받는 방법

법률

제22조(동의를 받는 방법) ① 개인정보처리자는 이 법에 따른 개인정보의 처리에 대하여 정보주체(제5항에 따른 법정대리인을 포함한다. 이하 이 조에서 같다)의 동의를 받을 때에는 각각의 동의 사항을 구분하여 정보주체가 이를 명확하게 인지할 수 있도록 알리고 각각 동의를 받아야 한다.

② 개인정보처리자는 제1항의 동의를 서면(「전자문서 및 전자거래 기본법」 제2조제1호에 따른 전자문서를 포함한다)으로 받을 때에는 개인정보의 수집·이용 목적, 수집·이용하려는 개인정보의 항목 등 대통령령으로 정하는 중요한 내용을 보호위원회가 고시로 정하는 방법에 따라 명확히 표시하여 알아보기 쉽게 하여야 한다.

③ 개인정보처리자는 제15조제1항제1호, 제17조제1항제1호, 제23조제1항제1호 및 제24조제1항제1호에 따라 개인정보의 처리에 대하여 정보주체의 동의를 받을 때에는 정보주체와의 계약 체결 등을 위하여 정보주체의 동의 없이 처리할 수 있는 개인정보와 정보주체의 동의가 필요한 개인정보를 구분하여야 한다. 이 경우 동의 없이 처리할 수 있는 개인정보라는 입증책임은 개인정보처리자가 부담한다.

④ 개인정보처리자는 정보주체에게 재화나 서비스를 홍보하거나 판매를 권유하기 위하여 개인정보의 처리에 대한 동의를 받으려는 때에는 정보주체가 이를 명확하게 인지할 수 있도록 알리고 동의를 받아야 한다.

⑤ 개인정보처리자는 정보주체가 제3항에 따라 선택적으로 동의할 수 있는 사항을 동의하지 아니하거나 제4항 및 제18조제2항제1호에 따른 동의를 하지 아니한다는 이유로 정보주체에게 재화 또는 서비스의 제공을 거부하여서는 아니 된다.

⑥ 개인정보처리자는 만 14세 미만 아동의 개인정보를 처리하기 위하여 이 법에 따른 동의를 받아야 할 때에는 그 법정대리인의 동의를 받아야 한다. 이 경우 법정대리인의 동의를 받기 위하여 필요한 최소한의 정보는 법정대리인의 동의 없이 해당 아동으로부터 직접 수집할 수 있다.

⑦ 제1항부터 제6항까지에서 규정한 사항 외에 정보주체의 동의를 받는 세부적인 방법 및 제6항에 따른 최소한의 정보의 내용에 관하여 필요한 사항은 개인정보의 수집매체 등을 고려하여 대통령령으로 정한다.

시행령

제17조(동의를 받는 방법) ① 개인정보처리자는 법 제22조에 따라 개인정보의 처리에 대하여 다음 각 호의 어느 하나에 해당하는 방법으로 정보주체의 동의를 받아야 한다.

1. 동의 내용이 적힌 서면을 정보주체에게 직접 발급하거나 우편 또는 팩스 등의 방법으로 전달하고, 정보주체가 서명하거나 날인한 동의서를 받는 방법

2. 전화를 통하여 동의 내용을 정보주체에게 알리고 동의의 의사표시를 확인하는 방법
3. 전화를 통하여 동의 내용을 정보주체에게 알리고 정보주체에게 인터넷주소 등을 통하여 동의 사항을 확인하도록 한 후 다시 전화를 통하여 그 동의 사항에 대한 동의의 의사표시를 확인하는 방법
4. 인터넷 홈페이지 등에 동의 내용을 게재하고 정보주체가 동의 여부를 표시하도록 하는 방법
5. 동의 내용이 적힌 전자우편을 발송하여 정보주체로부터 동의의 의사표시가 적힌 전자우편을 받는 방법
6. 그 밖에 제1호부터 제5호까지의 규정에 따른 방법에 준하는 방법으로 동의 내용을 알리고 동의의 의사표시를 확인하는 방법

② 법 제22조제2항에서 “대통령령으로 정하는 중요한 내용”이란 다음 각 호의 사항을 말한다.

1. 개인정보의 수집·이용 목적 중 재화나 서비스의 홍보 또는 판매 권유 등을 위하여 해당 개인정보를 이용하여 정보주체에게 연락할 수 있다는 사실
2. 처리하려는 개인정보의 항목 중 다음 각 목의 사항
 - 가. 제18조에 따른 민감정보
 - 나. 제19조제2호부터 제4호까지의 규정에 따른 여권번호, 운전면허의 면허번호 및 외국인등록번호

3. 개인정보의 보유 및 이용 기간(제공 시에는 제공받는 자의 보유 및 이용 기간을 말한다)

4. 개인정보를 제공받는 자 및 개인정보를 제공받는 자의 개인정보 이용 목적

③ 개인정보처리자가 정보주체로부터 법 제18조제2항제1호 및 제22조제4항에 따른 동의를 받거나 법 제22조제3항에 따라 선택적으로 동의할 수 있는 사항에 대한 동의를 받으려는 때에는 정보주체가 동의 여부를 선택할 수 있다는 사실을 명확하게 확인할 수 있도록 선택적으로 동의할 수 있는 사항 외의 사항과 구분하여 표시하여야 한다.

④ 개인정보처리자는 법 제22조제6항에 따라 만 14세 미만 아동의 법정대리인의 동의를 받기 위하여 해당 아동으로부터 직접 법정대리인의 성명·연락처에 관한 정보를 수집할 수 있다.

⑤ 중앙행정기관의 장은 제1항에 따른 동의방법 중 소관 분야의 개인정보처리자별 업무, 업종의 특성 및 정보주체의 수 등을 고려하여 적절한 동의방법에 관한 기준을 법 제12조제2항에 따른 개인정보 보호지침(이하 “개인정보 보호지침”이라 한다)으로 정하여 그 기준에 따라 동의를 받도록 개인정보처리자에게 권장할 수 있다.

제4조(서면 동의 시 중요한 내용의 표시 방법) 법 제22조제2항에서 “보호위원회가 고시로 정하는 방법”이란 다음 각 호의 방법을 말한다.

1. 글씨의 크기는 최소한 9포인트 이상으로서 다른 내용보다 20퍼센트 이상 크게 하여 알아보기 쉽게 할 것
2. 글씨의 색깔, 굵기 또는 밑줄 등을 통하여 그 내용이 명확히 표시되도록 할 것
3. 동의 사항이 많아 중요한 내용이 명확히 구분되기 어려운 경우에는 중요한 내용이 쉽게 확인될 수 있도록 그 밖의 내용과 별도로 구분하여 표시할 것

제12조(동의를 받는 방법) ① 개인정보처리자가 개인정보의 처리에 대하여 정보주체의 동의를 받을 때에는 정보주체의 동의 없이 처리할 수 있는 개인정보와 정보주체의 동의가 필요한 개인정보를 구분하여야 하며, 정보주체의 동의는 동의가 필요한 개인정보에 한한다. 이 경우 동의 없이 처리할 수 있는 개인정보라는 입증책임은 개인정보처리자가 부담한다.

② 개인정보처리자는 다음 각 호의 어느 하나에 해당하는 경우에는 정보주체에게 법 제18조제3항 각 호의 사항을 알리고 동의를 받아야 한다.

1. 개인정보를 수집·이용하고자 하는 경우로서 법 제15조제1항제2호 내지 제6호에 해당하지 않은 경우
2. 법 제18조제2항에 따라 개인정보를 수집 목적 외의 용도로 이용하거나 제공하고자 하는 경우
3. 법 제22조제3항에 해당하여 정보주체에게 재화나 서비스를 홍보하거나 판매를 권유하고자 하는 경우
4. 주민등록번호 외의 고유식별정보 처리가 필요한 경우로서 법령에 고유식별정보 처리 근거가 없는 경우
5. 민감정보를 처리하고자 하는 경우로서 법령에 민감정보 처리 근거가 없는 경우

③ 개인정보처리자는 제2항 각 호에 해당하여 개인정보를 처리하고자 하는 경우에는 정보주체에게 동의 또는 동의 거부를 선택할 수 있음을 명시적으로 알려야 한다.

④ 개인정보처리자는 법 제15조제1항제2호 내지 제6호에 따라 정보주체의 동의 없이 개인정보를 수집하는 경우에는 개인정보를 수집할 수 있는 법적 근거 등을 정보주체에게 알리기 위해 노력하여야 한다.

⑤ 개인정보처리자가 영 제17조제1항제2호의 규정에 따라 전화에 의한 동의와 관련하여 통화내용을 녹취할 때에는 녹취사실을 정보주체에게 알려야 한다.

⑥ 개인정보처리자가 친목단체를 운영하기 위하여 다음 각 호의 어느 하나에 해당하는 개인정보를 수집하는 경우에는 정보주체의 동의 없이 개인정보를 수집·이용할 수 있다.

1. 친목단체의 가입을 위한 성명, 연락처 및 친목단체의 회칙으로 정한 공통의 관심사나 목표와 관련된 인적 사항

- 2. 친목단체의 회비 등 친목유지를 위해 필요한 비용의 납부현황에 관한 사항
- 3. 친목단체의 활동에 대한 구성원의 참석여부 및 활동내용에 관한 사항
- 4. 기타 친목단체의 구성원 상호 간의 친교와 화합을 위해 구성원이 다른 구성원에게 알리기를 원하는 생일, 취향 및 가족의 애경사 등에 관한 사항

⑦ 개인정보처리자가 정보주체의 동의를 받기 위하여 동의서를 작성하는 경우에는 「개인정보 수집·제공 동의서 작성 가이드라인」을 준수하여야 한다.

제13조(법정대리인의 동의) ① 영 제17조제3항에 따라 개인정보처리자가 법정대리인의 성명·연락처를 수집할 때에는 해당 아동에게 자신의 신분과 연락처, 법정대리인의 성명과 연락처를 수집하고자 하는 이유를 알려야 한다.

② 개인정보처리자는 법 제22조제5항에 따라 수집한 법정대리인의 개인정보를 법정대리인의 동의를 얻기 위한 목적으로만 이용하여야 하며, 법정대리인의 동의 거부가 있거나 법정대리인의 동의 의사가 확인되지 않는 경우 수집일로부터 5일 이내에 파기해야 한다.

정보주체는 개인정보 처리에 대한 동의 여부를 결정하고 선택할 수 있는 권리가 보장되어 있으나, 실제로는 정보주체의 동의가 강제되는 경우가 많아 정보주체의 개인정보자기결정권을 보장하기 위하여 동의 방법을 법률로 구체화한 것이다.

1. 포괄 동의의 금지

개인정보처리자가 개인정보 처리에 대하여 정보주체의 동의를 받을 때에는 각각의 동의 사항을 구분하여 정보주체에게 명확히 알리고 각각 동의를 받아야 한다. 사항별로 동의를 받아야 하는 사항은 수집·이용 동의(제15조제1항제1호, 제39조의3제1항), 제3자 제공 동의(제17조제1항제1호), 국외 제3자 제공 동의(제17조제3항), 마케팅 목적 처리 동의(제22조제4항), 법정대리인의 동의(제22조제6항) 등이 있다.

특히, 정보주체가 좀 더 신중한 의사결정을 해야 할 필요가 있는 사항에 대해서는 동의의 내용과 의미를 명확하게 인지한 상태에서 결정할 수 있도록 통상의 동의와 구분해서 별도로 동의를 받아야 한다. 이때에도 개인정보처리자는 정보주체가 다른 개인정보처리의 목적과 별도로 동의여부를 표시할 수 있도록 조치를 취하고 동의를 받아야 한다. 다른 동의와 구분해서 별도 동의를 받아야 하는 경우에는 목적 외 이용·제공 동의(제18조제2항제1호), 개인정보를 제공받은 자의 이용·제공 제한(제19조제1호), 민감정보 처리 동의(제23조제1항제1호), 고유식별정보 처리 동의(제24조제1항제1호) 등이 해당된다. 예컨대, 고유식별정보(주민등록번호 제외)를 수집할 때는 「고유식별정보 수집·이용·제공에 대한 동의」를, 건강정보에 관한 정보를 수집할 때는 「건강정보(민감정보) 수집·이용·제공에 대한 동의」를 별도로 분리해서 목적 등을 고지하고 동의를 받아야 한다.

판례1 개인정보 수집, 제공에 관한 적법한 동의의 요건

개인정보 수집·제공에 관하여 적법한 동의를 받기 위해서는, 이용자가 개인정보 제공에 관한 결정권을 충분히 자유롭게 행사할 수 있도록, 미리 인터넷사이트에 통상의 이용자라면 용이하게 개인정보를 제공받는 자, 개인정보를 제공받는 자의 개인정보 이용 목적, 제공하는 개인정보의 항목, 개인정보를 제공받는 자의 개인정보 보유 및 이용 기간(이하 동의를 받을 때 이용자에게 알려야 할 사항을 통틀어 ‘법정 고지사항’이라 한다)의 구체적 내용을 알아볼 수 있을 정도로 법정 고지사항 전부를 명확하게 게재하여야 한다. 아울러, 법정 고지사항을 게재하는 부분과 이용자의 동의 여부를 표시할 수 있는 부분을 밀접하게 배치하여 이용자가 법정 고지사항을 인지하여 확인할 수 있는 상태에서 개인정보의 수집·제공에 대한 동의 여부를 판단할 수 있어야 하고, 그에 따른 동의의 표시는 이용자가 개인정보의 수집·제공에 동의를 한다는 명확한 인식하에 행하여질 수 있도록 실행 방법이 마련되어야 한다.

갑 회사가 이벤트 화면에서 법정 고지사항을 제일 하단에 배치한 것은 법정 고지사항을 미리 명확하게 인지·확인할 수 있게 배치한 것으로 볼 수 없는 점, 이벤트 화면에 스크롤바를 설치한 것만으로는 개인정보 수집·이용 및 제3자 제공에 관한 동의를 구하고 있고 화면 하단에 법정 고지사항이 존재한다는 점을 쉽게 인지하여 확인할 수 있는 형태라고 볼 수 없는 점, 이벤트에 참여하려면 일련의 팝업창이 뜨는데, 팝업창 문구 자체만으로는 수집·제공의 대상이 ‘개인정보’이고 제공처가 제3자인 보험회사라는 점을 쉽고 명확하게 밝힌 것으로 볼 수 없는데도 이용자가 팝업창에서 ‘확인’ 버튼만 선택하면 개인정보 수집·제3자 제공에 동의한 것으로 간주되도록 한 점 등을 종합하면, 갑 회사가 이벤트 화면을 통하여 이용자의 개인정보 수집 등을 하면서 개인정보의 수집·제3자 제공에 필요한 이용자의 적법한 동의를 받지 않았다고 본 원심판단은 정당하다(대법원 2016. 6. 28. 선고 2014두2638판결).

판례2 A사 1mm 고지를 통한 개인정보 수집·제공 사건

이 사건 경품행사는 △△ 승용차, 다이아몬드 반지 등을 경품으로 내걸었고, (중략) 응모권 뒷면과 인터넷 응모 화면에는 [개인정보 수집, 취급위탁, 이용 동의]라는 제목 하에 ‘수집/이용목적’은 ‘경품 추천 및 발송, 보험마케팅을 위한 정보 제공, 제휴상품 소개 및 제휴사에 대한 정보 제공 등의 업무’ 등이, [개인정보 제3자 제공]이라는 제목 하에 ‘개인정보를 제공받는 자’는 ‘R, S 등’이, ‘이용목적’은 ‘보험상품 등의 안내를 위한 전화 등 마케팅자료로 활용됩니다.’라는 내용 등이 약 1mm 크기의 글씨로 기재되어 있으며, 말미에는 ‘기재/동의 사항 일부 미기재, 미동의, 서명 누락 시 경품추첨에서 제외됩니다.’라는 사항이 붉은 글씨로 인쇄되어 있다. …(중략)… 더욱이 이 사건 경품행사를 위하여 사용된 응모권에 기재된 동의 관련 사항은 약 1mm 크기의 글씨로 기재되어 있어 소비자의 입장에서 보아 그 내용을 읽기가 쉽지 않다. 여기에 더하여 이 사건 광고를 통하여 단순 사은행사로 오인하고 경품행사에 응모하게 된 고객들의 입장에서 짧은 시간 동안 응모권을 작성하거나 응모화면에 입력을 하면서 그 내용을 정확히 파악하여 잘못된 인식을 바로잡기가 어려울 것으로 보인다. 이러한 조치는 개인정보처리자가 정보주체의 동의를 받을 때에는 각각의 동의 사항을 구분하여 정보주체가 이를 명확하게 인지할 수 있도록 하여야 한다는 「개인정보 보호법」상의 의무를 위반한 것이다(서울중앙지방법원 2018. 8. 16. 선고 2017노1296판결, 대법원 2019. 7. 25. 선고 2018도13694판결로 확정).

2. 중요한 내용의 표시방법

개인정보처리자가 이 법에 따른 동의를 서면 또는 전자문서로 받을 때에는 다음의 중요한 내용을 명확히 표시하여 알아보기 쉽게 하여야 한다. 이는 정보주체가 자신의 개인정보 처리와 관련하여 중요한 사항을 명확하게 인지한 상태에서 실질적인 동의권을 행사할 수 있도록 하기 위한 취지에서 마련된 것이다.

중요한 내용(영 제17조제2항)

1. 개인정보의 수집·이용 목적 중 재화나 서비스의 홍보 또는 판매 권유 등을 위하여 해당 개인 정보를 이용하여 정보주체에게 연락할 수 있다는 사실
2. 처리하려는 개인정보의 항목 중 민감정보, 여권번호, 운전면허의 면허번호 및 외국인등록번호
3. 개인정보의 보유 및 이용 기간(제공 시에는 제공받는 자의 보유 및 이용 기간)
4. 개인정보를 제공받는 자 및 개인정보를 제공받는 자의 개인정보 이용 목적

중요한 내용을 표시하는 방법은 다음과 같다(고시 제4조). 우선 글씨의 크기는 최소한 9포인트 이상으로서 다른 내용보다 20퍼센트 이상 크게 하여야 한다. 인터넷 웹사이트 또는 스마트폰 어플리케이션 등 화면 상에서 동의를 받는 경우에는 원본 글씨의 크기가 9포인트 이상이어야 하고 다른 내용보다 20퍼센트 이상 크게 하여 정보주체가 쉽게 알아볼 수 있도록 하여야 한다. 이 경우 화면 크기의 제약 등으로 원본 글씨 크기에도 불구하고 화면에서 나타나는 글씨의 크기는 9포인트 미만인 경우가 발생할 수 있으므로 정보주체가 화면 크기를 확대해서 볼 수 있도록 하여야 하며, 이를 제한하여서는 안 된다.

또한, 글씨의 색깔, 굵기 또는 밑줄 등을 통하여 그 내용이 명확히 표시되도록 하여야 한다. 이 경우 중요한 내용에 해당하는 글씨의 색은 동의서 양식 본문의 글씨 색과 명확히 구분할 수 있는 색으로 할 필요가 있다.

마지막으로, 동의 사항이 많아 중요한 내용이 명확히 구분되기 어려운 경우에는 중요한 내용이 쉽게 확인될 수 있도록 그 밖의 내용과 별도로 구분하여 표시하여야 한다. 구체적으로, 중요한 내용의 경우에는 줄을 달리하거나 글씨 간 간격의 충분한 띄어쓰기 등을 통해 그 밖의 내용과 별도로 구분하여 표시하는 것이 이에 해당할 수 있다.

3. 동의가 필요한 사항과 동의 없이 처리할 수 있는 사항에 대한 구분

개인정보처리자는 정보주체의 동의가 필요 없는 개인정보와 정보주체의 동의가 필요한 개인정보를 구분하여야 한다. 정보주체의 동의가 필요 없는 개인정보에는 계약의 체결 및 이행을 위해 필수적인 정보, 법령상 의무준수를 위해 불가피한 정보, 급박한 생명·신체·재산상 이익보호를 위해 필요한 정보, 개인정보처리자의 정당한 이익 달성을 위해 필요한 정

보 등이 해당되며, 이런 경우에는 동의를 받을 필요가 없다. 동의를 필요하지 않다는 입증책임은 개인정보처리자가 부담한다(표준지침 제12조제1항).

반면에 상품 광고 및 판매에 필요한 정보, 고객성향 분석을 위해 필요한 정보, 고유식별 정보(주민등록번호 제외), 민감정보, VIP회원 가입정보의 수집·이용을 위해서는 정보주체의 동의를 필요하다. 한편, 정보주체의 동의를 요하는 개인정보와 동의를 필요 없는 개인정보로 나뉘어 있는 경우로서 개인정보처리자가 전자에 대해서 동의를 얻고자 하는 때에는 후자에 관한 사항도 정보주체에게 알리는 것이 바람직하다. 이는 정보주체가 자신이 처리에 동의한 개인정보에 대해서만 개인정보처리가 이루어지는 것으로 오해하고 개인정보의 처리에 관한 불완전한 정보만을 제공받지 않기 위함이다.

참고 약관 동의의 유효성

약관과 개인정보 처리에 대한 동의를 일괄하여 한 번의 서명을 받는 경우에는 정보주체가 자신의 개인정보 처리에 대한 사항을 자세하게 인지하지 못할 우려가 있고 정보주체의 선택권 행사가 어려울 수 있으므로 개인정보 처리에 대한 동의는 약관에 대한 동의와는 별도로 동의를 받아야 한다.

4. 마케팅 광고에 대한 동의방법

상품의 판매권유 또는 홍보를 목적으로 개인정보처리에 대한 동의를 받을 때는 정보주체에게 판매권유 또는 홍보에 이용된다는 사실을 다른 동의와 구분하여 정보주체가 이를 명확히 인지할 수 있게 알린 후 동의를 받아야 한다.

5. 재화·서비스 등의 제공 거부 금지

정보주체가 선택정보의 처리에 대한 동의(제3항), 직접마케팅에 대한 동의(제4항), 목적외 이용·제공에 대한 동의(제18조제2항제1호)를 거부하였다는 이유로 개인정보처리자는 재화 또는 서비스의 제공을 거부하지 못한다. 또한 필요한 최소한의 정보 외의 개인정보 수집에 동의하지 않는다는 이유로 재화 또는 서비스의 제공을 거부하는 것도 금지된다(제16조제3항). 이는 개인정보의 수집에 대해 형식적으로 정보주체의 동의를 받았으나, 실질적으로 동의를 강요되는 불합리를 방지하기 위함이다. 그러나 합리적인 사유에 근거를 둔 거부는 가능하다.

참고 합리적 사유의 사례

- 계열사 고객정보DB를 통합하면서 정보 제공 및 공유에 동의하지 않는다고 서비스 제공을 중단하는 것은 불법이나, 정보 제공 및 공유에 동의한 고객들에 대하여 제공하는 5년간 무료 장기 주차권을 거부한 것은 불법이 아니다.
- 광고메일 수신에 동의하지 않는다고 신용카드 발급 또는 쇼핑몰회원 가입을 거절하는 것은 불법이나, 광고메일 수신자들에게만 부여하는 포인트나 마일리지를 주지 않는 것은 불법이 아니다.
- 회원 가입을 하지 않으면 물품이나 서비스 구입을 할 수 없게 하는 경우에는 최소수집 원칙 위반이나 회원제로 하지 않으면 물품이나 서비스 판매가 현실적으로 어려운 합리적인 이유가 있다면 위법이 아니다(인터넷뱅킹 등).

6. 아동을 대신한 법정대리인의 동의

만 14세 미만 아동의 경우 개인정보의 중요성이나 위험성에 대한 인식이 부족하고, 정보 수집 목적의 진위를 평가하는 능력이 부족하기 때문에 아동을 대상으로 한 무분별한 정보 수집을 방지하기 위하여 법정대리인이 미성년자를 대신해서 동의를 받도록 한 것이다.

법정대리인이란 본인의 의사에 의하지 않고 법률의 규정에 의하여 대리인이 된 자로 미성년자의 친권자(「민법」 제909조, 제911조, 제916조, 제920조), 후견인(「민법」 제931조에서 제936조까지), 법원이 선임한 부재자의 재산관리인(「민법」 제22조, 제23조) 등이 이에 해당한다.

법정대리인의 동의를 얻기 위해서는 법정대리인의 이름과 연락처를 알아야 하기 때문에 법정대리인의 동의를 받기 위하여 필요한 최소한의 정보(법정대리인 이름과 연락처)는 법정대리인의 동의 없이 해당 아동으로부터 직접 수집할 수 있다. 이 경우 해당 아동에게 자신의 신분과 연락처, 법정대리인의 성명과 연락처를 수집하고자 하는 이유를 알려야 한다(표준지침 제13조제1항). 또한 아동으로부터 수집한 법정대리인의 개인정보를 동의를 얻기 위한 용도로만 사용해야 하며, 동의에 대한 거부사유가 확인된 경우와 동의여부가 확인되지 아니한 채 3일이 경과한 경우에는 당해 개인정보를 파기하여야 한다(표준지침 제13조제2항).

7. 개인정보 수집매체 등을 고려한 세부적인 동의 방법

정보주체의 동의는 특정한 일부 방법으로 제한되는 것은 아니나 정보주체의 개인정보 보호를 위해서는 실제로 정보주체가 동의한 사실이 명확히 확인될 수 있어야 한다. 따라서 개인정보처리자의 편의를 위해 일괄적으로 동의 여부를 묻는 전자우편을 발송한 후 거부사표시가 없을 경우 동의로 간주한다는 등의 방법은 적절하지 않다.

이 법은 개인정보의 수집매체 등을 고려한 세부적인 동의획득방법을 대통령령에 위임하여 구체적인 상황에 따라 적절한 동의획득방법에 대한 기준을 제시할 수 있도록 하고 있다. 이에 따라, 대통령령에서는 세부적인 동의 획득 방법으로 ① 동의 내용이 적힌 서면을 정보주체에게 직접 발급하거나 우편 또는 팩스 등의 방법으로 전달하고, 정보주체가 서명하거나 날인한 동의서를 받는 방법 ② 전화를 통하여 동의 내용을 정보주체에게 알리고 동의의 의사표시를 확인하는 방법 ③ 전화를 통하여 동의 내용을 정보주체에게 알리고 정보주체에게 인터넷주소 등을 통하여 동의 사항을 확인하도록 한 후 다시 전화를 통하여 그 동의 사항에 대한 동의의 의사표시를 확인하는 방법 ④ 인터넷 홈페이지 등에 동의 내용을 게재하고 정보주체가 동의 여부를 표시하도록 하는 방법 ⑤ 동의 내용이 적힌 전자우편을 발송하여 정보주체로부터 동의의 의사표시가 적힌 전자우편을 받는 방법이라고 열거하고 있고 ⑥ 그 밖에 상기 5가지 방법에 준하는 방법으로 동의 내용을 알리고 동의의 의사표시를 확인할 수 있다고 규정하고 있다. 이에에는 전자문서를 통해 동의내용을 정보주체에게 알리고 정보주체가 전자서명을 받는 방법, 개인명의의 휴대전화 문자메세지를 이용한 동의, 신용카드 비밀번호를 입력하는 방법 등도 해당된다.

8. 다른 법률과의 관계

「신용정보법」은 동의 받는 방법에 관하여 규정하고 있으므로, 신용정보이용·제공자 등은 각각 해당 법령에 따라 동의를 받을 수 있다. 다만 만 14세 미만의 아동으로부터 개인정보 수집·이용·제공 등의 동의를 받는 경우에 대하여, 「신용정보법」은 관련 규정을 두고 있지 않으므로, 이에 대하여 「개인정보 보호법」을 따른다.

한편 2020. 2. 4. 개정 「신용정보법」은 정보활용 동의제도를 내실화하기 위해 신용정보주체가 정보활용 동의 사항을 이해할 수 있도록 정보활용 동의서를 단순화하고, 정보주체가 정보활용 현황을 활용목적별 기관별로 구분하여 개별적으로 동의 여부를 선택할 수 있도록 하였고, 개인정보 보호 등급제를 도입하였다.

신용정보법	<p>제32조(개인신용정보의 제공·활용에 대한 동의) ① 신용정보제공·이용자가 개인 신용정보를 타인에게 제공하려는 경우에는 대통령령으로 정하는 바에 따라 해당 신용정보주체로부터 다음 각 호의 어느 하나에 해당하는 방식으로 개인신용정보를 제공할 때마다 미리 개별적으로 동의를 받아야 한다. 다만, 기존에 동의한 목적 또는 이용 범위에서 개인신용정보의 정확성·최신성을 유지하기 위한 경우에는 그러하지 아니하다.</p> <ol style="list-style-type: none"> 1. 서면 2. 「전자서명법」 제2조제3호에 따른 공인전자서명이 있는 전자문서(「전자거래기본법」 제2조제1호에 따른 전자문서를 말한다) 3. 개인신용정보의 제공 내용 및 제공 목적 등을 고려하여 정보 제공 동의의 안
-------	---

	<p>정성과 신뢰성이 확보될 수 있는 유무선 통신으로 개인비밀번호를 입력하는 방식</p> <p>4. 유무선 통신으로 동의 내용을 해당 개인에게 알리고 동의를 받는 방법. 이 경우 본인 여부 및 동의 내용, 그에 대한 해당 개인의 답변을 음성녹음하는 등 증거자료를 확보·유지하여야 하며, 대통령령으로 정하는 바에 따른 사후 고지절차를 거친다.</p> <p>5. 그 밖에 대통령령으로 정하는 방식</p> <p>② 개인신용평가회사, 개인사업자신용평가회사, 기업신용조회회사 또는 신용정보집중기관으로부터 개인신용정보를 제공받으려는 자는 대통령령으로 정하는 바에 따라 해당 신용정보주체로부터 제1항 각 호의 어느 하나에 해당하는 방식으로 개인신용정보를 제공받을 때마다 개별적으로 동의(기준에 동의한 목적 또는 이용 범위에서 개인신용정보의 정확성·최신성을 유지하기 위한 경우는 제외한다)를 받아야 한다. 이 경우 개인신용정보를 제공받으려는 자는 개인신용정보의 조회 시 개인신용평점이 하락할 수 있는 때에는 해당 신용정보주체에게 이를 고지하여야 한다.</p> <p>③ 개인신용평가회사, 개인사업자신용평가회사, 기업신용조회회사 또는 신용정보집중기관이 개인신용정보를 제2항에 따라 제공하는 경우에는 해당 개인신용정보를 제공받으려는 자가 제2항에 따른 동의를 받았는지를 대통령령으로 정하는 바에 따라 확인하여야 한다.</p> <p>④ 신용정보회사등은 개인신용정보의 제공 및 활용과 관련하여 동의를 받을 때에는 대통령령으로 정하는 바에 따라 서비스 제공을 위하여 필수적 동의사항과 그 밖의 선택적 동의사항을 구분하여 설명한 후 각각 동의를 받아야 한다. 이 경우 필수적 동의사항은 서비스 제공과의 관련성을 설명하여야 하며, 선택적 동의사항은 정보제공에 동의하지 아니할 수 있다는 사실을 고지하여야 한다.</p> <p>⑤ 신용정보회사등은 신용정보주체가 선택적 동의사항에 동의하지 아니한다는 이유로 신용정보주체에게 서비스의 제공을 거부하여서는 아니 된다.</p> <p>⑥ 신용정보회사등(제9호의3을 적용하는 경우에는 데이터전문기관을 포함한다)이 개인신용정보를 제공하는 경우로서 다음 각 호의 어느 하나에 해당하는 경우에는 제1항부터 제5항까지를 적용하지 아니한다.</p> <ol style="list-style-type: none"> 1. 신용정보회사 및 채권추심회사가 다른 신용정보회사 및 채권추심회사 또는 신용정보집중기관과 서로 집중관리·활용하기 위하여 제공하는 경우 2. 제17조제2항에 따라 신용정보의 처리를 위탁하기 위하여 제공하는 경우 3. 영업양도·분할·합병 등의 이유로 권리·의무의 전부 또는 일부를 이전하면서 그와 관련된 개인신용정보를 제공하는 경우 4. 채권추심(추심채권을 추심하는 경우만 해당한다), 인가·허가의 목적, 기업의 신용도 판단, 유가증권의 양수 등 대통령령으로 정하는 목적으로 사용하는 자에게 제공하는 경우 5. 법원의 제출명령 또는 법관이 발부한 영장에 따라 제공하는 경우 6. 범죄 때문에 피해자의 생명이나 신체에 심각한 위험 발생이 예상되는 등 긴급한 상황에서 제5호에 따른 법관의 영장을 발부받을 시간적 여유가 없는 경우로서 검사 또는 사법경찰관의 요구에 따라 제공하는 경우. 이 경우 개인신용정보를 제공받은 검사는 지체 없이 법관에게 영장을 청구하여야 하고, 사법경찰관은 검사에게 신청하여 검사의 청구로 영장을 청구하여야 하며, 개인신용정보를 제공받은 때부터 36시간 이내에 영장을 발부받지 못하면 지체 없이 제
--	---

공발은 개인신용정보를 폐기하여야 한다.

7. 조세에 관한 법률에 따른 질문·검사 또는 조사를 위하여 관할 관서의 장이 서면으로 요구하거나 조세에 관한 법률에 따라 제출의무가 있는 과세자료의 제공을 요구함에 따라 제공하는 경우
 8. 국제협약 등에 따라 외국의 금융감독기구에 금융회사가 가지고 있는 개인신용정보를 제공하는 경우
 9. 제2조제1호의4나목 및 다목의 정보를 개인신용평가회사, 개인사업자신용평가회사, 기업신용등급제공업무·기술신용평가업무를 하는 기업신용조회회사 및 신용정보집중기관에 제공하거나 그로부터 제공받는 경우
 - 9의2. 통계작성, 연구, 공익적 기록보존 등을 위하여 가명정보를 제공하는 경우. 이 경우 통계작성에는 시장조사 등 상업적 목적의 통계작성을 포함하며, 연구에는 산업적 연구를 포함한다.
 - 9의3. 제17조의2제1항에 따른 정보집합물의 결합 목적으로 데이터전문기관에 개인신용정보를 제공하는 경우
 - 9의4. 다음 각 목의 요소를 고려하여 당초 수집한 목적과 상충되지 아니하는 목적으로 개인신용정보를 제공하는 경우
 - 가. 양 목적 간의 관련성
 - 나. 신용정보회사등이 신용정보주체로부터 개인신용정보를 수집한 경위
 - 다. 해당 개인신용정보의 제공이 신용정보주체에게 미치는 영향
 - 라. 해당 개인신용정보에 대하여 가명처리를 하는 등 신용정보의 보안대책을 적절히 시행하였는지 여부
 10. 이 법 및 다른 법률에 따라 제공하는 경우
 11. 제1호부터 제10호까지의 규정에 준하는 경우로서 대통령령으로 정하는 경우
 - ㉞ 제6항 각 호에 따라 개인신용정보를 타인에게 제공하려는 자 또는 제공받은 자는 대통령령으로 정하는 바에 따라 개인신용정보의 제공 사실 및 이유 등을 사전에 해당 신용정보주체에게 알려야 한다. 다만, 대통령령으로 정하는 불가피한 사유가 있는 경우에는 인터넷 홈페이지 게재 또는 그 밖에 유사한 방법을 통하여 사후에 알리거나 공시할 수 있다.
 - ㉟ 제6항제3호에 따라 개인신용정보를 타인에게 제공하는 신용정보제공·이용자로서 대통령령으로 정하는 자는 제공하는 신용정보의 범위 등 대통령령으로 정하는 사항에 관하여 금융위원회의 승인을 받아야 한다.
 - ㊱ 제8항에 따른 승인을 받아 개인신용정보를 제공받은 자는 해당 개인신용정보를 금융위원회가 정하는 바에 따라 현재 거래 중인 신용정보주체의 개인신용정보와 분리하여 관리하여야 한다.
 - ㊲ 신용정보회사등이 개인신용정보를 제공하는 경우에는 금융위원회가 정하여 고시하는 바에 따라 개인신용정보를 제공받는 자의 신원(身元)과 이용 목적을 확인하여야 한다.
 - ㊳ 개인신용정보를 제공한 신용정보제공·이용자는 제1항에 따라 미리 개별적 동의를 받았는지 여부 등에 대한 다툼이 있는 경우 이를 증명하여야 한다.
- 제34조의2(개인신용정보 등의 활용에 관한 동의의 원칙)** ① 신용정보회사등은 제15조제2항, 제32조제1항·제2항, 제33조제1항제2호, 제34조에 따라 신용정보주체로부터 동의(이하 “정보활용 동의”라 한다. 이하 이 조 및 제34조의3에서 같다)를 받는 경우 「개인정보 보호법」 제15조제2항, 제17조제2항 및 제18조제3항에 따라 신용정보주체에게 해당 각 조항에서 규정한 사항(이하 이 조에서

“고지사항”이라 한다)을 알리고 정보활용 동의를 받아야 한다. 다만, 동의 방식이나 개인신용정보의 특성 등을 고려하여 대통령령으로 정하는 경우에 대해서는 그러하지 아니하다.

② 대통령령으로 정하는 신용정보제공·이용자는 다음 각 호의 사항을 고려하여 개인인 신용정보주체로부터 정보활용 동의를 받아야 한다.

1. 보다 쉬운 용어나 단순하고 시청각적인 전달 수단 등을 사용하여 신용정보주체가 정보활용 동의 사항을 이해할 수 있도록 할 것
2. 정보활용 동의 사항과 금융거래 등 상거래관계의 설정 및 유지 등에 관한 사항이 명확하게 구분되도록 할 것
3. 정보를 활용하는 신용정보회사등이나 정보활용의 목적별로 정보활용 동의 사항을 구분하여 신용정보주체가 개별적으로 해당 동의를 할 수 있도록 할 것 (제32조제4항의 선택적 동의사항으로 한정한다)

③ 대통령령으로 정하는 신용정보제공·이용자는 제1항에도 불구하고 고지사항 중 그 일부를 생략하거나 중요한 사항만을 발췌하여 그 신용정보주체에게 알리고 정보활용 동의를 받을 수 있다. 다만, 개인인 신용정보주체가 고지사항 전부를 알려줄 것을 요청한 경우에는 그러하지 아니하다.

④ 제3항 본문에 따라 고지사항 중 그 일부를 생략하거나 중요한 사항만을 발췌하여 정보활용 동의를 받는 경우에는 같은 항 단서에 따라 신용정보주체에게 고지사항 전부를 별도로 요청할 수 있음을 알려야 한다.

⑤ 제3항 본문에 따른 생략·발췌에 관한 사항, 같은 항 단서에 따른 요청의 방법, 제4항에 따라 알리는 방법에 대해서는 대통령령으로 정한다.

제34조의3(정보활용 동의등급) ① 대통령령으로 정하는 신용정보제공·이용자는 정보활용 동의 사항에 대하여 금융위원회가 평가한 등급(이하 이 조에서 “정보활용 동의등급”이라 한다)을 신용정보주체에게 알리고 정보활용 동의를 받아야 한다. 정보활용 동의 사항 중 대통령령으로 정하는 중요사항을 변경한 경우에도 또한 같다.

② 금융위원회는 제1항에 따른 평가를 할 때 다음 각 호의 사항을 고려하여 정보활용 동의등급을 부여하여야 한다.

1. 정보활용에 따른 사생활의 비밀과 자유를 침해할 위험에 관한 사항(활용되는 개인신용정보가 「개인정보 보호법」 제23조에 따른 민감정보인지 여부를 포함한다)
2. 정보활용에 따라 신용정보주체가 받게 되는 이익이나 혜택
3. 제34조의2제2항제1호 및 제2호의 사항
4. 그 밖에 제1호부터 제3호까지의 규정에서 정한 사항과 유사한 사항으로서 대통령령으로 정하는 사항

③ 금융위원회는 제1항에 따른 신용정보제공·이용자가 거짓이나 그 밖의 부정한 방법으로 정보활용 동의등급을 부여받은 경우, 그 밖에 대통령령으로 정하는 경우에는 부여한 정보활용 동의등급을 취소하거나 변경할 수 있다.

④ 제1항 및 제2항에 따른 정보활용 동의등급의 부여, 제3항에 따른 취소·변경의 방법·절차 등에 대해서는 대통령령으로 정한다.

9. 벌칙규정

위반행위	벌칙
동의획득 방법 위반 (제22조제1항부터 제4항까지 위반)	1천만원 이하 과태료 (제75조제4항제2호)
선택적으로 동의 않은 경우 재화 또는 서비스의 제공을 거부한 자 (제22조제5항 위반)	3천만원 이하 과태료 (제75조제2항제2호)
만 14세 미만 아동 개인정보 처리시 법정대리인 동의를 받지 아니한 자 (제22조제6항 위반)	5천만원 이하의 과태료 (제75조제1항제2호)
만 14세 미만 아동 개인정보 수집 시 법정대리인 동의를 받지 아니한 정보통신서비스 제공자 (제22조제6항 위반)	위반행위 관련 매출액의 100분의 3이하 과징금 (제39조의15제1항제2호)

10. 질의 응답

Q PDA단말기를 이용한 서비스 이용계약을 체결하는 경우에 개인정보 수집·이용에 대한 동의방법으로 고객이 PDA단말기에 직접 서명하는 것도 가능한가?

A PDA단말기를 통하여 서명을 하는 방식도 가능하다. 다만, 이 경우 개인정보 수집 시의 동의사항을 이용자에게 명확히 고지하고 동의를 얻어야 한다. 동의사항이 많으면 동의내용을 확인할 수 있는 방법(인터넷 주소 등)을 안내 하여야 한다.

Q 여행사에서는 주로 전화로 문의·예약을 받는 경우가 많은데 전화로 개인정보를 수집할 경우, 고지사항을 모두 알리고 동의를 받으려면 통화시간이 매우 길어진다. 이용자의 동의획득을 위한 다른 방법은 없는가?

A 「개인정보 보호법」은 인터넷 사이트, 서면, 전자우편, 전화 등 각각의 서비스 유형에 따른 동의획득 방법을 규정하고 있다. 전화로 개인정보 수집에 대한 동의를 얻고자 하는 경우에는 동의 내용을 이용자에게 알리고 구두로 동의를 얻거나, 또는 고지사항이 기재된 인터넷 주소 등을 안내하고 추후 구두로 동의를 얻는 방법을 이용할 수 있다.

Q 개인정보처리자가 마케팅 동의를 철회를 방지하기 위해 정보주체에게 경품을 지급하는 등 일정한 대가(이하“경품 등”)를 지급하였는데, 정보주체가 경품을 수령한 뒤 마케팅 동의를 철회하는 경우, 정보주체는 경품 등을 반환할 의무가 있는지?

A 마케팅에 대해 동의하면서 그에 대한 일종의 대가로 경품 등을 수령한 뒤, 마케팅 동의만을 철회하게 되면 이는 사회 통념상 신의에 기한 계약이라고 볼 수 없다. 따라서 이러한 경우에는 그 경품에 대한 반환 의무가 있다. 다만 개인정보처리자는 마케팅 동의 철회시 지급한 경품 등을 반환하여야 한다는 사항을 명확히 고지하여 동의를 얻는 것이 보다 바람직하다.

제2절 개인정보의 처리 제한

제23조 | 민감정보의 처리 제한

법률	<p>제23조(민감정보의 처리 제한) ① 개인정보처리자는 사상·신념, 노동조합·정당의 가입·탈퇴, 정치적 견해, 건강, 성생활 등에 관한 정보, 그 밖에 정보주체의 사생활을 현저히 침해할 우려가 있는 개인정보로서 대통령령으로 정하는 정보(이하 “민감정보”라 한다)를 처리하여서는 아니 된다. 다만, 다음 각 호의 어느 하나에 해당하는 경우에는 그러하지 아니하다.</p> <ol style="list-style-type: none">1. 정보주체에게 제15조제2항 각 호 또는 제17조제2항 각 호의 사항을 알리고 다른 개인정보의 처리에 대한 동의와 별도로 동의를 받은 경우2. 법령에서 민감정보의 처리를 요구하거나 허용하는 경우 <p>② 개인정보처리자가 제1항 각 호에 따라 민감정보를 처리하는 경우에는 그 민감정보가 분실·도난·유출·위조·변조 또는 훼손되지 아니하도록 제29조에 따른 안전성 확보에 필요한 조치를 하여야 한다.</p>
시행령	<p>제18조(민감정보의 범위) 법 제23조제1항 각 호 외의 부분 본문에서 “대통령령으로 정하는 정보”란 다음 각 호의 어느 하나에 해당하는 정보를 말한다. 다만, 공공기관이 법 제18조제2항제5호부터 제9호까지의 규정에 따라 다음 각 호의 어느 하나에 해당하는 정보를 처리하는 경우의 해당 정보는 제외한다.</p> <ol style="list-style-type: none">1. 유전자검사 등의 결과로 얻어진 유전정보2. 「형의 실효 등에 관한 법률」 제2조제5호에 따른 범죄경력자료에 해당하는 정보3. 개인의 신체적, 생리적, 행동적 특징에 관한 정보로서 특정 개인을 알아볼 목적으로 일정한 기술적 수단을 통해 생성한 정보4. 인종이나 민족에 관한 정보

개인정보는 개인의 사생활 더 나아가서는 개인의 생명·신체·재산상 안전에 중대한 영향을 미칠 수 있으므로 모두 신중하게 다루어야 하지만, 특히 사회적 차별을 야기하거나 현저히 인권을 침해할 우려가 있는 민감한 개인정보는 보다 엄격히 보호되어야 한다.

1. 민감정보의 정의

제23조는 민감정보에 대한 정의를 두는 대신에 민감정보의 종류를 열거하고 있다. 이 법에서 민감정보란 ① 사상·신념 ② 노동조합·정당의 가입·탈퇴 ③ 정치적 견해 ④ 건

강, 성생활 등에 관한 정보 ⑤ 그 밖에 정보주체의 사생활을 현저히 침해할 우려가 있는 개인정보로서 대통령령이 정하는 정보이다.

1) 사상·신념에 관한 정보

‘사상·신념에 관한 정보’란 개인의 가치관에 기초로 하여 형성된 사유체계, 개인이 굳게 믿고 지키고자하는 믿음·생각 등을 말하는 것으로 각종 이데올로기 또는 사상적 경향, 종교적 신념 등에 관한 정보를 말한다.

2) 정치적 견해에 관한 정보

‘정치적 견해에 관한 정보’란 정치적 사안에 대한 입장이나 특정 정당의 지지 여부에 관한 정보를 말한다.

3) 노동조합·정당의 가입·탈퇴에 관한 정보

‘노동조합·정당의 가입·탈퇴에 관한 정보’란 노동조합 또는 정당에의 가입·탈퇴에 관한 정보를 말한다. 반드시 적법한 노동조합이거나 정당일 필요는 없다. 또한, 노동조합 또는 정당에의 가입 및 탈퇴에 관한 직접적인 정보 이외에 노동조합비 또는 정당 회비 납입내역 등 그 가입 여부를 확인할 수 있는 정보도 포함하는 것으로 본다.

4) 건강, 성생활 등에 관한 정보

‘건강 및 성생활 등에 관한 정보’란 개인의 과거 및 현재의 병력(病歷), 신체적·정신적 장애(장애등급 유무 등), 성적 취향 등에 관한 정보를 말한다. 혈액형은 이에 해당하지 않는다.

참고 건강, 성생활 등에 관한 정보 예시

- 발달장애인 성명, 주소(보호위원회 결정 제2019-18-293호)
- 중증장애인의 성명, 주소, 전화번호(보호위원회 결정 제2019-13-211호)
- 노인장기요양 등급을 받은 사람(치매질환자)의 성명, 등급, 등급판정일, 유효기간 기산일 및 만료일(보호위원회 결정 제2019-21-334호)
- 2~3년 간 건강보험 요양급여내역(헌법재판소 2018. 8. 30. 선고 2014헌마368결정)
- 성매매피해자 자활지원사업 대상자의 성명, 생년월일, 연령, 주소가 포함된 지원사업 관련 자료(보호위원회 결정 제2019-22-353호)

5) 그 밖에 정보주체의 사생활을 현저히 침해할 우려가 있는 개인정보

‘사생활을 현저하게 침해할 우려가 있는 개인정보’란 해당 정보를 수집·처리함으로써 「헌법」상 보장된 프라이버시권의 본질적 내용이 침해될 우려가 있는 것을 말한다. 해석의 여지가 크기 때문에 민감정보로 특별히 보호할 필요가 있다고 사회적 합의가 이루어진 정보를 상황에 맞게 규정할 수 있도록 대통령령에 위임하였다.

< 영 제18조에 따른 민감정보의 종류 >

1. 유전자검사 등의 결과로 얻어진 유전정보
2. 벌금 이상의 형의 선고·면제 및 선고유예, 보호감호, 치료감호, 보호관찰, 선고유예의 실효, 집행유예의 취소, 벌금 이상의 형과 함께 부과된 몰수, 추징, 사회봉사명령, 수강명령 등의 선고 또는 처분 등 범죄경력에 관한 정보
3. 개인의 신체적, 생리적, 행동적 특징에 관한 정보로서 특정 개인을 알아볼 목적으로 일정한 기술적 수단을 통해 생성한 정보
4. 인종이나 민족에 관한 정보

영 제18조에 따른 민감정보 중 개인의 신체적, 생리적, 행동적 특징에 관한 정보로서 특정 개인을 알아볼 목적으로 일정한 기술적 수단을 통해 생성한 정보 및 인종이나 민족에 관한 정보는 2020. 8. 5. 시행령 개정을 통하여 신설된 유형으로 그 구체적 의미는 다음과 같다.

‘개인의 신체적, 생리적, 행동적 특징에 관한 정보로서 특정 개인을 알아볼 목적으로 일정한 기술적 수단을 통해 생성한 정보’란 얼굴, 지문, 홍채, 필적 등에 관한 정보를 본인 확인이나 인증 등을 위해 다른 사람과 구별되는 특징을 추출하는 기술로 가공한 정보를 말한다. 예를 들어, 사진, 안면 영상 등은 그 자체로는 민감정보가 아니며, 특정 개인을 인증 또는 식별하기 위하여 기술적 수단을 통해 특정 정보를 생성한 경우에 해당 특정정보는 민감정보에 해당한다. 따라서 안면인식을 통해 연령·성별을 추정하여 유형에 맞는 광고를 내보내는 서비스, 이용자의 얼굴을 자동인식하여 스티커, 특수 효과 등을 적용하는 카메라 앱(App) 등을 운영하기 위하여 사진, 안면영상 등을 처리하는 경우에는 민감정보를 처리하는 것으로 판단되지 않는다.

인종이나 민족에 관한 정보도 민감정보이다. 인종은 인류를 지역과 신체적 특성에 따라 구분한 것이며, 민족은 일정한 지역에서 오랜 세월 동안 공동생활을 하면서 언어와 문화상의 공통성에 기초하여 역사적으로 형성된 사회 집단으로서, 인종이나 국가 단위인 국민과 반드시 일치하는 것은 아니다.

다만, 시행령에 따른 민감정보는 공공기관이 다음의 업무수행을 위하여 처리하는 경우에는 민감정보로 보지 아니하므로, 이 경우에는 정보주체로부터의 별도 동의 없이 처리가 가능하다.

- 개인정보를 목적 외의 용도로 이용하거나 이를 제3자에게 제공하지 아니하면 다른 법률에서 정하는 소관 업무를 수행할 수 없는 경우로서 보호위원회의 심의·의결을 거친 경우
- 조약, 그 밖의 국제협정의 이행을 위하여 외국정부 또는 국제기구에 제공하기 위하여 필요한 경우
- 범죄의 수사와 공소의 제기 및 유지를 위하여 필요한 경우
- 법원의 재판업무 수행을 위하여 필요한 경우
- 형(刑) 및 감호, 보호처분의 집행을 위하여 필요한 경우

참고 「형의 실효등에 관한 법률」

제2조제5호 “범죄경력자료”란 수사자료표 중 다음 각 목에 해당하는 사항에 관한 자료를 말한다.

- 가. 벌금 이상의 형의 선고, 면제 및 선고유예
- 나. 보호감호, 치료감호, 보호관찰
- 다. 선고유예의 실효
- 라. 집행유예의 취소
- 마. 벌금 이상의 형과 함께 부과된 몰수, 추징(追徵), 사회봉사명령, 수강명령(受講命令) 등의 선고 또는 처분

2. 민감정보의 처리 금지

민감정보는 원칙적으로 처리가 금지된다. 외국의 주요 입법례에서도 민감정보(특별한 범주의 정보)의 처리를 원칙적으로 금지하고 있으며 정보주체의 명시적 동의가 있는 경우 등 예외적인 사유에 해당할 때에만 처리를 인정하고 있다.

참고 1 EU 「일반 개인정보 보호법」 제9조(특별 범주의 개인정보 처리) 제1항

인종 또는 민족, 정치적 견해, 종교적 또는 철학적 신념, 노동조합의 가입여부를 나타내는 개인정보의 처리와 유전자 정보, 자연인을 고유하게 식별할 목적의 생체정보, 건강정보, 성생활 또는 성적 취향에 관한 정보의 처리는 금지된다.

제23조는 별도로 정보주체의 동의를 받은 경우와 법령에서 민감정보의 처리를 요구하거나 허용하는 경우에 한해 민감정보의 처리를 허용하고 있다.

- **정보주체의 별도 동의를 받은 경우** : 제15조제2항 각 호 또는 제17조제2항 각 호의 사항을 정보주체에게 알리고 다른 개인정보의 처리에 대한 동의와 분리해서 민감정보 처리에 대한 별도의 동의를 받은 경우
- **법령에서 처리를 요구하는 경우** : 법령에서 민감정보의 종류를 열거하고 그 처리를 요구하고 있는 경우(법정서식에 민감정보 기재사항이 있는 경우도 포함)

참고 2 「의료법」 제21조제2항

제21조(기록 열람 등) ② 제1항의 규정에 불구하고 의료인은 동일한 환자의 진료상 필요에 의하여 다른 의료기관에서 그 기록·임상소견서 및 치료경위서의 열람이나 사본의 송부를 요구한 때 또는 환자가 검사기록 및 방사선필름 등의 사본 교부를 요구한 때에는 이에 응하여야 한다.

■ 총포·도검·화약류 등 단속법 시행규칙 [별지 제10호의3서식] (신설 2011.2.22)

병력(病歷) 신고 및 개인정보 이용 동의서

(앞 쪽)

※ 다음 물음을 읽고 있음 또는 없음의 해당 []란에 √ 표시를 하며, 있음에 표시한 경우 그 내용을 적습니다.

접수번호	접수일자	처리일자	처리기간 10일
(1) 귀하는 정신분열증·정동장애(情動障礙)·고도의 성격장애 및 이에 준하는 증세로 인하여 치료받은 사실이 있습니까?			[]있음 []없음
(있는 경우)	병명	치료병원	
	치료개시일	치료종료일	
(2) 귀하는 경련성질환(간질) 등으로 치료받은 사실이 있습니까?			[]있음 []없음
(있는 경우)	병명	치료병원	
	치료개시일	치료종료일	
(3) 귀하는 마약·대마 향정신성의약품 알코올중독 등으로 치료 받거나 수사기관에 단속된 사실이 있습니까?			[]있음 []없음
(치료사실이 있는 경우)	병명	치료병원	
	치료개시일	치료종료일	
(단속된 사실이 있는 경우)	단속일시	단속기관	
	위반행위		
			년 월 일
신고인			(서명 또는 인)
지방경찰청장·경찰서장 귀하			
개인정보 이용동의서			
본인은 허가관청이「총포·도검·화약류 등 단속법」 제13조에 따른 총포 소지허가 결정사유 등의 해당여부 판단을 위해 국민건강보험공단이 보관 중인 본인의 동의일로부터 최근 5년간 치매, 정신분열병, 분열형 정동장애, 양극성 정동장애, 재발성 우울장애, 정신 발육지연, 간질의 치료경력을 조회하는 데 동의합니다.			
			년 월 일
동의인			(서명 또는 인)

참고 4 「보안관찰법시행령」 제6조제1항

제6조(보안관찰처분대상자의 신고) ①보안관찰처분대상자가 법 제6조제1항의 규정에 의하여 출소전에 신고할 때에는 다음 각 호의 사항을 기재한 신고서 5부를 작성하여 교도소, 소년 교도소, 구치소, 유치장, 군교도소 또는 영창(이하 “교도소등” 이라 한다)의 장에게 제출하여야 한다.

1. 원적·본적·주거(실제로 생활하는 거처. 이하 같다)·성명·생년월일·성별·주민등록번호
2. 가족 및 교우관계
3. 입소전의 직업·본인 및 가족의 재산상황
4. 학력·경력
5. 종교 및 가입한 단체
6. 병역관계
7. 출소예정일
8. 출소후의 거주예정지 및 그 도착예정일
9. 보안관찰해당범죄사실의 요지·판결법원·판결연월일·죄명·적용법조·형명·형기
10. 보안관찰해당범죄외의 전과관계
11. 법 제20조제3항에 해당하는 경우에는 거소제공 결정일자과 제공된 사회복지시설등의 명칭 및 그 소재지

참고 5 「병역법」 제11조의2

제11조의2(자료의 제출 요구 등) ① 지방병무청장은 병역판정검사와 관련하여 병역판정검사 전담의사, 병역판정검사전문의사 또는 제12조의2에 따라 신체검사를 위하여 파견된 군의관(軍醫官) 등이 질병이나 심신장애의 확인을 위하여 필요하다고 인정하는 경우 「의료법」에 따른 의료기관의 장, 「국민건강보험법」에 따른 국민건강보험공단의 장, 「초·중등교육법」에 따른 학교의 장 등에 대하여 병역판정검사 대상자의 진료기록·치료 관련 기록 내역, 학교생활기록부 등의 제출을 요구할 수 있다. 이 경우 자료 제출을 요구받은 사람은 특별한 사유가 없으면 요구에 따라야 한다.

② 누구든지 제1항에 따라 취득한 병역판정검사 대상자에 대한 정보·자료를 공개 또는 누설하거나 다른 사람에게 제공하는 등 병역판정검사 외의 목적으로 사용하여서는 아니 된다.

제23조는 개인정보 처리에 관하여 특별한 규정이므로 제15조, 제17조 및 제18조 등 개인정보 처리에 관한 규정에 우선하여 적용된다. 따라서 민감정보는 제23조제1항 각 호에서 정하는 예외 사유가 존재하는 경우에 한하여 처리할 수 있으며, 이에 해당하지 않으면 제15조제1항 각 호, 제17조제1항 각 호, 제18조제2항 각 호 등의 규정에 따른 요건을 갖추었다고 하여 처리 가능하다고 볼 수 없다. 한편, 헌법재판소는 국민건강공단이 민감정보인 영양급여내역을 수사기관에 제공한 사안에서 제23조제1항제2호 사유가 존재하고, 제18조제2항제7호에 따른 요건을 갖춘 경우 민감정보를 제공할 수 있다고 판시한 바 있다(헌법재판소 2018. 8. 30. 선고 2014헌마368결정 참고).

3. 민감정보의 안전성 확보조치

개인정보처리자가 제23조제1항 각 호에 따라 민감정보를 처리하는 경우에는 그 민감정

보가 분실·도난·유출·위조·변조 또는 훼손되지 아니하도록 제29조에 따른 안전성 확보에 필요한 조치를 하여야 한다(제23조제2항). 이에 따라 개인정보처리의 경우에는 영 제30조에 따른 기준을 준수하여야 하며, 정보통신서비스 제공자등의 경우에는 영 제30조가 아닌 영 제48조의2에 따른 기준을 준수하여야 한다.

4. 다른 법률과의 관계

제23조는 「신용정보법」상 신용정보제공·이용자에게도 적용된다. 따라서 신용정보제공·이용자는 정보주체의 별도의 동의가 있거나 법령상 허용근거가 있는 경우에만 민감정보를 처리할 수 있다. 따라서 보험료 산출 등을 위하여 개인의 질병 정보를 수집·조사하는 경우 해당 개인의 동의를 얻어야 한다.

한편, 2020년 2월 4일에 개정된 「신용정보법」은 금융위원회가 정보활용 동의등급을 부여 시 정보활용에 따른 사생활의 비밀과 자유를 침해할 위험에 관한 사항(「개인정보 보호법」상 민감정보인지 여부 포함) 등을 고려하도록 규정하고 있다.

신용정보법	<p>제34조의3(정보활용 동의등급) ① 대통령령으로 정하는 신용정보제공·이용자는 정보활용 동의 사항에 대하여 금융위원회가 평가한 등급(이하 이 조에서 “정보활용 동의등급”이라 한다)을 신용정보주체에게 알리고 정보활용 동의를 받아야 한다. 정보활용 동의 사항 중 대통령령으로 정하는 중요사항을 변경한 경우에도 또한 같다.</p> <p>② 금융위원회는 제1항에 따른 평가를 할 때 다음 각 호의 사항을 고려하여 정보활용 동의등급을 부여하여야 한다.</p> <ol style="list-style-type: none"> 1. 정보활용에 따른 사생활의 비밀과 자유를 침해할 위험에 관한 사항(활용되는 개인정보가 「개인정보 보호법」 제23조에 따른 민감정보인지 여부를 포함한다) 2. 정보활용에 따라 신용정보주체가 받게 되는 이익이나 혜택 3. 제34조의2제2항제1호 및 제2호의 사항 4. 그 밖에 제1호부터 제3호까지의 규정에서 정한 사항과 유사한 사항으로서 대통령령으로 정하는 사항
-------	---

5. 벌칙규정

위반행위	벌칙
민감정보 처리기준 위반 (제23조제1항 위반)	5년 이하의 징역 또는 5천만원 이하의 벌금 (제71조제1항제2호)
이용자의 동의 없이 민감정보를 수집한 정보통신서비스 제공자등 (제23조제1항제1호 위반)	위반행위 관련 매출액의 100분의 3 이하의 과징금 (제39조의15제1항제3호)
민감정보 보호를 위한 안전성 확보 조치를 취하지 아니하여 개인정보를 도난·유출·변조 또는 훼손당하거나 분실한 자 (제23조제2항 위반)	2년 이하의 징역 또는 2천만원 이하의 벌금 (제73조제1호)
민감정보 보호를 위한 안전성 확보조치 의무 위반 (제23조제2항 위반)	3천만원 이하 과태료 (제75조제2항제6호)

6. 질의 응답

Q 법과 시행령이 정한 것 이외에 개인에게 민감한 정보면 모두 민감정보가 될 수 있는가?

A 법과 시행령은 사상, 신념, 노동조합(정당)의 가입/탈퇴, 정치적 견해, 건강, 성생활, 유전정보, 범죄경력, 인종 민족 정보, 생체 인식 정보에 관한 정보로 한정하고 있으므로, 그 이외의 정보는 민감정보에 해당하지 않는다.

Q 장애우에 대한 요금감면 혜택을 제공하기 위해서는 상세한 장애등급 정보가 필요한데, 수집할 수 있는지?

A 「전기통신사업법」 제4조는 전기통신사업자에게 '보편적 의무' 제공을 의무화하고 있으며, 대통령령에서는 '보편적 의무' 중의 하나로 '장애인·저소득층 등에 대한 요금감면 서비스'를 규정하고 있다. 따라서 이 경우는 법 제23조제2호의 법령에서 민감정보의 처리를 요구하거나 허용하는 경우로서, 장애우 요금감면 혜택을 위한 장애등급 정보 수집이 가능하다.

Q 지문인식 출입통제 시스템을 통해 지문정보를 수집하는 경우, 해당 지문정보를 민감정보로 보아야 하는지?

A 허가된 출입자들만 출입을 허가할 목적으로 개인별 지문정보를 등록한 후 본인확인 수단으로 이용하거나 출입기록을 관리하는 경우, 이때의 지문정보의 처리는 특정개인을 알아볼 수 있도록 기술적 수단을 통해 특정정보를 생성하는 경우에 해당하여 민감정보의 처리로 보아야 한다.
지문정보를 수집하는 경우에도 특정 개인을 알아볼 목적이 아니라 무단으로 출입하고자 하는 사람을 통제하기 위해 출입 인가를 받은 사람의 범위에 있는지 여부만을 확인하려는 목적이라면 해당 정보는 민감정보가 아니다. 이 경우에도 개인을 알아볼 수 있다면 당해 지문정보는 개인정보에 해당할 수 있다.

Q 사진인화 서비스를 제공하기 위하여 개인별로 사진을 저장하고 일정기간 보관하는 경우, 개인을 알아볼 수 있는 사진에 대하여 민감정보 처리에 관한 별도의 동의가 필요한지?

A 해당 사진을 이용하여 특정개인을 알아볼 수 있도록 기술적 수단을 통해 특정정보를 생성하는 것이 아니라 사진 자체를 수집, 저장, 출력 하는 등의 처리를 하는 것은 민감정보의 처리에 해당하지 않는다.

제24조 | 고유식별정보의 처리 제한

법률

제24조(고유식별정보의 처리 제한) ① 개인정보처리자는 다음 각 호의 경우를 제외하고는 법령에 따라 개인을 고유하게 구별하기 위하여 부여된 식별정보로서 대통령령으로 정하는 정보(이하 “고유식별정보”라 한다)를 처리할 수 없다.

1. 정보주체에게 제15조제2항 각 호 또는 제17조제2항 각 호의 사항을 알리고 다른 개인정보의 처리에 대한 동의와 별도로 동의를 받은 경우

2. 법령에서 구체적으로 고유식별정보의 처리를 요구하거나 허용하는 경우

② 삭제

③ 개인정보처리자가 제1항 각 호에 따라 고유식별정보를 처리하는 경우에는 그 고유식별정보가 분실·도난·유출·위조·변조 또는 훼손되지 아니하도록 대통령령으로 정하는 바에 따라 암호화 등 안전성 확보에 필요한 조치를 하여야 한다.

④ 보호위원회는 처리하는 개인정보의 종류·규모, 종업원 수 및 매출액 규모 등을 고려하여 대통령령으로 정하는 기준에 해당하는 개인정보처리자가 제3항에 따라 안전성 확보에 필요한 조치를 하였는지에 관하여 대통령령으로 정하는 바에 따라 정기적으로 조사하여야 한다.

⑤ 보호위원회는 대통령령으로 정하는 전문기관으로 하여금 제4항에 따른 조사를 수행하게 할 수 있다.

시행령

제19조(고유식별정보의 범위) 법 제24조제1항 각 호 외의 부분에서 “대통령령으로 정하는 정보”란 다음 각 호의 어느 하나에 해당하는 정보를 말한다. 다만, 공공기관이 법 제18조제2항제5호부터 제9호까지의 규정에 따라 다음 각 호의 어느 하나에 해당하는 정보를 처리하는 경우의 해당 정보는 제외한다.

1. 「주민등록법」 제7조의2제1항에 따른 주민등록번호

2. 「여권법」 제7조제1항제1호에 따른 여권번호

3. 「도로교통법」 제80조에 따른 운전면허의 면허번호

4. 「출입국관리법」 제31조제5항에 따른 외국인등록번호

제21조(고유식별정보의 안전성 확보 조치) ① 법 제24조제3항에 따른 고유식별정보의 안전성 확보 조치에 관하여는 제30조 또는 제48조의2를 준용한다. 이 경우 “법 제29조”는 “법 제24조제3항”으로, “개인정보”는 “고유식별정보”로 본다.

② 법 제24조제4항에서 “대통령령으로 정하는 기준에 해당하는 개인정보처리자”란 다음 각 호의 어느 하나에 해당하는 개인정보처리자를 말한다.

1. 공공기관

2. 5만명 이상의 정보주체에 관하여 고유식별정보를 처리하는 자

③ 보호위원회는 제2항 각 호의 어느 하나에 해당하는 개인정보처리자에 대하여 법 제24조제4항에 따라 안전성 확보에 필요한 조치를 하였는지를 2년마다 1회 이상 조사해야 한다.

④ 제3항에 따른 조사는 제2항 각 호의 어느 하나에 해당하는 개인정보처리자에게 온라인 또는 서면을 통하여 필요한 자료를 제출하게 하는 방법으로 한다.

⑤ 법 제24조제5항에서 “대통령령으로 정하는 전문기관”이란 다음 각 호의 기관을 말한다.

1. 「정보통신망 이용촉진 및 정보보호 등에 관한 법률」 제52조에 따른 한국인터넷진흥원(이하 “한국인터넷진흥원”이라 한다)
2. 법 제24조제4항에 따른 조사를 수행할 수 있는 기술적·재정적 능력과 설비를 보유한 것으로 인정되어 보호위원회가 정하여 고시하는 법인, 단체 또는 기관

고유식별정보는 원래 공익목적으로 개인에게 부여된 것이나 그 편리성 때문에 공공부문은 물론 민간영역에서도 광범위하게 수집·이용되고 있다. 특히 주민등록번호의 유출과 도용으로 인한 피해 등이 급증하고 있다. 따라서 주민등록번호 등 고유식별정보의 오·남용을 방지하고 원래의 목적에 충실하게 사용될 수 있도록 그 처리를 일정 범위에서 제한할 필요가 있다.

1. 고유식별정보의 정의

고유식별정보란 법령에 따라 개인을 고유하게 구별하기 위하여 부여된 식별정보로서 대통령령으로 정하는 정보, 즉, ① 주민등록번호 ② 여권번호 ③ 운전면허번호 ④ 외국인등록번호를 말한다(제24조제1항, 영 제19조제1항 각 호).

법령에 의해서 개인에게 부여된 것이어야 하므로 기업, 학교 등이 소속 구성원에게 부여하는 사번, 학번 등은 고유식별정보가 될 수 없다. 또 법인이나 사업자에게 부여되는 법인등록번호, 사업자등록번호 등도 고유식별정보가 될 수 없다.

한편, 영 제19조에서는 고유식별번호의 범위를 주민등록번호, 여권번호, 운전면허번호, 외국인등록번호로 정하고 있는데 이들 정보가 민간 분야에서 DB매칭키 등으로 남용되어 개인 프라이버시 침해가능성이 높은 정보라는 점을 고려한 것이다. 다만 시행령에 따른 고유식별정보는 공공기관이 다음의 업무 수행을 위하여 처리하는 경우에는 고유식별정보로 보지 아니한다(영 제19조제1항 단서).

- 개인정보를 목적 외의 용도로 이용하거나 이를 제3자에게 제공하지 아니하면 다른 법률에서 정하는 소관 업무를 수행할 수 없는 경우로서 보호위원회의 심의·의결을 거친 경우

- 조약, 그 밖의 국제협정의 이행을 위하여 외국정부 또는 국제기구에 제공하기 위하여 필요한 경우
- 범죄의 수사와 공소의 제기 및 유지를 위하여 필요한 경우
- 법원의 재판업무 수행을 위하여 필요한 경우
- 형(刑) 및 감호, 보호처분의 집행을 위하여 필요한 경우

2. 고유식별정보의 처리금지

고유식별정보는 원칙적으로 처리할 수 없다. 다만, 별도로 정보주체의 동의를 받은 경우와 법령에서 고유식별정보의 처리를 요구하거나 허용하고 있는 경우에는 고유식별정보를 처리할 수 있다. 다만, 고유식별정보 중 주민등록번호의 처리에 관하여서는 제24조의2에서 별도로 규정하고 있으며, 이에 대해서는 후술한다.

정보주체의 별도의 동의를 받는 경우에 개인정보처리자는 제15조제2항 각 호 또는 제17조제2항 각 호의 사항을 정보주체에게 알리고 다른 개인정보의 처리에 대한 동의와 분리해서 고유식별정보 처리에 대한 동의를 받아야 한다.

법령에서 구체적으로 처리를 요구하거나 허용하는 경우란, 원칙적으로 법령에서 구체적으로 고유식별정보의 종류를 열거하고 그 처리를 요구하거나 허용하고 있는 것을 말한다.

‘법령’에 의한다고 규정하고 있으므로 법률 외에 시행령, 시행규칙이 포함되며 이에 첨부된 별지 서식이나 양식도 포함된다.

참고 1 「금융실명거래 및 비밀보장에 관한 법률」 시행령 제3조

제3조(실지명의) 법 제2조제4호의 규정에 의한 실지명의는 다음 각 호의 구분에 따른 명의로 한다.

1. 개인의 경우 : 주민등록표에 기재된 성명 및 주민등록번호. 다만, 재외국민의 경우에는 여권에 기재된 성명 및 여권번호(여권이 발급되지 아니한 재외국민은 「재외국민등록법」에 의한 등록부에 기재된 성명 및 등록번호)
- 2 ~ 3. 생략
4. 외국인의 경우 : 「출입국관리법」에 의한 등록외국인기록표에 기재된 성명 및 등록번호. 다만, 외국인등록증이 발급되지 아니한 자의 경우에는 여권 또는 신분증에 기재된 성명 및 번호

참고 2 「후견등기에 관한 법률」 제25조

제25조(성년후견등에 관한 기록사항) ① 성년후견등에 관하여는 다음 사항을 기록한다.

1. 후견의 종류, 심판을 한 가정법원, 사건의 표시 및 재판 확정일
2. 피성년후견인들의 성명, 성별, 출생 연월일, 주민등록번호 및 등록기준지(외국인인 경우에는 주민등록번호 및 등록기준지를 같음하여 국적 및 외국인등록번호를 기록한다)
3. 성년후견인들의 성명, 주민등록번호 및 주소 또는 사무소(법인인 경우에는 명칭, 법인등록번호 및 주된 사무소를 기록하고, 외국인인 경우에는 주민등록번호를 같음하여 국적 및 외국인등록번호를 기록한다)

참고 3 「아동학대범죄의 처벌 등에 관한 특례법 시행령」 제7조

제7조(민감정보 및 고유식별정보의 처리) ① 법무부장관 등 관계 행정기관의 장, 검사, 보호관찰소의 장, 교정시설의 장, 사법경찰관, 보호관찰관, 아동복지전담기관·아동복지시설의 장과 그 종사자, 수탁기관의 장과 그 직원은 다음 각 호의 사무를 수행하기 위하여 불가피한 경우 「개인정보 보호법」 제23조에 따른 건강 및 성생활에 관한 정보, 같은 법 시행령 제18조제1호 및 제2호에 따른 유전정보와 범죄경력자료에 해당하는 정보 및 같은 영 제19조에 따른 주민등록번호, 여권번호, 운전면허의 면허번호 또는 외국인등록번호가 포함된 자료를 처리할 수 있다.

이와 관련하여, 다른 법령에서 법 정책적 필요에 의해 개인정보처리자에 대해 단순히 신원확인 의무나 연령확인 의무만을 부과하고 있는 경우에는 고유식별정보 처리를 구체적으로 요구·허용한 것으로 보기 어렵다. 따라서 이 경우에는 신원·연령 확인을 위한 고유식별정보 처리 동의를 별도로 받거나, 주민등록번호를 사용하지 않는 수단을 이용하여 신원·연령을 확인하여야 한다.

참고 4 「청소년보호법」 제16조제1항

제16조(판매 금지 등) ① 청소년유해매체물로서 대통령령으로 정하는 매체물을 판매·대여·배포하거나 시청·관람·이용하도록 제공하려는 자는 그 상대방의 나이 및 본인 여부를 확인하여야 하고, 청소년에게 판매·대여·배포하거나 시청·관람·이용하도록 제공하여서는 아니 된다

참고 5 「청소년보호법」 제26조제1항

제26조(심야시간대의 인터넷게임 제공시간 제한) ① 인터넷게임의 제공자는 16세 미만의 청소년에게 오전 0시부터 오전 6시까지 인터넷게임을 제공하여서는 아니 된다.

참고 6 「정보통신망법」 제44조의5제1항

제44조의5(게시판 이용자의 본인 확인) ① 다음 각 호의 어느 하나에 해당하는 자가 게시판을 설치·운영하려면 그 게시판 이용자의 본인 확인을 위한 방법 및 절차의 마련 등 대통령령으로 정하는 필요한 조치(이하 “본인확인조치”라 한다)를 하여야 한다.

1. 국가기관, 지방자치단체, 「공공기관의 운영에 관한 법률」 제5조제3항에 따른 공기업·준정부기관 및 「지방공기업법」에 따른 지방공사·지방공단(이하 “공공기관등”이라 한다)
2. 삭제

또한, 법령에서 고유식별정보의 처리를 구체적으로 요구하거나 허용하고 있는 경우에는 원칙적으로 법령에 명시된 목적을 위하여 제3자로부터 고유식별정보를 제공받거나 제3자에게 제공하는 것도 허용되는 것으로 볼 수 있다.

3. 고유식별정보의 안전성 확보 조치

개인정보처리자가 고유식별정보를 처리하는 경우에는 그 고유식별정보가 분실·도난·유출·위조·변조 또는 훼손되지 아니하도록 대통령령으로 정하는 바에 따라 암호화 등 안전성 확보에 필요한 조치를 하여야 한다(제24조제3항). 이에 따라 개인정보처리자의 경우에는 영 제30조에 따른 기준을 준수하여야 하며, 정보통신서비스 제공자등의 경우에는 영 제30조가 아닌 영 제48조의2에 따른 기준을 준수하여야 한다(영 제21조제1항). 한편, 공공기관이 법 제18조제1항제5호~제9호에 따라 처리하는 고유식별정보는 제24조에 따른 고유식별정보로 보지 않는다(영 제19조제1항 단서).

또한, 보호위원회는 공공기관 또는 5만명 이상 정보주체의 고유식별정보를 처리하는 개인정보처리자에 대해서는 고유식별정보의 안전성 확보 조치를 하였는지를 2년마다 1회 이상 조사하여야 한다(제24조제4항, 영 제21조제2항, 제3항). 보호위원회는 온라인 또는 서면을 통하여 필요한 자료를 제출하게 하는 방법으로 조사를 수행하며, 한국인터넷진흥원 또는 보호위원회가 정하여 고시하는 전문기관으로 하여금 조사를 수행하게 할 수 있다(제24조제5항, 영 제21조제4항, 제5항).

4. 벌칙 규정

위반행위	벌칙
고유식별정보의 처리기준 위반 (제24조제1항 위반)	5년 이하의 징역 또는 5천만원 이하의 벌금 (제71조제4호)
고유식별정보 보호를 위한 안전성 확보 조치를 취하지 아니하여 개인정보를 도난·유출·변조 또는 훼손당하거나 분실한 자 (제24조제3항 위반)	2년 이하의 징역 또는 2천만원 이하의 벌금 (제73조제1호)
고유식별정보 보호를 위한 안전성 확보조치 의무 위반 (제24조제3항 위반)	3천만원 이하 과태료 (제75조제2항제6호)

제24조의2 | 주민등록번호 처리의 제한

법률

제24조의2(주민등록번호 처리의 제한) ① 제24조제1항에도 불구하고 개인정보 처리자는 다음 각 호의 어느 하나에 해당하는 경우를 제외하고는 주민등록번호를 처리할 수 없다.

1. 법률·대통령령·국회규칙·대법원규칙·헌법재판소규칙·중앙선거관리위원회규칙 및 감사원규칙에서 구체적으로 주민등록번호의 처리를 요구하거나 허용한 경우
2. 정보주체 또는 제3자의 급박한 생명, 신체, 재산의 이익을 위하여 명백히 필요하다고 인정되는 경우
3. 제1호 및 제2호에 준하여 주민등록번호 처리가 불가피한 경우로서 보호위원회가 고시로 정하는 경우

② 개인정보처리자는 제24조제3항에도 불구하고 주민등록번호가 분실·도난·유출·위조·변조 또는 훼손되지 아니하도록 암호화 조치를 통하여 안전하게 보관하여야 한다. 이 경우 암호화 적용 대상 및 대상별 적용 시기 등에 관하여 필요한 사항은 개인정보의 처리 규모와 유출 시 영향 등을 고려하여 대통령령으로 정한다.

③ 개인정보처리자는 제1항 각 호에 따라 주민등록번호를 처리하는 경우에도 정보주체가 인터넷 홈페이지를 통하여 회원으로 가입하는 단계에서는 주민등록번호를 사용하지 아니하고도 회원으로 가입할 수 있는 방법을 제공하여야 한다.

④ 보호위원회는 개인정보처리자가 제3항에 따른 방법을 제공할 수 있도록 관계 법령의 정비, 계획의 수립, 필요한 시설 및 시스템의 구축 등 제반 조치를 마련·지원할 수 있다.

시행령

제21조의2(주민등록번호 암호화 적용 대상 등) ① 법 제24조의2제2항에 따라 암호화 조치를 하여야 하는 암호화 적용 대상은 주민등록번호를 전자적인 방법으로 보관하는 개인정보처리자로 한다.

② 제1항의 개인정보처리자에 대한 암호화 적용 시기는 다음 각 호와 같다.

1. 100만명 미만의 정보주체에 관한 주민등록번호를 보관하는 개인정보처리자 : 2017년 1월 1일
2. 100만명 이상의 정보주체에 관한 주민등록번호를 보관하는 개인정보처리자 : 2018년 1월 1일

③ 보호위원회는 기술적·경제적 타당성 등을 고려하여 제1항에 따른 암호화 조치의 세부적인 사항을 정하여 고시할 수 있다.

1. 주민등록번호의 원칙적 처리 금지

고유식별정보 중 주민등록번호와 관련하여서는 원칙적으로 처리가 금지되고, 제24조의2 제1항 각 호의 사유에 해당하는 예외적인 경우에만 허용된다.

제24조의2는 주민등록번호의 보호를 다른 고유식별정보보다 더욱 강화함으로써 관행적 동의 절차에 따른 오·남용과 유출시 2차 피해 등을 근본적으로 예방하기 위해 제정된 규정 이므로 주민등록번호의 처리에 대하여는 제24조제1항 각 호의 요건이 적용되지 아니하고 제24조의2제1항 각 호의 요건이 적용된다.

주민등록번호 처리금지 예외 사유(제24조의2제1항 각 호)

1. 법률·대통령령·국회규칙·대법원규칙·헌법재판소규칙·중앙선거관리위원회규칙 및 감사원규칙에서 구체적으로 주민등록번호의 처리를 요구하거나 허용한 경우
2. 정보주체 또는 제3자의 급박한 생명, 신체, 재산의 이익을 위하여 명백히 필요하다고 인정되는 경우
3. 제1호 및 제2호에 준하여 주민등록번호 처리가 불가피한 경우로서 보호위원회가 고시로 정하는 경우

1호에서 말하는 “법률·대통령령·국회규칙·대법원규칙·헌법재판소규칙·중앙선거관리위원회규칙 및 감사원규칙에서 구체적으로 주민등록번호의 처리를 요구하거나 허용한 경우”란, 법률 등 중 최소한 어느 하나에 개인정보처리자로 하여금 주민등록번호의 처리를 요구하거나 허용하도록 하는 구체적인 규정이 존재하는 것을 말한다. 제1호는 주민등록번호를 처리할 수 있는 법령의 범위를 한정하고 있으므로 시행규칙을 근거로는 주민등록번호를 처리할 수 없다.

2호의 의미는 제15조제1항제5호에 관한 해설에 자세히 기술된 바와 같다. 단순히 정보주체의 생명, 신체, 재산상의 이익을 위한다는 이유만으로 바로 허용되는 것이 아니고, 명백히 주민등록번호의 처리가 정보주체나 제3자의 생명, 신체, 재산상의 이익을 위한 것이어야 하며 반드시 급박성이 인정되어야 한다. 충분한 시간적 여유가 있거나 다른 수단에 의하여 생명, 신체, 재산의 이익을 보호할 수 있다면 급박한 상태에 있다고 볼 수 없다.

제24조의2제1항 각 호에서 정하는 예외사유에 해당되지 않는 한 주민등록번호를 수집하여 이용하거나, 제3자에게 제공하거나 저장·보유하는 것이 금지된다. 이는 정보주체로부터 동의를 받아 주민등록번호를 수집하는 경우에도 마찬가지이다. 또한 예외사유에 해당하는 경우 개인정보처리자는 정보주체로부터 별도의 동의를 받을 필요는 없다.

2. 주민등록번호의 암호화 조치

주민등록번호를 전자적인 방법으로 보관하는 개인정보처리자는 주민등록번호가 분실·

도난·유출·위조·변조 또는 훼손되지 아니하도록 암호화 조치를 통하여 안전하게 보관하여야 한다(제24조의2제2항, 영 제21조의2제1항).

한편, 주민등록번호는 고유식별정보에도 해당하므로 개인정보처리자는 제24조의2제2항에 따른 암호화 조치를 하는 외에도 제24조제3항에 따른 고유식별정보의 안전성 확보를 위한 조치를 할 필요가 있다.

3. 주민등록번호 대체가입수단의 제공

개인정보처리자는 제24조의2제1항 각 호에 따라 주민등록번호를 처리하는 경우에도 정보주체가 인터넷 홈페이지를 통하여 회원으로 가입하는 단계에서는 주민등록번호를 사용하지 아니하고도 회원으로 가입할 수 있는 방법(이하 “주민등록번호 대체가입수단” 이라 한다)을 제공하여야 한다(제24조의2제3항). 보호위원회는 개인정보처리자가 주민등록번호 대체가입수단을 제공할 수 있도록 관계 법령의 정비, 계획의 수립, 필요한 시설 및 시스템의 구축 등 제반 조치를 마련·지원할 수 있다(제24조의2제4항).

4. 벌칙규정

위반행위	벌칙
주민등록번호를 처리한 자 (24조의2제1항 위반)	3천만원 이하 과태료 (제75조제2항제4의2)
주민등록번호 보호를 위한 암호화 조치를 하지 아니한 자 (24조의2제2항 위반)	3천만원 이하 과태료 (제75조제2항제4의3)
정보주체가 주민등록번호를 사용하지 아니할 수 있는 방법을 제공하지 아니한 자 (24조의2제3항 위반)	3천만원 이하 과태료 (제75조제2항제5호)

이 외에도 주민등록번호는 제24조에 따른 고유식별정보에도 해당한다. 따라서 개인정보처리자가 주민등록번호를 처리하면서 제24조제3항에 따른 고유식별정보의 안전성 확보 조치 의무를 위반한 경우에는 제24조제3항 위반에 따른 벌칙 규정이 적용된다.

5. 질의 응답

Q | **직원의 주민등록번호를 단체보험 가입 목적으로 처리하는 것이 가능한지?**

A | 「보험업법 시행령」 제102조제5항제4호는 보험회사가 「상법」 제735조의3(단체보험)에 따른 단체보험계약의 체결 등의 사무를 수행하기 위하여 필요한 범위에서 피보험자의 주민등록번호를 처리할 수 있도록 규정, 단체보험은 구성원으로부터 서면 동의를 받지 아니하고 단체가 보험계약자로서 피보험자인 구성원을 위하여 보험회사와 일괄 계약하는 보험으로서, 회사는 단체보험 가입 목적으로 직원의 주민등록번호를 보험회사에 제공할 수 있다.

Q | **주민등록번호가 기재된 신분증을 단순히 육안으로 확인한 후 돌려주는 행위도 주민등록번호 처리금지 원칙에 위배되는지?**

A | 신분 확인 목적으로 주민등록번호가 기재된 신분증을 육안으로 확인하고 돌려주는 행위는 주민등록번호를 수집하는 행위가 아니므로 주민등록번호 처리금지 원칙에 위배되지 않는다.

Q | **기업이 직원 채용 시 이력서·지원서 등에 주민등록번호를 기재하도록 하여도 되는지?**

A | 입사 지원자가 최종 합격하여 직원이 되기 전까지는 법률이나 대통령령에서 기업이 해당 지원자의 주민등록번호를 처리하도록 하는 규정이 없으므로 이력서·지원서 등에 주민등록번호를 기재하도록 하여서는 아니 된다.
대신 입사지원 단계에서는 주민등록번호 대신 생년월일이나 휴대전화번호 등을 수집하는 것으로 대체하고, 최종 합격한 후에는 고용보험 등 4대 보험 가입, 급여 원천 징수 등을 위해 관련 법령에서 정하는 바에 따라 기업이 해당 지원자의 주민등록번호를 수집하는 것은 가능하다.

제25조(영상정보처리기기의 설치·운영 제한) ① 누구든지 다음 각 호의 경우를 제외하고는 공개된 장소에 영상정보처리기기를 설치·운영하여서는 아니 된다.

1. 법령에서 구체적으로 허용하고 있는 경우
2. 범죄의 예방 및 수사를 위하여 필요한 경우
3. 시설안전 및 화재 예방을 위하여 필요한 경우
4. 교통단속을 위하여 필요한 경우
5. 교통정보의 수집·분석 및 제공을 위하여 필요한 경우

② 누구든지 불특정 다수가 이용하는 목욕실, 화장실, 발한실(發汗室), 탈의실 등 개인의 사생활을 현저히 침해할 우려가 있는 장소의 내부를 볼 수 있도록 영상정보처리기기를 설치·운영하여서는 아니 된다. 다만, 교도소, 정신보건 시설 등 법령에 근거하여 사람을 구금하거나 보호하는 시설로서 대통령령으로 정하는 시설에 대하여는 그러하지 아니하다.

③ 제1항 각 호에 따라 영상정보처리기기를 설치·운영하려는 공공기관의 장과 제2항 단서에 따라 영상정보처리기기를 설치·운영하려는 자는 공청회·설명회의 개최 등 대통령령으로 정하는 절차를 거쳐 관계 전문가 및 이해관계인의 의견을 수렴하여야 한다.

④ 제1항 각 호에 따라 영상정보처리기기를 설치·운영하는 자(이하 “영상정보처리기기운영자”라 한다)는 정보주체가 쉽게 인식할 수 있도록 다음 각 호의 사항이 포함된 안내판을 설치하는 등 필요한 조치를 하여야 한다. 다만, 「군사기지 및 군사시설 보호법」 제2조제2호에 따른 군사시설, 「통합방위법」 제2조제13호에 따른 국가중요시설, 그 밖에 대통령령으로 정하는 시설에 대하여는 그러하지 아니하다.

1. 설치 목적 및 장소
2. 촬영 범위 및 시간
3. 관리책임자 성명 및 연락처
4. 그 밖에 대통령령으로 정하는 사항

⑤ 영상정보처리기기운영자는 영상정보처리기기의 설치 목적과 다른 목적으로 영상정보처리기기를 임의로 조작하거나 다른 곳을 비춰서는 아니 되며, 녹음기능은 사용할 수 없다.

⑥ 영상정보처리기기운영자는 개인정보가 분실·도난·유출·위조·변조 또는 훼손되지 아니하도록 제29조에 따라 안전성 확보에 필요한 조치를 하여야 한다.

⑦ 영상정보처리기기운영자는 대통령령으로 정하는 바에 따라 영상정보처리기기 운영·관리 방침을 마련하여야 한다. 이 경우 제30조에 따른 개인정보처리방침을 정하지 아니할 수 있다.

⑧ 영상정보처리기기운영자는 영상정보처리기기의 설치·운영에 관한 사

무를 위탁할 수 있다. 다만, 공공기관이 영상정보처리기기 설치·운영에 관한 사무를 위탁하는 경우에는 대통령령으로 정하는 절차 및 요건에 따라야 한다.

제22조(영상정보처리기기 설치·운영 제한의 예외) ① 법 제25조제2항 단서에서 “대통령령으로 정하는 시설”이란 다음 각 호의 시설을 말한다.

1. 「형의 집행 및 수용자의 처우에 관한 법률」 제2조제1호에 따른 교정시설
2. 「정신건강증진 및 정신질환자 복지서비스 지원에 관한 법률」 제3조제5호부터 제7호까지의 규정에 따른 정신의료기관(수용시설을 갖추고 있는 것만 해당한다), 정신요양시설 및 정신재활시설

② 중앙행정기관의 장은 소관 분야의 개인정보처리자가 법 제25조제2항 단서에 따라 제1항 각 호의 시설에 영상정보처리기기를 설치·운영하는 경우 정보주체의 사생활 침해를 최소화하기 위하여 필요한 세부 사항을 개인정보 보호지침으로 정하여 그 준수를 권장할 수 있다.

제23조(영상정보처리기기 설치 시 의견 수렴) ① 법 제25조제1항 각 호에 따라 영상정보처리기기를 설치·운영하려는 공공기관의 장은 다음 각 호의 어느 하나에 해당하는 절차를 거쳐 관계 전문가 및 이해관계인의 의견을 수렴하여야 한다.

1. 「행정절차법」에 따른 행정예고의 실시 또는 의견청취
2. 해당 영상정보처리기기의 설치로 직접 영향을 받는 지역 주민 등을 대상으로 하는 설명회·설문조사 또는 여론조사

② 법 제25조제2항 단서에 따른 시설에 영상정보처리기기를 설치·운영하려는 자는 다음 각 호의 사람으로부터 의견을 수렴하여야 한다.

1. 관계 전문가
2. 해당 시설에 종사하는 사람, 해당 시설에 구금되어 있거나 보호받고 있는 사람 또는 그 사람의 보호자 등 이해관계인

제24조(안내판의 설치 등) ① 법 제25조제1항 각 호에 따라 영상정보처리기기를 설치·운영하는 자(이하 “영상정보처리기기운영자”라 한다)는 영상정보처리기기가 설치·운영되고 있음을 정보주체가 쉽게 알아볼 수 있도록 같은 조 제4항 각 호의 사항이 포함된 안내판을 설치하여야 한다. 다만, 건물 안에 여러 개의 영상정보처리기기를 설치하는 경우에는 출입구 등 잘 보이는 곳에 해당 시설 또는 장소 전체가 영상정보처리기기 설치지역임을 표시하는 안내판을 설치할 수 있다.

1. 삭제
2. 삭제
3. 삭제

② 제1항에도 불구하고 영상정보처리기기운영자가 설치·운영하는 영상정보

처리기가 다음 각 호의 어느 하나에 해당하는 경우에는 안내판 설치를 갈음하여 영상정보처리기기운영자의 인터넷 홈페이지에 법 제25조제4항 각 호의 사항을 게재할 수 있다.

1. 공공기관이 원거리 촬영, 과속·신호위반 단속 또는 교통흐름조사 등의 목적으로 영상정보처리기기를 설치하는 경우로서 개인정보 침해의 우려가 적은 경우
 2. 산불감시용 영상정보처리기기를 설치하는 경우 등 장소적 특성으로 인하여 안내판을 설치하는 것이 불가능하거나 안내판을 설치하더라도 정보주체가 쉽게 알아볼 수 없는 경우
- ③ 제2항에 따라 인터넷 홈페이지에 법 제25조제4항 각 호의 사항을 게재할 수 없으면 영상정보처리기기운영자는 다음 각 호의 어느 하나 이상의 방법으로 법 제25조제4항 각 호의 사항을 공개하여야 한다.
1. 영상정보처리기기운영자의 사업장·영업소·사무소·점포 등(이하 “사업장등”이라 한다)의 보기 쉬운 장소에 게시하는 방법
 2. 관보(영상정보처리기기운영자가 공공기관인 경우만 해당한다)나 영상정보처리기기운영자의 사업장등이 있는 시·도 이상의 지역을 주된 보급지역으로 하는 「신문 등의 진흥에 관한 법률」 제2조제1호가목·다목 또는 같은 조 제2호에 따른 일반일간신문·일반주간신문 또는 인터넷신문에 실는 방법
- ④ 법 제25조제4항 각 호 외의 부분 단서에서 “대통령령으로 정하는 시설”이란 「보안업무규정」 제32조에 따른 국가보안시설을 말한다.

제25조(영상정보처리기기 운영·관리 방침) ① 영상정보처리기기운영자는 법 제25조제7항에 따라 다음 각 호의 사항이 포함된 영상정보처리기기 운영·관리 방침을 마련하여야 한다.

1. 영상정보처리기기의 설치 근거 및 설치 목적
2. 영상정보처리기기의 설치 대수, 설치 위치 및 촬영 범위
3. 관리책임자, 담당 부서 및 영상정보에 대한 접근 권한이 있는 사람
4. 영상정보의 촬영시간, 보관기간, 보관장소 및 처리방법
5. 영상정보처리기기운영자의 영상정보 확인 방법 및 장소
6. 정보주체의 영상정보 열람 등 요구에 대한 조치
7. 영상정보 보호를 위한 기술적·관리적 및 물리적 조치
8. 그 밖에 영상정보처리기기의 설치·운영 및 관리에 필요한 사항

② 제1항에 따라 마련한 영상정보처리기기 운영·관리 방침의 공개에 관하여는 제31조제2항 및 제3항을 준용한다. 이 경우 “개인정보처리자”는 “영상정보처리기기운영자”로, “법 제30조제2항”은 “법 제25조제7항”으로, “개인정보 처리방침”은 “영상정보처리기기 운영·관리 방침”으로 본다.

제26조(공공기관의 영상정보처리기기 설치·운영 사무의 위탁) ① 법 제25조제 8항 단서에 따라 공공기관이 영상정보처리기기의 설치·운영에 관한 사무를 위탁하는 경우에는 다음 각 호의 내용이 포함된 문서로 하여야 한다.

1. 위탁하는 사무의 목적 및 범위
2. 재위탁 제한에 관한 사항
3. 영상정보에 대한 접근 제한 등 안전성 확보 조치에 관한 사항
4. 영상정보의 관리 현황 점검에 관한 사항
5. 위탁받는 자가 준수하여야 할 의무를 위반한 경우의 손해배상 등 책임에 관한 사항

② 제1항에 따라 사무를 위탁한 경우에는 제24조제1항부터 제3항까지의 규정에 따른 안내판 등에 위탁받는 자의 명칭 및 연락처를 포함시켜야 한다.

제27조(영상정보처리기기 설치·운영 지침) 보호위원회는 법 및 이 영에서 규정한 사항 외에 영상정보처리기기의 설치·운영에 관한 기준, 설치·운영 사무의 위탁 등에 관하여 법 제12조제1항에 따른 표준 개인정보 보호지침을 정하여 영상정보처리기기운영자에게 그 준수를 권장할 수 있다.

제35조(적용범위) 이 장은 영상정보처리기기운영자가 공개된 장소에 설치·운영하는 영상정보처리기기과 이 기기를 통하여 처리되는 개인영상정보를 대상으로 한다.

제36조(영상정보처리기기 운영·관리 지침) ① 영상정보처리기기 운영·관리 지침을 수립하거나 변경하는 경우에는 정보주체가 쉽게 확인할 수 있도록 공개하여야 한다.

② 영상정보처리기기 운영·관리 지침을 마련한 경우에는 법 제30조에 따른 개인정보 처리방침을 정하지 아니하거나, 영상정보처리기기 설치·운영에 관한 사항을 법 제30조에 따른 개인정보 처리방침에 포함하여 정할 수 있다.

제37조(관리책임자의 지정) ① 영상정보처리기기운영자는 개인영상정보의 처리에 관한 업무를 총괄해서 책임질 관리책임자를 지정하여야 한다.

② 제1항의 관리책임자는 법 제31조제2항에 따른 개인정보 보호책임자의 업무에 준하여 다음 각 호의 업무를 수행한다.

1. 개인영상정보 보호 계획의 수립 및 시행
2. 개인영상정보 처리 실태 및 관행의 정기적인 조사 및 개선
3. 개인영상정보 처리와 관련한 불만의 처리 및 피해구제
4. 개인영상정보 유출 및 오용·남용 방지를 위한 내부통제시스템의 구축
5. 개인영상정보 보호 교육 계획 수립 및 시행
6. 개인영상정보 파일의 보호 및 파기에 대한 관리·감독
7. 그 밖에 개인영상정보의 보호를 위하여 필요한 업무

③ 법 제31조에 따른 개인정보 보호책임자가 지정되어 있는 경우에는 그 개인

정보 보호책임자가 관리책임자의 업무를 수행할 수 있다.

제38조(사전의견 수렴) 영상정보처리기기의 설치 목적 변경에 따른 추가 설치 등의 경우에도 영 제23조제1항에 따라 관계 전문가 및 이해관계인의 의견을 수렴하여야 한다.

제39조(안내판의 설치) ① 영상정보처리기기운영자는 정보주체가 영상정보처리기기가 설치·운영 중임을 쉽게 알아볼 수 있도록 법 제25조제4항 본문에 따라 다음 각 호의 사항을 기재한 안내판 설치 등 필요한 조치를 하여야 한다.

1. 설치목적 및 장소
2. 촬영범위 및 시간
3. 관리책임자의 성명 또는 직책 및 연락처
4. 영상정보처리기기 설치·운영에 관한 사무를 위탁하는 경우, 수탁자의 명칭 및 연락처

② 제1항에 따른 안내판은 촬영범위 내에서 정보주체가 알아보기 쉬운 장소에 누구라도 용이하게 관독할 수 있게 설치되어야 하며, 이 범위 내에서 영상정보처리기기운영자가 안내판의 크기, 설치위치 등을 자율적으로 정할 수 있다.

③ 공공기관의 장이 기관 내 또는 기관 간에 영상정보처리기기의 효율적 관리 및 정보 연계 등을 위해 용도별·지역별 영상정보처리기기를 물리적·관리적으로 통합하여 설치·운영(이하 ‘통합관리’라 한다)하는 경우에는 설치목적 등 통합관리에 관한 내용을 정보주체가 쉽게 알아볼 수 있도록 제1항에 따른 안내판에 기재하여야 한다.

제40조(개인영상정보 이용·제3자 제공 등 제한 등) ① 영상정보처리기기운영자는 다음 각 호의 경우를 제외하고는 개인영상정보를 수집 목적 이외로 이용하거나 제3자에게 제공하여서는 아니 된다. 다만 제5호부터 제9호까지의 경우는 공공기관의 경우로 한정한다.

1. 정보주체에게 동의를 얻은 경우
2. 다른 법률에 특별한 규정이 있는 경우
3. 정보주체 또는 그 법정대리인이 의사표시를 할 수 없는 상태에 있거나 주소 불명 등으로 사전 동의를 받을 수 없는 경우로서 명백히 정보주체 또는 제3자의 급박한 생명, 신체, 재산의 이익을 위하여 필요하다고 인정되는 경우
4. 통계작성 및 학술연구 등의 목적을 위하여 필요한 경우로서 특정 개인을 알아볼 수 없는 형태로 개인영상정보를 제공하는 경우
5. 개인영상정보를 목적 외의 용도로 이용하거나 이를 제3자에게 제공하지 아니하면 다른 법률에서 정하는 소관 업무를 수행할 수 없는 경우로서 보호위원회의 심의·의결을 거친 경우

6. 조약, 그 밖의 국제협정의 이행을 위하여 외국정부 또는 국제기구에 제공하기 위하여 필요한 경우
7. 범죄의 수사와 공소의 제기 및 유지를 위하여 필요한 경우
8. 법원의 재판업무 수행을 위하여 필요한 경우
9. 형(刑) 및 감호, 보호처분의 집행을 위하여 필요한 경우

제41조(보관 및 파기) ① 영상정보처리기기운영자는 수집한 개인영상정보를 영상정보처리기기 운영·관리 방침에 명시한 보관 기간이 만료한 때에는 지체 없이 파기하여야 한다. 다만, 다른 법령에 특별한 규정이 있는 경우에는 그러하지 아니하다.

② 영상정보처리기기운영자가 그 사정에 따라 보유 목적의 달성을 위한 최소한의 기간을 산정하기 곤란한 때에는 보관 기간을 개인영상정보 수집 후 30일 이내로 한다.

③ 개인영상정보의 파기 방법은 다음 각 호의 어느 하나와 같다.

1. 개인영상정보가 기록된 출력물(사진 등) 등은 파쇄 또는 소각
2. 전자기적(電磁氣的) 파일 형태의 개인영상정보는 복원이 불가능한 기술적 방법으로 영구 삭제

제42조(이용·제3자 제공·파기의 기록 및 관리) ① 영상정보처리기기운영자는 개인영상정보를 수집 목적 이외로 이용하거나 제3자에게 제공하는 경우에는 다음 각 호의 사항을 기록하고 이를 관리하여야 한다.

1. 개인영상정보 파일의 명칭
2. 이용하거나 제공받은 자(공공기관 또는 개인)의 명칭
3. 이용 또는 제공의 목적
4. 법령상 이용 또는 제공근거가 있는 경우 그 근거
5. 이용 또는 제공의 기간이 정하여져 있는 경우에는 그 기간
6. 이용 또는 제공의 형태

② 영상정보처리기기운영자가 개인영상정보를 파기하는 경우에는 다음 사항을 기록하고 관리하여야 한다.

1. 파기하는 개인영상정보 파일의 명칭
2. 개인영상정보 파기 일시 (사전에 파기 시기 등을 정한 자동 삭제의 경우에는 파기 주기 및 자동 삭제 여부에 관한 확인 시기)
3. 개인영상정보 파기 담당자

제43조(영상정보처리기기 설치 및 관리 등의 위탁) ① 영상정보처리기기운영자가 영 제26조제1항에 따라 영상정보처리기기의 설치·운영에 관한 사무를 제3자에게 위탁하는 경우에는 그 내용을 정보주체가 언제든지 쉽게 확인할 수 있도록 영 제24조에 따른 안내판 및 영 제27조에 따른 영상정보처리기기 운영·관리 방침에 위탁자의 명칭 등을 공개하여야 한다.

② 영상정보처리기기운영자가 영 제26조제1항에 따라 영상정보처리기기의 설치·운영에 관한 사무를 제3자에게 위탁할 경우에는 그 사무를 위탁받은 자가 개인영상정보를 안전하게 처리하고 있는지를 관리·감독하여야 한다.

제44조(정보주체의 열람등 요구) ① 정보주체는 영상정보처리기기운영자가 처리하는 개인영상정보에 대하여 열람 또는 존재확인(이하 “열람등”이라 한다)을 해당 영상정보처리기기운영자에게 요구할 수 있다. 이 경우 정보주체가 열람등을 요구할 수 있는 개인영상정보는 정보주체 자신이 촬영된 개인영상정보 및 명백히 정보주체의 급박한 생명, 신체, 재산의 이익을 위하여 필요한 개인영상정보에 한한다.

② 영상정보처리기기운영자가 공공기관인 경우에는 해당 기관의 장에게 별지 제2호 서식에 따른 개인영상정보 열람·존재확인 청구서(전자문서를 포함한다)로 하여야 한다.

③ 영상정보처리기기운영자는 제1항에 따른 요구를 받았을 때에는 지체 없이 필요한 조치를 취하여야 한다. 이때에 영상정보처리기기운영자는 열람등 요구를 한 자가 본인이거나 정당한 대리인인지를 주민등록증·운전면허증·여권 등의 신분증명서를 제출받아 확인하여야 한다.

④ 제3항의 규정에도 불구하고 다음 각 호에 해당하는 경우에는 영상정보처리기기운영자는 정보주체의 개인영상정보 열람등 요구를 거부할 수 있다. 이 경우 영상정보처리기기운영자는 10일 이내에 서면 등으로 거부 사유를 정보주체에게 통지하여야 한다.

1. 범죄수사·공소유지·재판수행에 중대한 지장을 초래하는 경우(공공기관에 한함)

2. 개인영상정보의 보관기간이 경과하여 파기한 경우

3. 기타 정보주체의 열람등 요구를 거부할 만한 정당한 사유가 존재하는 경우

⑤ 영상정보처리기기운영자는 제3항 및 제4항에 따른 조치를 취하는 경우 다음 각 호의 사항을 기록하고 관리하여야 한다.

1. 개인영상정보 열람등을 요구한 정보주체의 성명 및 연락처

2. 정보주체가 열람등을 요구한 개인영상정보 파일의 명칭 및 내용

3. 개인영상정보 열람등의 목적

4. 개인영상정보 열람등을 거부한 경우 그 거부의 구체적 사유

5. 정보주체에게 개인영상정보 사본을 제공한 경우 해당 영상정보의 내용과 제공한 사유

⑥ 정보주체는 영상정보처리기기운영자에게 정보주체 자신의 개인영상정보에 대한 파기를 요구하는 때에는 제1항에 의하여 보존을 요구하였던 개인영상정보에 대하여만 그 파기를 요구할 수 있다. 영상정보처리기기운영자가 해당 파기조치를 취한 경우에는 그 내용을 기록하고 관리하여야 한다.

제45조(개인영상정보 관리대장) 제42조제1항 및 제2항, 제44조제5항 및 제6항에 따른 기록 및 관리는 별지 제3호 서식에 따른 ‘개인영상정보 관리대장’을 활용할 수 있다.

제46조(정보주체 이외의 자의 개인영상정보 보호) 영상정보처리기기운영자는 제44조제2항에 따른 열람등 조치를 취하는 경우, 만일 정보주체 이외의 자를 명백히 알아볼 수 있거나 정보주체 이외의 자의 사생활 침해의 우려가 있는 경우에는 해당되는 정보주체 이외의 자의 개인영상정보를 알아볼 수 없도록 보호조치를 취하여야 한다.

제47조(개인영상정보의 안전성 확보를 위한 조치) 영상정보처리기기운영자는 개인영상정보가 분실·도난·유출·변조 또는 훼손되지 아니하도록 법 제29조 및 영 제30조제1항에 따라 안전성 확보를 위하여 다음 각 호의 조치를 하여야 한다.

1. 개인영상정보의 안전한 처리를 위한 내부 관리계획의 수립·시행, 다만 「개인정보의 안전성 확보조치 기준 고시」 제2조제4호에 따른 ‘소상공인’은 내부관리계획을 수립하지 아니할 수 있다.
2. 개인영상정보에 대한 접근 통제 및 접근 권한의 제한 조치
3. 개인영상정보를 안전하게 저장·전송할 수 있는 기술의 적용 (네트워크 카메라의 경우 안전한 전송을 위한 암호화 조치, 개인영상정보파일 저장시 비밀번호 설정 등)
4. 처리기록의 보관 및 위조·변조 방지를 위한 조치 (개인영상정보의 생성 일시 및 열람할 경우에 열람 목적·열람자·열람 일시 등 기록·관리 조치 등)
5. 개인영상정보의 안전한 물리적 보관을 위한 보관시설 마련 또는 잠금장치 설치

제48조(개인영상정보처리기기의 설치·운영에 대한 점검) ① 공공기관의 장이 영상정보처리기기를 설치·운영하는 경우에는 이 지침의 준수 여부에 대한 자체점검을 실시하여 다음 해 3월 31일까지 그 결과를 보호위원회에 통보하고 영 제34조제3항에 따른 시스템에 등록하여야 한다. 이 경우 다음 각 호의 사항을 고려하여야 한다.

1. 영상정보처리기기의 운영·관리 방침에 열거된 사항
2. 관리책임자의 업무 수행 현황
3. 영상정보처리기기의 설치 및 운영 현황
4. 개인영상정보 수집 및 이용·제공·파기 현황
5. 위탁 및 수탁자에 대한 관리·감독 현황
6. 정보주체의 권리행사에 대한 조치 현황
7. 기술적·관리적·물리적 조치 현황
8. 영상정보처리기 설치·운영의 필요성 지속 여부 등

- ② 공공기관의 장은 제1항과 제3항에 따른 영상정보처리기기 설치·운영에 대한 자체점검을 완료한 후에는 그 결과를 홈페이지 등에 공개하여야 한다.
- ③ 공공기관 외의 영상정보처리기기운영자는 영상정보처리기기 설치·운영으로 인하여 정보주체의 개인영상정보의 침해가 우려되는 경우에는 자체점검 등 개인영상정보의 침해 방지를 위해 적극 노력하여야 한다.

1. 적용범위 및 적용대상

가 적용범위 : 영상정보처리기기

제25조에 의하여 설치·운영이 금지 또는 제한되는 영상정보처리기기는 일정한 공간에 지속적으로 설치되어 사람 또는 사물의 영상 등을 촬영하거나 이를 유·무선망을 통하여 전송하는 장치에 한정한다(제2조제7호). 구체적으로 폐쇄회로 텔레비전(CCTV)과 네트워크 카메라가 이에 속한다(영 제3조). 차량에 설치되어 외부를 촬영하는 블랙박스는 일정한 공간에 지속적으로 설치된 것으로 볼 수 없고 이동성을 전제로 하므로 이에 속한다고 볼 수 없다.

참고 「개인정보 보호법」 제2조제7호

7. “영상정보처리기기”란 일정한 공간에 지속적으로 설치되어 사람 또는 사물의 영상 등을 촬영하거나 이를 유·무선망을 통하여 전송하는 장치로서 대통령령으로 정하는 장치를 말한다.

나 적용대상 : 누구든지

제25조의 적용 대상은 공개된 장소에 영상정보처리기기를 설치·운영하는 ‘모든 자’에 게 적용된다. 즉 업무를 목적으로 개인정보파일을 운용하기 위하여 영상정보를 처리하는 ‘개인정보처리자’가 아니더라도 영상정보처리기기를 설치·운영하는 자라면 누구든지 영상정보처리기기에 관한 규제대상에 포함된다. 또한, 영상정보처리기기를 공동으로 설치·운영하는 경우에는 해당 기기를 설치·운영하는 자들 모두 적용대상이 된다.

2. ‘공개된 장소’에서의 설치·운영 금지

가 공개된 장소의 의미

이 법은 ‘공개된 장소’에 설치·운영되는 영상정보처리기기에 대해서만 적용된다. ‘공개된 장소’란 도로, 공원, 광장, 지하철역 등의 공공장소와 같이 불특정 다수가 출입하거나

이용할 수 있도록 허용된 장소, 즉 정보주체가 접근하거나 통행하는 데에 제한을 받지 아니하는 장소를 의미한다. 따라서 특정인들 또는 특정한 용건이 있는 사람만 출입할 수 있거나, 출입이 엄격히 통제되는 장소는 여기서 말하는 ‘공개된 장소’에 해당하지 않는다.

참고 1 공개된 장소의 예시

- 도로, 공원, 공항, 항만, 주차장, 놀이터, 지하철역 등의 공공장소
- 백화점, 대형마트, 상가, 놀이공원(테마파크) 등 시설
- 버스, 택시 등 누구나 탑승할 수 있는 대중교통

판례 공개된 장소

- 다른 도로와 연결되어 있고 차단기가 설치되어 있지 않거나 설치되어 있더라도 별다른 통제가 없고 개방되어 누구나 차량으로 통행하는 아파트단지 또는 대학구내의 통행로는 불특정 다수의 사람이나 차량의 통행을 위하여 공개된 장소로 본다(대법원 2006.1.13. 선고 2005도6986 판결).
- 특정상가 건물을 위한 것이 아니고 관리인이 상주·관리하지 않고 출입차단장치가 없으며 무료로 운영되어 불특정 다수인이 수시로 이용할 수 있는 공영주차장은 불특정 다수의 사람 또는 차량의 통행을 위하여 공개된 장소로 본다(대법원 2005. 9. 15. 선고 2005도3781 판결).
- 일반인의 자유로운 출입이 가능하여 다수인이 왕래하는 공개된 장소, 일반인의 자유로운 출입이 가능하도록 공개된 장소인지는 장소의 구조, 사용관계와 공개성 및 접근성 여부, 그에 대한 구체적 지배·관리형태 등 여러 사정을 종합적으로 고려하여 판단한다(대법원 2015. 9. 10. 선고 2014도17290 판결).

제25조는 공개된 장소에 영상정보처리기를 설치·운영하는 것만을 규제하고 있으므로, 비공개된 장소 및 순수한 사적(私的) 장소에 영상정보처리기를 설치·운영하는 경우에는 어떠한 원칙이 적용되는지에 대한 문제가 있다.

1) 비공개된 장소에 영상정보처리기를 설치·운영하는 경우

제25조가 ‘공개된 장소’에 설치된 영상정보처리기기만을 규제하고 있는 것은 불특정 다수가 출입·이용하는 공개된 장소에서는 개인영상정보의 수집(촬영) 및 이용 등에 대해 일일이 동의를 받는 것이 현실적으로 불가능하므로 이를 대신하여 안내판 설치, 사전 의견수렴 등의 보호조치를 통하여 불특정 다수의 개인정보 및 사생활을 보호하고자 하는 취지이다.

따라서, 비공개 장소에 설치된 영상정보처리기기에 대해서는 그 설치·운영자가 업무를 목적으로 영상정보에 대한 개인정보파일을 운용하기 위하여 영상정보처리기기를 설치·운영하는 ‘개인정보처리자’에 해당하는 경우에 한해 제15조(개인정보 수집·이용) 등의 일반 원

칙이 적용된다고 판단된다.

즉 업무를 목적으로 개인영상정보 파일을 운용하는 개인정보처리자는 그 구성원이나 출입·이용이 허가된 사람들의 동의를 받거나(제15조제1항제1호), 그 영상정보처리기기의 설치·운영이 개인정보처리자의 정당한 이익 달성을 위하여 필요하고 명백하게 정보주체의 권리보다 우선하는 경우(제15조제1항제6호) 등에 한하여 ‘비공개된 장소’에 영상정보처리기기를 설치하여 개인영상정보를 수집·이용할 수 있다.

이 경우 안내판 설치의무 등 이 법에서 공개된 장소에 영상정보처리기기를 설치한 영상정보 처리기기 운영자에게 적용되는 의무는 비공개 장소의 영상정보처리기기 운영자에게는 규정상 적용되지 아니할 것으로 보이나, 정보주체가 직접 촬영 대상이 된다는 점에서 그 보호의 필요성이 큰 만큼 영상정보처리기기 운영 현황을 분명히 알려준다는 차원에서 이 법에서 정한 안내판 등 설치의무를 준수하는 것이 바람직하다고 할 것이다.

한편, 비공개된 장소에 설치하는 영상정보처리기기에 대해 다른 법률에서 별도의 규정을 두고 있는 경우에는 그에 따른 원칙·절차를 준수하여야 한다.

참고 「형사소송법」 제244조의2

- 제244조의2(피의자진술의 영상녹화)** ① 피의자의 진술은 영상녹화할 수 있다. 이 경우 미리 영상 녹화사실을 알려주어야 하며, 조사의 개시부터 종료까지의 전 과정 및 객관적 정황을 영상 녹화하여야 한다.
- ② 제1항에 따른 영상녹화가 완료된 때에는 피의자 또는 변호인 앞에서 지체 없이 그 원본을 봉인하고 피의자로 하여금 기명날인 또는 서명하게 하여야 한다.
- ③ 제2항의 경우에 피의자 또는 변호인의 요구가 있는 때에는 영상녹화물을 재생하여 시청하게 하여야 한다. 이 경우 그 내용에 대하여 이의를 진술하는 때에는 그 취지를 기재한 서면을 첨부하여야 한다.

2) 순수한 사적(私的) 장소에 영상정보처리기기를 설치·운영하는 경우

영상정보처리기기가 개인의 주택 등 순수한 사적(私的) 공간에 설치되어 있는 경우에는 이 법 적용이 배제된다. 예를 들어 단독주택·연립주택 등의 대문, 현관 등에 범죄예방(방범) 목적으로 감시용 CCTV를 설치하는 경우가 그것이다. 이 경우에는 그 영상정보처리기기 설치된 장소가 공개된 장소가 아니며, 그 영상정보처리기기를 설치·운영하는 개인 등도 ‘개인정보처리자’에 해당한다고 보기 어려우므로 이 법이 적용되지 않는다.

다만, 이러한 경우에도 단독주택·연립주택 등의 대문, 현관을 통하여 방문하는 자만이 촬영되고 주택 외부 등 공개된 장소가 촬영되지 않도록 CCTV의 촬영 각도를 최대한 주택의 내부 쪽으로 고정하여, 타인의 사생활을 침해하거나 불필요한 개인영상정보가 수집되지 않도록 해야 할 것이다.

<영상정보처리기기 설치·운영 관련 쟁점 사례>

사례 1 택시·버스 등의 CCTV

택시, 버스 등 영업용 차량 내부에 설치되어 탑승공간 및 승객을 촬영하는 CCTV는 ‘일정한 공간에 지속적으로’ 설치·촬영되고 있다는 점에서 이 법에 따른 영상정보처리기기에 해당하며, 불특정 다수의 승객이 탑승하는 공간이라는 점에서 ‘공개된 장소’에 설치·운영되는 경우에 해당한다. 따라서 영업용 차량 내부에 설치된 CCTV는 제25조의 적용을 받는다.

사례 2 택시·버스 등에 설치된 블랙박스

택시·버스 등 영업용 차량 내부에 설치되어 외부(차량, 도로 등)를 촬영하는 이른바 ‘블랙박스’의 경우에는 일정한 공간을 촬영하는 것이 아니므로 이 법에 따른 영상정보처리기기에 해당하지 않으며, 제25조의 적용을 받지 않는다.

한편, 택시·버스 등의 운영 주체(버스회사, 개인택시 운전자 등)는 “개인정보파일을 운용하기 위하여 개인영상정보를 처리”하는 개인정보처리자로 보기 어려우므로, 이 법의 다른 개인정보 보호 원칙도 적용되지 않는다. 다만 버스·택시회사 등에서 교통사고 대응을 위하여, 블랙박스로 촬영된 영상정보를 사고일시·피해자 등의 개인정보에 따라 배열·구성하여 쉽게 검색할 수 있도록 한 경우에는 개인정보파일에 해당하므로 이 법 적용을 받는다.

사례 3 개인 승용차에 설치된 블랙박스

개인 소유의 차량은 공개된 장소가 아니며 순수한 사적(私的) 공간으로서, 여기에 설치된 ‘블랙박스’는 이 법의 적용을 받지 않는다.

사례 4 관공서, 기업 등의 건물에 설치된 CCTV

관공서의 민원실, 기업 건물의 로비 등은 불특정 다수가 출입하고 있으므로 여기에 설치된 영상정보처리기기는 제25조의 적용을 받는다.

그러나 출입이 엄격히 통제되고 있고 내부 직원이나 허가를 받은 사람만 출입이 허용되는 관공서 건물 내부 또는 기업 사옥의 내부 공간은 ‘비공개된 장소’에 해당하므로, 제25조의 적용을 받지 않는다.

다만 이 경우에 해당 관공서, 기업 등이 “업무를 목적으로 개인정보파일을 운용하기 위하여 개인 영상정보를 처리”하기 위하여 내부 공간에 영상정보처리기기를 설치·운영하는 경우에는 이 법의 다른 개인정보 보호 원칙이 적용된다. 즉 그 구성원의 동의를 받거나 개인정보처리자의 정당한 이익을 달성하기 위하여 필요한 경우 등에 한하여 영상정보처리기기 설치·운영이 허용된다.

사례 5 사업장 내부에 설치된 CCTV

민간기업 등에서 기업 자산 도난방지, 시설안전, 근로자의 근무행태 모니터링 등을 목적으로 영상정보처리기기를 설치·운영하는 경우가 있다. 사업장 내부에 설치된 영상정보처리기기는 사용자 측의 근로 관리권한과 근로자 측의 사생활 보호권이 서로 상충될 우려가 있다.

외부인의 출입이 통제되는 근로공간은 원칙적으로 비공개 장소에 해당하므로 제25조는 적용되지 않으며, 그 외의 일반적 개인정보 보호원칙 적용을 받아야 한다. 따라서 근로자로부터 원칙적으로 동

의를 받아야 하겠으나, 회사자산의 도난 방지, 시설안전의 목적으로 특정 장소에 CCTV를 설치하는 경우 등 개인정보처리자의 정당한 이익 달성을 위하여 필요하고 명백하게 정보주체의 권리보다 우선하는 경우(제15조제1항제6호)에는 근로자의 동의 없이도 영상정보처리기기 설치·운영이 가능하다 할 것이다.

이와 관련하여, 「근로자참여 및 협력증진에 관한 법률」에서는 CCTV와 같은 근로자 감시 장비는 노사 양자의 협의사항으로 규정하고 있으므로, 근로 모니터링 목적의 CCTV 설치 범위 및 사생활 침해 방지조치 등을 노사 협의에 따라 정하여 설치·운영할 수 있다고 규정하고 있다.

나 영상정보처리기기 설치의 예외적 허용

공개된 장소에 영상정보처리기기를 설치·운영하는 것은 원칙적으로 금지되나, 다른 법의 보호를 위하여 필요한 경우에는 예외적으로 설치·운영이 허용되고 있다. 이 법은 총 5가지의 설치·운영 허용 사유를 규정하고 있다.

1) 법령에서 구체적으로 허용하는 경우

일부 법령에서는 장소의 특수성 등을 고려하여 영상정보처리기기의 설치를 의무화하고 있거나 설치를 허용하고 있다.

< 영상정보처리기기의 설치를 규정하고 있는 법령 >

관련 법령	내 용
주차장법 시행규칙	주차대수 30대를 초과하는 규모의 자주식 주차장으로서 지하식 또는 건축물식에 의한 노외주차장에는 관리사무소에서 주차장 내부 전체를 볼 수 있는 폐쇄회로 텔레비전 (녹화장치 포함) 또는 네트워크 카메라를 포함하는 방범설비를 설치·관리하여야 함 (제6조제1항제11호)
아동복지법	유치원, 초등학교, 특수학교, 보육시설, 도시공원 등 아동보호구역으로 지정된 시설에서는 폐쇄회로 텔레비전을 설치·운영할 수 있음(제32조)
폐광지역개발 지원에 관한 특별법 시행령	카지노사업자는 호텔의 내부 및 외부의 주요 지점에 폐쇄회로 텔레비전을 설치·운영하여야 함(제14조제2항)
외국인보호규칙	외국인보호시설의 소장은 보호시설의 안전대책 확보를 위하여 폐쇄회로 텔레비전을 설치·운영할 수 있음(제37조제2항)
공중위생관리법 시행규칙	목욕장업자는 목욕실, 발한실, 탈의실 이외의 시설에 무인감시카메라를 설치할 수 있음(별표 1)
국제항해선박 및 항만시설의 보안에 관한 법률 시행규칙	국제여객선터미널의 여객 대기지역, 항만시설 내 국토해양부령으로 정하는 지역에 설치하는 울타리 등에 폐쇄회로 텔레비전을 설치하여야 함(별표 4)
생명윤리 및 안전에 관한 법률 시행규칙	체세포복제배아연구기관은 실험실 및 보관시설의 감시를 위하여 CCTV 등을 설치하여야 함(별표 4)

관련 법령	내 용
지하공공보도시설의 결정·구조 및 설치기준에 관한 규칙	지하공공보도시설의 중앙방재실은 자체 감시카메라(CCTV) 설비를 갖추어야 함(제12조)
여객자동차 운수사업법	운송사업자는 여객자동차운송사업에 사용되는 차량의 운행상황 기록, 교통사고 상황 파악, 차량 내 범죄예방을 위하여 대통령령으로 정하는 여객자동차운송사업의 사업용 자동차에 영상기록장치를 설치하여야 함(제27조의3제1항)

2) 범죄 예방 및 수사를 위하여 필요한 경우

제2호의 ‘범죄’는 법 위반으로 인해 형사처벌이 부과되는 행위를 말하며, 행정질서벌인 과태료가 부과되거나 그 밖에 과징금 또는 면허취소 등의 행정제재 처분이 부과되는 행위는 본 호의 범죄에 해당되지 않는다(보호위원회 결정 제2019-11-178호 참고).

여기서 범죄는 형법상의 범죄 이외에 각종 개별법이나 단속법상의 범죄도 포함된다. 예컨대 「경범죄처벌법」상의 각종 경범죄(도로 등에서의 물품강매·청객, 광고물 무단 부착 등, 쓰레기 무단 투기, 노상방뇨 등, 공원·명승지·유원지등의 자연훼손, 자릿세 징수 등, 압표매매)를 예방·수사하기 위해서도 감시카메라를 설치·운영할 수 있다. 우범 지역의 도로나 골목길에 CCTV를 설치·운영하는 경우, 은행 ATM 시설에 범죄방지용 CCTV를 설치·운영하는 경우, 백화점·편의점 등에서 도난방지용 CCTV를 설치·운영하는 경우, 회사의 자체창고에 도난방지용 CCTV를 설치·운영하는 경우 등이 이에 해당된다.

3) 시설안전 및 화재 예방을 위하여 필요한 경우

각종 자연재해, 시설 노후화, 인위적 훼손·난동, 방화, 낙서 등으로부터 공공시설, 문화재, 사유재산 등을 보호하기 위하여 필요한 경우 영상정보처리기기의 설치·운영이 허용된다. 즉 지하철역 안전사고 예방, 공공건물의 전기·가스·수도 등 시설관리 및 화재예방, 문화재 시설 안전 및 보호를 위한 경우 등이 이에 해당된다.

4) 교통단속을 위하여 필요한 경우

각종 차량 및 사람들의 교통법규 위반을 단속·예방하기 위하여 필요한 경우 영상정보처리기기의 설치·운영이 허용된다. 주·정차 위반, 신호위반, 규정 속도위반 등 교통법규 위반행위 단속을 위해 CCTV를 설치하는 것이 이에 해당된다.

5) 교통정보의 수집·분석 및 제공을 위하여 필요한 경우

원활한 교통 흐름을 위한 교통량 분석, 교통사고 등에 관한 정보를 수집·제공하기 위하여 필요한 경우 영상정보처리기기의 설치·운영이 허용된다. 즉 고속도로, 주요 간선도로 등의 교통량을 수집하여 분석하기 위해 필요한 경우 등이 이에 해당된다.

결정례 공공기관이 기설치·운영 중인 영상정보처리기에 설치 목적을 추가하기 위한 요건

부산광역시가 차량 방범용으로 설치·운영 중인 영상정보처리기를 고농도 미세먼지 비상저감조치에 따른 운행 제한 자동차의 단속 및 과태료 부과 목적을 추가하여 이를 병행 활용하기 위해서는 미세먼지 저감 및 관리에 관한 특별법 제18조제4항에 따라 비상저감조치 시 자동차 운행 제한의 방법으로써 영상정보처리기의 설치에 관한 근거 조례를 제정하고(「개인정보 보호법」 제25조제1항 각 호 해당), 「행정절차법」에 따른 행정예고의 실시 또는 의견청취 등의 절차를 거쳐(「개인정보 보호법」 제25조제3항 해당) 차량방범용 영상정보처리기의 설치 목적에 그 활용 목적을 추가하여 이를 병행 활용할 수 있다(보호위원회 결정 제2019-12-199호).

3. 개인의 사생활을 현저히 침해할 우려가 있는 장소 내부의 설치·운영 금지

가 개인의 사생활을 현저히 침해할 우려가 있는 장소

개인의 사생활이 현저히 침해될 우려가 있는 장소에 대해서는 당연히 영상정보처리기의 설치·운영을 엄격히 제한할 필요가 있다. 이에 따라 이 법은 누구든지 불특정 다수가 이용하는 목욕실, 화장실, 발한실(發汗室), 탈의실 등 개인의 사생활을 현저히 침해할 우려가 있는 장소의 내부를 볼 수 있도록 영상정보처리기를 설치·운영하는 행위를 금지하고 있다.

나 예외적 허용

공익적 목적에 의해 사람을 구급·보호하는 시설의 목욕실, 화장실 등에는 그 안에서의 자해·자살, 폭력행위, 탈출 등을 방지하기 위하여 영상정보처리기를 설치·운영할 필요성이 있다. 이에 따라 이 법은 교도소·구치소·외국인보호시설·소년원이나 정신보건시설 등과 같이 법령에 근거하여 사람을 구급·보호하는 시설로서 대통령령으로 정하는 시설에 대해서는 예외를 인정하고 있다. 구체적인 시설은 다음과 같다.

< 개인의 사생활을 현저히 침해할 우려가 있는 장소의 예외적 설치·운영 허용 >

관련 법령	내 용
형의 집행 및 수용자의 처우에 관한 법률	교정시설 (제2조제1호) ※ 교도소·구치소 및 그 지소
정신건강증진 및 정신질환자 복지서비스 지원에 관한 법률	정신의료기관(수용시설을 갖추고 있는 것만 해당), 정신요양시설 및 정신재활시설(제3조제5호부터 제7호)

이와 관련하여, 관계 중앙행정기관의 장은 소관 분야의 개인정보처리자(교도소·구치소 및 그 지소, 정신의료기관 등)가 해당시설에 영상정보처리기를 설치·운영하는 경우 정보주체의 사생활 침해를 최소화하기 위하여 필요한 세부 사항을 개인정보 보호지침으로 정하여 그 준수를 권장할 수 있다(영 제22조제2항).

4. 영상정보처리기의 설치·운영 절차·방법

가 전문가 자문 및 이해관계인 의견수렴

영상정보처리기의 무분별한 설치·운영 및 이로 인한 사생활 침해를 방지하기 위하여 설치·운영시 관계인의 의견을 수렴하여 반영할 필요가 있다.

1) 공공기관의 경우

공공기관이 공개된 장소에 영상정보처리기를 설치·운영하려는 경우에는 다음 각 호의 어느 하나에 해당하는 절차를 거쳐 관계 전문가 및 이해관계인의 의견을 수렴하여야 한다.

- ① 「행정절차법」에 따른 행정예고의 실시 또는 의견청취
- ② 해당 영상정보처리기의 설치로 직접 영향을 받는 지역 주민 등을 대상으로 하는 설명회·설문조사 또는 여론조사

2) 개인 사생활 침해우려 장소에 설치 시 의견수렴

법 제25조제2항 및 영 제22조에 따른 교정시설이나 정신의료기관 등에 영상정보처리기를 설치·운영하려는 자는 다음 각 호의 사람으로부터 모두 의견을 수렴하여야 한다.

- ① 관계 전문가
- ② 해당 시설에 종사하는 사람, 해당 시설에 구금되어 있거나 보호받고 있는 사람 또는 그 사람의 보호자 등 이해관계인

나 영상정보처리기기 설치·운영 안내

1) 안내판 설치

영상정보처리기는 공개된 장소에 지속적으로 설치·운영되고 있으므로, 촬영 대상자는 자기의 모습이 촬영되는지에 대해 통제권을 행사하는 것이 사실상 불가능하다. 따라서 법 제25조의 적용을 받는 영상정보처리기에 대해서는 그 촬영사실을 알리는 안내판 설치를 통해 촬영 대상자의 개인정보 자기결정권을 보장하는 것이 필요하다.

영상정보처리기기 운영자는 정보주체가 영상정보처리기기가 설치·운영 중임을 쉽게 알아볼 수 있도록 안내판을 설치하여야 한다. 안내판 기재 항목은 다음과 같다.

- | |
|--|
| <ul style="list-style-type: none">① 설치목적 및 장소② 촬영범위 및 시간③ 관리책임자 및 연락처④ 그 밖에 대통령령으로 정하는 사항 |
|--|

위의 ④의 “그 밖에 대통령령으로 정하는 사항” 으로는 공공기관이 영상정보처리기관이 설치·운영 사무를 위탁하고 있는 경우 위탁받는 자의 명칭 및 연락처(영 제26조제2항)가 해당한다. 한편, 표준지침 제39조는 민간 사업자가 영상정보처리기기를 설치·운영 사무를 위탁하는 경우에도 위탁받는 자의 명칭 및 연락처를 안내판에 기재하도록 규정하고 있다.

다만, 백화점, 역사 등 규모가 큰 건물의 경우에는 다수의 영상정보처리기기가 설치되어 있는데, 이러한 각각의 기기에 대해 개별적으로 안내판 설치를 강제하는 것은 과도한 규제가 될 수 있다. 따라서 건물 안에 다수의 영상정보처리기기를 설치하는 경우에는 출입구 등 잘 보이는 곳에 해당 시설 또는 장소 전체가 영상정보처리기기 설치지역임을 표시하는 안내판을 설치할 수 있다(영 제24조제1항 단서).

안내판은 촬영범위 내에서 정보주체가 알아보기 쉬운 장소에 누구라도 용이하게 관독될 수 있게 설치되어야 하고, 이를 충족하였다면 그 범위 내에서 안내판의 크기나 설치위치는 영상정보처리기기 운영자가 자율적으로 정할 수 있다(표준지침 제39조제2항).

공공기관은 영상정보처리기기의 효율적 관리와 정보 연계를 위해 통합 관리하는 경우가 있다. 이러한 때에는 설치목적 등 통합관리에 관한 내용을 정보주체가 쉽게 알아볼 수 있도록 제39조제1항에 따른 안내판에 기재하여야 한다(표준지침 제39조제3항).

2) 인터넷 홈페이지 게재

영상정보처리기기의 운영 현황에 따라서는 안내판을 설치하는 것이 의미가 없거나 정보주체가 알아볼 수 없는 상황이 있을 수 있다.

따라서 법에서는 공공기관이 원거리 촬영, 과속·신호위반 단속 또는 교통흐름조사 등의 목적으로 영상정보처리기기를 설치하는 경우로서 개인정보침해의 우려가 적은 경우 또는 영상정보처리기기운영자가 산불감시용 영상정보처리기기를 설치하는 경우 등 장소적 특성으로 인하여 안내판을 설치하는 것이 불가능하거나 안내판을 설치하더라도 정보주체가 이를 쉽게 알아볼 수 없는 경우에는 안내판 설치를 갈음하여 영상정보처리기기운영자의 인터넷 홈페이지에 영 제25조제4항 각 호의 사항을 게재할 수 있도록 하였다.

3) 사업장·영업소 등 게재

소규모 사업자나 소상공인 등은 아예 인터넷 홈페이지가 없는 경우가 있을 수 있다. 이처럼 영상정보처리기기운영자가 인터넷 홈페이지에 게재사항을 게재할 수 없는 경우에는 영상정보처리기기운영자의 사업장·영업소·사무소·점포 등(이하 “사업장등”이라 한다)의 보기 쉬운 장소에 게시하거나 관보(영상정보처리기기운영자가 공공기관인 경우로 한정한다)나 영상정보처리기기운영자의 사업장등이 소재하는 특별시·광역시·도 또는 특별자치도(이하 “시·도”라 한다) 이상의 지역을 주된 보급지역으로 하는 「신문 등의 진흥에 관한 법률」 제2조제1호·제2호에 따른 일반일간신문, 일반주간신문 또는 인터넷신문에 실는 방법으로 게재사항을 공개하여야 한다(영 제24조제2항).

4) 안내판 설치의무 면제

국가안보 등 중대한 공익적 목적을 위해 설치·운영되는 영상정보처리기기에 대해서는 안내판 설치가 오히려 그 목적달성에 장애가 될 수도 있다. 따라서 이러한 시설에 대해서는 안내판 설치의 면제가 필요하다. 즉 공공기관의 장이 ① 「군사기지 및 군사시설 보호법」 제2조제2호에 따른 군사시설 ② 「통합방위법」 제2조제13호에 따른 국가중요시설 ③ 「보안업무규정」 제32조에 따른 국가보안시설에 영상정보처리기기를 설치할 때에는 안내판을 설치하지 아니할 수 있도록 하고 있다.

〈 안내판 설치 의무 면제 시설 〉

구 분	내 용
군사시설	전투진지, 군사목적에 위한 장애물, 폭발물 관련 시설, 사격장, 훈련장, 군용전기통신설비, 그 밖에 군사목적에 직접 공용(供用)되는 시설
국가중요시설	“국가중요시설”이란 공공기관, 공항·항만, 주요 산업시설 등 적에 의하여 점령 또는 파괴되거나 기능이 마비될 경우 국가안보와 국민생활에 심각한 영향을 주게 되는 시설을 말한다.
국가보안시설	국가안전보장에 연쇄적 혼란을 초래할 우려가 있는 시설

5) 영상정보처리기기를 공동으로 설치·운영하려는 경우

영상정보처리기기를 공동으로 설치·운영하려는 자가 영 제24조제1항부터 제3항까지 따른 안내판 설치, 인터넷 홈페이지 게재 또는 사업장·영업소 등 게재를 하는 경우, 법 제25조제4항 각 호의 사항 외에도 해당 영상정보처리기기가 공동으로 설치·운영된다는 사실 및 각 설치·운영 주체들의 명칭도 함께 기재하는 것이 바람직하다.

5. 영상정보처리기기운영자의 의무

가 임의조작 및 녹음기능 사용 금지

영상정보처리기기는 일정한 장소에 지속적으로 설치·운영되고 있으므로, 만일 음성·음향을 녹음하는 기능을 갖추고 있다면 본의 아니게 사람들 간의 대화를 녹음하는 결과를 가져온다. 그러나 타인간의 대화를 청취·녹음하는 행위는 「통신비밀보호법」에서 엄격히 금지하고 있으므로(제3조), 이 법에 따른 영상정보처리기기는 녹음기능을 제한할 필요가 있다. 또한 운영자에 의한 임의조작을 가능하게 할 경우에도 역시 사생활 침해의 우려가 커진다. 여기서 조작이란 영상정보처리기기를 회전시키거나 영상을 확대 또는 축소하는 등 촬영 범위나 대상을 인위적으로 변경시키는 행위를 말한다(보호위원회 결정 제2018-22-247호 참고).

따라서 이 법은 영상정보처리기기운영자는 영상정보처리기기의 설치 목적과 다른 목적으로 영상정보처리기기를 임의로 조작하거나 다른 곳을 비출 수 없도록 하고, 녹음기능 역시 사용할 수 없도록 규정하고 있다(제25조제5항).

참고 「통신비밀보호법」 제3조 등

제3조(통신 및 대화비밀의 보호) ① 누구든지 이 법과 형사소송법 또는 군사법원법의 규정에 의하지 아니하고는 우편물의 검열·전기통신의 감청 또는 통신사실확인자료의 제공을 하거나 공개되지 아니한 타인간의 대화를 녹음 또는 청취하지 못한다. 다만, 다음 각 호의 경우에는 당해 법률이 정하는 바에 의한다.

1. 환부우편물등의 처리 : 우편법 제28조·제32조·제35조·제36조등의 규정에 의하여 폭발물등 우편금지품이 들어 있다고 의심되는 소포우편물(이와 유사한 郵便物을 포함한다)을 개피하는 경우, 수취인에게 배달할 수 없거나 수취인이 수령을 거부한 우편물을 발송인에게 환부하는 경우, 발송인의 주소·성명이 누락된 우편물로서 수취인이 수취를 거부하여 환부하는 때에 그 주소·성명을 알기 위하여 개피하는 경우 또는 유가물이 든 환부불능우편물을 처리하는 경우
2. 수출입우편물에 대한 검사 : 관세법 제256조·제257조 등의 규정에 의한 신서외의 우편물에 대한 통관검사절차
3. 구속 또는 복역중인 사람에 대한 통신 : 형사소송법 제91조, 군사법원법 제131조, 「형의 집행 및 수용자의 처우에 관한 법률」 제41조·제43조·제44조 및 「군에서의 형의 집행 및 군수용자의 처우에 관한 법률」 제42조·제44조 및 제45조에 따른 구속 또는 복역중인 사람에 대한 통신의 관리
4. 파산선고를 받은 자에 대한 통신 : 「채무자 회생 및 파산에 관한 법률」 제484조의 규정에 의하여 파산선고를 받은 자에게 보내온 통신을 파산관재인이 수령하는 경우
5. 혼신제거등을 위한 전파감시 : 전파법 제49조 내지 제51조의 규정에 의한 혼신제거등 전파필서유지를 위한 전파감시의 경우

제14조(타인의 대화비밀 침해금지) ① 누구든지 공개되지 아니한 타인 간의 대화를 녹음하거나 전자장치 또는 기계적 수단을 이용하여 청취할 수 없다.

결정례 CCTV 위치를 표시한 디지털 지도 화면에서 CCTV 아이콘 선택 행위가 조작에 해당하는지 여부

아산경찰서가 아산시 내 설치된 CCTV의 위치를 표시한 디지털 지도 화면에서 CCTV 아이콘을 선택하여 그 장소에 설치된 CCTV 영상정보를 제공받은 사안에서 본 건 지도에서 CCTV 아이콘을 선택하는 것은 필요한 영상정보를 구체적으로 특정하여 제공을 요청하기 위한 것으로 아산경찰서가 CCTV 아이콘을 선택하더라도 해당 CCTV의 촬영 범위나 대상이 변경되지 아니하며 아산시가 수집 중인 영상정보가 변경 없이 제공될 예정이다. 따라서 아산경찰서가 본 건 지도에서 CCTV 아이콘을 선택하여 그 장소에 설치된 CCTV의 영상정보를 제공받는 것은 영상정보처리기기 조작에 해당하지 아니한다(보호위원회 결정 제2018-22-247호).

나 안전성 확보조치 의무

영상정보처리기기운영자는 개인정보가 분실·도난·유출·위조·변조 또는 훼손되지 아니하도록 제29조에 따라 안전성 확보에 필요한 조치를 하여야 한다.

참고 「개인정보 보호법」 제29조

제29조(안전조치의무) 개인정보처리자는 개인정보가 분실·도난·유출·위조·변조 또는 훼손되지 아니하도록 내부 관리계획 수립, 접속기록 보관 등 대통령령으로 정하는 바에 따라 안전성 확보에 필요한 기술적·관리적 및 물리적 조치를 하여야 한다.

다만 개인영상정보는 비디오테이프나 메모리 등에 영상 파일로 생성·저장되므로 그 안전성 확보조치도 일반적인 개인정보와는 다르다. 이에 따라 표준지침에서는 다음과 같이 개인영상정보에 대한 안전성 확보조치를 별도로 규정하고 있다(표준지침 제47조).

< 개인영상정보에 대한 안전성 확보 조치 >

- 개인영상정보의 안전한 처리를 위한 내부 관리계획의 수립·시행, 다만 「개인정보의 안전성 확보조치 기준 고시」 제2조제4호에 따른 '소상공인'은 내부관리계획을 수립하지 아니할 수 있다.
- 개인영상정보에 대한 접근 통제 및 접근 권한의 제한 조치
- 개인영상정보를 안전하게 저장·전송할 수 있는 기술의 적용 (네트워크 카메라의 경우 안전한 전송을 위한 암호화 조치, 개인영상정보파일에 대한 비밀번호 설정 등)
- 처리기록의 보관 및 위조·변조 방지를 위한 조치 (개인영상정보의 생성 일시, 열람할 경우에 열람 목적·열람자·열람 일시 등 기록·관리 조치 등)
- 개인영상정보의 안전한 물리적 보관을 위한 보관시설 마련 또는 잠금장치 설치

다 영상정보처리기기 운영·관리 방침 제정

영상정보처리기기운영자는 다음 각 호의 사항이 포함된 영상정보처리기기 운영·관리 방침을 마련하여야 한다.

영 제25조제1항

1. 영상정보처리기기의 설치 근거 및 설치 목적
2. 영상정보처리기기의 설치 대수, 설치 위치 및 촬영 범위
3. 관리책임자, 담당 부서 및 영상정보에 대한 접근 권한이 있는 사람
4. 영상정보의 촬영시간, 보관기간, 보관장소 및 처리방법
5. 영상정보처리기기운영자의 영상정보 확인 방법 및 장소
6. 정보주체의 영상정보 열람 등 요구에 대한 조치
7. 영상정보 보호를 위한 기술적·관리적 및 물리적 조치
8. 그 밖에 영상정보처리기기의 설치·운영 및 관리에 필요한 사항

영상정보처리기기운영자가 영상정보처리기기 운영·관리 방침을 마련한 경우에는 법 제 30조에 따른 개인정보 처리방침을 정하지 아니할 수 있다(제25조제7항). 또한 영상정보처리기기 설치·운영에 관한 사항을 법 제30조에 따른 개인정보 처리방침에 포함하여 정할 수도 있다(표준지침 제36조제2항).

영상정보처리기기운영자가 영상정보처리기기 운영·관리 방침을 정한 경우에는 이를 공개하여야 한다. 공개에 관하여는 영 제31조제2항 및 제3항을 준용한다(영 제25조제2항). 즉, 영상정보처리기기 운영·관리 방침은 원칙적으로 영상정보처리기기 운영자의 인터넷 홈페이지에 지속적으로 게재해야 하며, 인터넷 홈페이지에 게재할 수 없는 경우에는 다음 각 호의 어느 하나 이상의 방법으로 영상정보처리기기 운영·관리 방침을 공개해야 한다.

1. 개인정보처리자의 사업장등의 보기 쉬운 장소에 게시하는 방법
2. 관보(개인정보처리자가 공공기관인 경우만 해당한다)나 개인정보처리자의 사업장등이 있는 시·도 이상의 지역을 주된 보급지역으로 하는 「신문 등의 진흥에 관한 법률」 제2조제1호 가목·다목 및 같은 조 제2호에 따른 일반일간신문, 일반주간신문 또는 인터넷신문에 실는 방법
3. 같은 제목으로 연 2회 이상 발행하여 정보주체에게 배포하는 간행물·소식지·홍보지 또는 청구서 등에 지속적으로 실는 방법
4. 재화나 용역을 제공하기 위하여 개인정보처리자와 정보주체가 작성한 계약서 등에 실어 정보주체에게 발급하는 방법

라 개인정보영상정보 관리책임자 지정

영상정보처리기기운영자는 개인정보영상정보의 처리에 관한 업무를 총괄해서 책임지는 개인정보영상정보 관리책임자를 지정하여야 한다. 관리책임자는 제31조에 따른 개인정보 보호책임자에 준하여 업무를 수행한다. 다만, 개인정보 보호책임자가 이미 지정되어 있는 경우에는 중복하여 책임자를 지정할 필요는 없으므로, 그 개인정보 보호책임자가 개인정보영상정보 관리책임자의 업무를 수행할 수 있다.

마 개인영상정보 관리대장 작성

영상정보처리기기운영자는 개인영상정보를 수집목적 이외로 이용하거나 제3자에게 제공한 경우, 아래 사항을 기록·관리해야 한다(표준지침 제42조제1항).

<개인영상정보 목적 외 이용·제3자 제공시 기록사항>

1. 개인영상정보 파일의 명칭
2. 이용하거나 제공받은 자(공공기관 또는 개인)의 명칭
3. 이용 또는 제공의 목적
4. 법령상 이용 또는 제공근거가 있는 경우 그 근거
5. 이용 또는 제공의 기간이 정하여져 있는 경우에는 그 기간
6. 이용 또는 제공의 형태

또한 영상정보처리기기운영자가 개인영상정보를 파기하는 경우에도 다음 사항을 기록하고 관리하여야 한다(표준지침 42조제2항).

<개인영상정보 파기시 기록사항>

1. 파기하는 개인영상정보 파일의 명칭
2. 개인영상정보 파기 일시 (사전에 파기 시기 등을 정한 자동 삭제의 경우에는 파기 주기 및 자동 삭제 여부에 관한 확인 시기)
3. 개인영상정보 파기 담당자

또한 영상정보처리기기운영자는 정보주체가 개인영상정보에 대한 열람등요구 또는 파기 요구를 한 경우에는 그에 대한 조치사항과 내용을 기록·관리하여야 한다(표준지침 제44조제5항 및 제6항).

<정보주체의 개인영상정보 열람등 요구시 기록사항>

1. 개인영상정보 열람등을 요구한 정보주체의 성명 및 연락처
2. 정보주체가 열람등을 요구한 개인영상정보 파일의 명칭 및 내용
3. 개인영상정보 열람등의 목적
4. 개인영상정보 열람등을 거부한 경우 그 거부의 구체적 사유
5. 정보주체에게 개인영상정보 사본을 제공한 경우 해당 영상정보의 내용과 제공한 사유

영상정보처리기기운영자가 위의 사항을 기록·관리하는 경우에는 표준지침 별지서식 제3호에 따른 ‘개인영상정보 관리대장’ 양식을 활용할 수 있다.

< 개인영상정보 관리대장 >

번호	구분	일시	파일명/형태	담당자	목적/사유	이용·제공 받는 제3자/열람등 요구자	이용·제공 근거	이용·제공 형태	기간
1	<input type="checkbox"/> 이용 <input type="checkbox"/> 제공 <input type="checkbox"/> 열람 <input type="checkbox"/> 파기								
2	<input type="checkbox"/> 이용 <input type="checkbox"/> 제공 <input type="checkbox"/> 열람 <input type="checkbox"/> 파기								
3	<input type="checkbox"/> 이용 <input type="checkbox"/> 제공 <input type="checkbox"/> 열람 <input type="checkbox"/> 파기								

바 영상정보처리기기 설치·운영 사무의 위탁

영상정보처리기기의 설치·운영은 직접 하는 경우도 있지만, 상당수는 외부의 전문업체에 설치·운영을 위탁하는 형태로 이루어지고 있다. 이러한 운영 현실을 감안하여, 이 법은 영상정보처리기기 운영자는 영상정보처리기기의 설치·운영에 관한 사무를 위탁할 수 있도록 허용하고 있다(제25조제8항).

특히, 공공기관이 영상정보처리기기 설치·운영에 관한 사무를 위탁하는 경우에는 다음 각 호의 내용이 포함된 문서로 하여야 하며, 안내판에 수탁자의 명칭 및 연락처를 게재하여야 한다(영 제26조).

< 공공기관 영상정보처리기기 설치·운영 위탁시 문서 포함사항 >

- | |
|--|
| <ol style="list-style-type: none"> 1. 위탁하는 사무의 목적 및 범위 2. 재위탁 제한에 관한 사항 3. 영상정보에 대한 접근 제한 등 안전성 확보 조치에 관한 사항 4. 영상정보의 관리 현황 점검에 관한 사항 5. 위탁받는 자가 준수하여야 할 의무를 위반한 경우의 손해배상 등 책임에 관한 사항 |
|--|

다만, 민간기업·단체·개인이 영상정보처리기기 설치·운영에 관한 사무를 위탁하는 경우에는 위탁방법 등에 관하여 특별한 제한을 두고 있지 않으므로, 결과적으로는 제26조(업무위탁에 따른 개인정보의 처리 제한)의 규정이 적용된다.

사 영상정보처리기기 설치·운영 점검

영상정보처리기기는 설치된 이후에도 그 설치목적에 맞게 운영되는지, 개인영상정보의 침해 우려는 없는지 등을 지속적으로 점검하여 문제점을 보완할 필요가 있다. 특히 공공기관은 공익목적 수행을 위해 다수의 영상정보처리기기를 운영하고 있으므로 민간에 비해 더욱 엄격한 점검이 필요하다.

공공기관의 장이 영상정보처리기기를 설치·운영하는 경우에는 아래의 사항을 고려하여 이 법 및 표준지침 준수 여부에 대한 자체점검을 실시하고, 다음 해 3월 31일까지 그 결과를 보호위원회에 통보하고 영 제34조제3항에 따른 시스템(개인정보 보호 포털)에 등록하여야 한다. 또한 그 결과를 포털시스템 홈페이지를 통해서 공개하여야 한다.

< 공공기관 영상정보처리기기 점검시 고려사항 >

1. 영상정보처리기기의 운영·관리 방침에 열거된 사항
2. 관리책임자의 업무 수행 현황
3. 영상정보처리기기의 설치 및 운영 현황
4. 개인영상정보 수집 및 이용·제공·파기 현황
5. 위탁 및 수탁자에 대한 관리·감독 현황
6. 정보주체의 권리행사에 대한 조치 현황
7. 기술적·관리적·물리적 조치 현황
8. 영상정보처리기 설치·운영의 필요성 지속 여부 등

공공기관 외의 영상정보처리기기운영자는 영상정보처리기기 설치·운영 점검이 의무화 되어 있지는 않으나, 정보주체의 개인영상정보의 침해가 우려되는 경우에는 자체점검 등 개인영상정보의 침해 방지를 위해 적극 노력하여야 한다.

6. 개인영상정보의 열람등 요구

일반적으로 영상정보처리기기를 통하여 촬영된 영상은 그 기기를 설치·운영하는 자가 열람·활용하는 것이 일반적이지만, 경우에 따라서는 영상정보처리기기를 통해 촬영된 정보주체가 자신에 관한 영상정보를 활용하기를 원하는 경우도 있을 수 있다. 예를 들어 공공시설에서 물건 도난이나 기타 범죄 행위를 겪은 당사자가 그 범죄 수사 등을 위해 영상정보의 열람이나 존재확인을 요구하는 경우가 그것이다. 이에 따라 표준지침에서는 개인영상정보의 열람등 요구에 대한 규정을 두고 있다.

가 개인영상정보 열람등 요구

정보주체는 영상정보처리기기운영자가 처리하는 개인영상정보에 대하여 존재 또는 열람 확인을 해당 영상정보처리기기운영자에게 요구하는 경우가 있을 수 있다(예를 들어 자신의 물건의 도난을 확인하기 위하여 CCTV 촬영 화면을 열람 요구). 그러나 정보주체와 관련이 없는 개인영상정보에 대해서도 열람등을 허용하면 그 영상에 촬영된 타인의 사생활 침해가 발생할 수도 있다. 따라서 열람등을 요구할 수 있는 개인영상정보는 정보주체 자신이 촬영된 개인영상정보 및 명백히 정보주체의 급박한 생명, 신체, 재산의 이익을 위하여 필요한 개인영상정보에 한한다.

나 영상정보처리기기운영자의 조치

영상정보처리기기운영자는 개인영상정보 열람등 요구를 받았을 때에는 지체 없이 필요한 조치를 취하여야 한다. 다만 이 경우에도 사생활 침해 방지 등을 위해, 열람등 요구를 한 자가 본인이거나 정당한 대리인인지를 주민등록증·운전면허증·여권 등의 신분증명서를 제출받아 확인하여야 한다. 또한, 열람등으로 인하여 정보주체 이외의 자를 명백히 알아볼 수 있거나 정보주체 이외의 자의 사생활 침해의 우려가 있는 경우에는 열람등 요구를 한 정보주체 이외의 자의 개인영상정보를 알아볼 수 없도록 마스킹 처리를 하는 등의 보호조치를 취하여야 한다.

영상정보처리기기운영자는 다음의 사유에 해당하는 경우에는 정보주체의 열람등 요구를 거부할 수 있다. 이 경우 영상정보처리기기운영자는 10일 이내에 서면 등으로 거부 사유를 정보주체에게 통지하여야 한다.

< 개인영상정보 열람등 요구에 대한 거부 사유 >

1. 범죄수사·공소유지·재판수행에 중대한 지장을 초래하는 경우(공공기관에 한함)
2. 개인영상정보의 보관기간이 경과하여 파기한 경우
3. 기타 정보주체의 열람등 요구를 거부할 만한 정당한 사유가 존재하는 경우

7. 영상정보처리기기 설치·운영 지침의 제정·권장

보호위원회는 이 법 및 영에서 규정한 사항 외에 영상정보처리기기의 설치·운영에 관한 기준, 설치·운영 사무의 위탁 등에 대해 제12조제1항에 따른 표준지침으로 정하여 영상정보처리기기운영자에게 그 준수를 권장할 수 있다.

8. 공개된 장소에 설치된 영상정보처리기에 대한 법적용의 일부제외

앞서 설명한 바와 같이, 공개된 장소에 영상정보처리기를 설치·운영하는 경우에는 일반적 개인정보 보호 원칙이 적용되기 곤란하므로 제25조에서 별도의 규제를 두고 있다. 이에 따라서 이 법은 공개된 장소에 영상정보처리기를 설치·운영하여 처리되는 개인정보에 대하여는 제15조(개인정보의 수집·이용), 제22조(동의를 받는 방법), 제27조제1항·제2항(영업양도 등에 따른 개인정보의 이전 제한), 제34조(개인정보 유출 통지 등) 및 제37조(개인정보의 처리정지 등)를 적용하지 아니하도록 규정하고 있다.

법률의 일부 적용제외(제58조제2항)

- 제15조(개인정보의 수집·이용) 정보주체에 대한 개인정보 수집·이용 고지 및 동의획득 의무 ⇒ 안내판 설치 등의 의무로 대체
- 제22조(동의를 받는 방법) 정보주체에게 각각의 동의사항을 구분하여 알리고 개별적으로 동의 ⇒ 공개된 장소에 설치된 영상정보처리기는 불특정 다수의 특성상 동의곤란
- 제27조(영업양도 등에 따른 개인정보의 이전 제한) 영업의 양도·합병시 통지의무 ⇒ 불특정 다수의 특성상 통지곤란
- 제34조(개인정보 유출 통지 등) 개인정보 유출사고 발생시 정보주체에 대한 통지 및 관계기관에 대한 신고의무 ⇒ 불특정 다수의 특성상 통지곤란
- 제37조(개인정보의 처리정지 등) 개인정보처리자가 처리하고 있는 자신의 개인정보에 대한 처리정지 요구 ⇒ 특정 정보주체만 처리정지 불가

다만, 공개된 장소에서 영상정보처리기를 설치·운영하여 개인정보를 수집하는 행위가 제15조제1항제2호, 제3호, 제5호 중 어느 하나에 해당하는 경우에는 제17조제1항제2호에 따라 영상정보처리기를 설치·운영한 자가 개인정보를 그 수집 목적 범위 내에서 개인영상정보를 제3자에게 제공하는 것은 가능하다.

결정례 개인영상정보의 수집이 제15조제1항제3호에 해당하는 경우 제17조에 따른 제3자 제공 허용 여부

지방자치단체의 범죄 예방 또는 시설안전 업무는 「지방자치법」 제9조제1항의 자치사무에 해당한다고 볼 수 있어, 서울특별시 중구가 범죄 예방이나 시설안전을 목적으로 본 건 CCTV를 설치하여 개인영상정보를 수집하는 것은 「개인정보 보호법」 제15조제1항제3호의 ‘공공기관의 법령 등에서 정하는 소관업무를 위하여 불가피한 경우’에 해당한다. 한양도성 보존·관리 업무는 화재·재난, 문화재 손상행위 등에 의한 한양도성의 멸실·훼손 방지 등을 그 내용으로 하므로, 이는 시설안전, 문화재 손상 범죄 예방 등을 목적으로 하는 것에 해당한다. 따라서 서울특별시 중구가 본 건 CCTV로 수집한 개인영상정보를 각 범죄 예방 또는 시설안전의 설치 목적 부분 내에서 서울특별시에 제공하는 것은 「개인정보 보호법」 제15조제1항제3호에 따라 개인영상정보를 수집한 목적 범위에서 이를 제공하는 경우로서 같은 법 제17조제1항에 따라 허용된다 할 것이다.

9. 벌칙규정

위반행위	벌칙
설치·운영기준을 위반한 자 (제25조제1항 위반)	3천만원 이하의 과태료 (제75조제2항제7호)
안전성 확보에 필요한 조치를 하지 아니한 자 (제25조제6항 위반)	3천만원 이하의 과태료 (제75조제2항제6호)
화장실, 목욕실 등에 설치·운영한 자 (제25조제2항 위반)	5천만원 이하의 과태료 (제75조제1항제3호)
안내판 설치 등 조치의무 위반 (제25조제4항 위반)	1천만원 이하의 과태료 (제75조제4항제3호)
부정한 목적으로 영상정보처리기기를 임의 조작하거나 다른 곳을 비추는 자, 녹음기능을 사용한 자 (제25조제5항 위반)	3년 이하의 징역 또는 3천만원 이하의 벌금 (제72조제1호)
안전성 확보에 필요한 조치를 하지 아니하여 개인정보를 분실·도난·유출·위조·변조 또는 훼손당한 자 (제25조제6항 위반)	2년 이하의 징역 또는 2천만원 이하의 벌금 (제73조제1호)

10. 질의 응답

Q | 안내판은 CCTV가 설치된 곳마다 설치해야 하는가?

A 공개된 장소에 설치된 CCTV마다 안내판을 설치하는 것이 원칙이나, 건물 안에 다수의 CCTV를 운영하는 경우 출입구 등 정보주체가 출입하면서 잘 볼 수 있는 곳에 시설 또는 장소 전체가 영상정보 처리기기 설치지역임을 표시하는 안내판을 설치할 수 있다.

또한, 공공기관이 원거리 촬영, 과속·신호위반 단속 또는 교통흐름 조사 등 목적으로 설치하는 경우로 개인정보 침해 우려가 적은 경우에 해당하거나 산불감시용 등 장소적 특성으로 인하여 안내판을 설치하는 것이 불가능 하거나 설치하더라도 정보주체가 쉽게 알아볼 수 없는 경우에는 안내판 설치를 갈음하여 영상정보처리 기기운영자의 인터넷 홈페이지에 CCTV설치 목적 및 장소, 촬영범위 및 시간, 관리책임자 및 연락처를 게재할 수 있다. (인터넷홈페이지를 운영하지 않는 경우에는 사업장 등에 게시, 일반일간신문, 일반 주간신문 또는 인터넷 신문에 실는 방법 가능)

Q | CCTV 촬영 화면을 공익 목적으로 공개할 수 있는가?

A 영상정보처리기로 촬영된 화면을 공익 목적으로 일반 대중에게 공개·제공하는 경우가 있다. 예를 들어 교통정보 CCTV 화면, 관광지·유적지의 CCTV 화면을 일반 시민에게 인터넷·스마트폰으로 제공하는 경우가 이에 해당한다.

이러한 경우는, 그 영상정보처리기의 본래 설치·운영 목적 제25조제1항 각호의 목적에 부합하고, 그 촬영영상이 교통정보나 관광지 등의 전경(全景)이 비추어지는 정도에 그치고 개인을 구체적으로 식별할 수 있을 정도가 아니라면 이를 공익 목적으로 공개하는 것은 무방하다.

Q | 경찰청에서 교통영상정보를 외부기관에 제공할 수 있는가?

A 경찰청이 교통영상정보를 외부기관에 연계·송출하면서 개인정보가 포함될 정도로 CCTV를 제어한 경우라면 제18조제1항에 저촉된다. 다만, 동법 제17조 제1항, 제18조제2항 등의 예외 사유에 해당되는 경우 내지 제58조에 해당되는 경우에는 예외적으로 외부기관에 연계·송출할 수 있다.

Q | 안내판의 규격이나 재질에 대한 기준은 어떠한가?

A 안내판은 촬영범위 내에서 정보주체가 알아보기 쉬운 장소에 누구라도 용이하게 판독될 수 있게 설치되면 되며, 그 범위 안에서는 영상정보처리기기 운영자가 안내판 크기, 설치위치 등을 자율적으로 정할 수 있다.

<안내판 및 홈페이지 게재 내용 예시>

CCTV 설치 안내	
◆ 설치목적 : 범죄예방	
◆ 장 소 : 00동 00번지	
◆ 촬영범위 : 100M 전방향	
◆ 시 간 : 24시간 (종일)	
◆ 관리책임자 : 00부 00과 과장	
◆ 연 락 처 : 02-000-0000 (설치·운영을 위탁한 경우)	
◆ 수탁관리자 : 000, 02-000-0000	

Q 지방자치단체에서 공개된 장소에 설치한 CCTV를 통해 쓰레기 불법투기행위가 촬영된 경우, 불법투기자 인적사항을 조회하기 위한 목적으로 지역주민에게 해당 영상을 공개할 수 있는가?

A 개인정보 보호 원칙을 규정한 「개인정보 보호법」 제3조는 지방자치단체를 포함한 개인정보처리자에게 '정보주체의 사생활 침해'를 최소화하는 방법으로 개인정보를 처리'하도록 의무를 부여하고 있다. 따라서 지방자치단체가 정보주체의 개인정보를 공개하는 것은 법률의 근거가 명확한 경우에 한하여 정보주체의 사생활 침해를 최소화하는 방법으로 이루어져야 할 것이다.

불법 투기자의 영상 촬영, 즉 개인정보 수집의 직접적인 목적은 불법 투기행위의 증거자료 수집에 국한되는 것으로 봄이 상당하다고 할 것이다. 따라서 동 증거자료를 일반에 공개하는 것까지 수집 목적 범위에 포함된다고 보기에는 무리가 있다고 할 것이다. 투기자의 인적사항 조회는 지방자치단체 자체 조사 또는 관계 기관 조회 등을 통해서도 가능하며 경찰도 이러한 절차를 활용하고 있는 바, 지방자치단체는 정보주체의 사생활 침해를 최소화할 수 있는 방법으로 개인정보를 처리해야 할 것이다.

제26조 | 업무위탁에 따른 개인정보의 처리 제한

법률

제26조(업무위탁에 따른 개인정보의 처리 제한) ① 개인정보처리자가 제3자에게 개인정보의 처리 업무를 위탁하는 경우에는 다음 각 호의 내용이 포함된 문서에 의하여야 한다.

1. 위탁업무 수행 목적 외 개인정보의 처리 금지에 관한 사항
2. 개인정보의 기술적·관리적 보호조치에 관한 사항
3. 그 밖에 개인정보의 안전한 관리를 위하여 대통령령으로 정한 사항

② 제1항에 따라 개인정보의 처리 업무를 위탁하는 개인정보처리자(이하 “위탁자”라 한다)는 위탁하는 업무의 내용과 개인정보 처리 업무를 위탁받아 처리하는 자(이하 “수탁자”라 한다)를 정보주체가 언제든지 쉽게 확인할 수 있도록 대통령령으로 정하는 방법에 따라 공개하여야 한다.

③ 위탁자가 재화 또는 서비스를 홍보하거나 판매를 권유하는 업무를 위탁하는 경우에는 대통령령으로 정하는 방법에 따라 위탁하는 업무의 내용과 수탁자를 정보주체에게 알려야 한다. 위탁하는 업무의 내용이나 수탁자가 변경된 경우에도 또한 같다.

④ 위탁자는 업무 위탁으로 인하여 정보주체의 개인정보가 분실·도난·유출·위조·변조 또는 훼손되지 아니하도록 수탁자를 교육하고, 처리 현황 점검 등 대통령령으로 정하는 바에 따라 수탁자가 개인정보를 안전하게 처리하는지를 감독하여야 한다.

⑤ 수탁자는 개인정보처리자로부터 위탁받은 해당 업무 범위를 초과하여 개인정보를 이용하거나 제3자에게 제공하여서는 아니 된다.

⑥ 수탁자가 위탁받은 업무와 관련하여 개인정보를 처리하는 과정에서 이 법을 위반하여 발생한 손해배상책임에 대하여는 수탁자를 개인정보처리자의 소속 직원으로 본다.

⑦ 수탁자에 관하여는 제15조부터 제25조까지, 제27조부터 제31조까지, 제33조부터 제38조까지 및 제59조를 준용한다.

시행령

제28조(개인정보의 처리 업무 위탁 시 조치) ① 법 제26조제1항제3호에서 “대통령령으로 정한 사항”이란 다음 각 호의 사항을 말한다.

1. 위탁업무의 목적 및 범위
2. 재위탁 제한에 관한 사항
3. 개인정보에 대한 접근 제한 등 안전성 확보 조치에 관한 사항
4. 위탁업무와 관련하여 보유하고 있는 개인정보의 관리 현황 점검 등 감독에 관한 사항
5. 법 제26조제2항에 따른 수탁자(이하 “수탁자”라 한다)가 준수하여야 할 의무를 위반한 경우의 손해배상 등 책임에 관한 사항

② 법 제26조제2항에서 “대통령령으로 정하는 방법”이란 개인정보 처리 업무를 위탁하는 개인정보처리자(이하 “위탁자”라 한다)가 위탁자의 인력

	<p>넷 홈페이지에 위탁하는 업무의 내용과 수탁자를 지속적으로 게재하는 방법을 말한다.</p> <p>③ 제2항에 따라 인터넷 홈페이지에 게재할 수 없는 경우에는 다음 각 호의 어느 하나 이상의 방법으로 위탁하는 업무의 내용과 수탁자를 공개하여야 한다.</p> <ol style="list-style-type: none"> 1. 위탁자의 사업장등의 보기 쉬운 장소에 게시하는 방법 2. 관보(위탁자가 공공기관인 경우만 해당한다)나 위탁자의 사업장등이 있는 시·도 이상의 지역을 주된 보급지역으로 하는 「신문 등의 진흥에 관한 법률」 제2조제1호가목·다목 및 같은 조 제2호에 따른 일반일간신문, 일반주간신문 또는 인터넷신문에 실는 방법 3. 같은 제목으로 연 2회 이상 발행하여 정보주체에게 배포하는 간행물·소식지·홍보지 또는 청구서 등에 지속적으로 실는 방법 4. 재화나 용역을 제공하기 위하여 위탁자와 정보주체가 작성한 계약서 등에 실어 정보주체에게 발급하는 방법 <p>④ 법 제26조제3항 전단에서 “대통령령으로 정하는 방법”이란 서면, 전자우편, 팩스, 전화, 문자전송 또는 이에 상당하는 방법(이하 “서면등의 방법”이라 한다)을 말한다.</p> <p>⑤ 위탁자가 과실 없이 제4항에 따른 방법으로 위탁하는 업무의 내용과 수탁자를 정보주체에게 알릴 수 없는 경우에는 해당 사항을 인터넷 홈페이지에 30일 이상 게재하여야 한다. 다만, 인터넷 홈페이지를 운영하지 아니하는 위탁자의 경우에는 사업장등의 보기 쉬운 장소에 30일 이상 게시하여야 한다.</p> <p>⑥ 위탁자는 수탁자가 개인정보 처리 업무를 수행하는 경우에 법 또는 이 영에 따라 개인정보처리자가 준수하여야 할 사항과 법 제26조제1항 각 호의 사항을 준수하는지를 같은 조 제4항에 따라 감독하여야 한다.</p>
표준 지침	<p>제16조(수탁자의 선정 시 고려사항) 개인정보의 처리 업무를 위탁하는 개인정보처리자(이하 “위탁자”라 한다)가 개인정보 처리 업무를 위탁받아 처리하는 자(이하 “수탁자”라 한다)를 선정할 때에는 인력과 물적 시설, 재정 부담능력, 기술 보유의 정도, 책임능력 등 개인정보 처리 및 보호 역량을 종합적으로 고려하여야 한다.</p> <p>제17조(개인정보보호 조치의무) 수탁자는 위탁받은 개인정보를 보호하기 위하여 「개인정보의 안전성 확보조치 기준 고시」에 따른 관리적·기술적·물리적 조치를 하여야 한다.</p>

최근 비용절감, 업무효율화, 서비스 개선 등 다양한 목적으로 민간기업은 물론 공공기관들조차 각종 업무를 외부 기업이나 개인에게 위탁하는 사례가 증가하고 있다. 업무위탁은 현대사회의 분업화에 따라 나타난 자연스런 경영방식의 하나이나 대부분 고객의 개인정보도 함께 이전하게 되어 개인정보가 재유통되거나 남용될 위험이 크므로 이에 대한 대책이 필요하다.

< 업무위탁으로 인한 개인정보 침해유형 >

- 판매실적 증대를 위한 무분별한 재위탁 등 개인정보의 재제공
- 다른 회사의 상품·서비스를 동시 취급하면서 개인정보를 공유
- 고객 개인정보를 이용하여 부가서비스 등 다른 서비스에 무단 가입
- 서비스가입신청서 등 개인정보의 분실·유출
- 고객DB를 빼내어 판매
- 정보시스템 안전조치 미비로 인한 개인정보 유출 등

1. 업무위탁의 유형

업무위탁의 유형은 크게 개인정보의 수집·관리 업무 그 자체를 위탁하는 개인정보처리업무 위탁과 개인정보의 이용·제공이 수반되는 일반업무를 위탁하는 개인정보취급업무 위탁으로 구분될 수 있다. 또한 개인정보취급업무 위탁은 다시 홍보·판매권유 등 마케팅업무를 위탁과 상품배달·애프터서비스 등 계약이행업무를 위탁으로 구분할 수도 있다.

2. 업무위탁과 제3자 제공의 차이

업무위탁과 개인정보 제3자 제공 모두 개인정보가 다른 사람에게 이전하거나 다른 사람과 공동으로 이용하게 된다는 측면에서는 동일하지만 개인정보 이전의 목적이 전혀 다르고 이전된 개인정보에 대한 관리·감독 등 법률적 관계도 전혀 다르다.

업무위탁의 경우에는 개인정보처리자의 업무처리 범위 내에서 개인정보 처리가 행해지고 위탁자인 개인정보처리자의 관리·감독을 받지만, 제3자 제공은 제3자의 이익을 위해서 개인정보 처리가 행해지고 제3자가 자신의 책임 하에 개인정보를 처리하게 된다.

판례는 개인정보 제3자 제공은 본래의 개인정보 수집·이용 목적의 범위를 넘어 정보를 제공받는 자의 업무처리와 이익을 위하여 개인정보가 이전되는 경우인 반면, 개인정보의 처리위탁은 본래의 개인정보 수집·이용 목적과 관련된 위탁자 본인의 업무 처리와 이익을 위하여 개인정보가 이전되는 경우를 의미한다고 실시하고 있다(대법원 2017. 4. 7. 선고 2016도13263 판결 참고). 동 판례에 따르면 개인정보 처리위탁에 있어 수탁자는 위탁자로부터 위탁사무 처리에 따른 대가를 지급받는 것 외에는 개인정보 처리에 관하여 독자적인 이익을 가지지 않고 정보제공자의 관리·감독 아래 위탁받은 범위 내에서만 개인정보를 처리하게 되므로 「개인정보 보호법」 제17조에 정한 ‘제3자’에 해당하지 않는다고 한다.

판례 개인정보 처리위탁에 있어 '수탁자'가 제3자 제공의 '제3자'에 해당하는지 여부 등

「개인정보 보호법」 제17조에서 말하는 개인정보의 '제3자 제공'은 본래의 개인정보 수집·이용 목적의 범위를 넘어 정보를 제공받는 자의 업무처리와 이익을 위하여 개인정보가 이전되는 경우인 반면, 「개인정보 보호법」 제26조에서 말하는 개인정보의 '처리위탁'은 본래의 개인정보 수집·이용 목적과 관련된 위탁자 본인의 업무 처리와 이익을 위하여 개인정보가 이전되는 경우를 의미한다. 개인정보 처리위탁에 있어 수탁자는 위탁자로부터 위탁사무 처리에 따른 대가를 지급받는 것 외에는 개인정보 처리에 관하여 독자적인 이익을 가지지 않고, 정보제공자의 관리·감독 아래 위탁받은 범위 내에서만 개인정보를 처리하게 되므로, 「개인정보 보호법」 제17조에 정한 '제3자'에 해당하지 않는다. 한편 어떠한 행위가 개인정보의 제공인지 아니면 처리위탁인지는 개인정보의 취득 목적과 방법, 대가 수수 여부, 수탁자에 대한 실질적인 관리·감독 여부, 정보주체 또는 이용자의 개인정보 보호 필요성에 미치는 영향 및 이러한 개인정보를 이용할 필요가 있는 자가 실질적으로 누구인지 등을 종합하여 판단하여야 한다(대법원 2017. 4. 7. 선고 2016도13263 판결).

따라서 업무위탁의 경우에는 수탁자에게 개인정보가 이전되더라도 개인정보에 대한 개인정보처리자의 관리·감독권이 미치지만, 제3자 제공의 경우에는 일단 개인정보가 제3자에게 제공되고 나면 개인정보처리자의 관리·감독권이 미치지 못한다.

< 업무위탁과 제3자 제공의 비교 >

구분	업무위탁	제3자 제공
관련조항	제26조	제17조
예시	·배송업무 위탁, TM 위탁 등	·사업제휴, 개인정보 판매 등
이전목적	·위탁자의 이익을 위해 처리 (수탁업무 처리)	·제3자의 이익을 위해 처리
예측 가능성	·정보주체가 사전 예측 가능 (정보주체의 신뢰 범위내)	·정보주체가 사전 예측 곤란 (정보주체의 신뢰 범위밖)
이전 방법	·원칙 : 위탁사실 공개 ·예외 : 위탁사실 고지(마케팅 업무위탁)	·원칙 : 제공목적 등 고지 후 정보주체 동의 획득
관리·감독책임	위탁자 책임	제공받는 자 책임
손해배상책임	위탁자 부담(사용자 책임)	제공받는 자 부담

한편 개인정보가 제3자에게 이전되는 목적에 따라 업무위탁과 제3자 제공의 성격을 겸하는 경우가 있을 수 있다. 이 경우 법에서 제3자 제공의 요건만 갖추어도 된다는 예외 규정도 없을 뿐 아니라, 정보주체로 하여금 자신의 정보가 어떻게 활용되고 있는지 정확히 알려야 한다는 측면에서 제3자 제공과 관련하여서는 해당 조항에서 정하고 있는 동의 요건을, 업무위탁과 관련하여서는 아래 정하는 방법에 따른 절차와 방법을 갖추어야 할 것이다.

3. 업무위탁의 절차·방법

가 위탁 목적 등의 문서화

개인정보처리자가 제3자에게 개인정보의 처리 업무를 위탁하는 경우에는 다음 각 호의 내용이 포함된 문서에 의하여야 한다. 이 경우 문서는 법적 구속력이 있는 계약서(계약서와 동일한 효력을 가진 문서 포함)를 말한다.

1. 위탁업무 수행 목적 외 개인정보의 처리 금지에 관한 사항
2. 개인정보의 기술적·관리적 보호조치에 관한 사항
3. 위탁업무의 목적 및 범위
4. 재위탁 제한에 관한 사항
5. 개인정보에 대한 접근 제한 등 안전성 확보 조치에 관한 사항
6. 위탁업무와 관련하여 보유하고 있는 개인정보의 관리 현황 점검 등 감독에 관한 사항
7. 수탁자가 준수하여야 할 의무를 위반한 경우의 손해배상 등 책임에 관한 사항

나 일반 위탁업무 내용 등의 공개

개인정보 처리 업무를 위탁하는 개인정보처리자(위탁자)는 위탁하는 업무의 내용과 개인정보 처리 업무를 위탁받아 처리하는 자(수탁자)를 정보주체가 언제든지 쉽게 확인할 수 있도록 자신의 인터넷 홈페이지에 지속적으로 게재하는 방법으로 공개하여야 한다(영 제28조제2항).

위탁자가 위탁업무의 내용, 수탁자의 이름 등을 인터넷 홈페이지에 게재할 수 없는 경우에는 다음 각 호의 어느 하나 이상의 방법으로 공개하여야 한다(영 제28조제3항).

위탁업무 등의 공개방법(영 제28조제3항)

1. 위탁자의 사업장등의 보기 쉬운 장소에 게시하는 방법
2. 관보(위탁자가 공공기관인 경우만 해당한다)나 위탁자의 사업장등이 있는 시·도 이상의 지역을 주된 보급지역으로 하는 「신문 등의 진흥에 관한 법률」 제2조제1호가목·다목 및 같은 조 제2호에 따른 일반일간신문, 일반주간신문 또는 인터넷신문에 실는 방법
3. 같은 제목으로 연 2회 이상 발행하여 정보주체에게 배포하는 간행물·소식지·홍보지 또는 청구서 등에 지속적으로 실는 방법
4. 재화나 용역을 제공하기 위하여 위탁자와 정보주체가 작성한 계약서 등에 실어 정보주체에게 발급하는 방법

다 홍보, 판매권유 등 위탁업무 내용 등의 통지

위탁자가 재화 또는 서비스를 홍보하거나 판매를 권유하는 업무를 위탁하는 경우에는 서면, 전자우편, 모사전송, 전화, 문자전송 또는 이에 상당하는 방법으로 위탁하는 업무의 내용과 수탁자를 정보주체에게 알려야 한다(영 제28조제4항). 위탁하는 업무의 내용이나 수탁자가 변경된 경우에도 또한 같다.

위탁자가 과실 없이 서면, 전자우편 등의 방법으로 위탁하는 업무의 내용과 수탁자를 정보주체에게 알릴 수 없는 경우에는 해당 사항을 인터넷 홈페이지에 30일 이상 게시하여야 한다. 다만, 인터넷 홈페이지를 운영하지 않는 위탁자의 경우에는 사업장등의 보기 쉬운 장소에 30일 이상 게시하여야 한다(영 제28조제5항).

라 수탁자 선정시 고려사항

개인정보처리자가 개인정보 처리 업무 수탁자를 선정할 때에는 수탁자의 ① 인력 ② 물적 시설 ③ 재정 부담능력 ④ 기술 보유의 정도 ⑤ 책임능력 등 수탁자의 개인정보 처리 및 보호역량을 종합적으로 고려하여 선정하여야 한다(표준지침 제16조).

사례 위탁업무가 단발성으로 이루어지는 경우

위탁업무가 1회(단발)성으로 이루어지는 경우로서 위탁기간이 매우 짧아 위탁기간 내 홈페이지 공개나 수탁업체 교육이 불가능한 경우에는 위탁계약 체결시 수탁업체가 지켜야 할 사항을 계약서류 등을 통해 명확히 고지하고 수탁업체가 관련 직원에게 전달하여 교육할 수 있도록 요청할 수 있음

4. 위탁자의 책임과 의무

가 수탁자에 대한 교육 및 감독

위탁자는 업무 위탁으로 인하여 정보주체의 개인정보가 분실·도난·유출·변조 또는 훼손되지 아니하도록 수탁자를 교육하고, 수탁자가 개인정보를 안전하게 처리하는지를 감독하여야 한다(제4항).

또한 위탁자는 수탁자가 이 법 또는 영에 따라 개인정보처리자가 준수하여야 할 사항 및 위·수탁 계약(제26조제1항 각 호)의 내용에 따라 준수하여야 할 사항의 준수 여부를 확인·점검하여야 한다(영 제28조제6항).

따라서 위탁자는 수탁자에 대하여 정기적인 교육을 실시하는 외에 수탁자의 개인정보

처리 현황 및 실태, 목적 외 이용·제공, 재위탁 여부, 안전성 확보조치 여부 등을 정기적으로 조사·점검하여야 한다.

나 위탁자의 불법행위로 인한 손해배상책임

수탁자가 위탁받은 업무와 관련하여 개인정보를 처리하는 과정에서 이 법을 위반하여 발생한 손해배상책임에 대하여는 수탁자를 개인정보처리자의 소속 직원으로 본다.

손해배상책임에 있어서 수탁자를 개인정보처리자의 소속직원으로 본다는 것은 개인정보처리자가 수탁자의 사용자로 간주된다는 것인 바 개인정보처리자는 수탁자가 발생시킨 손해에 대하여 민법상의 사용자책임(대위책임)을 부담한다.

「민법」 제756조의 사용자책임은 ‘부진정 연대책무’ 이므로 손해를 입은 정보주체는 수탁자와 개인정보처리자 중 선택하여 손해배상청구를 할 수 있다. 즉 위탁자가 수탁자를 대위하여 사용자책임을 지더라도 수탁자에 대해서도 독립해서 불법행위가 성립하므로 수탁자 자신도 손해배상책임을 진다. 이 때 위탁자가 지는 손해배상책임은 「민법」 제756조에 의한 사용자책임이고, 수탁자가 지는 손해배상책임은 「민법」 제750조에 의한 불법행위책임이다. 위탁자가 정보주체에 대해서 지는 손해배상책임은 수탁자의 선임·감독에 대한 책임이고 수탁자의 가해행위에 관한 것이 아니다. 위탁자와 수탁자와의 관계에 있어서 수탁자의 과실로 손해가 발생했다라도 위탁자가 수탁자의 선임 및 감독에 대하여 상당한 주의를 다한 때 또는 상당한 주의를 했더라도 손해가 발생했을 경우에는 위탁자의 손해배상책임은 발생하지 아니한다. 그러나 이에 대한 입증책임은 위탁자가 부담한다.

만약 위탁자가 수탁자의 과실로 인하여 정보주체에게 손해배상을 한 때에는 수탁자에게 구상권을 행사할 수 있다.

참고 부진정 연대책무

부진정 연대책무란 연대책무자들의 의사와 관계없이 우연히 발생한 연대책무를 말한다. 여러 명의 채무자가 동일한 내용의 채무에 관해 각각 독립해서 그 전부의 급부를 이행할 의무를 부담하기로 하고 그 중 한 사람 또는 여러 사람이 급부를 하면 모든 채무자의 채무가 소멸하는 점은 연대책무와 같다. 그러나 채무자 사이에 주관적 관련성이 없으므로 그중 한 사람에게 대해 생긴 사유는 변제 등 채권의 목적을 달성하는 사유 이외에는 다른 채무자에게 영향을 미치지 않는다. 예를 들어, 택시 운전자가 사고를 낸 경우에 그 운전자는 불법행위자로서 당연히 책임이 있으며 택시회사는 사용자로서 책임을 지게 된다. 이 때 택시회사는 본인의 의사와 관계없이 우연히 택시운전자와 연대책임 관계에 있게 되는데 이를 부진정 연대책무라 한다. 이 경우 피해자가 사고를 낸 운전자에게 대해 손해배상에 관한 권리를 포기하거나 채무를 면제할 의사표시를 했다고 하더라도 다른 채무자인 택시회사에 대해서는 그 면책의 효력이 미치지 않는다. 즉 피해자는 운전자와 택시회사를 상대로 각각 손해배상을 청구할 수도 있고 택시회사만을 상대로 손해배상을 청구할 수도 있는 것이다.

수탁자로부터 개인정보 처리업무를 재위탁 받아 처리하는 과정에서 손해가 발생한 경우, 정보주체는 재위탁자인 수탁자에게 그 배상을 청구할 수 있다. 재수탁자가 재위탁자인 수탁자로부터 위탁받은 업무와 관련하여 개인정보를 처리하는 과정에서 이 법을 위반하여 발생한 손해배상책임에 대해서는 재수탁자를 재위탁자인 수탁자의 소속 직원으로 볼 수 있으므로(제6항 참고) 재위탁자인 수탁자는 「민법」 제756조에 따른 사용자 책임을 부담하게 되기 때문이다. 예를 들어 A회사가 고객정보 관리업무를 B회사에게 위탁을 하고 (재위탁 금지에 관한 규정이 없는 경우), B회사는 위탁된 고객정보 관리업무를 C회사에게 다시 재위탁하는 경우, C회사의 관리업무상 과실로 인해 정보주체가 손해를 입은 경우, C회사는 B회사의 직원이므로 정보주체는 B회사에게 손해배상을 청구할 수 있다. 한편 B회사 역시 A회사의 직원이므로 궁극적으로는 A회사가 손해배상 책임져야 한다.

5. 수탁자의 책임과 의무

가 수탁업무 목적 외 개인정보 이용·제공 금지

수탁자는 개인정보처리자로부터 위탁받은 해당 업무 범위를 초과하여 개인정보를 이용하거나 제3자에게 제공하여서는 아니 된다. 예를 들어 개인정보처리자로부터 개인정보의 처리를 위탁받은 이후, 위탁 업무와 별개로 수탁자의 목적으로 마케팅 등을 하는 것은 금지된다. 만약, 이와 같이 수탁자의 목적으로도 이용이 필요하다면 「개인정보 보호법」 또는 관련 법에 따른 제3자 제공 기준과 절차를 준수하여야 한다.

나 개인정보처리자의 의무 등 준용

수탁자에 대해서는 제15조부터 제25조까지, 제27조부터 제31조까지, 제33조부터 제38조까지 및 제59조의 규정을 준용한다. 수탁자도 이 법의 적용대상인 개인정보처리자에 해당되거나 수탁자의 법규 준수의무를 명확히 하기 위하여 별도의 조문으로 관련 규정이 준용됨을 명시한 것이다. 다만, 수탁자가 정보통신서비스 제공자등으로부터 개인정보 처리 업무를 위탁 받은 경우에는 그 위탁받은 업무 범위내에서는 “제6장 정보통신서비스 제공자등에 관한 특례규정”을 준수하여야 한다.

개인정보 처리 업무를 위탁받아 처리하는 수탁자는 개인정보를 보호하기 위하여 “개인정보의 안전성 확보조치 기준 고시”가 정하고 있는 기술적·물리적·관리적 조치를 하여야 한다(표준지침 제17조).

6. 다른 법률과의 관계

「신용정보법」은 신용정보회사등의 신용정보 처리 업무 위탁의 경우에 적용되며, 「개인정보 보호법」 제26조제1항부터 제3항까지 및 제5항의 규정을 준용하도록 규정하고 있다(「신용정보법」 제17조제1항).

한편, 이 법은 재위탁 자체를 금지하지 않는 대신 개인정보처리자가 개인정보 처리 업무를 수탁자에게 위탁할 때 재위탁 제한에 관한 사항을 정할 수 있도록 규정하고 있으나(영 제28조제1항제2호), 「신용정보법」은 원칙적으로 재위탁을 금지하고 있다(「신용정보법」 제17조제7항).

신용정보법	<p>제17조(수집·조사 및 처리의 위탁) ① 신용정보회사등은 제3자에게 신용정보의 처리 업무를 위탁할 수 있다. 이 경우 개인신용정보의 처리 위탁에 대해서는 「개인정보 보호법」 제26조제1항부터 제3항까지의 규정을 준용한다.</p> <p>② 신용정보회사등은 신용정보의 처리를 위탁할 수 있으며 이에 따라 위탁을 받은 자(이하 “수탁자”라 한다)의 위탁받은 업무의 처리에 관하여는 제19조부터 제21조까지, 제22조의4부터 제22조의7까지, 제22조의9, 제40조, 제43조, 제43조의2, 제45조, 제45조의2 및 제45조의3(해당 조문에 대한 벌칙 및 과태료규정을 포함한다)을 준용한다.</p> <p>③ 제2항에 따라 신용정보의 처리를 위탁하려는 신용정보회사등으로서 대통령령으로 정하는 자는 제공하는 신용정보의 범위 등을 대통령령으로 정하는 바에 따라 금융위원회에 알려야 한다.</p> <p>④ 신용정보회사등은 제2항에 따라 신용정보의 처리를 위탁하기 위하여 수탁자에게 개인신용정보를 제공하는 경우 특정 신용정보주체를 식별할 수 있는 정보는 대통령령으로 정하는 바에 따라 암호화 등의 보호 조치를 하여야 한다.</p> <p>⑤ 신용정보회사등은 수탁자에게 신용정보를 제공한 경우 신용정보를 분실·도난·유출·위조·변조 또는 훼손당하지 아니하도록 대통령령으로 정하는 바에 따라 수탁자를 교육하여야 하고 수탁자의 안전한 신용정보 처리에 관한 사항을 위탁계약에 반영하여야 한다.</p> <p>⑥ 수탁자가 개인신용정보를 이용하거나 제3자에게 제공하는 경우에는 「개인정보 보호법」 제26조제5항에 따른다.</p> <p>⑦ 수탁자는 제2항에 따라 위탁받은 업무를 제3자에게 재위탁하여서는 아니 된다. 다만, 신용정보의 보호 및 안전한 처리를 저해하지 아니하는 범위에서 금융위원회가 인정하는 경우에는 그러하지 아니하다.</p>
-------	---

7. 벌칙규정

위반행위	벌칙
업무 위탁 시 같은 항 각 호의 내용이 포함된 문서에 의하지 아니한 자 (제26조제1항 위반)	1천만원 이하의 과태료 (제75조제4항제4호)

위탁하는 업무의 내용과 수탁자를 공개하지 아니한 자 (제26조제2항 위반)	1천만원 이하의 과태료 (제75조제4항제5호)
업무위탁에 따른 개인정보 제공을 알리지 아니한 자 (제26조제3항 위반)	3천만원 이하의 과태료 (제75조제2항제1호)
수탁자 관리·감독을 소홀히 하여 수탁자가 「개인정보 보호법」을 위반한 경우 (제26조제4항 관련)	위반행위 관련 매출액의 100분의 3이하 과징금 (제39조의15제1항제4호)
위탁받은 해당 업무 범위를 초과하여 개인정보를 이용하거나 제3자에게 제공한 수탁자, 그 사정을 알면서도 영리 또는 부정한 목적으로 개인정보를 제공받은 자 (제26조제5항 위반)	5년 이하의 징역 또는 5천만원 이하의 벌금 (제71조제2호)

8. 질의 응답

- Q** | 여행사를 운영하면서 예약확인 및 고객 상담업무를 전문 콜센터에서 처리하고 있는데, 고객 대상 이벤트와 여행상품 홍보 업무도 해당 콜센터에서 모두 진행하려고 한다. 법률상 문제가 없는지?
- A** | 본래의 서비스 이행을 위한 처리위탁 업무가 아닌 별도의 이벤트, 홍보 등의 업무를 위탁하기 위해서는 그 위탁하는 업무의 내용과 수탁자를 정보주체에게 통지하여야 한다.
- Q** | 병원과 의료정보 전달시스템 관리업체 간에 환자의 정보를 공유하는 것도 처리위탁에 따른 동의를 받아야 하는가?
- A** | 「의료법」 등에 따른 전자처방전, 전자의무기록 등의 공유·제공을 위해 관리업체를 활용하는 것은 서비스 제공에 관한 계약을 이행하기 위해 필요한 개인정보 처리위탁에 해당하므로 별도의 동의획득 없이 정보주체에 대하여 공개하여야 하며 위탁 업무 중 홍보·판매 업무가 포함되어 있는 경우 정보주체에게 통지하여야 한다.
- Q** | 대리점 직원(수탁자)이 고객의 개인정보를 부정 이용해 고객에게 피해를 입혔다면, 대리점 직원의 행위에 대해 본사(위탁자)도 책임이 있는가?
- A** | 위탁자(본사)는 수탁자(대리점)에 대해 법률의 개인정보보호 규정을 준수하도록 관리·감독할 의무가 있으며, 수탁자가 법령을 위반해 정보주체에게 손해를 발생시킨 경우에는 위탁자가 이에 대한 책임을 지도록 하고 있다. 따라서 대리점 직원의 행위에 대해서는 본사가 손해배상 책임을 부담한다.

제27조 | 영업양도 등에 따른 개인정보의 이전 제한

<p style="text-align: center;">법률</p>	<p>제27조(영업양도 등에 따른 개인정보의 이전 제한) ① 개인정보처리자는 영업의 전부 또는 일부의 양도·합병 등으로 개인정보를 다른 사람에게 이전하는 경우에는 미리 다음 각 호의 사항을 대통령령으로 정하는 방법에 따라 해당 정보주체에게 알려야 한다.</p> <ol style="list-style-type: none"> 1. 개인정보를 이전하려는 사실 2. 개인정보를 이전받는 자(이하 “영업양수자등”이라 한다)의 성명(법인의 경우에는 법인의 명칭을 말한다), 주소, 전화번호 및 그 밖의 연락처 3. 정보주체가 개인정보의 이전을 원하지 아니하는 경우 조치할 수 있는 방법 및 절차 <p>② 영업양수자등은 개인정보를 이전받았을 때에는 지체 없이 그 사실을 대통령령으로 정하는 방법에 따라 정보주체에게 알려야 한다. 다만, 개인정보처리자가 제1항에 따라 그 이전 사실을 이미 알린 경우에는 그러하지 아니하다.</p> <p>③ 영업양수자등은 영업의 양도·합병 등으로 개인정보를 이전받은 경우에는 이전 당시의 본래 목적으로만 개인정보를 이용하거나 제3자에게 제공할 수 있다. 이 경우 영업양수자등은 개인정보처리자로 본다.</p>
<p style="text-align: center;">시행령</p>	<p>제29조(영업양도 등에 따른 개인정보 이전의 통지) ① 법 제27조제1항 각 호 외의 부분과 같은 조 제2항 본문에서 “대통령령으로 정하는 방법”이란 서면 등의 방법을 말한다.</p> <p>② 법 제27조제1항에 따라 개인정보를 이전하려는 자(이하 이 항에서 “영업양도자등”이라 한다)가 과실 없이 제1항에 따른 방법으로 법 제27조제1항 각 호의 사항을 정보주체에게 알릴 수 없는 경우에는 해당 사항을 인터넷 홈페이지에 30일 이상 게재하여야 한다. 다만, 인터넷 홈페이지에 게재할 수 없는 정당한 사유가 있는 경우에는 다음 각 호의 어느 하나 이상의 방법으로 법 제27조제1항 각 호의 사항을 정보주체에게 알릴 수 있다.</p> <ol style="list-style-type: none"> 1. 영업양도자등의 사업장등의 보기 쉬운 장소에 30일 이상 게시하는 방법 2. 영업양도자등의 사업장등이 있는 시·도 이상의 지역을 주된 보급지역으로 하는 「신문 등의 진흥에 관한 법률」 제2조제1호가목·다목 및 같은 조 제2호에 따른 일반일간신문·일반주간신문 및 인터넷신문에 실는 방법

영업양도, 합병 등으로 영업자산을 다른 사업자에게 이전할 때에는 기존 사업자가 가지고 있던 개인정보DB 등에 관한 권리·의무도 포괄적으로 다른 사업자에게 승계된다. 그 결과 정보주체에게 원치 않는 결과가 초래될 수 있으므로 영업양도, 합병 등으로 인한 개인정보의 이전 시에는 정보주체가 회원탈퇴, 동의철회 등의 권리를 행사할 수 있는 기회를 미리 부여하여야 한다. 여기서 영업양도, 합병 등은 민간사업자를 대상으로 한다.

1. 영업양도·양수자 등의 통지의무

가 영업양도자등의 통지의무

영업의 전부 또는 일부의 양도·합병 등으로 개인정보를 다른 사람에게 이전하는 개인정보처리자(이하 “영업양도자등”이라 한다)는 미리 해당 정보주체에게 그 사실을 알려야 한다(제1항, 영 제29조제1항). 개인정보 이전에 대하여 정보주체의 동의를 받지 않는 대신 정보주체가 개인정보 이전에 대하여 거부할 수 있는 기회를 갖도록 하기 위한 것이다.

나 영업양수자등의 통지의무

개인정보를 이전받는 자(이하 “영업양수자등”이라 한다)는 개인정보를 이전받았을 때에는 지체 없이 그 사실을 정보주체에게 알려야 한다. 다만, 개인정보처리자가 정보주체에게 그 이전 사실을 이미 알린 경우에는 그러하지 아니하다.

영업양도자등이 개인정보의 이전사실을 통지하지 아니한 경우 영업양수자등이 대신 해서 통지하여 정보주체가 그 사실을 알고 필요한 조치를 취할 수 있도록 하기 위한 것이다.

2. 영업양도·양수 등의 통지방법

영업양도자등 또는 영업양수자등이 영업양도·양수 등의 사실을 정보주체에게 통지할 때에는 다음 각 호의 사항을 서면등의 방법으로 해당 정보주체에게 알려야 한다(제1항 각 호, 영 제29조제1항).

서면등의 방법이란 서면, 전자우편, 팩스, 전화, 문자전송 또는 이에 상당하는 방법을 이용한 개별적 통지방법을 의미하며, 인터넷 홈페이지 게시와 같은 방법은 원칙적으로 허용되지 않는다.

영업양도 시 통지사항(제27조제1항)

1. 개인정보를 이전하려는 사실
2. 개인정보를 이전받는 자(영업양수자등)의 성명(법인의 경우에는 법인의 명칭을 말한다), 주소, 전화번호 및 그 밖의 연락처
3. 정보주체가 개인정보의 이전을 원하지 아니하는 경우 조치할 수 있는 방법 및 절차

영업양도자등이 과실 없이 서면등의 방법으로 제27조제1항 각 호의 사항을 정보주체에게 알릴 수 없는 경우에는 해당 사항을 인터넷 홈페이지에 30일 이상 게재하여야 한다(영 제29조제2항)

본문). 다만, 인터넷 홈페이지에 게재할 수 없는 정당한 사유가 있는 경우에는 사업장등의 보기 쉬운 장소에 30일 이상 게시하는 방법, 일반일간신문·일반주간신문 및 인터넷신문에 실는 방법 중 하나 이상의 방법으로 정보주체에게 알려야 한다(영 제29조제2항 단서).

3. 영업양도·양수 등의 통지시기

영업양도자등이 정보주체에게 개인정보의 이전 사실 등을 통지할 때에는 개인정보를 이전하기 전에 미리 통지하여야 한다. 법문(法文)상 개인정보를 이전하는 경우에 미리 통지하여야 하며 최소한 정보주체가 이전 사실을 확인하고 회원탈퇴 등의 권리를 행사할 수 있는 충분한 시간적 여유가 주어져야 할 것이다. 또한 법문상 개인정보를 “이전” 하는 경우에 통지하도록 하고 있는데, 이는 실제 개인정보 DB가 이전되는 시점이 아닌 합병 등 계약 체결 시점에 통지하는 것으로 보아야 할 것이다.

영업양수자등이 정보주체에게 개인정보의 이전사실 등을 통지할 때에는 개인정보를 이전 받은 후 지체 없이 통지하여야 한다.

4. 개인정보의 목적 외 이용·제공 금지

영업양수자등은 영업의 양도·합병 등으로 개인정보를 이전받은 경우에는 이전 당시의 본래 목적으로만 개인정보를 이용하거나 제3자에게 제공할 수 있다. 이 경우 영업양수자등은 개인정보처리자로 본다.

‘개인정보처리자로 본다.’ 는 이 법에 의한 개인정보처리자로서 권리와 의무를 진다는 것을 의미한다. 영업양수자등도 개인정보를 이전받은 순간 이 법의 적용대상인 개인정보처리자에 해당되나 영업양수자등의 법규 준수 의무를 명확히 하기 위하여 별도의 조문으로 이를 확인한 것이다.

따라서 영업양수자등이 영업양수·합병 당시의 개인정보 처리 목적과 다른 용도로 개인정보를 이용·제공하고자 한다면 개인정보의 목적 외 이용·제공에 관한 규정(제18조)에 따라 정보주체의 별도 동의를 받거나 다른 요건을 충족하여야 한다.

5. 본조의 적용대상

본조는 ‘영업의 전부 또는 일부의 양도·합병 등’ 으로 규정되어 있으므로 「상법」 제 530조의2에 의한 회사의 분할 및 분할합병의 경우에도 적용된다고 해석해야 할 것이다.

회사분할이란 하나의 회사를 둘 이상의 회사로 분할하고 분할된 영업재산을 자본으로

하여 회사를 신설하거나 다른 회사와 합병시키는 것이다. 본래의 회사(분할회사)는 소멸하거나 줄어든 상태로 존속하게 되고, 분할회사의 권리의무를 승계한 분할 신설회사(또는 분할 합병회사)의 주식은 분할회사가 취득하거나 분할회사의 주주들이 일정비율대로 나눠 갖는다.

본조는 이처럼 개인정보 DB 등에 관한 권리, 의무가 포괄적으로 이전되는 상황을 전제로 영업양도 및 합병을 그 예시로 규정하고 있으므로, 인적·물적 분할, 자산양수도 등의 거래를 통해 사업부문이 이전되는 등 사실상 영업양도와 유사한 효과가 발생하는 경우 본조에 준하여 개인정보의 이전과 관련하여 본조의 적용을 받도록 하는 것이 합리적이다.

6. 다른 법률과의 관계

「신용정보법」 상으로도 영업양도, 분할, 합병 등의 이유로 권리·의무의 전부 또는 일부를 이전하면서 그와 관련된 개인신용정보를 제공하는 경우에는 정보주체로부터의 동의를 받지 않아도 되는 것으로 규정하고 있다. 즉, 「신용정보법」 제32조제6항 각 호에 따라 개인신용정보를 타인에게 제공하려는 자 또는 제공받은 자는 대통령령으로 정하는 바에 따라 개인신용정보의 제공 사실 및 이유 등을 사전에 해당 신용정보주체에게 알려야 한다. 다만, 대통령령으로 정하는 불가피한 사유가 있는 경우에는 인터넷 홈페이지 게재 또는 그 밖에 유사한 방법을 통하여 사후에 알리거나 공시할 수 있다.

또한, 동법 제32조제6항제3호에 따라 개인신용정보를 타인에게 제공하는 신용정보제공·이용자로서 대통령령으로 정하는 자는 제공하는 신용정보의 범위 등 대통령령으로 정하는 사항에 관하여 금융위원회의 승인을 받아야 한다(「신용정보법」 제32조제8항).

제8항에 따른 승인을 받아 개인신용정보를 제공받은 자는 해당 개인신용정보를 금융위원회가 정하는 바에 따라 현재 거래 중인 신용정보주체의 개인신용정보와 분리하여 관리하여야 한다(「신용정보업감독규정」 제38조의4 참조).

신용정보법	<p>제32조(개인신용정보의 제공·활용에 대한 동의) ⑥ 신용정보회사등(제9호의3을 적용하는 경우에는 데이터전문기관을 포함한다)이 개인신용정보를 제공하는 경우로서 다음 각 호의 어느 하나에 해당하는 경우에는 제1항부터 제5항까지를 적용하지 아니한다.</p> <p>3. 영업양도·분할·합병 등의 이유로 권리·의무의 전부 또는 일부를 이전하면서 그와 관련된 개인신용정보를 제공하는 경우</p> <p>⑦ 제6항 각 호에 따라 개인신용정보를 타인에게 제공하려는 자 또는 제공받은 자는 대통령령으로 정하는 바에 따라 개인신용정보의 제공 사실 및 이유 등을 사전에 해당 신용정보주체에게 알려야 한다. 다만, 대통령령으로 정하는 불가피한 사유가 있는 경우에는 인터넷 홈페이지 게재 또는 그 밖에 유사한 방법을 통하여 사후에 알리거나 공시할 수 있다.</p> <p>⑧ 제6항제3호에 따라 개인신용정보를 타인에게 제공하는 신용정보제공·이</p>
-------	--

	<p>용자로서 대통령령으로 정하는 자는 제공하는 신용정보의 범위 등 대통령령으로 정하는 사항에 관하여 금융위원회의 승인을 받아야 한다.</p> <p>⑨ 제8항에 따른 승인을 받아 개인신용정보를 제공받은 자는 해당 개인신용정보를 금융위원회가 정하는 바에 따라 현재 거래 중인 신용정보주체의 개인신용정보와 분리하여 관리하여야 한다.</p>
--	---

7. 가명정보의 적용 제외

제27조는 영업양도 등에 따라 가명정보를 이전하는 경우에는 적용되지 않는다(제28조의7).

8. 벌칙규정

위반행위	벌칙
영업양도 등에 따른 개인정보 이전사실 미통지 (제27조제1항 또는 제2항 위반)	1천만원 이하의 과태료 (제75조제4항제6호)
이전 당시의 본래 목적 외로 개인정보를 이용하거나 제3자에게 제공 또는 그 사실을 알면서 영리 또는 부정한 목적으로 개인정보를 제공받은 자(제27조제3항 위반)	5년이하의 징역 또는 5천만원 이하의 벌금 (제71조제2호)

9. 질의 응답

Q | 다른 사업자와 영업을 합병하게 되어서 고객을 대상으로 통지를 하려고 하는데, 우리 회사 및 합병 회사가 모두 다 통지를 해야 하는가?

A | 영업 양도, 합병 등으로 개인정보를 이전하는 경우에는 원칙적으로는 개인정보를 이전하는 자 및 이전받는 자 모두가 "개인정보 이전 사실, 이전받는 자의 성명(명칭)·주소·전화번호 등 연락처, 이용자가 개인정보 이전을 원하지 않는 경우 동의 철회 방법·절차"를 이용자에게 알려야 한다.

다만, 경제현실상 양도자와 양수자 모두가 이를 통지하게 되면 비용상의 부담 및 정보주체의 혼란을 야기할 우려도 있으므로, 「개인정보 보호법」은 개인정보를 이전하는 자(사업자)가 관련 사실을 알린 경우에는 이전받는 자(영업양수자등)는 알리지 않아도 되도록 규정하고 있다.

제28조 | 개인정보취급자에 대한 감독

법률	<p>제28조(개인정보취급자에 대한 감독) ① 개인정보처리자는 개인정보를 처리함에 있어서 개인정보가 안전하게 관리될 수 있도록 임직원, 파견근로자, 시간제근로자 등 개인정보처리자의 지휘·감독을 받아 개인정보를 처리하는 자(이하 “개인정보취급자”라 한다)에 대하여 적절한 관리·감독을 행하여야 한다.</p> <p>② 개인정보처리자는 개인정보의 적절한 취급을 보장하기 위하여 개인정보취급자에게 정기적으로 필요한 교육을 실시하여야 한다.</p>
표준지침	<p>제2조(용어의 정의) 이 지침에서 사용하는 용어의 뜻은 다음과 같다.</p> <p>6. “개인정보취급자”란 개인정보처리자의 지휘·감독을 받아 개인정보를 처리하는 업무를 담당하는 자로서 임직원, 파견근로자, 시간제근로자 등을 말한다.</p> <p>제15조(개인정보취급자에 대한 감독) ① 개인정보처리자는 개인정보취급자를 업무상 필요한 한도 내에서 최소한으로 두어야 하며, 개인정보취급자의 개인정보 처리 범위를 업무상 필요한 한도 내에서 최소한으로 제한하여야 한다.</p> <p>② 개인정보처리자는 개인정보 처리시스템에 대한 접근권한을 업무의 성격에 따라 당해 업무수행에 필요한 최소한의 범위로 업무담당자에게 차등 부여하고 접근권한을 관리하기 위한 조치를 취해야 한다.</p> <p>③ 개인정보처리자는 개인정보취급자에게 보안서약서를 제출하도록 하는 등 적절한 관리·감독을 해야 하며, 인사이동 등에 따라 개인정보취급자의 업무가 변경되는 경우에는 개인정보에 대한 접근권한을 변경 또는 말소해야 한다.</p>

1. 개인정보취급자와 개인정보처리자의 차이

개인정보처리자란 업무를 목적으로 개인정보파일을 운용하기 위하여 스스로 또는 다른 사람을 통하여 개인정보를 처리하는 자를 말한다. 즉 공공기관, 법인, 단체 및 개인 등이 이에 해당한다(제2조제5호).

이에 비해, 개인정보취급자란 개인정보처리자의 지휘·감독을 받아 개인정보를 처리하는 임직원, 파견근로자, 시간제근로자 등을 말한다(제28조제1항).

즉, 개인정보취급자는 개인정보 처리 업무를 담당하고 있는 자라면 정규직, 비정규직, 하도급, 시간제 등 모든 근로형태를 불문한다. 고용관계가 없더라도 실질적으로 개인정보처리자의 지휘·감독을 받아 개인정보를 처리하는 자는 개인정보취급자에 포함된다.

개인정보 처리업무 등을 수탁받아 처리하고 있는 수탁자도 개인정보취급자라고 할 수 있으나, 수탁자에 대한 교육 및 관리·감독규정은 제26조에서 별도로 규정하고 있으므로 그에 따른다.

2. 개인정보취급자에 대한 관리·감독

개인정보처리자는 개인정보를 처리함에 있어서 개인정보에 대한 무분별한 접근권한 부여로 인하여 개인정보의 접근 및 유출, 오·남용이 발생하는 것을 방지하기 위하여 개인정보가 안전하게 관리될 수 있도록 개인정보취급자에 대하여 적절한 관리·감독을 행하여야 한다.

적절한 관리·감독은 개인정보취급자의 지위·직책, 담당 업무의 내용, 업무 숙련도 등에 따라 각기 달라져야 한다. 또한 관리·감독은 1회성으로 그쳐서는 안 되고 조직적·체계적으로 이루어져야 하며 반드시 평가·피드백 시스템이 강구되어야 한다. 이를 위해 개인정보처리자는 개인정보취급자의 범위를 최소한으로 제한하고, 그들에 의한 개인정보의 열람 및 처리의 범위를 업무상 필요한 한도에서 최소한으로 제한하여야 하고(표준지침 제15조제1항). 또한 개인정보 처리시스템에 접근할 수 있는 권한을 업무수행에 필요한 '최소한의 범위에서' 관련 업무담당자에게 차등적으로 부여하는 등 개인정보 처리시스템 접근권한을 관리하여야 한다(표준지침 제15조제2항). 그 외에 개인정보취급자에 대한 관리·감독의 방안으로 보안서약서 제출 등을 의무화하고, 개인정보취급자가 변경된 경우 접근권한의 변경 등 관리방안을 구체적으로 마련하여야 한다(표준지침 제15조제3항).

3. 개인정보취급자에 대한 정기적 교육

개인정보처리자는 개인정보의 적절한 취급을 보장하기 위하여 개인정보취급자에게 정기적으로 필요한 교육을 실시하여야 한다. 교육은 사내교육, 외부교육, 위탁교육 등 여러 종류가 있을 수 있으나 연간 교육계획을 수립하여 모든 개인정보취급자가 일정 시간 이상 교육에 참여하도록 해야 한다. 또한 개인정보취급자의 지위·직책, 담당 업무의 내용, 업무 숙련도 등에 따라 교육 내용도 각기 달라져야 한다.

4. 다른 법률과의 관계

「신용정보법」은 신용정보회사등(개인정보처리자)의 지휘·감독을 받아 개인신용정보를 처리하는 자(개인정보취급자)에 대한 관리·감독과 관련한 규정을 두고 있지 않으므로 신용정보회사등은 「개인정보 보호법」에 따라 개인신용정보를 처리하는 자에 대한 관리·감독 의무를 이행하여야 한다.

5. 질의 응답

Q | 업무 처리를 위해서 아르바이트 직원에게 고객 개인정보를 열람할 수 있도록 했는데, 이 경우도 개인정보취급자에 해당하는가?

A | 아르바이트 등 임시직 직원도 업무상 필요에 의해 개인정보를 열람·처리하고 있다면 개인정보취급자에 해당된다. 따라서 이 경우에도 개인정보의 열람·처리 범위를 업무상 필요한 한도 내에서 최소한으로 제한해야 하며, 보안서약서를 징구하는 등 필요한 관리조치를 취하여야 한다.

제3절 가명정보의 처리에 관한 특례

제28조의2 | 가명정보의 처리 등

법률

제28조의2(가명정보의 처리 등) ① 개인정보처리자는 통계작성, 과학적 연구, 공익적 기록보존 등을 위하여 정보주체의 동의 없이 가명정보를 처리할 수 있다.

② 개인정보처리자는 제1항에 따라 가명정보를 제3자에게 제공하는 경우에는 특정 개인을 알아보기 위하여 사용될 수 있는 정보를 포함해서는 아니 된다.

1. 가명정보 처리의 특례

개인정보처리자는 원칙적으로 제18조제2항에 정한 사유에 해당하지 않는 한 수집 목적 범위 외로 개인정보를 이용할 수 없으나, 통계작성, 과학적 연구, 공익적 기록보존 등을 위하여 정보주체의 동의 없이 가명처리가 가능하다. 다만, 제28조의7(적용범위)과 같이 가명정보를 대상으로 하는 규정을 적용하는 경우에는 양자를 구분하여야 한다.

처리는 법 제2조제2호에서 규정하는 바와 같이 개인정보의 수집, 생성, 연계, 연동, 기록, 저장, 보유, 가공, 편집, 검색, 출력, 정정(訂正), 복구, 이용, 제공, 공개, 파기(破棄), 그 밖에 이와 유사한 행위를 말한다.

가 통계작성

통계란 특정 집단이나 대상 등에 관하여 작성하는 수량적인 정보를 의미한다. 통계작성의 목적은 시장조사와 같은 상업적 목적으로도 가능하다. 다만, 통계는 집합적인 데이터로 이름, 연락처 등 특정 개인에 관한 정보가 포함되어 있지 않아 통계의 대상이 된 정보주체에 대해서는 1:1 맞춤형 타겟 마케팅이 불가능하다.

참고 통계 작성의 예시

- 회사가 도로구조 개선 및 휴게공간 추가설치 등 고객센터 개선 을 위하여 월별 시간대별 차량 평균속도, 상습 정체구간, 사고구간 및 원인 등에 대한 통계를 작성하는 경우
- 백화점, 마트 등 유통경로별 상품판매 전략을 수립하기 위하여 판매 상품을 구입한 회원의 연령, 성별, 선호색상, 구입처, 기능 및 가격 등에 관한 통계를 작성하는 경우

나 과학적 연구

과학적 연구란 기술의 개발과 실증, 기초연구, 응용연구 및 민간 투자 연구 등 과학적 방법을 적용하는 연구를 말한다(제2조제8호 참고). 과학적 연구는 기술의 개발과 실증, 기초 연구, 응용 연구뿐만 아니라 새로운 기술·제품·서비스 개발 등 산업적 목적을 위해서도 수행이 가능하며 민간 투자 연구도 가능하다.

참고 과학적 연구의 예시

- 코로나19 위험 경고를 위해 생활패턴과 코로나19 감염률의 상관관계에 대한 가설을 세우고, 건강 관리용 모바일 앱을 통해 수집한 생활습관, 위치정보, 감염증상, 성별, 나이, 감염원 등을 가명처리하고 감염자의 데이터와 비교·분석하여 가설을 검증하는 경우
- 연령, 성별에 따른 체중관리 운동 시뮬레이션 프로그램 또는 운동관리 애플리케이션을 개발하기 위하여 웨어러블 기기를 이용하여 수집한 맥박, 운동량, 평균 수면시간 등에 관한 정보와 이미 보유한 성별, 연령, 체중을 가명처리하여 활용하는 경우

다 공익적 기록보존

공익적 기록보존이란, 공공의 이익을 위하여 지속적으로 열람할 가치가 있는 기록을 보존하는 것을 의미한다. 공공기관이 처리하는 경우에만 공익적 목적이 인정되는 것은 아니며, 민간기업, 단체 등이 일반적인 공익을 위하여 기록을 보존하는 경우도 공익적 기록보존 목적이 인정된다.

참고 공익적 기록보존의 예시

- 연구소가 현대사 연구 과정에서 수집한 정보 중에서 사료 가치가 있는 생존 인물에 관한 정보를 기록·보관하고자 하는 경우

2. 가명정보 제3자 제공 시의 금지사항

통계작성, 과학적 연구, 공익적 기록보존 등을 위하여 가명정보를 제3자에게 제공하는 경우, 특정 개인을 알아보기 위하여 사용될 수 있는 정보를 포함하여서는 안 된다. 따라서 가명정보를 원래의 상태로 복원할 수 있는 추가 정보 외에도 특정 개인을 알아보기 위하여 사용될 수 있는 정보들은 명칭, 종류, 형태나 내용을 불문하고 제3자에게 제공하여서는 아니 된다.

개인정보처리자는 가명정보를 제3자에게 제공할 때, 제3자가 법에서 허용하는 목적으로 가명정보를 처리하는지에 대하여 추가 자료를 제출받아 확인할 수 있으며, 제3자가 처

리하고 있는 개인정보 중 제공대상이 되는 가명정보와 결합 가능성이 있는 개인정보 목록 등을 확인하여 가명 처리 할 때 고려할 수 있다. 이때, 가명정보를 합법적인 목적으로 처리하는지와 가명정보가 재식별 되지 않는지에 대한 책임은 기본적으로 제3자에게 있으므로, 이와 같은 내용을 포함하여 서면으로 별도의 계약을 체결하는 것도 가능하다.

3. 관련 법률

「신용정보법」에서는 「개인정보 보호법」의 가명정보 처리 특례와 동일한 취지로 통계(상업적 통계 포함) 작성, 연구(산업적 연구를 포함), 공익적 기록보존 등을 위한 경우에는 개인신용정보주체의 동의 없이 가명정보를 제3자에게 제공할 수 있다는 규정을 두고 있다(「신용정보법」 제32조제6항제9호의2, 제33조제1항제4호)

신용정보법	<p>제32조(개인신용정보의 제공·활용에 대한 동의) ⑥ 신용정보회사등(제9호의3을 적용하는 경우에는 데이터전문기관을 포함한다)이 개인신용정보를 제공하는 경우로서 다음 각 호의 어느 하나에 해당하는 경우에는 제1항부터 제5항까지를 적용하지 아니한다.</p> <p>9의2. 통계작성, 연구, 공익적 기록보존 등을 위하여 가명정보를 제공하는 경우. 이 경우 통계작성에는 시장조사 등 상업적 목적의 통계작성을 포함하며, 연구에는 산업적 연구를 포함한다.</p> <p>제33조(개인신용정보의 이용) ① 개인신용정보는 다음 각 호의 어느 하나에 해당하는 경우에만 이용하여야 한다.</p> <p>1.~3. (생략)</p> <p>4. 제32조제6항 각 호의 경우</p> <p>5. (생략)</p>
-------	--

4. 벌칙규정

위반행위	벌칙
가명정보 처리 규정을 위반하여 가명정보를 이용하거나 제3자에게 제공한 자 및 그 사정을 알면서도 영리 또는 부정한 목적으로 가명정보를 제공받은 자 (제28조의2 위반)	5년 이하의 징역 또는 5천만원 이하의 벌금 (제71조제2호)

5. 질의 응답

Q | 가명정보를 통계작성, 과학적 연구, 공익적 기록보존 등을 위하여 정보주체의 동의 없이 공개할 수 있는지?

A | 정보주체의 동의 없이 가명정보를 제공·공개하기 위해서는 통계작성, 과학적 연구, 공익적 기록보존 등의 목적에 해당하여야 하고(제28조의2제1항), 특정 개인을 알아볼 수 있는 정보가 포함되어서는 아니 된다(제28조의2제2항).
하지만, 가명정보를 불특정 다수에게 공개하는 경우에는 공개의 목적이 통계작성, 과학적 연구, 공익적 기록보존 등의 목적에 해당하는지가 불분명하고(제28조의2제1항 위반 우려), 불특정 다수 중 누군가는 공개하는 정보와 결합하여 특정 개인을 알아볼 수 있는 정보를 가지고 있을 수 있어(제28조의2제2항 위반 우려), 가명정보의 공개는 사실상 제한된다.

Q | **가명정보를 통계 작성 목적으로 제공받으면 통계 작성 목적으로만 처리하여야 하는지?**

A | 가명정보를 정보주체의 동의 없이 처리할 수 있는 목적 범위는 통계작성, 과학적 연구, 공익적 기록보존 등의 목적이다. 따라서 가명정보를 통계작성 목적으로 제공받았다 하더라도 통계 작성 외에 과학적 연구, 공익적 기록 보존 목적 등으로 해당 정보주체의 동의 없이 처리할 수 있다.

Q | **가명정보를 과학적 연구 등 목적으로 제공하는 경우 대가를 받을 수 있는지?**

A | 가명정보를 과학적 연구 등 법에서 허용하는 범위로 제공하면서 대가를 받는 것은 금지하고 있지 않다. 다만, 가명정보 제공 대상이나 가명처리 목적이 특정되지 않은 상황에서 가명처리 하는 것과 그 가명정보를 제공하고 대가를 받는 것은 판매가 목적인 경우로 볼 수 있어 허용되지 않는다.

Q | **민감정보 또는 고유식별번호를 과학적 연구 등 목적으로 동의 없이 처리할 수 있는지?**

A | 가명정보의 처리에 관한 특례(제3절)는 일반 개인정보에 대한 규정에 우선하여 적용되므로 민감정보 또는 고유식별정보도 가명처리의 대상이 될 수 있다. 다만, 최소처리원칙(제3조제2항)에 따라 처리 목적과의 관련성을 고려하여 가명정보 처리 목적과 관련이 없는 민감정보 또는 고유식별정보는 삭제하여야 한다.

제28조의3 | 가명정보의 결합 제한

<p style="text-align: center;">법률</p>	<p>제28조의3(가명정보의 결합 제한) ① 제28조의2에도 불구하고 통계작성, 과학적 연구, 공익적 기록보존 등을 위한 서로 다른 개인정보처리자 간의 가명정보의 결합은 보호위원회 또는 관계 중앙행정기관의 장이 지정하는 전문기관이 수행한다.</p> <p>② 결합을 수행한 기관 외부로 결합된 정보를 반출하려는 개인정보처리자는 가명정보 또는 제58조의2에 해당하는 정보로 처리한 뒤 전문기관의 장의 승인을 받아야 한다.</p> <p>③ 제1항에 따른 결합 절차와 방법, 전문기관의 지정과 지정 취소 기준·절차, 관리·감독, 제2항에 따른 반출 및 승인 기준·절차 등 필요한 사항은 대통령령으로 정한다.</p>
<p style="text-align: center;">시행령</p>	<p>제29조의2(결합전문기관의 지정 및 지정 취소) ① 법 제28조의3제1항에 따른 전문기관(이하 “결합전문기관”이라 한다)의 지정 기준은 다음 각 호와 같다.</p> <ol style="list-style-type: none"> 1. 보호위원회가 정하여 고시하는 바에 따라 가명정보의 결합·반출 업무를 담당하는 조직을 구성하고, 개인정보 보호와 관련된 자격이나 경력을 갖춘 사람을 3명 이상 상시 고용할 것 2. 보호위원회가 정하여 고시하는 바에 따라 가명정보를 안전하게 결합하기 위하여 필요한 공간, 시설 및 장비를 구축하고 가명정보의 결합·반출 관련 정책 및 절차 등을 마련할 것 3. 보호위원회가 정하여 고시하는 기준에 따른 재정 능력을 갖출 것 4. 최근 3년 이내에 법 제66조에 따른 공표 내용에 포함된 적이 없을 것 <p>② 법인, 단체 또는 기관이 법 제28조의3제1항에 따라 결합전문기관으로 지정을 받으려는 경우에는 보호위원회가 정하여 고시하는 결합전문기관 지정 신청서에 다음 각 호의 서류(전자문서를 포함한다. 이하 같다)를 첨부하여 보호위원회 또는 관계 중앙행정기관의 장에게 제출해야 한다.</p> <ol style="list-style-type: none"> 1. 정관 또는 규약 2. 제1항에 따른 지정 기준을 갖추었음을 증명할 수 있는 서류로서 보호위원회가 정하여 고시하는 서류 <p>③ 보호위원회 또는 관계 중앙행정기관의 장은 제2항에 따라 지정신청서를 제출한 법인, 단체 또는 기관이 제1항에 따른 지정 기준에 적합한 경우에는 결합전문기관으로 지정할 수 있다.</p> <p>④ 결합전문기관 지정의 유효기간은 지정을 받은 날부터 3년으로 하며, 보호위원회 또는 관계 중앙행정기관의 장은 결합전문기관이 유효기간의 연장을 신청하면 제1항에 따른 지정 기준에 적합한 경우에는 결합전문기관으로 재지정할 수 있다.</p>

⑤ 보호위원회 또는 관계 중앙행정기관의 장은 결합전문기관이 다음 각 호의 어느 하나에 해당하는 경우에는 결합전문기관의 지정을 취소할 수 있다. 다만, 제1호 또는 제2호에 해당하는 경우에는 지정을 취소해야 한다.

1. 거짓이나 부정한 방법으로 결합전문기관으로 지정을 받은 경우
2. 결합전문기관 스스로 지정 취소를 요청하거나 폐업한 경우
3. 제1항에 따른 결합전문기관의 지정 기준을 충족하지 못하게 된 경우
4. 결합 및 반출 등과 관련된 정보의 유출 등 개인정보 침해사고가 발생한 경우
5. 그 밖에 법 또는 이 영에 따른 의무를 위반한 경우

⑥ 보호위원회 또는 관계 중앙행정기관의 장은 제5항에 따라 결합전문기관의 지정을 취소하려는 경우에는 청문을 해야 한다.

⑦ 보호위원회 또는 관계 중앙행정기관의 장은 결합전문기관을 지정, 재지정 또는 지정 취소한 경우에는 이를 관보에 공고하거나 보호위원회 또는 해당 관계 중앙행정기관의 홈페이지에 게시해야 한다. 이 경우 관계 중앙행정기관의 장이 결합전문기관을 지정, 재지정, 또는 지정 취소한 경우에는 보호위원회에 통보해야 한다.

⑧ 제1항부터 제7항까지에서 규정한 사항 외에 결합전문기관의 지정, 재지정 및 지정 취소 등에 필요한 사항은 보호위원회가 정하여 고시한다.

제29조의3(개인정보처리자 간 가명정보의 결합 및 반출 등) ① 결합전문기관에 가명정보의 결합을 신청하려는 개인정보처리자(이하 “결합신청자”라 한다)는 보호위원회가 정하여 고시하는 결합신청서에 다음 각 호의 서류를 첨부하여 결합전문기관에 제출해야 한다.

1. 사업자등록증, 법인등기부등본 등 결합신청자 관련 서류
2. 결합 대상 가명정보에 관한 서류
3. 결합 목적을 증명할 수 있는 서류
4. 그 밖에 가명정보의 결합 및 반출에 필요하다고 보호위원회가 정하여 고시하는 서류

② 결합전문기관은 법 제28조의3제1항에 따라 가명정보를 결합하는 경우에는 특정 개인을 알아볼 수 없도록 해야 한다. 이 경우 보호위원회는 필요하면 한국인터넷진흥원 또는 보호위원회가 지정하여 고시하는 기관으로 하여금 특정 개인을 알아볼 수 없도록 하는 데에 필요한 업무를 지원하도록 할 수 있다.

③ 결합신청자는 법 제28조의3제2항에 따라 결합전문기관이 결합한 정보를 결합전문기관 외부로 반출하려는 경우에는 결합전문기관에 설치된 안전성 확보에 필요한 기술적·관리적·물리적 조치가 된 공간에서 제2항에 따라 결합된 정보를 가명정보 또는 법 제58조의2에 해당하는 정보로 처리한 뒤 결합전문기관의 승인을 받아야 한다.

④ 결합전문기관은 다음 각 호의 기준을 충족하는 경우에는 법 제28조의3제2항에 따른 반출을 승인해야 한다. 이 경우 결합전문기관은 결합된 정보의 반출을 승인하기 위하여 반출심사위원회를 구성해야 한다.

1. 결합 목적과 반출 정보가 관련성이 있을 것
2. 특정 개인을 알아볼 가능성이 없을 것
3. 반출 정보에 대한 안전조치 계획이 있을 것

⑤ 결합전문기관은 결합 및 반출 등에 필요한 비용을 결합신청자에게 청구할 수 있다.

⑥ 제1항부터 제5항까지에서 규정한 사항 외에 가명정보의 결합 절차와 방법, 반출 및 승인 등에 필요한 사항은 보호위원회가 정하여 고시한다.

제29조의4(결합전문기관의 관리·감독 등) ① 보호위원회 또는 관계 중앙행정기관의 장은 결합전문기관을 지정한 경우에는 해당 결합전문기관의 업무 수행능력 및 기술·시설 유지 여부 등을 관리·감독해야 한다.

② 결합전문기관은 제1항에 따른 관리·감독을 위하여 다음 각 호의 서류를 매년 보호위원회 또는 관계 중앙행정기관의 장에게 제출해야 한다.

1. 가명정보의 결합·반출 실적보고서
2. 결합전문기관의 지정 기준을 유지하고 있음을 증명할 수 있는 서류
3. 가명정보의 안전성 확보에 필요한 조치를 하고 있음을 증명할 수 있는 서류로서 보호위원회가 정하여 고시하는 서류

③ 보호위원회는 다음 각 호의 사항을 관리·감독해야 한다.

1. 결합전문기관의 가명정보의 결합 및 반출 승인 과정에서의 법 위반 여부
2. 결합신청자의 가명정보 처리 실태
3. 그 밖에 가명정보의 안전한 처리를 위하여 필요한 사항으로서 보호위원회가 정하여 고시하는 사항

가명정보의 결합 및 반출 등에 관한 고시(보호위원회 고시 제2020-9호)

제1장 총칙

제1조(목적) 이 고시는 「개인정보 보호법」(이하 “법”이라 한다) 제28조의3과 「개인정보 보호법 시행령」(이하 “령”이라 한다) 제29조의2부터 제29조의4까지의 규정에 따른 결합전문기관 지정 및 가명정보의 결합·반출에 관한 기준·절차 등을 정함을 목적으로 한다.

제2조(정의) 이 고시에서 사용하는 용어의 뜻은 다음과 같다.

1. “보호위원회등”이란 법 제28조의3제1항에 따라 전문기관을 지정할 수 있는 개인정보 보호위원회(이하 “보호위원회”라 한다) 또는 관계 중앙행정기관의 장을 말한다.
2. “결합신청자”란 가명정보의 결합을 신청하는 개인정보처리자를 말한다.
3. “결합키”란 결합 대상인 가명정보의 일부로서 해당 정보만으로는 특정 개인을 알

- 아볼 수 없으나 다른 정보주체와 구별할 수 있도록 조치한 정보를 말한다.
4. “결합키연계정보”란 동일 정보주체에 관한 가명정보를 결합할 수 있도록 서로 다른 결합신청자의 결합키를 연계한 정보를 말한다.
 5. “결합전문기관”이란 법 제28조의3제1항에 따라 서로 다른 개인정보처리자 간의 가명정보 결합을 수행하기 위해 보호위원회등이 지정하는 전문기관을 말한다.
 6. “결합기관리기관”이란 결합키연계정보를 생성하여 결합전문기관에 제공하는 등 가명정보의 안전한 결합을 지원하는 업무를 하는 한국인터넷진흥원을 말한다.

제2장 가명정보 결합체계 협의회 등

제3조(가명정보 결합체계 협의회) ① 가명정보의 결합체계와 관련하여 다음 각 호에 관한 사항을 협의하기 위해 영 제5조의2제4항에 따라 가명정보 결합체계 협의회를 보호위원회에 둔다.

1. 개인정보의 가명처리 및 가명정보 결합체계 연구·개선에 관한 사항
 2. 가명정보의 결합과 관련한 개인정보 보호 및 활용에 필요한 사항
 3. 결합전문기관의 지정·재지정 및 지정 취소에 관한 사항
 4. 결합전문기관의 관리·감독에 관한 사항
 5. 그 밖에 이 고시의 집행 등에 관하여 협의를 필요로 하는 사항
- ② 가명정보 결합체계 협의회에는 보호위원회 및 관계 중앙행정기관의 가명정보 결합 등에 관한 업무를 담당하는 부서의 장이 참여한다.

제4조(보호위원회의 지원) ① 보호위원회는 결합신청자, 결합전문기관 및 결합기관리기관 간 결합신청, 결합, 반출 등에 필요한 시스템을 구축하여 운영할 수 있다.

② 보호위원회는 반출심사의 전문성을 확보하기 위해 반출심사위원회의 위원의 교육계획을 수립하여 운영할 수 있다.

제3장 결합전문기관의 지정 등

제5조(결합전문기관의 지정 절차) ① 결합전문기관으로 지정받으려는 법인, 단체 또는 기관은 별지 제1호서식의 결합전문기관 지정신청서에 다음 각 호의 서류(전자문서를 포함한다. 이하 같다)를 첨부하여 보호위원회등에게 제출하여야 한다.

1. 정관 또는 규약
 2. 별표1의 결합전문기관 지정 기준에 관한 서류
- ② 보호위원회등은 결합전문기관 지정 기준의 적합 여부를 결합전문기관 지정심사위원회(이하 “지정심사위원회”라 한다)를 구성하여 심사하여야 한다. 이 경우 지정심사위원회는 개인정보 보호에 관한 학식과 경험이 풍부한 5명의 위원으로 구성한다.
- ③ 보호위원회등은 제2항에 따른 심사 결과 별표1의 결합전문기관 지정 기준을 충족한다고 인정하는 경우 결합전문기관으로 지정할 수 있다. 이 경우 별지 제2호서식의 결합전문기관 지정서를 발급하여야 한다.

제6조(결합전문기관의 재지정) ① 결합전문기관은 재지정을 받으려는 경우에는 지

정기간 만료일 6개월 전부터 3개월 전까지 별표1의 결합전문기관 지정 기준에 부합함을 증명할 수 있는 서류를 갖추어 재지정을 신청하여야 한다. 이 경우 보호위원회등은 결합전문기관의 지정기간 만료일 6개월전에 만료 사실을 알려줄 수 있다.

② 보호위원회등은 제1항에 따른 재지정 신청을 받은 때에는 별표1의 결합전문기관 지정 기준을 충족하고 있는지를 제5조제2항의 절차에 따라 심사하여 신청을 받은 날부터 3개월 이내에 그 결과를 신청기관에 통지하여야 한다. 심사 결과 보호위원회등이 결합전문기관의 재지정을 결정한 경우에는 별지 제2호서식의 결합전문기관 지정서를 발급하여야 한다.

③ 결합전문기관이 제1항에 따라 재지정을 신청한 경우 그 신청에 대한 처리 결과를 통지받을 때까지는 결합전문기관의 지정이 계속 유효한 것으로 본다.

제7조(결합전문기관 지정에 따른 고시 등) 보호위원회등은 결합전문기관을 지정, 재지정 또는 지정 취소하는 경우 영 제29조의2제7항에 따라 다음 각 호의 사항을 관보에 공고하거나 보호위원회등의 홈페이지에 게시해야 한다. 이 경우 관계 중앙행정기관의 장은 다음 각 호의 사항을 보호위원회에 통보해야 한다.

1. 결합전문기관의 명칭 및 주소
2. 담당 부서 및 연락처
3. 지정 유효기간(지정 또는 재지정의 경우에 한정한다)
4. 취소 일시 및 취소 사유(지정 취소의 경우에 한정한다)

제4장 가명정보의 결합 신청 및 반출 등

제8조(가명정보의 결합 신청 등) ① 결합신청자는 별지 제3호서식의 결합 신청서와 다음 각 호의 서류를 결합전문기관에 제출하여야 한다.

1. 사업자등록증, 법인등기부등본 등 결합신청자 관련 서류
2. 결합 대상 가명정보에 관한 서류
3. 결합 목적을 증명할 수 있는 서류
4. 반출 정보의 안전조치계획 및 이를 증명할 수 있는 서류

② 결합전문기관은 제1항에 따른 신청서 및 첨부서류를 확인하고 보완이 필요한 경우 결합신청자에게 보완을 요구하여야 한다. 이 경우 결합전문기관은 필요하면 결합신청자에게 결합하려는 가명정보의 가명처리 수준에 대하여 권고할 수 있다.

③ 결합전문기관은 가명정보의 결합 일정 및 절차 등 결합에 필요한 사항을 결합신청자와 협의하여야 한다.

④ 결합기관리기관은 결합키 생성에 필요한 사항을 결합신청자와 협의하여야 한다.

제9조(가명정보의 결합) ① 결합신청자는 제8조제3항에 따른 협의 결과에 따라 결합키는 결합기관리기관에게 송부하고, 그 외의 결합을 하려는 정보는 결합전문기관에게 송부하여야 한다. 이 경우 결합신청자는 결합에 필요한 일련번호를 포함하여 결합기관리기관과 결합전문기관에게 각각 송부하여야 한다.

- ② 결합기관리기관은 결합신청자로부터 결합키를 제공받아 지체 없이 결합키연계정보를 생성하여 결합전문기관에 제공하여야 한다.
- ③ 결합기관리기관은 결합신청자의 요청이 있는 경우 제2항에 따른 결합키연계정보 생성과정에서 결합률을 확인하여 결합신청자에게 통보하여야 한다.
- ④ 결합전문기관은 결합기관리기관으로부터 결합키연계정보를 제공받아 가명정보의 결합을 완료하는 등으로 결합키연계정보가 불필요하게 된 때에는 이를 지체 없이 파기하여야 한다.

제10조(결합된 정보의 반출 전 처리) 결합신청자는 결합된 정보를 영 제29조의3제3항에 따른 안전성 확보에 필요한 기술적·관리적·물리적 조치가 된 공간에서 가명정보 또는 법 제58조의2에 해당하는 정보로 처리할 수 있다. 이 경우 결합전문기관은 자문 등 필요한 지원을 할 수 있다.

제11조(반출승인) ① 결합전문기관은 결합신청자가 반출을 요청하는 경우 지체 없이 반출심사위원회를 구성하여 반출 여부를 심사하여야 한다.

- ② 결합전문기관은 제1항에 따라 반출심사위원회를 구성하는 경우 개인정보 보호에 관하여 경험과 학식이 풍부한 사람으로서 다음 각 호에 해당하는 사람을 고루 포함하여 3인 이상 7인 이하의 위원으로 구성하여야 한다.

1. 개인정보 보호와 관련한 업무 경력이 있거나 관련 단체로부터 추천을 받은 사람
2. 개인정보처리자로 구성된 단체에서 활동한 경력이 있거나 관련 단체로부터 추천을 받은 사람
3. 그 밖에 개인정보 보호와 관련한 경력과 전문성이 있는 사람

③ 반출심사위원회는 다음 각 호의 사항을 고려하여 반출 심사를 하여야 한다.

1. 결합 목적과 반출 정보가 관련성이 있을 것
2. 특정 개인을 알아볼 가능성이 없을 것
3. 반출 정보에 대한 안전조치 계획이 있을 것

④ 결합신청자는 제3항에 따른 반출심사에 필요한 사항을 제출하고 이를 설명하여야 한다.

⑤ 결합신청자의 임직원 등 이해관계자는 반출심사위원회 위원으로 참여할 수 없다.

제5장 전문기관의 책무 및 전문기관에 대한 관리·감독

제12조(안전성 확보 등에 필요한 조치) ① 결합전문기관은 가명정보의 결합·반출 등으로 해당 가명정보의 결합·반출과정에서 제공받거나 생성한 정보가 불필요하게 된 때에는 이를 지체 없이 파기하여야 한다.

② 제1항에도 불구하고 결합전문기관은 매년 1월 31일까지 다음 각 호의 사항을 보호위원회에 제출하여야 한다.

1. 결합 신청서 및 제8조제1항 각 호의 첨부서류
2. 반출심사에 대한 결과 및 심사위원 명단
3. 결합정보 및 심사 대상 정보에 대한 파기 대장

③ 결합기관리기관은 가명정보의 결합이 완료되는 등 결합키와 결합키연계

정보가 불필요하게 된 때에는 지체 없이 파기하여야 한다.

제13조(결합전문기관의 관리·감독) ① 결합전문기관은 매년 1월 31일까지 다음 각 호의 서류를 작성하여 보호위원회등에게 제출하여야 한다.

1. 가명정보의 결합 및 반출 실적 보고서
 2. 별표1의 결합전문기관 지정 기준을 유지하고 있음을 증명할 수 있는 서류
- ② 보호위원회등은 결합전문기관의 지정 취소사유가 영 제29조의2제5항제3호부터 제5호까지에 해당하는 경우 결합전문기관에 시정·보완을 요구할 수 있다.

제6장 보칙

제14조(재검토기한) 보호위원회는 「훈령·예규 등의 발령 및 관리에 관한 규정」에 따라 이 고시에 대하여 2020년 8월 5일 기준으로 매 2년이 되는 시점(매 2년째의 8월 4일까지를 말한다)마다 그 타당성을 검토하여 개선 등의 조치를 하여야 한다.

1. 결합전문기관의 지정 및 지정 취소 등

이 법은 산업 분야별 데이터의 특성을 고려한 결합전문기관 운영이 이루어질 수 있도록 보호위원회 외에도 관계 중앙행정기관의 장에게 결합전문기관의 지정권을 부여하고 있다. 따라서, 보호위원회 또는 관계 중앙행정기관의 장은 소관 사무와 관련된 법인, 단체 또는 기관을 결합전문기관으로 지정할 수 있다.

가 지정기준

보호위원회 또는 관계 중앙행정기관의 장은(이하 ‘보호위원회등’이라 한다) 「가명정보의 결합 및 반출 등에 관한 고시」(이하 ‘결합 및 반출 고시’라 한다) [별표 1]에 기재된 조직·인력, 시설·장비, 정책·절차, 재정 능력 등 지정 기준을 고려하여 법인, 단체 또는 기관을 결합전문기관으로 지정할 수 있다.

참고 결합전문기관 지정 기준 (‘가명정보 결합 및 반출 등에 관한 고시’ [별표1])

- (조직·인력) 8인 이상으로 구성된 결합전문기관 담당조직 운영, 담당조직의 관리책임자 지정, 담당조직 인력에 대한 교육계획 수립
 - 정보보호, 정보통신, 정보기술, 개인정보 보호, 데이터 분석, 통계학, 법학 등 관련 분야 전문가를 3인 이상 담당조직에 포함
- (시설·장비) 가명정보 결합, 가명정보 또는 법 제58조의2에 해당하는 정보로 처리, 반출심사에 필요한 시설·장비 구축과 데이터 및 네트워크에 대한 보안조치 마련
- (정책·절차) 가명정보 결합, 가명정보 또는 법 제58조의2에 해당하는 정보로의 처리를 위한 정책 및 절차, 반출심사를 위한 정책 및 절차, 출입통제 정책 및 절차, 데이터 반출·입 정책 및 절차 등
- (재정능력) 자본금 50억 이상(비영리법인의 경우 기본재산 또는 자본총계 50억 이상)
- (법규준수) 최근 3년 이내(결합전문기관 지정 신청일 기준)에 법 제66조에 따라 공표된 적이 없을 것

나 지정절차

결합전문기관으로 지정받고자 하는 법인, 단체 또는 기관(이하 “결합전문기관 지정신청자”)은 보호위원회등에게 결합 및 반출 고시[별지 제1호의 서식]의 지정 신청서와 함께 정관 또는 규약과 결합전문기관 지정 기준에 관한 서류를 첨부하여 제출하여야 한다.

다 심사방법

보호위원회등은 개인정보 보호에 관한 학식과 경험이 풍부한 사람 5인으로 구성된 결합전문기관 지정심사위원회를 통하여 지정 기준의 적합 여부를 심사하여야 한다. 이 경우 보호위원회등은 심사 결과, 결합전문기관 지정에 관한 기준을 충족한다고 인정하는 경우 해당 결합전문기관 지정신청자를 결합전문기관으로 지정할 수 있으며, 지정이 결정되는 경우 결합전문기관 지정서를 결합전문기관 지정신청자에게 발급하여야 한다.

라 유효기간 및 재지정

결합전문기관 지정은 결합전문기관으로 지정받은 날로부터 3년간 유효하며 재지정을 받으려고 하는 자는 보호위원회등에게 지정기간 만료일 6개월부터 3개월 전까지 재지정을 신청할 수 있다. 결합전문기관으로부터 재지정 신청을 받은 보호위원회등은 결합전문기관 지정심사위원회를 통하여 결합전문기관 지정 기준을 충족하는지 여부를 심사해야 하며, 신청을 받은 날부터 3개월 이내에 재지정 여부에 대한 결과를 신청자에 통지하여야 한다. 이 경우, 결합전문기관은 재지정 신청에 대한 처리 결과를 통지받을 때까지 결합전문기관의 지정이 계속 유효한 것으로 본다.

마 결합전문기관의 지정 취소

보호위원회등은 결합전문기관이 영 제29조의2제5항에 따라 ① 거짓이나 부정한 방법으로 결합전문기관으로 지정을 받은 사실이 확인된 경우 ② 결합전문기관이 스스로 지정 취소를 요청하거나 폐업한 경우 ③ 고시에서 정하는 지정 기준을 충족하지 못하게 된 경우 ④ 결합 및 분석 등과 관련된 정보의 유출 등 침해사고가 발생한 경우 ⑤ 그 밖에 법 또는 시행령에 따른 의무를 위반한 경우에는 결합전문기관의 지정을 취소할 수 있다. 특히, 보호위원회등은 ①, ②에 해당하는 경우에는 지정을 취소하여야 하며, ③부터 ⑤에 해당하는 경우에는 시정 및 보완을 요구할 수 있다. 보호위원회등은 결합전문기관의 지정을 취소하려는 경우 청문을 하여야 한다.

2. 가명정보 결합 반출

제28조의2에서는 가명정보를 과학적 연구 등 목적으로 정보주체의 동의 없이 처리할 수 있도록 하는 바, 개인정보처리자는 이용·제공·결합 등 다양한 처리를 통해 가명정보를 가치 있게 활용할 수 있다. 반면, 제28조의3은 다양한 처리 중 다른 개인정보처리자간의 가명정보의 결합은 개인정보처리자가 스스로 하지 못하도록 하고 반드시 보호위원회등이 지정한 전문기관을 통하도록 하고 있다.

여기서 결합은 누군지는 특정할 수 없는 한 사람에 관한 정보를 하나로 합치는 것을 의미한다. 예컨대 어떤 사람들의 소비 성향에 관한 정보와 이동 경로에 관한 정보를 결합할 수 있다면 이동 경로 및 시간대별 서비스 개선 사항 등을 발견할 수 있어 정보주체의 만족도 제고나 산업 발전에 기여할 수 있다.

가 결합 신청

가명정보의 결합을 신청하려는 개인정보처리자(이하 ‘결합신청자’라 한다. 이 때, 결합된 정보를 반출 받아 해당 정보를 처리하려는 자도 개인정보처리자에 포함된다)는 결합신청서와 ① 사업자등록증, 법인등기부등본 등 결합신청자 관련 서류 ② 결합 대상 가명정보에 관한 서류 ③ 결합 목적을 증명할 수 있는 서류 ④ 반출 정보의 안전조치계획 및 이를 증명할 수 있는 서류를 준비하여 결합전문기관에 제출하여야 한다.

보호위원회는 결합신청자, 결합전문기관, 결합기관리기관 간에 결합 신청, 결합, 반출 등을 쉽게 처리하기 위한 시스템을 구축하여 운용할 수 있다. 이 경우 결합신청자는 보호위원회가 제공하는 시스템을 통해 결합 신청 등을 수행할 수 있다.

나 가명정보의 결합

이 법은 결합기관리기관과 결합전문기관 두 기관을 통하여 가명정보를 결합하도록 하고 있다.

서로 다른 개인정보처리자 간 가명정보를 결합할 때 매개체로 이용되는 값인 ‘결합키’는 해당 정보만으로는 특정 개인을 알아볼 수 없으나 다른 정보주체와 구별할 수 있도록 조치한 정보로서 통상 개인을 식별할 수 있는 정보를 이용하여 생성한다.

만약, 누군가가 결합키를 생성한 방법인 알고리즘을 알게되는 등 결합키를 원래의 정보로 복원하는 것이 가능해진 경우 정보주체를 식별할 수 있게 되는데, 이때 정보주체를 식별한 자가 결합키 외에 얼마나 많은 정보를 보유하고 있는지가 개인정보 보호에 있어 중요한 쟁점이 된다. 이 법은 이러한 경우에도 정보주체 권리 침해를 최소화할 수 있도록 결

합기관리기관은 결합키만을 보유하고, 결합전문기관은 그 외 정보만을 보유하도록 제도적인 안전장치를 마련하였다.

결합신청자는 일련번호⁵⁾와 결합키를 결합기관리기관에 송부하고, 일련번호와 결합대상정보⁶⁾를 결합전문기관에 각각 송부하여야 한다. 결합기관리기관⁷⁾은 결합키를 결합신청자로부터 전송 받아 생성한 결합키연계정보⁸⁾를 결합전문기관에 제공하여 가명정보의 안전한 결합을 지원하는 역할을 하며, 결합전문기관은 결합기관리기관으로부터 결합키연계정보를 제공받아 특정 개인을 알아볼 수 없도록 가명정보를 결합하여 결합대상정보를 하나로 만들면 결합은 완료된다.

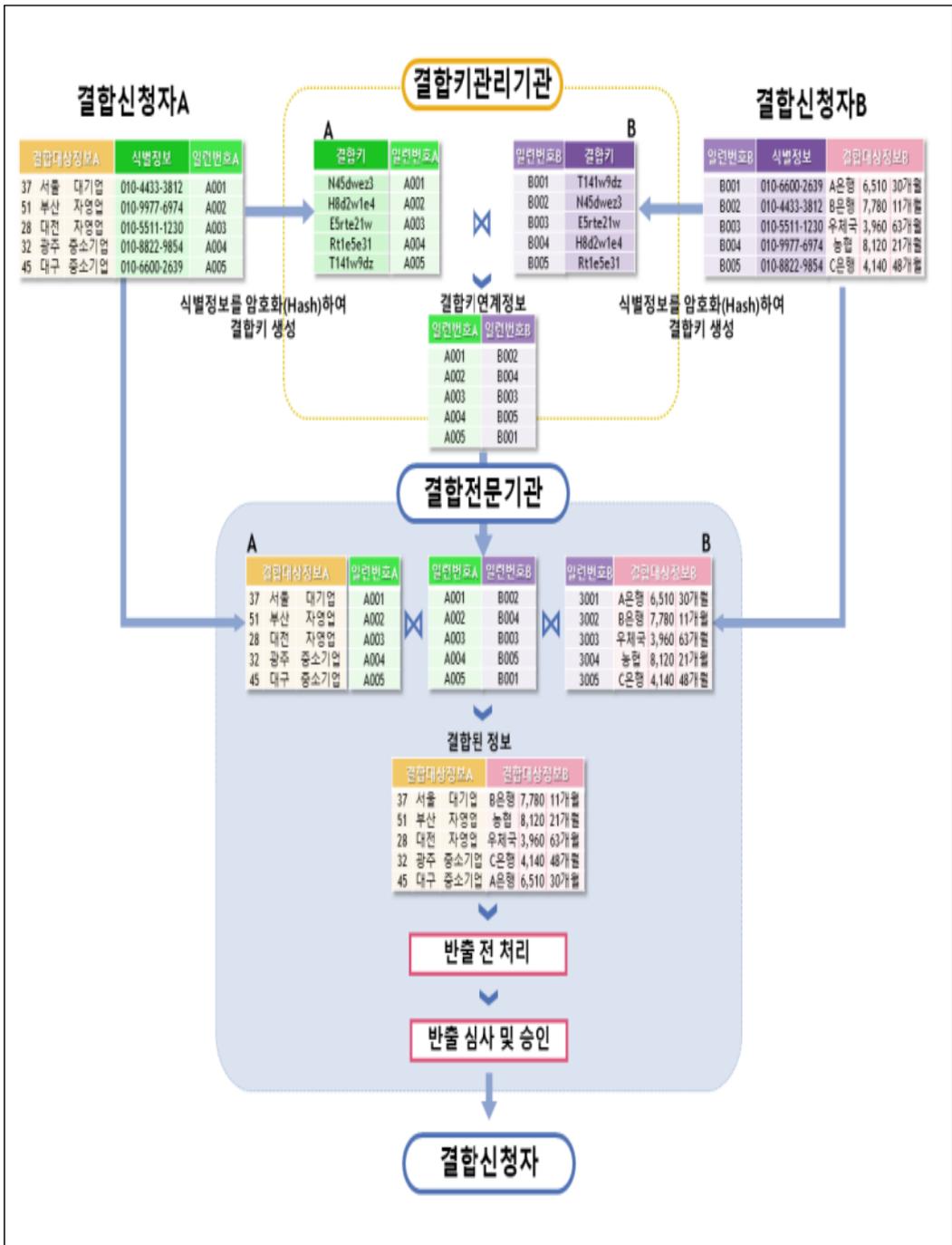
5) 결합신청자가 각 정보 주체의 레코드에 부여한 번호

6) 가명정보에서 결합키를 제외한 정보

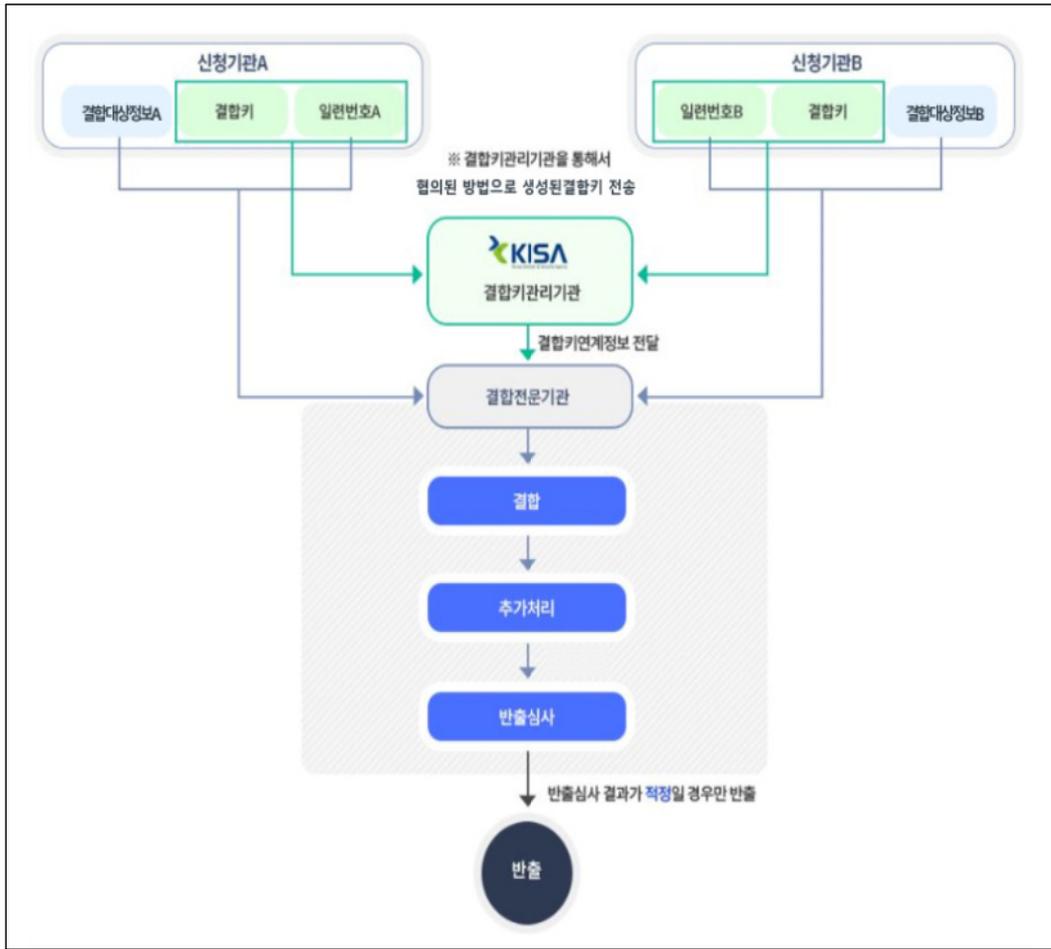
7) 현재는 한국인터넷진흥원 한 곳이나, 보호위원회는 추가로 지정하여 고시 할 수 있음

8) 정보주체에 관한 가명정보를 결합할 수 있도록 서로 다른 결합신청자의 결합키를 연계한 정보

< 가명정보 결합체계도(그림 A) >



< 가명정보 결합체계도(그림 B) >



1. 결합신청자는 각자 보유한 개인정보를 활용하여 ①일련번호와 ②결합키를 생성하고, ③ 결합대상정보에 대해 가명처리를 수행
2. 결합신청자는 결합신청이 접수된 후 1번 단계에서 생성한 결과물(①, ②, ③) 중 결합 키관리기관에는 ①, ②번을 결합전문기관에는 ①, ③번을 송신
3. 결합키관리기관은 결합신청자로부터 수신한 정보를 이용하여 '결합키연계정보'를 생성하여 결합전문기관에 전달
4. 결합전문기관은 결합키연계정보를 이용하여 결합신청자로부터 수신한 결합대상정보를 결합
5. 결합신청자는 결합전문기관 내에서 결합된 정보에 대한 추가 가명처리를 하고 전문기관에 반출심사 요청
6. 결합전문기관은 반출심사위원회를 구성하여 반출여부를 심사하고 '적정'인 경우 반출 승인

다 결합된 정보의 반출 전 처리

결합전문기관은 결합신청자가 가명정보 또는 제28조의2에 해당하는 정보로 처리(이하 ‘가명처리등’이라 한다)할 수 있도록 영 제29조의3제3항에 따른 기술적·관리적·물리적 조치가 된 공간(이하 “반출 전 처리를 위한 공간”이라 한다)을 제공하여야 하는데, 해당 공간은 기술적·관리적·물리적 보호조치를 통하여 안전성이 충분히 확보된 공간을 의미한다. 반출 전 처리를 위한 공간은 클라우드를 통해서도 구축될 수 있다. 다만, 반출심사가 이루어지기 전 결합된 정보는 특정 개인을 알아볼 수 있는 가능성이 있어 재식별의 위험이 있으므로 클라우드의 이용은 결합전문기관 내부에서만 가능하고 결합전문기관 외부에서의 이용은 허용되지 않는다.

결합신청자는 결합된 정보를 반출 전 처리를 위한 공간에서 가명처리등을 할 수 있다. 이는 각 결합신청자가 결합을 위하여 가명정보를 제공하였으나 결합된 정보의 특성에 따라 특정 개인을 알아볼 가능성을 대비한 것이다. 즉, 결합신청자로 하여금 안전한 공간에서 특정 개인을 알아볼 수 있는지 여부를 확인하도록 하고, 만일 특정 개인을 알아볼 우려가 있는 경우에는 즉시 가명처리등을 하도록 한 것이다. 이 경우, 결합전문기관은 가명처리등을 위해 필요한 자문을 할 수 있다.

라 반출 심사 및 승인

결합전문기관은 결합신청자가 결합된 정보에 대해 반출을 신청한 경우 개인정보 보호에 관하여 경험과 학식이 풍부한 전문가 3인 이상 7인 이하로 반출심사위원회를 구성하여 반출 여부를 심사하여야 한다. 반출심사위원회는 반출 심사 시 ① 결합 목적과 반출 정보가 관련성이 있을 것 ② 특정 개인을 알아볼 수 가능성이 없을 것 ③ 반출 정보에 대한 안전조치 계획이 있을 것을 고려하여야 한다.

마 비용에 관한 사항

결합전문기관은 결합 및 반출 등에 필요한 비용을 결합신청자에게 청구할 수 있다.

3. 결합전문기관의 관리·감독 등

결합전문기관은 관리·감독을 위해 보호위원회에 매년 1월 31일까지 ① 결합신청서 및 결합 및 반출 고시 제8조제1항 각 호의 첨부 서류 ② 반출심사에 대한 결과 및 심사위원

명단 ③ 결합정보 및 심사 대상 정보에 대한 파기 대장을 제출하여야 하고, 결합전문기관을 지정한 보호위원회등에게는 가명정보의 결합 및 반출 실적 보고서 결합전문기관 지정 기준을 유지하고 있음을 증명할 수 있는 서류를 제출하여야 한다. 보호위원회등은 결합전문기관이 제출한 서류를 확인하고 지정 취소사유가 확인되는 경우 시정·보완을 요구하거나 결합전문기관의 지정을 취소할 수 있다.

4. 관련 법률

「신용정보법」에서도 금융위원회가 「개인정보 보호법」의 결합전문기관과 유사한 역할을 수행하는 데이터전문기관을 지정할 수 있도록 하고, 이러한 데이터전문기관은 가명정보를 결합하여 결합신청자의 신청에 따라 가명정보 또는 익명정보를 전달할 수 있도록 규정하고 있다. 또한 「개인정보 보호법」에 따른 결합전문기관에서의 반출심사와 유사하게 데이터전문기관은 결합한 정보집합물의 가명처리 또는 익명처리에 대한 적정성 평가를 수행하도록 하고 있다(「신용정보법」 제17조의2, 제26조의4 참조). 「신용정보법」은 「개인정보 보호법」의 특별법으로 이에 따라 결합을 수행하였을 경우 「개인정보 보호법」에 따른 결합 절차를 별도로 수행하지 않아도 된다. 다만, 결합된 정보에 개인정보가 포함되어 있을 경우 안전조치의무, 금지의무, 과징금 부과 등에 있어서는 「개인정보 보호법」의 적용 대상이 된다.

신용정보법	<p>제17조의2(정보집합물의 결합 등) ① 신용정보회사등(대통령령으로 정하는 자는 제외한다. 이하 이 조 및 제40조의2에서 같다)은 자기가 보유한 정보집합물을 제3자가 보유한 정보집합물과 결합하려는 경우에는 제26조의4에 따라 지정된 데이터전문기관을 통하여 결합하여야 한다.</p> <p>② 제26조의4에 따라 지정된 데이터전문기관이 제1항에 따라 결합된 정보집합물을 해당 신용정보회사등 또는 그 제3자에게 전달하는 경우에는 가명처리 또는 익명처리가 된 상태로 전달하여야 한다.</p> <p>③ 제1항 및 제2항에서 규정한 사항 외에 정보집합물의 결합·제공·보관의 절차 및 방법에 대해서는 대통령령으로 정한다.</p> <p>제26조의4(데이터전문기관) ① 금융위원회는 제17조의2에 따른 정보집합물의 결합 및 제40조의2에 따른 익명처리의 적정성 평가를 전문적으로 수행하는 법인 또는 기관(이하 “데이터전문기관”이라 한다)을 지정할 수 있다.</p> <p>② 데이터전문기관은 다음 각 호의 업무를 수행한다.</p> <ol style="list-style-type: none"> 1. 신용정보회사등이 보유하는 정보집합물과 제3자가 보유하는 정보집합물 간의 결합 및 전달 2. 신용정보회사등의 익명처리에 대한 적정성 평가 3. 제1호 및 제2호와 유사한 업무로서 대통령령으로 정하는 업무
-------	---

- ③ 데이터전문기관은 제2항제1호 및 제2호의 업무를 전문적으로 수행하기 위하여 필요하면 대통령령으로 정하는 바에 따라 적정성평가위원회를 둘 수 있다.
- ④ 데이터전문기관은 다음 각 호의 어느 하나에 해당하는 경우에는 대통령령으로 정하는 위험관리체계를 마련하여야 한다.
 1. 제2항제1호의 업무와 같은 항 제2호의 업무를 함께 수행하는 경우
 2. 제2항 각 호의 업무와 이 법 또는 다른 법령에 따른 업무를 함께 수행하는 경우
- ⑤ 제1항에 따른 지정의 기준 및 취소, 제3항에 따른 적정성평가위원회의 구성·운영에 관하여 필요한 사항은 대통령령으로 정한다.

5. 벌칙규정

위반행위	벌칙
가명정보의 결합 제한을 위반하여 가명정보를 처리하거나 제3자에게 제공한 자 및 그 사정을 알면서도 영리 또는 부정한 목적으로 가명정보를 제공받은 자 (제28조의3 위반)	5년 이하의 징역 또는 5천만원 이하의 벌금 (제71조제4의2호)

제28조의4 | 가명정보에 대한 안전조치 의무 등

법률	<p>제28조의4(가명정보에 대한 안전조치의무 등) ① 개인정보처리자는 가명정보를 처리하는 경우에는 원래의 상태로 복원하기 위한 추가 정보를 별도로 분리하여 보관·관리하는 등 해당 정보가 분실·도난·유출·위조·변조 또는 훼손되지 않도록 대통령령으로 정하는 바에 따라 안전성 확보에 필요한 기술적·관리적 및 물리적 조치를 하여야 한다.</p> <p>② 개인정보처리자는 가명정보를 처리하고자 하는 경우에는 가명정보의 처리 목적, 제3자 제공 시 제공받는 자 등 가명정보의 처리 내용을 관리하기 위하여 대통령령으로 정하는 사항에 대한 관련 기록을 작성하여 보관하여야 한다.</p>
시행령	<p>제29조의5(가명정보에 대한 안전성 확보 조치) ① 개인정보처리자는 법 제28조의4 제1항에 따라 가명정보 및 가명정보를 원래의 상태로 복원하기 위한 추가 정보(이하 이 조에서 “추가정보”라 한다)에 대하여 다음 각 호의 안전성 확보 조치를 해야 한다.</p> <ol style="list-style-type: none"> 1. 제30조 또는 제48조의2에 따른 안전성 확보 조치 2. 가명정보와 추가정보의 분리 보관. 다만, 추가정보가 불필요한 경우에는 추가정보를 파기해야 한다. 3. 가명정보와 추가정보에 대한 접근 권한의 분리. 다만, 「소상공인 보호 및 지원에 관한 법률」 제2조에 따른 소상공인으로서 가명정보를 취급할 자를 추가로 둘 여력이 없는 경우 등 접근 권한의 분리가 어려운 정당한 사유가 있는 경우에는 업무 수행에 필요한 최소한의 접근 권한만 부여하고 접근 권한의 보유 현황을 기록으로 보관하는 등 접근 권한을 관리·통제해야 한다. <p>② 법 제28조의4제2항에서 “대통령령으로 정하는 사항”이란 다음 각 호의 사항을 말한다.</p> <ol style="list-style-type: none"> 1. 가명정보 처리의 목적 2. 가명처리한 개인정보의 항목 3. 가명정보의 이용내역 4. 제3자 제공 시 제공받는 자 5. 그 밖에 가명정보의 처리 내용을 관리하기 위하여 보호위원회가 필요하다고 인정하여 고시하는 사항

제28조의4는 개인정보처리자에게 개인정보를 가명처리하여 통계 작성, 과학적 연구, 공익적 기록보존 등의 목적으로 처리하는 경우에도 다른 개인정보와 마찬가지로 개인정보 보호에 필요한 조치를 하고, 가명정보의 처리 과정에서 침해사고가 발생하는 경우 등에 대비해 관련 기록을 작성하여 보관하도록 하고 있다.

1. 가명정보 등의 안전조치

가 가명정보에 대한 안전조치

개인정보처리자는 가명정보 또는 추가정보가 분실·도난·유출·위조·변조 또는 훼손되지 않도록 영 제30조에 따라 안전성 확보에 필요한 조치를 하여야 한다. 한편, 정보통신서비스 제공자에 해당하는 경우에는 영 제48조의2에 따라 안전성 확보에 필요한 조치를 하여야 한다.

나 추가정보의 분리 보관 등

가명처리에서 생성·사용된 추가정보는 특정 개인을 알아보는 행위를 방지하기 위하여 가명정보와 별도로 분리하여 보관하여야 한다. 추가정보의 보관이 목적이 아니므로 해당 추가정보가 불필요할 때에는 파기하여야 한다.

또한, 추가정보를 별도 분리 보관하는 경우 추가정보에 비인가자들이 접근하지 못하도록 접근 권한을 분리하고 접근통제를 강화하여야 한다. 추가정보에 접근할 수 있는 자는 업무에 필요한 최소한으로 인원으로 엄격하게 통제하여야 하며, 가명정보에 접근할 수 없도록 권한을 분리하여야 한다. 다만, 「소상공인 보호 및 지원에 관한 법률」 제2조에 따른 소상공인으로서 가명정보를 취급할 자를 추가로 둘 여력이 없는 경우 등 접근 권한의 분리가 어려운 정당한 사유가 있는 경우에는 업무 수행에 필요한 최소한의 접근 권한만 부여하고 접근 권한의 보유 현황을 기록으로 보관하는 등 접근 권한을 관리·통제해야 한다.

2. 가명정보에 대한 기록·보관

개인정보처리자는 가명정보를 처리하고자 하는 경우 가명정보의 처리 목적, 가명처리한 개인정보의 항목, 가명정보의 이용내역, 가명정보를 제3자에게 제공하는 경우 제공받는 자에 관한 사항을 작성하여 보관하여야 한다.

3. 관련 법률

「신용정보법」에서도 「개인정보 보호법」과 같이 신용정보회사들이 가명처리를 하는

경우 가명처리에 사용한 추가정보를 분리하여 보관하거나 삭제하여야 하며, 가명정보에 대하여 제3자의 불법적인 접근, 입력된 정보의 변경·훼손 및 파괴, 그 밖의 위험으로부터 가명정보를 보호하기 위하여 내부관리계획을 수립하고 접속기록을 보관하는 등 기술적·물리적·관리적 보안대책을 수립·시행하도록 규정하고 있다(「신용정보법」 제40조의2제1항, 제2항).

신용정보법	<p>제40조의2(가명처리·익명처리에 관한 행위규칙) ① 신용정보회사등은 가명처리에 사용한 추가정보를 대통령령으로 정하는 방법으로 분리하여 보관하거나 삭제하여야 한다.</p> <p>② 신용정보회사등은 가명처리한 개인신용정보에 대하여 제3자의 불법적인 접근, 입력된 정보의 변경·훼손 및 파괴, 그 밖의 위험으로부터 가명정보를 보호하기 위하여 내부관리계획을 수립하고 접속기록을 보관하는 등 대통령령으로 정하는 바에 따라 기술적·물리적·관리적 보안대책을 수립·시행하여야 한다.</p>
-------	---

4. 벌칙규정

위반행위	벌칙
안전성 확보에 필요한 조치를 하지 아니하여 개인정보를 분실·도난·유출·위조·변조 또는 훼손당한 자 (제28조의4제1항 위반)	2년 이하의 징역 또는 2천만원 이하의 벌금 (제73조제1호)
안전성 확보에 필요한 조치를 하지 아니한 자 (제28조의4제1항 위반)	3천만원 이하의 과태료 (제75조제2항제6호)
관련 기록을 작성하여 보관하지 아니한 자 (제28조의4제2항 위반)	1천만원 이하의 과태료 (제75조제4항제6의2호)

제28조의5 | 가명정보 처리 시 금지의무 등

법률

- 제28조의5(가명정보 처리 시 금지의무 등)** ① 누구든지 특정 개인을 알아보기 위한 목적으로 가명정보를 처리해서는 아니 된다.
- ② 개인정보처리자는 가명정보를 처리하는 과정에서 특정 개인을 알아볼 수 있는 정보가 생성된 경우에는 즉시 해당 정보의 처리를 중지하고, 지체 없이 회수·파기하여야 한다.

가명정보는 통계작성, 과학적 연구, 공익적 기록보존 등 제한된 목적으로 정보주체의 동의 없이 처리할 수 있도록 안전조치를 한 정보이다. 따라서 제28조의5는 특정 개인을 알아볼 수 없도록 한 속성은 유지되어야 하므로 재식별 금지의무 등을 규정하고 있다.

1. 특정 개인을 알아보기 위한 목적의 가명정보 처리 금지

가 적용 범위

본 조항은 가명정보를 보유하고 있는 개인정보처리자는 물론 그에 소속된 개인정보취급자나, 가명정보를 제공받은 자 또는 적법하지 않은 방법으로 가명정보를 입수한 자 등을 가리지 않고 누구든지 특정 개인을 알아보기 위한 목적으로 가명정보를 처리하여서는 안 된다는 금지의무를 정하고 있다.

나 특정 개인을 알아보기 위한 목적의 처리

특정 개인을 알아보기 위하여 가명정보를 처리하는 것은 해당 가명 정보의 정보주체가 누구인지 알아볼 수 있도록 하는 행위 일체를 의미한다. 즉, 가명처리 시 사용한 알고리즘, 매핑테이블 등을 사용하여 원래 정보로 복원하는 행위는 물론이고, 보유하고 있는 다른 정보나 공개된 정보와의 결합 또는 대조·비교 등을 통해 특정 개인을 알아보기 위한 시도는 모두 금지된다.

한편, 의도하지 않게 특정 개인을 알아보게 되는 것 자체는 행정적 제재 또는 형사 처벌의 대상이 아니다. 의도하지 않게 특정 개인을 알아보게 되었는지 여부는 행위자가 가명정보를 입수한 경위, 특정 개인이 식별된 정황, 그로부터 얻게 된 정보의 내용, 정보 획득에 대한 경제적·비경제적 이익 등의 유인·동기 등을 종합적으로 고려하여 판단한다.

2. 가명정보의 처리중지 및 회수·파기 의무

개인정보처리자는 가명정보의 처리 과정에서 특정 개인을 알아볼 수 있는 정보가 생성된 사실이 확인된 경우 즉시 처리중지, 회수, 파기 등 위험을 제거하기 위해 적절한 조치를 하여야 한다. 여기에서 ‘특정 개인을 알아볼 수 있는 정보’란 정보주체를 알아볼 수 있게 하는 정보를 말한다. 특정 개인을 알아볼 수 있는 정보는 가명정보 중 일부의 정보주체에 관한 것일 수도 있고, 다수의 정보주체에 해당하는 것일 수도 있다.

가명정보의 처리를 위탁한 경우 수탁자가 해당 가명정보에 대한 처리중지 및 회수·파기를 완료하여야만 개인정보처리자 스스로의 의무 이행을 다 한 것으로 볼 수 있다.

3. 벌칙규정

위반행위	벌칙
특정 개인을 알아보기 위한 목적으로 가명정보를 처리 (제28조의5제1항 위반)	5년 이하의 징역 또는 5천만원 이하의 벌금 (제71조 제4의3호) 전체 매출액의 100분의 3 이하의 과징금(제28조의6제1항)
특정 개인을 알아볼 수 있는 정보가 생성되었음에도 가명정보의 이용을 중지하지 않거나 또는 회수·파기하지 아니한 자 (제28조의5제2항 위반)	3천만원 이하의 과태료 (제75조 제2항 제7의2호)

4. 관련 법률

「신용정보법」 역시 신용정보회사등이 가명정보를 영리 또는 부정한 목적으로 특정 개인을 알아볼 수 있게 처리하는 것을 금지하고 있으며(「신용정보법」 제40조의2제6항), 신용정보회사등이 가명정보를 이용하는 과정에서 특정 개인을 알아볼 수 있게 된 경우 즉시 그 가명정보를 회수하여 처리를 중지하고, 특정 개인을 알아볼 수 있게 된 정보는 즉시 삭제하도록 의무를 부과하고 있다(「신용정보법」 제40조의2제7항).

신용정보법	<p>제40조의2(가명처리·익명처리에 관한 행위규칙)</p> <p>⑥ 신용정보회사등은 영리 또는 부정한 목적으로 특정 개인을 알아볼 수 있게 가명정보를 처리하여서는 아니 된다.</p> <p>⑦ 신용정보회사등은 가명정보를 이용하는 과정에서 특정 개인을 알아볼 수 있게 된 경우 즉시 그 가명정보를 회수하여 처리를 중지하고, 특정 개인을 알아볼 수 있게 된 정보는 즉시 삭제하여야 한다.</p>
-------	---

제28조의6 | 가명정보 처리에 대한 과징금 부과 등

<p style="text-align: center;">법률</p>	<p>제28조의6(가명정보 처리에 대한 과징금 부과 등) ① 보호위원회는 개인정보처리자가 제28조의5제1항을 위반하여 특정 개인을 알아보기 위한 목적으로 정보를 처리한 경우 전체 매출액의 100분의 3 이하에 해당하는 금액을 과징금으로 부과할 수 있다. 다만, 매출액이 없거나 매출액의 산정이 곤란한 경우로서 대통령령으로 정하는 경우에는 4억원 또는 자본금의 100분의 3 중 큰 금액 이하로 과징금을 부과할 수 있다.</p> <p>② 과징금의 부과·징수 등에 필요한 사항은 제34조의2제3항부터 제5항까지의 규정을 준용한다.</p>
<p style="text-align: center;">시행령</p>	<p>제29조의6(가명정보 처리에 대한 과징금의 부과기준 등) ① 법 제28조의6에서 “전체 매출액”이란 해당 개인정보처리자의 직전 3개 사업연도의 연평균 매출액을 말한다. 다만, 해당 사업연도 초일 현재 사업을 개시한지 3년이 되지 아니하는 경우에는 그 사업개시 후 직전 사업연도 말일까지의 매출액을 연평균 매출액으로 환산한 금액을 말하며, 해당 사업연도에 사업을 개시한 경우에는 사업개시일부터 위반행위일까지의 매출액을 연매출액으로 환산한 금액을 말한다.</p> <p>② 법 제28조의6에서 “대통령령으로 정하는 경우”란 다음 각 호의 어느 하나에 해당하는 경우를 말한다.</p> <ol style="list-style-type: none"> 1. 영업을 개시하지 아니하거나 영업을 중단하는 등의 사유로 영업실적이 없는 경우 2. 재해 등으로 인하여 매출액 산정자료가 소멸되거나 훼손되는 등 객관적인 매출액의 산정이 곤란한 경우 <p>③ 보호위원회는 제1항에 따른 매출액 산정을 위하여 재무제표 등 자료가 필요한 경우 20일 이내의 기간을 정하여 해당 개인정보처리자에게 관련 자료의 제출을 요청할 수 있다.</p> <p>④ 법 제28조의6에 따른 과징금의 산정기준과 산정절차는 별표 1의3과 같다.</p>

과징금이란 “행정법상의 의무를 위반하거나 이행하지 않는 자에 대하여 행정청이 부과하는 금전적인 제재”를 의미한다. 이는 형사법상의 금전적인 제재수단인 벌금과 구별된다.

이 법은 특정 개인을 알아보기 위한 목적으로 가명정보를 처리한 경우와 주민등록번호의 분실·도난·유출·위조·변조 또는 훼손된 경우, 정보통신서비스 제공자등이 이 법을 위반한 경우로서 일정한 경우(제39조의15 참고)에 한하여 과징금 규정을 두고 있다.

1. 과징금 부과 내용

보호위원회는 개인정보처리자가 제28조의5제1항을 위반하여 특정 개인을 알아보기 위한 목적으로 정보를 처리한 경우 전체 매출액의 100분의 3 이하에 해당하는 금액을 과징금으로 부과할 수 있다. 이 때 전체 매출액이란 해당 개인정보처리자의 직전 3개 사업연도의 연평균 매출액을 말하며, 당해연도 초일 현재 사업을 개시한지 3년이 되지 아니하는 경우에는 그 사업개시 후 직전 사업연도 말일까지의 매출액을 연평균 매출액으로 환산한 금액을 말하며, 또는 해당 사업연도에 사업을 개시한 경우에는 사업개시일부터 위반행위일까지의 매출액을 연매출액으로 환산한 금액이 전체 매출액으로서 과징금 산정의 기초가 된다.

매출액이 없거나 매출액의 산정이 곤란한 경우로서 개인정보처리자가 영업을 개시하지 아니하거나 영업을 중단하는 등의 사유로 영업실적이 없는 경우 또는 재해 등으로 인하여 매출액 산정자료가 소멸되거나 훼손되는 등 객관적인 매출액의 산정이 곤란한 경우에는 4억원 또는 자본금의 100분의 3 중 큰 금액 이하로 과징금을 부과할 수 있다.

구체적인 과징금 부과 기준은 다음 표와 같다.

〈과징금의 부과기준(영 제40조의2제1항, 별표 1의3)〉

1. 과징금의 산정단계

과징금은 법 제28조의6제1항에 따른 위반행위와 이에 영향을 미치는 행위를 종합적으로 고려하여 제2호가목에 따라 산정된 기준금액에 같은 호 나목에 따른 필수적 가중·감경, 같은 호 다목에 따른 추가적 가중·감경을 순차적으로 거쳐 산정한다. 다만, 가중하는 경우에도 법 제28조의6제1항에 따른 과징금 금액의 상한을 넘을 수 없다.

2. 과징금의 산정단계에 따른 산정방식과 고려사유

가. 기준금액의 산정

1) 기준금액은 제29조의6제1항에 따른 매출액에 위반행위의 중대성에 따라 다음과 같이 구분된 과징금의 산정비율(부과기준율)을 곱하여 산출한 금액으로 한다.

위반행위의 중대성	부과기준율
매우 중대한 위반행위	1천분의 27
중대한 위반행위	1천분의 21
일반 위반행위	1천분의 15

2) 제29조의6제2항 각 호의 어느 하나에 해당하는 경우에는 1)에도 불구하고 위반행위의 중대성에 따라 기준금액을 다음과 같이 한다.

위반행위의 중대성	기준금액
매우 중대한 위반행위	3억 6천만원
중대한 위반행위	2억 8천만원
일반 위반행위	2억원

3) 위반행위의 중대성은 고의·중과실 여부, 영리 목적의 유무, 위반행위로 인한 개인정보의 피해규모, 개인정보의 공중에 노출 여부 및 위반행위로 인하여 취득한 이익의 규모 등을 종합적으로 고려하여 판단한다.

나. 필수적 가중·감경

위반행위의 기간과 횟수 등을 고려하여 기준금액의 100분의 50의 범위에서 가중하거나 감경해야 한다.

다. 추가적 가중·감경

개인정보 보호를 위한 노력 정도, 위반행위에 대한 조사의 협조 여부, 위반행위의 주도 여부 등을 종합적으로 고려하여 필수적 가중·감경을 거친 금액의 100분의 50의 범위에서 가중하거나 감경할 수 있다.

3. 세부 기준

위반행위의 중대성 판단 기준, 필수적 가중·감경 및 추가적 가중·감경을 위한 세부 기준과 그 밖에 과징금의 부과에 필요한 사항은 보호위원회가 정하여 고시한다.

제28조의7 | 적용범위

법률

제28조의7(적용범위) 가명정보는 제20조, 제21조, 제27조, 제34조제1항, 제35조부터 제37조까지, 제39조의3, 제39조의4, 제39조의6부터 제39조의8까지의 규정을 적용하지 아니한다.

1. 가명정보에 적용되지 않는 규정

통계작성, 과학적 연구, 공익적 기록보존 등의 목적으로 처리하는 가명정보에 대하여는 아래의 규정을 적용하지 아니한다. 이는 법 제28조의5에서 누구든지 가명정보를 개인을 알아볼 목적으로 처리하는 것을 금지하고 있는데 아래의 규정은 개인을 알아보아야만 가능한 사항이기 때문이다.

한편, 정보통신서비스제공자는 분실·도난·유출 규모에 관계없이 보호위원회 또는 전문기관에 신고해야 하는 제39조의4제1항의 특례 규정은 적용이 배제되나, 일정 규모 이상(1천명 이상)의 정보주체에 관한 가명정보가 유출된 경우에는 제34조의3항에 따라 보호위원회 또는 전문기관에 대한 신고 의무를 진다.

가명정보에 적용되지 않는 규정

제20조(정보주체 이외로부터 수집한 개인정보의 수집 출처 등 고지)
제21조(개인정보의 파기)
제27조(영업양도 등에 따른 개인정보의 이전 제한)
제34조(개인정보 유출 통지 등) 제1항
제35조(개인정보 열람)
제36조(개인정보의 정정·삭제)
제37조(개인정보의 처리정지 등)
제39조의3(개인정보의 수집·이용 동의 등에 대한 특례)
제39조의4(개인정보 유출등의 통지·신고에 대한 특례)
제39조의6(개인정보의 파기에 대한 특례)
제39조의7(이용자의 권리 등에 대한 특례)
제39조의8(개인정보 이용내역의 통지)

2. 가명정보에 적용되는 규정

원칙적으로 본 조에서 언급되지 아니한 「개인정보 보호법」의 조항은 가명정보의 성질에 반하지 않는 한 가명정보에도 적용된다. 예컨대, 개인정보처리자는 가명정보를 처리

하는 경우 개인정보 보호 원칙(제3조)에 따라서 처리 목적의 범위에 필요한 범위에서 적합하게 가명정보를 처리하여야 하며, 가명정보 처리 업무를 위탁하는 경우에는 법 제26조의 요건을 모두 준수하여야 한다. 또한 개인정보 처리방침에 가명정보 관련 내용(가명정보의 처리 목적, 제3자 제공에 관한 사항, 위탁에 관한 사항 등)을 포함하여야 한다.

3. 관련 법률

「신용정보법」에서는 가명정보에 대하여 신용정보주체에 대한 통지 고지 또는 설명 의무 조항, 개인신용정보의 전송요구권, 조회권, 열람 정정권, 삭제 요구권, 동의 철회권 등 신용정보주체의 권리 조항 등의 규정을 적용하지 아니한다고 정하고 있다(「신용정보법」 제40조의3). 또한, 「신용정보법」은 추가로 가명정보 누설 시 신용정보주체에 대한 통지의무, 감독당국에 대한 신고의무를 적용을 배제하고 있다.

「신용정보법」상 가명정보는 상거래관계 종료일로부터 최장 5년 이내에 삭제하여야 하는 개인신용정보 파기 의무의 예외에 해당한다. 신용정보회사등은 ① 추가정보 및 추가정보 및 가명정보에 대한 관리적·물리적·기술적 보호조치 수준 ② 가명정보의 재식별시 정보주체에 미치는 영향 ③ 가명정보의 재식별 가능성 ④ 가명정보의 이용목적 및 그 목적 달성에 필요한 최소기간을 고려하여 가명처리한 자가 가명처리 시 정한 기간 동안 가명정보를 보유할 수 있다(「신용정보법」 제20조의2제2항제2호의2 및 동법 시행령 제17조의2제3항).

신용정보법	<p>제40조의3(가명정보에 대한 적용 제외) 가명정보에 관하여는 제32조제7항, 제33조의2, 제35조, 제35조의2, 제35조의3, 제36조, 제36조의2, 제37조, 제38조, 제38조의2, 제38조의3, 제39조 및 제39조의2부터 제39조의4까지의 규정을 적용하지 아니한다.</p> <p>제20조의2(개인신용정보의 보유기간 등) ② 「개인정보 보호법」 제21조제1항에도 불구하고 신용정보제공·이용자는 금융거래 등 상거래관계가 종료된 날부터 최장 5년 이내(해당 기간 이전에 정보 수집·제공 등의 목적이 달성된 경우에는 그 목적이 달성된 날부터 3개월 이내)에 해당 신용정보주체의 개인신용정보를 관리대상에서 삭제하여야 한다. 다만, 다음 각 호의 경우에는 그러하지 아니하다.</p> <p>2의2. 가명정보를 이용하는 경우로서 그 이용 목적, 가명처리의 기술적 특성, 정보의 속성 등을 고려하여 대통령령으로 정하는 기간 동안 보존하는 경우</p>
-------	--

4. 벌칙 규정

가명정보에 적용되는 규정을 위반하는 경우, 해당 위반행위에 대한 벌칙 규정이 적용된다. 예를 들어, 제59조제2호를 위반하여 업무상 알게 된 가명정보를 누설하거나 권한 없이 다른 사람이 이용하도록 제공한 자는 5년 이하의 징역 또는 5천만원 이하의 벌금에 처한다.

제4장

개인정보의 안전한 관리

- 제29조 안전조치의무
- 제30조 개인정보 처리방침의 수립 및 공개
- 제31조 개인정보 보호책임자의 지정
- 제32조 개인정보파일의 등록 및 공개
- 제32조의2 개인정보 보호 인증
- 제33조 개인정보 영향평가
- 제34조 개인정보 유출 통지 등
- 제34조의2 과징금의 부과 등



제29조 | 안전조치의무

<p>법률</p>	<p>제29조(안전조치의무) 개인정보처리자는 개인정보가 분실·도난·유출·위조·변조 또는 훼손되지 아니하도록 내부 관리계획 수립, 접속기록 보관 등 대통령령으로 정하는 바에 따라 안전성 확보에 필요한 기술적·관리적 및 물리적 조치를 하여야 한다.</p>
<p>시행령</p>	<p>제30조(개인정보의 안전성 확보 조치) ① 개인정보처리자는 법 제29조에 따라 다음 각 호의 안전성 확보 조치를 하여야 한다.</p> <ol style="list-style-type: none"> 1. 개인정보의 안전한 처리를 위한 내부 관리계획의 수립·시행 2. 개인정보에 대한 접근 통제 및 접근 권한의 제한 조치 3. 개인정보를 안전하게 저장·전송할 수 있는 암호화 기술의 적용 또는 이에 상응하는 조치 4. 개인정보 침해사고 발생에 대응하기 위한 접속기록의 보관 및 위조·변조 방지를 위한 조치 5. 개인정보에 대한 보안프로그램의 설치 및 갱신 6. 개인정보의 안전한 보관을 위한 보관시설의 마련 또는 잠금장치의 설치 등 물리적 조치 <p>② 보호위원회는 개인정보처리자가 제1항에 따른 안전성 확보 조치를 하도록 시스템을 구축하는 등 필요한 지원을 할 수 있다.</p> <p>③ 제1항에 따른 안전성 확보 조치에 관한 세부 기준은 보호위원회가 정하여 고시한다.</p>
<p>표준지침</p>	<p>제47조(개인영상정보의 안전성 확보를 위한 조치) 영상정보처리기기운영자는 개인영상정보가 분실·도난·유출·변조 또는 훼손되지 아니하도록 법 제29조 및 영 제30조제1항에 따라 안전성 확보를 위하여 다음 각 호의 조치를 하여야 한다.</p> <ol style="list-style-type: none"> 1. 개인영상정보의 안전한 처리를 위한 내부 관리계획의 수립·시행, 다만 「개인정보의 안전성 확보조치 기준 고시」 제2조제4호에 따른 ‘소상공인’은 내부관리계획을 수립하지 아니할 수 있다. 2. 개인영상정보에 대한 접근 통제 및 접근 권한의 제한 조치 3. 개인영상정보를 안전하게 저장·전송할 수 있는 기술의 적용 (네트워크 카메라의 경우 안전한 전송을 위한 암호화 조치, 개인영상정보파일 저장 시 비밀번호 설정 등) 4. 처리기록의 보관 및 위조·변조 방지를 위한 조치 (개인영상정보의 생성 일시 및 열람할 경우에 열람 목적·열람자·열람 일시 등 기록·관리 조치 등) 5. 개인영상정보의 안전한 물리적 보관을 위한 보관시설 마련 또는 잠금장치 설치

개인정보의 안전성 확보조치 기준(보호위원회 고시 제2020-2호)

제1조(목적) 이 기준은 「개인정보 보호법」(이하 “법”이라 한다) 제23조제2항, 제24조제3항 및 제29조와 같은 법 시행령(이하 “영”이라 한다) 제21조 및 제30조에 따라 개인정보처리자가 개인정보를 처리함에 있어서 개인정보가 분실·도난·유출·위조·변조 또는 훼손되지 아니하도록 안전성 확보에 필요한 기술적·관리적 및 물리적 안전조치에 관한 최소한의 기준을 정하는 것을 목적으로 한다.

제2조(정의) 이 기준에서 사용하는 용어의 뜻은 다음과 같다.

1. “정보주체”란 처리되는 정보에 의하여 알아볼 수 있는 사람으로서 그 정보의 주체가 되는 사람을 말한다.
2. “개인정보파일”이란 개인정보를 쉽게 검색할 수 있도록 일정한 규칙에 따라 체계적으로 배열하거나 구성한 개인정보의 집합물(集合物)을 말한다.
3. “개인정보처리자”란 업무를 목적으로 개인정보파일을 운영하기 위하여 스스로 또는 다른 사람을 통하여 개인정보를 처리하는 공공기관, 법인, 단체 및 개인 등을 말한다.
4. “대기업”이란 「독점규제 및 공정거래에 관한 법률」 제14조에 따라 공정거래위원회가 지정한 기업집단을 말한다.
5. “중견기업”이란 「중견기업 성장촉진 및 경쟁력 강화에 관한 특별법」 제2조에 해당하는 기업을 말한다.
6. “중소기업”이란 「중소기업기본법」 제2조 및 동법 시행령 제3조에 해당하는 기업을 말한다.
7. “소상공인”이란 「소상공인 보호 및 지원에 관한 법률」 제2조에 해당하는 자를 말한다.
8. “개인정보 보호책임자”란 개인정보처리자의 개인정보 처리에 관한 업무를 총괄해서 책임지는 자로서 영 제32조제2항에 해당하는 자를 말한다.
9. “개인정보취급자”란 개인정보처리자의 지휘·감독을 받아 개인정보를 처리하는 업무를 담당하는 자로서 임직원, 파견근로자, 시간제근로자 등을 말한다.
10. “개인정보처리시스템”이란 데이터베이스시스템 등 개인정보를 처리할 수 있도록 체계적으로 구성된 시스템을 말한다.
11. “위험도 분석”이란 개인정보 유출에 영향을 미칠 수 있는 다양한 위험요소를 식별·평가하고 해당 위험요소를 적절하게 통제할 수 있는 방안 마련을 위한 종합적으로 분석하는 행위를 말한다.
12. “비밀번호”란 정보주체 또는 개인정보취급자 등이 개인정보처리시스템, 업무용 컴퓨터 또는 정보통신망 등에 접속할 때 식별자와 함께 입력하여 정당한 접속 권한을 가진 자라는 것을 식별할 수 있도록 시스템에

전달해야 하는 고유의 문자열로서 타인에게 공개되지 않는 정보를 말한다.

13. “정보통신망”이란 「전기통신기본법」 제2조제2호에 따른 전기통신설비를 이용하거나 전기통신설비와 컴퓨터 및 컴퓨터의 이용기술을 활용하여 정보를 수집·가공·저장·검색·송신 또는 수신하는 정보통신체계를 말한다.
14. “공개된 무선망”이란 불특정 다수가 무선접속장치(AP)를 통하여 인터넷을 이용할 수 있는 망을 말한다.
15. “모바일 기기”란 무선망을 이용할 수 있는 PDA, 스마트폰, 태블릿PC 등 개인정보 처리에 이용되는 휴대용 기기를 말한다.
16. “바이오정보”란 지문, 얼굴, 홍채, 정맥, 음성, 필적 등 개인을 식별할 수 있는 신체적 또는 행동적 특징에 관한 정보로서 그로부터 가공되거나 생성된 정보를 포함한다.
17. “보조저장매체”란 이동형 하드디스크, USB메모리, CD(Compact Disk), DVD(Digital Versatile Disk) 등 자료를 저장할 수 있는 매체로서 개인정보처리시스템 또는 개인용 컴퓨터 등과 용이하게 연결·분리할 수 있는 저장매체를 말한다.
18. “내부망”이란 물리적 망분리, 접근 통제시스템 등에 의해 인터넷 구간에서의 접근이 통제 또는 차단되는 구간을 말한다.
19. “접속기록”이란 개인정보취급자 등이 개인정보처리시스템에 접속하여 수행한 업무내역에 대하여 개인정보취급자 등의 계정, 접속일시, 접속지 정보, 처리한 정보주체 정보, 수행업무 등을 전자적으로 기록한 것을 말한다. 이 경우 “접속”이란 개인정보처리시스템과 연결되어 데이터 송신 또는 수신이 가능한 상태를 말한다.
20. “관리용 단말기”란 개인정보처리시스템의 관리, 운영, 개발, 보안 등의 목적으로 개인정보처리시스템에 직접 접속하는 단말기를 말한다.

제3조(안전조치 기준 적용) 개인정보처리자가 개인정보의 안전성 확보에 필요한 조치를 하는 경우에는 [별표] 개인정보처리자 유형 및 개인정보 보유량에 따른 안전조치 기준을 적용하여야 한다. 이 경우 개인정보처리자가 어느 유형에 해당하는지에 대한 입증책임은 당해 개인정보처리자가 부담한다.

제4조(내부 관리계획의 수립·시행) ① 개인정보처리자는 개인정보의 분실·도난·유출·위조·변조 또는 훼손되지 아니하도록 내부 의사결정 절차를 통하여 다음 각 호의 사항을 포함하는 내부 관리계획을 수립·시행하여야 한다.

1. 개인정보 보호책임자의 지정에 관한 사항
2. 개인정보 보호책임자 및 개인정보취급자의 역할 및 책임에 관한 사항

3. 개인정보취급자에 대한 교육에 관한 사항
4. 접근 권한의 관리에 관한 사항
5. 접근 통제에 관한 사항
6. 개인정보의 암호화 조치에 관한 사항
7. 접속기록 보관 및 점검에 관한 사항
8. 악성프로그램 등 방지에 관한 사항
9. 물리적 안전조치에 관한 사항
10. 개인정보 보호조직에 관한 구성 및 운영에 관한 사항
11. 개인정보 유출사고 대응 계획 수립·시행에 관한 사항
12. 위험도 분석 및 대응방안 마련에 관한 사항
13. 재해 및 재난 대비 개인정보처리시스템의 물리적 안전조치에 관한 사항
14. 개인정보 처리업무를 위탁하는 경우 수탁자에 대한 관리 및 감독에 관한 사항
15. 그 밖에 개인정보 보호를 위하여 필요한 사항

② [별표]의 유형1에 해당하는 개인정보처리자는 제1항에 따른 내부 관리계획을 수립하지 아니할 수 있고, [별표]의 유형2에 해당하는 개인정보처리자는 제1항제12호부터 제14호까지를 내부 관리계획에 포함하지 아니할 수 있다.

③ 개인정보처리자는 제1항 각 호의 사항에 중요한 변경이 있는 경우에는 이를 즉시 반영하여 내부 관리계획을 수정하여 시행하고, 그 수정 이력을 관리하여야 한다.

④ 개인정보보호책임자는 접근권한 관리, 접속기록 보관 및 점검, 암호화 조치 등 내부 관리계획의 이행 실태를 연1회 이상으로 점검·관리 하여야 한다.

제5조(접근 권한의 관리) ① 개인정보처리자는 개인정보처리시스템에 대한 접근 권한을 업무 수행에 필요한 최소한의 범위로 업무 담당자에 따라 차등 부여하여야 한다.

② 개인정보처리자는 전보 또는 퇴직 등 인사이동이 발생하여 개인정보취급자가 변경되었을 경우 지체없이 개인정보처리시스템의 접근 권한을 변경 또는 말소하여야 한다.

③ 개인정보처리자는 제1항 및 제2항에 의한 권한 부여, 변경 또는 말소에 대한 내역을 기록하고, 그 기록을 최소 3년간 보관하여야 한다.

④ 개인정보처리자는 개인정보처리시스템에 접속할 수 있는 사용자계정을 발급하는 경우 개인정보취급자 별로 사용자계정을 발급하여야 하며, 다른 개인정보취급자와 공유되지 않도록 하여야 한다.

⑤ 개인정보처리자는 개인정보취급자 또는 정보주체가 안전한 비밀번호를 설정하여 이행할 수 있도록 비밀번호 작성규칙을 수립하여 적용하여야 한다.

⑥ 개인정보처리자는 권한 있는 개인정보취급자만이 개인정보처리시스템에

접근할 수 있도록 계정정보 또는 비밀번호를 일정 횟수 이상 잘못 입력한 경우 개인정보처리시스템에 대한 접근을 제한하는 등 필요한 기술적 조치를 하여야 한다.

⑦ [별표]의 유형1에 해당하는 개인정보처리자는 제1항 및 제6항을 아니할 수 있다.

제6조(접근통제) ① 개인정보처리자는 정보통신망을 통한 불법적인 접근 및 침해사고 방지를 위해 다음 각 호의 기능을 포함한 조치를 하여야 한다.

1. 개인정보처리시스템에 대한 접속 권한을 IP(Internet Protocol) 주소 등으로 제한하여 허가받지 않은 접근을 제한

2. 개인정보처리시스템에 접속한 IP (Internet Protocol)주소 등을 분석하여 불법적인 개인정보 유출 시도 탐지 및 대응

② 개인정보처리자는 개인정보취급자가 정보통신망을 통해 외부에서 개인정보처리시스템에 접속하려는 경우 가상사설망(VPN : Virtual Private Network) 또는 전용선 등 안전한 접속수단을 적용하거나 안전한 인증수단을 적용하여야 한다.

③ 개인정보처리자는 취급중인 개인정보가 인터넷 홈페이지, P2P, 공유설정, 공개된 무선망 이용 등을 통하여 열람권한이 없는 자에게 공개되거나 유출되지 않도록 개인정보처리시스템, 업무용 컴퓨터, 모바일 기기 및 관리용 단말기 등에 접근 통제 등에 관한 조치를 하여야 한다.

④ 고유식별정보를 처리하는 개인정보처리자는 인터넷 홈페이지를 통해 고유식별정보가 유출·변조·훼손되지 않도록 연 1회 이상 취약점을 점검하고 필요한 보완 조치를 하여야 한다.

⑤ 개인정보처리자는 개인정보처리시스템에 대한 불법적인 접근 및 침해사고 방지를 위하여 개인정보취급자가 일정시간 이상 업무처리를 하지 않는 경우에는 자동으로 시스템 접속이 차단되도록 하여야 한다.

⑥ 개인정보처리자가 별도의 개인정보처리시스템을 이용하지 아니하고 업무용 컴퓨터 또는 모바일 기기를 이용하여 개인정보를 처리하는 경우에는 제1항을 적용하지 아니할 수 있으며, 이 경우 업무용 컴퓨터 또는 모바일 기기의 운영체제(OS : Operating System)나 보안프로그램 등에서 제공하는 접근 통제 기능을 이용할 수 있다.

⑦ 개인정보처리자는 업무용 모바일 기기의 분실·도난 등으로 개인정보가 유출되지 않도록 해당 모바일 기기에 비밀번호 설정 등의 보호조치를 하여야 한다.

⑧ [별표]의 유형1에 해당하는 개인정보처리자는 제2항, 제4항부터 제5항까지의 조치를 아니할 수 있다.

제7조(개인정보의 암호화) ① 개인정보처리자는 고유식별정보, 비밀번호, 바이

오정보를 정보통신망을 통하여 송신하거나 보조저장매체 등을 통하여 전달하는 경우에는 이를 암호화하여야 한다.

② 개인정보처리자는 비밀번호 및 바이오정보는 암호화하여 저장하여야 한다. 다만, 비밀번호를 저장하는 경우에는 복호화되지 아니하도록 일방향 암호화하여 저장하여야 한다.

③ 개인정보처리자는 인터넷 구간 및 인터넷 구간과 내부망의 중간 지점(DMZ : Demilitarized Zone)에 고유식별정보를 저장하는 경우에는 이를 암호화하여야 한다.

④ 개인정보처리자가 내부망에 고유식별정보를 저장하는 경우에는 다음 각 호의 기준에 따라 암호화의 적용여부 및 적용범위를 정하여 시행할 수 있다.

1. 법 제33조에 따른 개인정보 영향평가의 대상이 되는 공공기관의 경우에는 해당 개인정보 영향평가의 결과

2. 암호화 미적용시 위험도 분석에 따른 결과

⑤ 개인정보처리자는 제1항, 제2항, 제3항, 또는 제4항에 따라 개인정보를 암호화하는 경우 안전한 암호알고리즘으로 암호화하여 저장하여야 한다.

⑥ 개인정보처리자는 암호화된 개인정보를 안전하게 보관하기 위하여 안전한 암호 키 생성, 이용, 보관, 배포 및 파기 등에 관한 절차를 수립·시행하여야 한다.

⑦ 개인정보처리자는 업무용 컴퓨터 또는 모바일 기기에 고유식별정보를 저장하여 관리하는 경우 상용 암호화 소프트웨어 또는 안전한 암호화 알고리즘을 사용하여 암호화한 후 저장하여야 한다.

⑧ [별표]의 유형1 및 유형2에 해당하는 개인정보처리자는 제6항을 아니할 수 있다.

제8조(접속기록의 보관 및 점검) ① 개인정보처리자는 개인정보취급자가 개인정보처리시스템에 접속한 기록을 1년 이상 보관·관리하여야 한다. 다만, 5만명 이상의 정보주체에 관하여 개인정보를 처리하거나, 고유식별정보 또는 민감정보를 처리하는 개인정보처리시스템의 경우에는 2년 이상 보관·관리하여야 한다.

② 개인정보처리자는 개인정보의 오·남용, 분실·도난·유출·위조·변조 또는 훼손 등에 대응하기 위하여 개인정보처리시스템의 접속기록 등을 월 1회 이상 점검하여야 한다. 특히 개인정보를 다운로드한 것이 발견되었을 경우에는 내부관리 계획으로 정하는 바에 따라 그 사유를 반드시 확인하여야 한다.

③ 개인정보처리자는 개인정보취급자의 접속기록이 위·변조 및 도난, 분실되지 않도록 해당 접속기록을 안전하게 보관하여야 한다.

제9조(악성프로그램 등 방지) 개인정보처리자는 악성프로그램 등을 방지·치료

할 수 있는 백신 소프트웨어 등의 보안 프로그램을 설치·운영하여야 하며, 다음 각 호의 사항을 준수하여야 한다.

1. 보안 프로그램의 자동 업데이트 기능을 사용하거나, 일 1회 이상 업데이트를 실시하여 최신의 상태로 유지
2. 악성프로그램 관련 경보가 발령된 경우 또는 사용 중인 응용 프로그램이나 운영체제 소프트웨어의 제작업체에서 보안 업데이트 공지가 있는 경우 즉시 이에 따른 업데이트를 실시
3. 발견된 악성프로그램 등에 대해 삭제 등 대응 조치

제10조(관리용 단말기의 안전조치) 개인정보처리자는 개인정보 유출 등 개인정보 침해사고 방지를 위하여 관리용 단말기에 대해 다음 각 호의 안전조치를 하여야 한다.

1. 인가 받지 않은 사람이 관리용 단말기에 접근하여 임의로 조작하지 못하도록 조치
2. 본래 목적 외로 사용되지 않도록 조치
3. 악성프로그램 감염 방지 등을 위한 보안조치 적용

제11조(물리적 안전조치) ① 개인정보처리자는 전산실, 자료보관실 등 개인정보를 보관하고 있는 물리적 보관 장소를 별도로 두고 있는 경우에는 이에 대한 출입통제 절차를 수립·운영하여야 한다.

② 개인정보처리자는 개인정보가 포함된 서류, 보조저장매체 등을 잠금장치가 있는 안전한 장소에 보관하여야 한다.

③ 개인정보처리자는 개인정보가 포함된 보조저장매체의 반출·입 통제를 위한 보안대책을 마련하여야 한다. 다만, 별도의 개인정보처리시스템을 운영하지 아니하고 업무용 컴퓨터 또는 모바일 기기를 이용하여 개인정보를 처리하는 경우에는 이를 적용하지 아니할 수 있다.

제12조(재해·재난 대비 안전조치) ① 개인정보처리자는 화재, 홍수, 단전 등의 재해·재난 발생 시 개인정보처리시스템 보호를 위한 위기대응 매뉴얼 등 대응절차를 마련하고 정기적으로 점검하여야 한다.

② 개인정보처리자는 재해·재난 발생 시 개인정보처리시스템 백업 및 복구를 위한 계획을 마련하여야 한다.

③ [별표]의 유형1 및 유형2에 해당하는 개인정보처리자는 제1항부터 제2항까지 조치를 이행하지 아니할 수 있다.

제13조(개인정보의 파기) ① 개인정보처리자는 개인정보를 파기할 경우 다음 각 호 중 어느 하나의 조치를 하여야 한다.

1. 완전파괴(소각·파쇄 등)
2. 전용 소자장비를 이용하여 삭제
3. 데이터가 복원되지 않도록 초기화 또는 덮어쓰기 수행

② 개인정보처리자가 개인정보의 일부만을 파기하는 경우, 제1항의 방법으로 파기하는 것이 어려울 때에는 다음 각 호의 조치를 하여야 한다.

1. 전자적 파일 형태인 경우 : 개인정보를 삭제한 후 복구 및 재생되지 않도록 관리 및 감독
2. 제1호 외의 기록물, 인쇄물, 서면, 그 밖의 기록매체인 경우 : 해당 부분을 마스킹, 천공 등으로 삭제

제14조(재검토 기한) 개인정보보호위원회는 「훈령·예규 등의 발령 및 관리에 관한 규정」에 따라 이 고시에 대하여 2020년 8월 11일을 기준으로 매 3년이 되는 시점(매 3년째의 8월 10일까지를 말한다)마다 그 타당성을 검토하여 개선 등의 조치를 하여야 한다.

개인정보는 한번 분실·도난·유출·위조·변조 또는 훼손되면 정보주체에게 비가역적 피해를 줄 수 있다. 따라서 개인정보는 유출 등의 피해에 대한 사후 구제나 대응보다는 사전 예방이 무엇보다 중요하다. 이에 개인정보가 분실·도난·유출·위조·변조 또는 훼손되지 않도록 적절한 안전성 확보조치를 세우고 이를 실행하는 것이 개인정보 보호의 기본적인 요건이라고 할 수 있다. 이를 위하여 이 법 및 시행령과 「개인정보의 안전성 확보조치 기준(고시, 이하 ‘안전성 확보조치 기준’ 이라 한다)」에서는 개인정보의 안전성 확보에 필요한 구체적 기준을 명시하고 있다.

한편, 안전성 확보조치 기준은 개인정보처리자가 준수하여야 할 최소한의 기준을 정하고 있으므로(제1조 참고), 개인정보처리자는 사업 규모, 개인정보 보유 수, 그 당시의 최신 보안 기술 등을 고려해서 스스로의 환경에 맞는 개인정보 보호 조치 기준을 수립·시행하는 등 선량한 관리자로서의 주의 의무를 다하여야 한다.

판례 고시에서 정하는 조치 기준을 준수한 경우 민사상 손해배상책임 인정 여부

구 「정보통신망 이용촉진 및 정보보호 등에 관한 법률 시행령(2011. 8. 29. 대통령령 제23104호로 개정되기 전의 것)」 제15조 제6항은 “방송통신위원회는 제1항부터 제5항까지의 규정에 따른 사항과 법 제28조 제1항 제6호에 따른 그 밖에 개인정보의 안전성 확보를 위하여 필요한 보호조치의 구체적인 기준을 정하여 고시하여야 한다.”라고 규정하고 있다. 이에 따라 방송통신위원회가 마련한 「개인정보의 기술적·관리적 보호조치 기준」(방송통신위원회 고시 제2011-1호, 이하 ‘고시’라고 한다)은 해킹 등 침해사고 당시의 기술 수준 등을 고려하여 정보통신서비스 제공자가 구 「정보통신망 이용촉진 및 정보보호 등에 관한 법률(2012. 2. 17. 법률 제11322호로 개정되기 전의 것)」 제28조제1항 등에 따라 준수해야 할 기술적·관리적 보호조치를 구체적으로 규정하고 있다. 그러므로 정보통신서비스 제공자가 고시에서 정하고 있는 기술적·관리적 보호조치를 다하였다면, 특별한 사정이 없는 한 정보통신서비스 제공자가 개인정보의 안전성 확보에 필요한 보호조치를 취하여야 할 법률상 또는 계약상 의무를 위반하였다고 보기는 어렵다. 다만 고시는 정보통신서비스 제공자가 반드시 준수해야 할 최소한의 기준을 정한 것으로 보는 것이 타당하다. 따라서 정보통신서비스 제공자가 고시에서 정하고 있는 기술적·관리적 보호조치를 다하였다고 하더라도,

정보통신서비스 제공자가 마땅히 준수해야 한다고 일반적으로 쉽게 예상할 수 있고 사회통념상으로도 합리적으로 기대 가능한 보호조치를 다하지 아니한 경우에는 위법행위로 평가될 수 있다. 나아가 정보통신서비스 제공자가 고시에서 정하고 있는 기술적·관리적 보호조치를 다하였다고 하더라도, 불법행위에 도움을 주지 말아야 할 주의의무를 위반하여 타인의 불법행위를 용이하게 하였고 이러한 방조행위와 불법행위에 의한 피해자의 손해 발생 사이에 상당인과관계가 인정된다면 「민법」 제760조 제3항에 따른 책임을 면할 수 없다(대법원 2018. 1. 25. 선고 2015다24904, 24911, 24928, 24935 판결).

1. 안전조치 의무의 이행

이 법 시행령에서는 개인정보의 유출 등 피해를 막기 위한 조치로서 조직·인력 등에 대한 관리적 보호 조치, 개인정보처리시스템 등에 대한 기술적 보호 조치, 개인정보가 보관된 장소나 매체에 대한 물리적 보호조치를 규정하고 있다.

특히 개인정보처리자는 그 유형 및 개인정보 보유량에 따른 안전조치 기준을 차등하여 적용하여야 하며, 어느 유형에 해당하는지에 대한 입증책임은 당해 개인정보처리자가 부담한다(안전성 확보조치 기준 제3조).

개인정보 처리자의 유형은 ① 1만명 미만의 정보주체에 관한 개인정보를 보유한 소상공인, 단체, 개인(유형1, 완화) ② 100만명 미만의 정보주체에 관한 개인정보를 보유한 중소기업, 10만명 미만의 정보주체 관한 개인정보를 보유한 대기업, 중견기업, 공공기관, 1만명 이상의 정보주체에 관한 개인정보를 보유한 소상공인, 단체, 개인(유형2, 표준) ③ 10만명 이상의 정보주체에 관한 개인정보를 보유한 대기업, 중견기업, 공공기관, 100만명 이상의 정보주체에 관한 개인정보를 보유한 중소기업, 단체(유형3, 강화)로 구분되며, 개인정보처리자 유형별로 적용되는 안전성 확보조치 기준 조항은 다음과 같다(안전성 확보조치 기준 별표).

- 유형1(완화) : 제5조(제2항부터 제5항까지), 제6조(제1항, 제3항, 제6항 및 제7항), 제7조(제1항부터 제5항까지, 제7항), 제8조, 제9조, 제10조, 제11조, 제13조
- 유형2(표준) : 제4조(제1항 제1호부터 제11호까지 및 제 15호, 제3항부터 제4항까지), 제5조, 제6조(제1항부터 제7항까지), 제7조(제1항부터 제5항까지, 제7항), 제8조, 제9조, 제10조, 제11조, 제13조
- 유형3(강화) : 제4조부터 제13조까지

가 관리적 안전조치

개인정보처리자는 개인정보에 대한 관리적 안전조치로서 내부관리계획을 수립·시행하여야 한다(영 제30조제1항제1호).

여기서 ‘내부 관리계획’이란 개인정보처리자가 개인정보가 분실·도난·유출·위조·변조 또는 훼손되지 아니하도록 안전하게 처리하기 위하여 내부 의사결정절차를 통하여 수립·시행하는 내부 기준을 의미한다.

정보주체의 개인정보를 보호하기 위한 조치를 적절히 시행하기 위해서는 개인정보취급자 전체에 통용되는 내부규정이 필요하다. 이를 기초로 세부 지침이나 안내서를 마련하여 개인정보취급자 전원이 개인정보 보호에 필요한 동일한 기준에 따라 동일한 행동을 취하도록 할 필요가 있다.

이를 위하여 공공기관, 사업자 등의 개인정보처리자는 취급하는 개인정보가 분실·도난·유출·위조·변조 또는 훼손되지 아니하도록 안전성을 확보하기 위하여 개인정보 보호 활동에 대한 조직 내부의 개인정보 관리를 위한 내부관리계획을 수립하고, 개인정보 관련 모든 임직원 및 관련자에게 알림으로써 이를 준수할 수 있도록 하여야 한다.

내부 관리계획을 수립하도록 하는 이유는 개인정보 보호 활동이 임기응변식이 아니라 체계적이고 전사적인 계획 내에서 수행될 수 있도록 하는데 목적이 있으며, 이를 위한 경영층의 방향제시와 지원이 필수적이다.

내부 관리계획에는 개인정보 보호 조직의 구성 및 운영에 관한 다음과 같은 사항이 포함되어야 한다(안전성 확보조치 기준 제4조제1항).

- 개인정보 보호책임자의 지정에 관한 사항
- 개인정보 보호책임자 및 개인정보취급자의 역할 및 책임에 관한 사항
- 개인정보취급자에 대한 교육에 관한 사항
- 접근 권한의 관리에 관한 사항
- 접근 통제에 관한 사항
- 개인정보 암호화 조치에 관한 사항
- 접속기록 보관 및 점검에 관한 사항
- 악성프로그램 등 방지에 관한 사항
- 물리적 안전조치에 관한 사항
- 개인정보 보호조직에 관한 구성 및 운영에 관한 사항
- 개인정보 유출사고 대응 계획 수립, 시행에 관한 사항
- 위험도 분석 및 대응방안 마련에 관한 사항
- 재해 및 재난 대비 개인정보처리시스템의 물리적 안전조치에 관한 사항

- 개인정보 처리 업무를 위탁하는 경우 수탁자에 대한 관리 및 감독에 관한 사항
- 그 밖에 개인정보 보호를 위하여 필요한 사항

개인정보처리자는 내부 관리계획에서 정한 사항에 중요한 변경이 있는 경우 이를 즉시 반영하여 내부관리계획을 수정하여 시행하고, 그 수정 이력을 관리하여야 한다(안전성 확보조치 기준 제4조제3항). 특히 개인정보 보호책임자는 연 1회 이상으로 내부 관리계획의 이행 실태를 점검·관리하여야 한다(안전성 확보조치 기준 제4조제4항).

한편, 유형1의 경우 내부 관리계획을 수립하지 아니할 수 있으며, 유형2의 경우 위험도 분석 및 대응방안 마련에 관한 사항, 재해 및 재난 대비 개인정보처리시스템의 물리적 안전 조치에 관한 사항, 개인정보 처리업무를 위탁하는 경우 수탁자에 대한 관리 및 감독에 관한 사항은 내부 관리계획에 포함하지 아니할 수 있다.

나 기술적 안전조치

개인정보처리자는 개인정보의 안전한 관리를 위하여 다음 각 호의 기술적 안전조치를 강구하여야 한다(영 제30조제1항제2호~제5호).

기술적 안전조치

1. 개인정보에 대한 접근 통제 및 접근 권한의 제한 조치
2. 개인정보를 안전하게 저장·전송할 수 있는 암호화 기술의 적용 또는 이에 상응하는 조치
3. 개인정보 침해사건의 발생에 대응하기 위한 접속기록의 보관 및 위조·변조 방지를 위한 조치
4. 개인정보에 대한 보안프로그램의 설치 및 갱신

1) 접근 권한의 제한·관리

개인정보를 처리할 수 있는 담당자의 수는 그 목적 달성에 필요한 최소한의 인원으로 제한할 필요가 있으며, 그 관리 권한도 이에 따라 통제될 필요가 있다. 이에 따라 이 법 시행령 및 고시에서는 접근 권한의 제한·관리를 규정하고 있다.

먼저, 개인정보처리자는 개인정보처리시스템에 대한 접근권한을 업무 수행에 필요한 최소한의 범위로 업무 담당자에 따라 차등 부여하여야 한다(안전성 확보조치 기준 제5조제1항). 그리고 만약 전보 또는 퇴직 등 인사이동이 발생하여 개인정보취급자가 변경되었을 경우에는 지체없이 개인정보처리시스템의 접근권한을 변경 또는 말소하여야 한다(안전성 확보조치 기준 제5조제2항).

한편, 개인정보처리자는 제1항 및 제2항에 의한 권한 부여, 변경 또는 말소에 대한 내역을 기록하고, 그 기록을 최소 3년간 보관하여야 한다(안전성 확보조치 기준 제5조제3항).

또한 개인정보처리자는 개인정보처리시스템에 접속할 수 있는 사용자 계정을 발급하는 경우, 개인정보취급자 별로 한 개의 사용자계정을 발급하여야 하며, 다른 개인정보취급자와 공유되지 않도록 하여야 한다(안전성 확보조치 기준 제5조제4항). 이를 규제하는 이유는 다수의 개인정보취급자가 동일한 업무를 수행한다 하더라도 하나의 아이디를 공유하지 않도록 함으로써, 개인정보 처리내역에 대한 책임 추적성(Traceability)을 확보하기 위한 것이다.

이와 관련하여, 개인정보처리자는 개인정보취급자 또는 정보주체가 안전한 비밀번호를 설정하여 이행할 수 있도록 비밀번호 작성규칙을 수립하여 적용하여야 한다(안전성 확보조치 기준 제5조제5항). 안전하지 못한 비밀번호를 사용할 경우 정당한 접속권한을 가지지 않은 자가 비밀번호를 추측하거나 접속을 시도하는 등으로 개인정보가 노출될 위험성이 있기 때문이다. 안전한 비밀번호란 제3자가 쉽게 추측할 수 없으며 비밀번호 해킹 등을 통해서도 비밀번호를 얻어낼 수 없거나 얻어내는데 많은 시간이 요구되는 것을 의미한다. 따라서 개인정보취급자나 정보주체가 생일, 전화번호 등 추측하기 쉬운 숫자나 문자 등을 비밀번호로 이용하지 않도록 비밀번호 작성규칙을 수립하고 개인정보처리시스템에 적용함으로써, 개인정보에 대한 안전한 접근통제를 달성할 수 있다.

일반적으로 비밀번호의 최소 길이는 그 비밀번호를 구성하는 문자의 종류에 따라 최소 10자리 또는 8자리 이상의 길이로 구성하여야 한다.

- 최소 8자리 이상 : 두 종류 이상의 문자를 이용하여 구성한 경우
 - ※ 문자 종류 : 알파벳 대문자와 소문자, 특수문자
- 최소 10자리 이상 : 하나의 문자 종류로 구성한 경우
 - ※ 단, 숫자로만 구성할 경우 취약할 수 있음

그리고 추측하기 어려운 비밀번호를 설정해야 하며, 비밀번호가 제3자에게 노출되었을 경우 지체없이 새로운 비밀번호로 변경해야 한다.

- 생성한 비밀번호에 12345678 등과 같은 일련번호, 전화번호 등과 같은 쉬운 문자열이 포함되지 않아야 함
- love, happy 등과 같은 잘 알려진 단어 또는 키보드 상에서 나란히 있는 문자열도 포함되지 않아야 함

또한 개인정보처리자는 권한 있는 개인정보취급자만이 개인정보처리시스템에 접근할 수 있도록 계정정보 또는 비밀번호를 일정 횟수 이상 잘못 입력한 경우 개인정보처리시스템에 대한 접근을 제한하는 등 필요한 기술적 조치를 하여야 한다(안전성 확보조치 기준 제5조제6항).

한편 별표 유형 1에 해당하는 개인정보처리자는 안전성 확보조치 기준 제5조제1항 및 제6항을 적용하지 아니할 수 있다.

2) 접근 통제

사업자, 공공기관 등 개인정보처리자는 정보통신망을 통한 불법적인 접근 및 침해사고 방지를 위해 IP 주소 등을 통해 비인가자의 접근을 차단할 수 있는 보안시스템을 설치·운영해야 한다. 이를 위해, 개인정보처리자는 정보통신망을 통한 불법적인 접근 및 침해사고 방지를 위해 다음 각 호의 기능을 포함한 조치를 하여야 한다(안전성 확보조치 기준 제6조제1항).

- ① 개인정보처리시스템에 대한 접속 권한을 IP(Internet Protocol)주소 등으로 제한하여 인가받지 않은 접근을 제한
- ② 개인정보처리시스템에 접속한 IP(Internet Protocol)주소 등을 분석하여 불법적인 개인정보 유출 시도를 탐지

또한, 개인정보취급자가 정보통신망을 통해 외부에서 개인정보처리시스템에 접속하려는 경우에는 가상사설망(VPN, Virtual Private Network) 또는 전용선 등 안전한 접속수단을 적용하거나 안전한 인증수단을 적용하여야 한다(안전성 확보조치 기준 제6조제5항). 여기에서 가상사설망이라 함은 개인정보 취급자가 개인정보처리시스템에 대해 원격으로 접속할 때 암호 프로토콜 기술 등을 통해 안전한 암호통신을 할 수 있도록 해주는 보안시스템을 의미한다.

그리고 개인정보처리자가 관리하고 있는 개인정보는 인터넷 홈페이지, P2P 서비스 등을 통해서도 공개·유출될 수 있다. 이를 방지하기 위해 개인정보처리자는 취급중인 개인정보가 인터넷 홈페이지, P2P, 공유설정, 공개된 무선망 이용 등을 통하여 열람권한이 없는 자에게 공개되거나 외부에 유출되지 않도록 개인정보처리시스템, 업무용 컴퓨터, 모바일 기기 및 관리용 단말기 등에 접근 통제 등에 관한 조치를 취하여야 한다(안전성 확보조치 기준 제6조제3항).

또한 고유식별정보를 처리하는 개인정보처리자는 인터넷 홈페이지를 통해 고유식별정보가 유출·변조·훼손되지 않도록 연 1회 이상 취약점을 점검하고 필요한 보완 조치를 하여야 한다(안전성 확보조치 기준 제6조제4항).

한편, 개인정보처리자는 권한 있는 개인정보취급자만이 개인정보처리시스템에 접근할 수 있도록 계정정보 또는 비밀번호를 일정 횟수 이상 잘못 입력한 경우 개인정보처리시스템에 대한 접근을 제한하는 등 필요한 기술적 조치를 취하여야 한다(안전성 확보조치 기준 제6조제6항).

한편, 소상공인이나 영세사업자와 같이 규모가 작은 개인정보처리자의 경우에는 별도의 개인정보처리시스템 없이 업무용 컴퓨터(PC) 또는 모바일 기기만을 이용해서 개인정보를 처리하는 경우도 있을 수 있다. 이러한 경우에는 접근통제 시스템 설치 의무화에 관한 안전성 확보조치 기준 제6조제1항은 적용하지 아니할 수 있으며, 이 경우 업무용 컴퓨터 또는 모바일 기기의 운영체제(OS : Operating System)나 보안프로그램 등에서 제공하는 접근통

제 기능을 이용할 수 있다(안전성 확보조치 기준 제6조제6항). 예를 들어 윈도우(Windows)에서 제공하는 방화벽 기능을 이용하는 방법이 이에 해당한다.

또한 별표 유형 1에 해당하는 유형의 개인정보처리자의 경우 접근 통제에 관한 안전성 확보조치 기준 제6조제2항, 제4항, 제5항은 적용하지 아니할 수 있다.

마지막으로, 모바일 기기는 성능이 높아 대량의 개인정보를 저장하거나 전송할 수 있으나, 휴대와 이동이 편리하여 기기 분실·도난시 해당 기기에 저장된 또는 해당 기기의 개인정보처리시스템 접속 등을 통한 개인정보 유출의 위험성이 높다. 이에 개인정보처리자는 업무용 모바일 기기의 분실·도난 등으로 개인정보가 유출되지 않도록 해당 모바일 기기에 비밀번호 설정 등의 보호조치를 하여야 한다(안전성 확보조치 기준 제6조제7항).

3) 개인정보의 암호화

‘암호화’는 개인정보취급자의 실수 또는 해커의 공격 등으로 인해 개인정보가 비인가자에게 유·노출되더라도 그 주요 내용을 확인할 수 없게 하는 보안기술을 의미한다. 주요 개인정보가 암호화되지 않고 개인정보처리시스템에 저장되거나 네트워크를 통해 전송될 경우, 불법적인 노출 및 위·변조 등의 위험이 있으므로 암호화 등의 안전한 보호조치가 제공되어야 한다.

먼저 암호화의 대상과 관련하여, 모든 개인정보를 암호화한다면 보호 수준은 높아질 수 있으나 사업자 및 공공기관 등 개인정보처리자의 부담이 매우 커진다. 이에 따라 안전성 확보조치 기준 고시에서는 암호화 대상 개인정보로서 고유식별정보, 비밀번호 및 바이오정보만을 정하고 있다(안전성 확보조치 기준 제7조제1항)⁹⁾. 단, 개인정보처리자가 위 개인정보를 암호화하는 경우 안전한 암호 알고리즘으로 암호화하여 저장하여야 한다(안전성 확보조치 기준 제7조제5항).

다음으로, 안전성 확보조치 기준은 암호화의 기준에 대해, 전송시와 저장시의 암호화로 구분하여 규정하고, 개인정보 저장시에는 다시 그 저장대상 개인정보가 어떤 것인지, 저장구간은 어떻게 되는지에 대해 차등적으로 규율하고 있다.

- 개인정보처리자는 암호화 대상 개인정보를 정보통신망을 통하여 송신하거나 보조저장매체 등을 통하여 전달하는 경우에는 이를 반드시 암호화하여야 한다(안전성 확보조치 기준 제7조제1항).
- 개인정보처리자는 비밀번호 및 바이오정보를 저장하는 경우에는 반드시 암호화하여 저장

9) 이에 비해, 기술적·관리적 보호조치 기준에서는 암호화 대상 개인정보로서 주민등록번호, 여권번호, 운전면허번호, 외국인등록번호, 신용카드번호, 계좌번호, 바이오정보를 규정하고 있다(기술적·관리적 보호조치 기준 제6조제2항).

하여야 한다. 단 비밀번호를 저장하는 경우에는 복호화되지 아니하도록 일방향 암호화하여 저장하여야 한다(안전성 확보조치 기준 제7조제2항).

- 개인정보처리자는 인터넷 구간 또는 인터넷 구간과 내부망의 중간 지점(DMZ : Demilitarized Zone)에 고유식별정보를 저장하는 경우에는 이를 암호화하여야 한다(안전성 확보조치 기준 제7조제3항).
- 개인정보처리자가 내부망에 고유식별정보를 저장하는 경우에는 다음 기준에 따라 암호화의 적용여부 및 적용범위를 정하여 시행할 수 있다(안전성 확보조치 기준 제7조제4항).
 - ① 법 제33조에 따른 개인정보 영향평가의 대상이 되는 공공기관의 경우에는 해당 개인정보 영향평가의 결과
 - ② 개인정보 영향평가의 대상이 되는 공공기관 외의 개인정보처리자의 경우에는 암호화 미적용시 위험도 분석에 따른 결과

또한 고유식별정보는 개인정보처리시스템이 아닌 단순한 업무용 컴퓨터 또는 모바일 기기에 저장되는 경우에도 손쉽게 유출·도용될 우려가 있다. 따라서 주민등록번호 등 고유식별정보는 업무용 컴퓨터 또는 모바일 기기에 저장하여 관리하는 경우 상용 암호화 소프트웨어 또는 안전한 암호화 알고리즘을 사용하여 암호화한 후 저장하여야 한다.

그리고 개인정보처리자는 암호화된 개인정보를 안전하게 보관하기 위하여 안전한 암호 키 생성, 이용, 보관, 배포 및 파괴 등에 관한 절차를 수립·시행하여야 한다(안전성 확보조치 기준 제7조제6항). 다만, 별표 유형1 및 유형2에 해당하는 개인정보처리자는 제6항을 적용하지 아니할 수 있다.

4) 접속기록 보관 및 위조·변조 방지조치

개인정보처리시스템에 대한 개인정보취급자 등의 접속기록은 개인정보의 입·출력 및 수정사항, 파일별·담당자별 데이터 접근내역 등을 자동으로 기록하는 로그 파일을 생성하여 불법적인 접근 또는 행동을 확인할 수 있는 중요한 자료이다. 따라서 안전성 확보조치 기준에서는 접속기록을 일정기간 의무적으로 보관하도록 규정하고 있다.

개인정보처리자는 개인정보취급자가 개인정보처리시스템에 접속한 기록을 최소 1년 이상 보관·관리하여야 한다. 다만, 5만명 이상의 정보주체에 관하여 개인정보를 처리하거나, 고유식별정보 또는 민감정보를 처리하는 개인정보처리시스템의 경우에는 2년 이상 보관·관리하여야 한다(안전성 확보조치 기준 제8조제1항). 그리고 개인정보처리자는 개인정보의 분실·도난·유출·위조·변조 또는 훼손 등에 대응하기 위하여 개인정보처리시스템의 접속기록 등을 월 1회 이상 점검하여야 하고, 특히 개인정보를 다운로드 한 것이 발견되었을 경우에는 내부 관리계획으로 정하는 바에 따라 그 사유를 반드시 확인하여야 한

다(개인정보의 안전성 확보조치 기준 제8조제2항). 또한 개인정보취급자의 접속기록이 위·변조 및 도난, 분실되지 않도록 해당 접속기록을 안전하게 보관하여야 한다(안전성 확보조치 기준 제8조제3항).

5) 보안프로그램 설치·운영

이른바 ‘악성 프로그램’이란 제작자가 악의적으로 피해를 주고자 만든 프로그램 및 실행 가능한 코드를 의미하는 것으로 악성 코드라고 불리기도 한다. 여기에는 컴퓨터 바이러스(Computer Virus), 인터넷 웜(Internet Worm), 트로이 목마, 스파이웨어 등의 형태가 있다. 개인정보처리자는 백신 소프트웨어 등의 보안 프로그램 설치·운영을 의무화함으로써 악성 프로그램으로 인한 개인정보 유출등을 예방할 필요성이 있다. 이에 개인정보처리자는 다음 기준을 준수하여야 한다(안전성 확보조치 기준 제9조).

- ① 보안 프로그램의 자동 업데이트 기능을 사용하거나, 일 1회 이상 업데이트를 실시하여 최신의 상태로 유지
- ② 악성 프로그램 관련 경보가 발령된 경우 또는 사용 중인 응용 프로그램이나 운영체제 소프트웨어의 제작업체에서 보안 업데이트 공지가 있는 경우, 즉시 이에 따른 업데이트를 실시
- ③ 발견된 악성프로그램 등에 대해 삭제 등 대응 조치

6) 관리용 단말기의 안전조치

‘관리용 단말기’란 개인정보처리시스템의 관리, 운영, 개발, 보안 등의 목적으로 개인정보처리시스템에 직접 접속하는 단말기를 말한다(안전성 확보조치 기준 제2조제20호). 관리용 단말기를 통한 개인정보 유출 사고가 자주 문제되고 있으므로, 이와 관련한 안전조치가 매우 중요하다. 이에 개인정보처리자는 개인정보 유출 등 개인정보 침해사고 방지를 위하여 관리용 단말기에 대해 다음과 같은 안전조치를 취하여야 한다(안전성 확보조치 기준 제10조).

- ① 인가 받지 않은 사람이 관리용 단말기에 접근하여 임의로 조작하지 못하도록 조치
- ② 본래 목적 외로 사용되지 않도록 조치
- ③ 악성프로그램 감염방지 등을 위한 보안조치 적용

다 물리적 안전조치

개인정보처리자는 개인정보의 안전한 관리를 위하여 다음 각 호의 물리적 안전조치를 강구하여야 한다(영 제30조제1항제6호).

물리적 안전조치

1. 개인정보의 안전한 보관을 위한 보관시설의 마련
2. 잠금장치의 설치 등

개인정보를 대량으로 보관하고 있는 전산실·자료보관실을 별도로 두고 있는 경우나, 개인정보 저장매체를 별도 관리하고 있는 경우에는 이러한 물리적 저장장소에 대한 비인가자의 접근으로 인하여 개인정보의 절도, 파괴 등 물리적 위협이 발생하지 않도록 필요한 절차를 수립하여야 한다.

이를 위해, 먼저 개인정보처리자는 전산실, 자료보관실 등 개인정보를 보관하고 있는 물리적 보관장소를 별도로 두고 있는 경우에는 이에 대한 출입통제 절차를 수립·운영하여야 한다(안전성 확보조치 기준 제11조제1항).

또한, 개인정보처리자는 개인정보가 포함된 서류, 보조저장매체 등을 잠금장치가 있는 안전한 장소에 보관하여야 한다(안전성 확보조치 기준 제11조제2항).

그리고 개인정보처리자는 개인정보가 포함된 보조저장매체의 반출·입 통제를 위한 보안 대책을 마련하여야 한다. 다만 별도의 개인정보처리시스템을 운영하지 아니하고 업무용 컴퓨터 또는 모바일 기기를 이용하여 개인정보를 처리하는 경우에는 이를 적용하지 아니할 수 있다(안전성 확보조치 기준 제11조제3항).

라 재해·재난 대비 안전조치

개인정보처리자는 화재, 홍수, 단전 등의 재해·재난 발생시 개인정보처리시스템 보호를 위한 위기대응 매뉴얼 등 대응절차를 마련하고 정기적으로 점검하여야 한다. 특히 개인정보처리자는 재해·재난 발생시 개인정보처리시스템 백업 및 복구를 위한 계획을 마련하여야 한다. 다만 별표 유형 1 및 유형 2에 해당하는 개인정보처리자는 제1항부터 제2항까지 조치를 이행하지 아니할 수 있다(안전성 확보조치 기준 제12조).

2. 시스템 구축 등의 지원

보호위원회는 개인정보처리자가 영 제30조제1항에 따른 안전성 확보조치를 하도록 시스템을 구축하는 등 필요한 지원을 할 수 있다.

보호위원회는 개인정보의 유출 여부를 원격 모니터링할 수 있는 원격 점검시스템, 사고 발생시 신속한 복구지원을 위한 기술지원시스템 등을 구축·운영할 수 있다.

3. 안전성 확보조치 세부기준의 제정·고시

해킹 등 개인정보 침해 기술은 하루가 다르게 발전하고 있기 때문에 보다 신속하게 대응할 수 있도록 제30조제1항에 따른 안전성 확보 조치에 관한 세부기준은 보호위원회가 고시로 정할 수 있도록 하였다.

4. 다른 법률과의 관계

「신용정보법」은 신용정보전산시스템의 보안에 관하여 특별히 규정하고 있다. 따라서 신용정보회사등은 신용정보전산시스템에 대하여 동법이 정하는 기술적·물리적·관리적 보안대책을 수립·시행하여야 한다.

신용정보법	<p>제19조(신용정보전산시스템의 안전보호) ① 신용정보회사등은 신용정보전산시스템(제25조제6항에 따른 신용정보공동전산망을 포함한다. 이하 같다)에 대한 제3자의 불법적인 접근, 입력된 정보의 변경·훼손 및 파괴, 그 밖의 위험에 대하여 대통령령으로 정하는 바에 따라 기술적·물리적·관리적 보안대책을 수립·시행하여야 한다.</p> <p>② 신용정보제공·이용자가 다른 신용정보제공·이용자 또는 개인신용평가회사, 개인사업자신용평가회사, 기업신용조회회사와 서로 이 법에 따라 신용정보를 제공하는 경우에는 금융위원회가 정하여 고시하는 바에 따라 신용정보 보안 관리 대책을 포함한 계약을 체결하여야 한다.</p>
-------	--

5. 벌칙규정

위반행위	벌칙
안전성 확보 조치를 취하지 아니하여 개인정보를 도난·유출·변조 또는 훼손하거나 분실한 자 (제29조 위반)	2년 이하의 징역 또는 2천만원 이하의 벌금 (제73조제1호)
안전성 확보조치 의무 위반 (제29조 위반)	3천만원 이하 과태료 (제75조제2항제6호)

6. 질의 응답

- Q** | 바이러스 방지를 위한 백신 프로그램을 설치해야 한다고 해서 프로그램을 구입하고 PC에 설치하였다. 더 이상의 보호조치는 필요 없는가?
- A** | 사업자는 백신 소프트웨어의 설치·운영 등 컴퓨터 바이러스에 의한 침해 방지조치를 취하여야 한다. 백신 소프트웨어는 최초에 설치하는 것도 중요하지만, 이후 자동 업데이트 기능 사용 또는 일 1회 이상 업데이트를 실시하여 최신의 컴퓨터 바이러스나 악성코드를 방지할 수 있도록 하는 것이 필요하다.

제30조 | 개인정보 처리방침의 수립 및 공개

법률

제30조(개인정보 처리방침의 수립 및 공개) ① 개인정보처리자는 다음 각 호의 사항이 포함된 개인정보의 처리 방침(이하 “개인정보 처리방침”이라 한다)을 정하여야 한다. 이 경우 공공기관은 제32조에 따라 등록대상이 되는 개인정보파일에 대하여 개인정보 처리방침을 정한다.

1. 개인정보의 처리 목적
 2. 개인정보의 처리 및 보유 기간
 3. 개인정보의 제3자 제공에 관한 사항(해당되는 경우에만 정한다)
 - 3의2. 개인정보의 파기절차 및 파기방법(제21조제1항 단서에 따라 개인정보를 보존하여야 하는 경우에는 그 보존근거와 보존하는 개인정보 항목을 포함한다)
 4. 개인정보처리의 위탁에 관한 사항(해당되는 경우에만 정한다)
 5. 정보주체와 법정대리인의 권리·의무 및 그 행사방법에 관한 사항
 6. 제31조에 따른 개인정보 보호책임자의 성명 또는 개인정보 보호업무 및 관련 고충사항을 처리하는 부서의 명칭과 전화번호 등 연락처
 7. 인터넷 접속정보파일 등 개인정보를 자동으로 수집하는 장치의 설치·운영 및 그 거부에 관한 사항(해당하는 경우에만 정한다)
 8. 그 밖에 개인정보의 처리에 관하여 대통령령으로 정한 사항
- ② 개인정보처리자가 개인정보 처리방침을 수립하거나 변경하는 경우에는 정보주체가 쉽게 확인할 수 있도록 대통령령으로 정하는 방법에 따라 공개하여야 한다.
- ③ 개인정보 처리방침의 내용과 개인정보처리자와 정보주체 간에 체결한 계약의 내용이 다른 경우에는 정보주체에게 유리한 것을 적용한다.
- ④ 보호위원회는 개인정보 처리방침의 작성지침을 정하여 개인정보처리자에게 그 준수를 권장할 수 있다.

시행령

제31조(개인정보 처리방침의 내용 및 공개방법 등) ① 법 제30조제1항제8호에서 “대통령령으로 정한 사항”이란 다음 각 호의 사항을 말한다.

1. 처리하는 개인정보의 항목
 2. 삭제 <2020. 8. 4.>
 3. 제30조 또는 제48조의2에 따른 개인정보의 안전성 확보 조치에 관한 사항
- ② 개인정보처리자는 법 제30조제2항에 따라 수립하거나 변경한 개인정보 처리방침을 개인정보처리자의 인터넷 홈페이지에 지속적으로 게재하여야 한다.
- ③ 제2항에 따라 인터넷 홈페이지에 게재할 수 없는 경우에는 다음 각 호의 어느 하나 이상의 방법으로 수립하거나 변경한 개인정보 처리방침을 공개하여야 한다.

1. 개인정보처리자의 사업장등의 보기 쉬운 장소에 게시하는 방법
2. 관보(개인정보처리자가 공공기관인 경우만 해당한다)나 개인정보처리자의 사업장등이 있는 시·도 이상의 지역을 주된 보급지역으로 하는 「신문등의 진흥에 관한 법률」 제2조제1호가목·다목 및 같은 조 제2호에 따른 일반일간신문, 일반주간신문 또는 인터넷신문에 실는 방법
3. 같은 제목으로 연 2회 이상 발행하여 정보주체에게 배포하는 간행물·소식지·홍보지 또는 청구서 등에 지속적으로 실는 방법
4. 재화나 용역을 제공하기 위하여 개인정보처리자와 정보주체가 작성한 계약서 등에 실어 정보주체에게 발급하는 방법

제18조(개인정보 처리방침의 작성기준 등) ① 개인정보처리자가 개인정보 처리방침을 작성하는 때에는 법 제30조제1항 각 호 및 영 제31조제1항 각 호의 사항을 명시적으로 구분하되, 알기 쉬운 용어로 구체적이고 명확하게 표현하여야 한다.

② 개인정보처리자는 처리하는 개인정보가 개인정보의 처리 목적에 필요한 최소한이라는 점을 밝혀야 한다.

제19조(개인정보 처리방침의 기재사항) 개인정보처리자가 개인정보 처리방침을 작성할 때에는 법 제30조제1항에 따라 다음 각 호의 사항을 모두 포함하여야 한다.

1. 개인정보의 처리 목적
2. 처리하는 개인정보의 항목
3. 개인정보의 처리 및 보유 기간
4. 개인정보의 제3자 제공에 관한 사항(해당하는 경우에만 정한다)
5. 개인정보의 파기에 관한 사항
6. 개인정보 처리 위탁자 담당자 연락처, 위탁자의 관리 현황 점검 결과 등 개인정보처리 위탁에 관한 사항(해당하는 경우에만 정한다)
7. 영 제30조제1항에 따른 개인정보의 안전성 확보조치에 관한 사항
8. 개인정보의 열람, 정정·삭제, 처리정지 요구권 등 정보주체의 권리·의무 및 그 행사방법에 관한 사항
9. 개인정보 처리방침의 변경에 관한 사항
10. 개인정보 보호책임자에 관한 사항
11. 개인정보의 열람청구를 접수·처리하는 부서
12. 정보주체의 권익침해에 대한 구제방법

제20조(개인정보 처리방침의 공개) ① 개인정보처리자가 법 제30조제2항에 따라 개인정보 처리방침을 수립하는 경우에는 인터넷 홈페이지를 통해 지속적으로 게재하여야 하며, 이 경우 “개인정보 처리방침”이라는 명칭을 사용하되, 글자 크기, 색상 등을 활용하여 다른 고지사항과 구분함으로써 정보주체

가 쉽게 확인할 수 있도록 하여야 한다.

② 개인정보처리자가 인터넷 홈페이지를 운영하지 않는 경우 또는 인터넷 홈페이지 관리상의 하자가 있는 경우에는 영 제31조제3항 각 호의 어느 하나 이상의 방법으로 개인정보 처리방침을 공개하여야 한다. 이 경우에도 “개인정보 처리방침”이라는 명칭을 사용하되, 글자 크기, 색상 등을 활용하여 다른 고지사항과 구분함으로써 정보주체가 쉽게 확인할 수 있도록 하여야 한다.

③ 개인정보처리자가 영 제31조제3항제3호의 방법으로 개인정보 처리방침을 공개하는 경우에는 간행물·소식지·홍보지·청구서 등이 발행될 때마다 계속하여 게재하여야 한다.

제21조(개인정보 처리방침의 변경) 개인정보처리자가 개인정보 처리방침을 변경하는 경우에는 변경 및 시행의 시기, 변경된 내용을 지속적으로 공개하여야 하며, 변경된 내용은 정보주체가 쉽게 확인할 수 있도록 변경 전·후를 비교하여 공개하여야 한다.

개인정보 처리방침은 개인정보처리자가 개인정보 처리에 관한 절차 및 기준 등을 정해 공개한 자율규제 장치의 일종이다. 이를 통해 개인정보처리자는 개인정보 처리에 관한 투명성을 높일 수 있고, 정보주체는 개인정보처리자가 자신의 개인정보를 어떻게 처리하고 있는지를 비교·확인할 수 있게 된다.

1. 개인정보 처리방침의 수립

개인정보처리자는 다음 각 호의 10개 항목이 포함된 개인정보 처리방침을 정하여야 한다.

1. 개인정보의 처리 목적
2. 개인정보의 처리 및 보유 기간
3. 개인정보의 제3자 제공에 관한 사항(해당되는 경우에만 정한다)
4. 개인정보의 파기절차 및 파기방법(제21조제1항 단서에 따라 개인정보를 보존하여야 하는 경우에는 그 보존근거와 보존하는 개인정보 항목을 포함한다)
5. 개인정보처리의 위탁에 관한 사항(해당되는 경우에만 정한다)
6. 정보주체와 법정대리인의 권리·의무 및 그 행사방법에 관한 사항
7. 제31조에 따른 개인정보 보호책임자의 성명 또는 개인정보보호업무 및 관련 고충사항을 처리하는 부서의 명칭과 전화번호 등 연락처
8. 인터넷 접속정보파일 등 개인정보를 자동으로 수집하는 장치의 설치·운영 및 그 거부에 관한 사항(해당하는 경우에만 정한다)
9. 처리하는 개인정보의 항목
10. 제30조 또는 제48조의2에 따른 개인정보의 안전성 확보 조치에 관한 사항

위에 언급한 필수적 기재사항 이외에도 개인정보 처리방침에는 개인정보를 처리함에

있어 필요한 사항을 포함할 수 있다.

다만, 공공기관의 경우에는 법 제32조에 따라 보호위원회에 등록하도록 되어 있는 개인정보파일에 한하여 개인정보 처리방침을 정하면 된다. 등록대상에서 제외된 개인정보파일 예컨대 국가안보 등과 관련된 개인정보파일에 대하여 개인정보 처리방침을 정해 공개하게 할 경우 업무수행에 심각한 지장을 초래할 수 있기 때문이다.

또한, 공공기관이 아닌 개인정보처리자가 내부직원의 개인정보만을 수집 이용하고 있는 경우에는 개인정보 처리방침을 정하여 외부에 공개할 필요는 없지만, 인터넷, 사업장 등에 게재하여 직원이 자신의 개인정보가 어떻게 처리되고 있는지 확인할 수 있도록 하여야 한다.

제32조에 따른 등록대상에서 제외되는 개인정보파일

1. 제32조제2항 관련
 - 가. 국가 안전, 외교상 비밀, 그 밖에 국가의 중대한 이익에 관한 사항을 기록한 개인정보파일
 - 나. 범죄의 수사, 공소의 제기 및 유지, 형 및 감호의 집행, 교정처분, 보호처분, 보안관찰 처분과 출입국관리에 관한 사항을 기록한 개인정보파일
 - 다. 「조세범처벌법」에 따른 범칙행위 조사 및 「관세법」에 따른 범칙행위 조사에 관한 사항을 기록한 개인정보파일
 - 라. 공공기관의 내부적 업무처리만을 위하여 사용 되는 개인정보파일
 - 마. 다른 법령에 따라 비밀로 분류된 개인정보파일
2. 제58조 관련
 - 가. 공공기관이 처리하는 개인정보 중 「통계법」에 따라 수집되는 개인정보파일
 - 나. 국가안전보장과 관련된 정보 분석을 목적으로 수집 또는 제공 요청되는 개인정보파일
 - 다. 공중위생 등 공공의 안전과 안녕을 위하여 긴급히 필요한 경우로서 일시적으로 처리되는 개인정보파일
 - 라. 영상정보처리기를 통하여 처리되는 개인영상정보파일
3. 표준 개인정보 보호지침 제50조 관련
 - 가. 자료·물품 또는 금전의 송부, 회성 행사 수행 등의 목적만을 위하여 운용하는 경우로서 저장하거나 기록하지 않고 폐기할 목적으로 수집된 개인정보파일
 - 나. 「금융실명거래 및 비밀보장에 관한 법률」에 따른 금융기관이 금융업무 취급을 위해 보유하는 개인정보파일

2. 개인정보 처리방침의 작성 기준

개인정보처리자가 개인정보 처리방침을 작성하는 때에는 정보주체가 기재사항 각각의 의미와 내용을 쉽게 알 수 있도록 하기 위하여 기재사항을 명시적으로 구분하고 알기 쉬운 용어로 구체적이고 명확하게 표현하여야 한다(표준지침 제18조제1항). 이에 따라 정보주체가 전문적인 지식이 없이도 쉽게 이해하고 개인정보의 제공 내역 등에 관하여 혼동이 없도록 하여야 한다.

제3조제1항에서 개인정보 보호 원칙의 제1원칙으로서 “개인정보처리자는 개인정보의 처리 목적을 명확하게 하여야 하고 그 목적에 필요한 범위에서 최소한의 개인정보만을 적법하고 정당하게 수집하여야 한다.” 고 규정하고 있으며, 법 제16조에서도 개인정보처리자에게 최소수집의무를 부과하고 있다. 이러한 의무를 명확히 하는 측면에서 개인정보처리자는 개인정보 처리방침에서 명시하는 개인정보 항목이 개인정보의 처리 목적에 필요한 최소한의 개인정보라는 점을 밝혀야 한다(표준지침 제18조제2항).

3. 개인정보 처리방침의 공개

개인정보처리자가 개인정보 처리방침을 수립한 경우에는 정보주체가 쉽게 확인할 수 있도록 개인정보처리자의 인터넷 홈페이지에 지속적으로 게재하는 방법으로 이를 공개하여야 한다(영 제31조제2항). 이 경우 공개된 개인정보 처리방침을 쉽게 인지할 수 있도록 법령상의 표현인 “개인정보 처리방침”이라는 표준화된 명칭을 사용하되, 글자 크기, 색상 등을 활용하여 다른 고지사항과 구분함으로써 정보주체가 쉽게 확인할 수 있도록 하여야 한다(표준지침 제20조제1항).

이 법은 온라인·오프라인을 구분하지 않고 적용되기 때문에 개인정보처리자가 인터넷 홈페이지를 운영하지 않는 경우도 존재하고, 인터넷 홈페이지를 운영하더라도 인터넷 홈페이지 관리상의 하자가 있는 경우도 발생할 수 있다. 이러한 경우에도 개인정보 처리방침의 공개의무가 면제되는 것은 아니며, 다음 중 하나 이상의 방법으로 개인정보 처리방침을 공개하여야 한다(영 제31조제3항).

- 개인정보처리자의 사업장등의 보기 쉬운 장소에 게시하는 방법
- 관보(개인정보처리자가 공공기관인 경우만 해당한다)나 개인정보처리자의 사업장등이 있는 시·도 이상의 지역을 주된 보급지역으로 하는 「신문 등의 진흥에 관한 법률」 제2조제1호 및 제2호에 따른 일반일간신문, 일반주간신문 또는 인터넷신문에 실는 방법
- 같은 제목으로 연 2회 이상 발행하여 정보주체에게 배포하는 간행물·소식지·홍보지 또는 청구서 등에 지속적으로 실는 방법(발행될 때마다 계속하여 게재하여야 함)
- 재화나 용역을 제공하기 위하여 개인정보처리자와 정보주체가 작성한 계약서 등에 실어 정보주체에게 발급하는 방법

개인정보처리자가 위의 방법으로 개인정보 처리방침을 공개하는 때에도 인터넷홈페이지에 게재하는 경우와 마찬가지로 “개인정보 처리방침”이라는 명칭을 사용하되, 글자 크기, 색상 등을 활용하여 다른 고지사항과 구분함으로써 정보주체가 쉽게 확인할 수 있도록 하여야 한다(표준지침 제20조제2항).

4. 개인정보 처리방침의 변경

개인정보 처리방침은 개인정보처리자의 개인정보 처리에 관한 중요 사항들을 담고 있기 때문에 그에 대한 변경은 정보주체의 권익에 큰 영향을 줄 수 있다. 따라서 개인정보처리자가 개인정보 처리방침의 내용을 변경하는 경우에도 개인정보 처리방침 수립시와 동일한 방법으로 변경 사실을 공개해야 하며, 개인정보처리자는 정보주체가 쉽게 확인할 수 있도록 변경된 개인정보 처리방침을 인터넷 홈페이지에 지속적으로 게재하여야 한다(영 제31조제2항). 이 경우에 변경된 내용은 정보주체가 쉽게 확인할 수 있도록 변경 전·후를 비교하여 공개하여야 한다(표준지침 제21조). 개인정보처리자는 가급적 변경의 이유와 내용을 정보주체가 쉽게 알아볼 수 있도록 비교표 등을 첨부하여야 하며 언제든지 변경된 사항을 쉽게 확인해 볼 수 있도록 조치하여야 할 것이다.

인터넷 홈페이지가 없어 홈페이지에 게재할 수 없는 때에는 사업장등의 보기 쉬운 장소에 게시하거나 계약서, 청구서, 간행물, 소식지, 홍보지 등에 지속적으로 실어 보내거나 관보·신문 등에 게재하여야 한다(영 제31조제3항).

5. 개인정보 처리방침의 법적 효력

개인정보 처리방침의 내용과 개인정보처리자와 정보주체 간에 체결한 계약의 내용이 다른 경우에는 정보주체에게 유리한 것을 적용하도록 규정하고 있다.

6. 개인정보 처리방침의 작성지침 제정·권장

보호위원회는 개인정보 처리방침의 작성지침을 정하여 개인정보처리자에게 그 준수를 권장할 수 있다. 영세 업종이나 취약분야의 경우 개인정보처리자가 개인정보 처리방침을 정하는 것이 쉽지 않기 때문이다. 이러한 취지에 따라 개인정보 처리방침의 작성지침에 대하여 표준지침에서 규정하고 있다.

7. 다른 법률과의 관계

「신용정보법」은 신용정보제공·이용자에 대하여 신용정보활용체제를 공시할 것을 요구하고 있으므로 이에 관하여는 동법에서 정하는 바에 따른다. 그러나 「개인정보 보호법」상 개인정보 처리방침과는 적용대상 및 기재 항목이 상이하므로, 이 법에 따른 개인정보 처리방침 또한 작성하여야 한다.

신용정보법	<p>제31조(신용정보활용체제의 공시) ① 개인신용평가회사, 개인사업자신용평가회사, 기업신용조회회사, 신용정보집중기관 및 대통령령으로 정하는 신용정보제공·이용자는 다음 각 호의 사항을 대통령령으로 정하는 바에 따라 공시하여야 한다.</p> <ol style="list-style-type: none"> 1. 개인신용정보 보호 및 관리에 관한 기본계획(총자산, 종업원 수 등을 고려하여 대통령령으로 정하는 자로 한정한다) 2. 관리하는 신용정보의 종류 및 이용 목적 3. 신용정보를 제공받는 자 4. 신용정보주체의 권리의 종류 및 행사 방법 5. 신용평가에 반영되는 신용정보의 종류, 반영비중 및 반영기간(개인신용평가회사, 개인사업자신용평가회사 및 기업신용등급제공업무·기술신용평가업무를 하는 기업신용조회회사로 한정한다) 6. 「개인정보 보호법」 제30조 제1항 제6호 및 제7호의 사항 7. 그 밖에 신용정보의 처리에 관한 사항으로서 대통령령으로 정하는 사항 <p>② 제1항 각 호의 공시 사항을 변경하는 경우에는 「개인정보 보호법」 제30조 제2항에 따른 방법을 준용한다.</p>
-------	--

8. 벌칙규정

위반행위	벌칙
개인정보처리방침을 정하지 않거나 공개하지 않은 자(제30조제1항 또는 제2항 위반)	1천만원 이하 과태료 (제75조제4항제7호)

제31조 | 개인정보 보호책임자의 지정

법률

- 제31조(개인정보 보호책임자의 지정)** ① 개인정보처리자는 개인정보의 처리에 관한 업무를 총괄해서 책임질 개인정보 보호책임자를 지정하여야 한다.
- ② 개인정보 보호책임자는 다음 각 호의 업무를 수행한다.
1. 개인정보 보호 계획의 수립 및 시행
 2. 개인정보 처리 실태 및 관행의 정기적인 조사 및 개선
 3. 개인정보 처리와 관련한 불만의 처리 및 피해 구제
 4. 개인정보 유출 및 오용·남용 방지를 위한 내부통제시스템의 구축
 5. 개인정보 보호 교육 계획의 수립 및 시행
 6. 개인정보파일의 보호 및 관리·감독
 7. 그 밖에 개인정보의 적절한 처리를 위하여 대통령령으로 정한 업무
- ③ 개인정보 보호책임자는 제2항 각 호의 업무를 수행함에 있어서 필요한 경우 개인정보의 처리 현황, 처리 체계 등에 대하여 수시로 조사하거나 관계 당사자로부터 보고를 받을 수 있다.
- ④ 개인정보 보호책임자는 개인정보 보호와 관련하여 이 법 및 다른 관계 법령의 위반 사실을 알게 된 경우에는 즉시 개선조치를 하여야 하며, 필요하면 소속 기관 또는 단체의 장에게 개선조치를 보고하여야 한다.
- ⑤ 개인정보처리자는 개인정보 보호책임자가 제2항 각 호의 업무를 수행함에 있어서 정당한 이유 없이 불이익을 주거나 받게 하여서는 아니 된다.
- ⑥ 개인정보 보호책임자의 지정요건, 업무, 자격요건, 그 밖에 필요한 사항은 대통령령으로 정한다.

시행령

- 제32조(개인정보 보호책임자의 업무 및 지정요건 등)** ① 법 제31조제2항제7호에서 “대통령령으로 정한 업무”란 다음 각 호와 같다.
1. 법 제30조에 따른 개인정보 처리방침의 수립·변경 및 시행
 2. 개인정보 보호 관련 자료의 관리
 3. 처리 목적이 달성되거나 보유기간이 지난 개인정보의 파기
- ② 개인정보처리자는 법 제31조제1항에 따라 개인정보 보호책임자를 지정하려는 경우에는 다음 각 호의 구분에 따라 지정한다.
1. 공공기관: 다음 각 목의 구분에 따른 기준에 해당하는 공무원 등
가. 국회, 법원, 헌법재판소, 중앙선거관리위원회의 행정사무를 처리하는 기관 및 중앙행정기관: 고위공무원단에 속하는 공무원(이하 “고위공무원”이라 한다) 또는 그에 상당하는 공무원
나. 가목 외에 정무직공무원을 장(長)으로 하는 국가기관: 3급 이상 공무원(고위공무원을 포함한다) 또는 그에 상당하는 공무원
다. 가목 및 나목 외에 고위공무원, 3급 공무원 또는 그에 상당하는 공무원 이상의 공무원을 장으로 하는 국가기관: 4급 이상 공무원 또는

그에 상당하는 공무원

라. 가목부터 다목까지의 규정에 따른 국가기관 외의 국가기관(소속 기관을 포함한다): 해당 기관의 개인정보 처리 관련 업무를 담당하는 부서의 장

마. 시·도 및 시·도 교육청: 3급 이상 공무원 또는 그에 상당하는 공무원

바. 시·군 및 자치구: 4급 공무원 또는 그에 상당하는 공무원

사. 제2조제5호에 따른 각급 학교: 해당 학교의 행정사무를 총괄하는 사람

아. 가목부터 사목까지의 규정에 따른 기관 외의 공공기관: 개인정보 처리 관련 업무를 담당하는 부서의 장. 다만, 개인정보 처리 관련 업무를 담당하는 부서의 장이 2명 이상인 경우에는 해당 공공기관의 장이 지명하는 부서의 장이 된다.

2. 공공기관 외의 개인정보처리자: 다음 각 목의 어느 하나에 해당하는 사람
가. 사업주 또는 대표자

나. 임원(임원이 없는 경우에는 개인정보 처리 관련 업무를 담당하는 부서의 장)

③ 제2항에도 불구하고 개인정보처리자가 「소상공인 보호 및 지원에 관한 법률」 제2조에 따른 소상공인에 해당하는 경우에는 별도의 지정 없이 그 사업주 또는 대표자를 개인정보 보호책임자로 지정한 것으로 본다. 다만, 개인정보처리자가 별도로 개인정보 보호책임자를 지정한 경우에는 그렇지 않다.

④ 보호위원회는 개인정보 보호책임자가 법 제31조제2항의 업무를 원활히 수행할 수 있도록 개인정보 보호책임자에 대한 교육과정을 개설·운영하는 등 지원을 할 수 있다.

표준지침

제22조(개인정보 보호책임자의 공개) ① 개인정보처리자가 개인정보 보호책임자를 지정하거나 변경하는 경우 개인정보 보호책임자의 지정 및 변경 사실, 성명과 부서의 명칭, 전화번호 등 연락처를 공개하여야 한다.

② 개인정보처리자는 개인정보 보호책임자를 공개하는 경우 개인정보 보호와 관련한 고충처리 및 상담을 실제로 처리할 수 있는 연락처를 공개하여야 한다. 이 경우 개인정보 보호책임자와 개인정보 보호 업무를 처리하는 담당자의 성명, 부서의 명칭, 전화번호 등 연락처를 함께 공개할 수 있다.

제23조(개인정보 보호책임자의 교육) 영 제32조제3항에 따라 보호위원회가 개설 운영할 수 있는 개인정보 보호책임자에 대한 교육의 내용은 다음 각 호와 같다.

1. 개인정보 보호 관련 법령 및 제도의 내용
2. 법 제31조제2항 및 영 제32조제1항 각 호의 업무수행에 필요한 사항
3. 그 밖에 개인정보처리자의 개인정보 보호를 위하여 필요한 사항

- 제24조(교육계획의 수립 및 시행)** ① 보호위원회는 매년 초 당해연도 개인정보 보호 보호책임자 교육계획을 수립하여 시행한다.
- ② 보호위원회는 제1항의 교육계획에 따라 사단법인 한국개인정보보호협의회 등의 단체에 개인정보 보호책임자 교육을 실시하게 할 수 있다.
- ③ 보호위원회는 개인정보 보호책임자가 지리적·경제적 여건에 구애받지 않고 편리하게 교육을 받을 수 있는 여건 조성을 위해 노력하여야 한다.

1. 개인정보 보호책임자의 지정

개인정보 보호책임자도 개인정보 법규 준수, 유출 및 오남용 방지 등 개인정보처리자의 개인정보보호 활동을 촉진하기 위한 자율적 규제 장치의 하나라고 할 수 있다. 개인정보처리자는 개인정보의 처리에 관한 업무를 총괄해서 책임질 개인정보 보호책임자를 지정하여야 한다(제1항). 조직 내에서 개인정보 처리에 관한 업무를 총괄하여 책임질 임원 내지 부서장급의 책임자를 지정·운영함으로써 개인정보처리자의 내부 관리체계를 더욱 공고히 할 수 있을 것이다.

2. 개인정보 보호책임자 자격요건

분야별로 개인정보 보호책임자의 자격요건은 다음 각 호와 같다(영 제32조제2항).

개인정보 보호책임자의 자격요건 (영 제32조제2항)

1. 공공기관의 경우 다음 각 목의 구분에 따른 기준에 해당하는 공무원 등
 - 가. 국회, 법원, 헌법재판소, 중앙선거관리위원회의 행정사무를 처리하는 기관 및 중앙행정기관 : 고위공무원단에 속하는 공무원(이하 “고위공무원”이라 한다) 또는 그에 상당하는 공무원
 - 나. 가목 외에 정무직공무원을 장으로 하는 국가기관 : 3급 이상 공무원(고위공무원을 포함한다) 또는 그에 상당하는 공무원
 - 다. 가목 및 나목 외에 고위공무원, 3급 공무원 또는 그에 상당하는 공무원 이상의 공무원을 장으로 하는 국가기관 : 4급 이상 공무원 또는 그에 상당하는 공무원
 - 라. 가목부터 다목까지의 규정에 따른 국가기관 외의 국가기관(그 소속 기관을 포함한다) : 해당 기관의 개인정보 처리 관련 업무를 담당하는 부서의 장
 - 마. 시·도 및 시·도 교육청 : 3급 이상 공무원 또는 그에 상당하는 공무원
 - 바. 시·군 및 자치구 : 4급 공무원 또는 그에 상당하는 공무원
 - 사. 제2조제5호에 따른 각급 학교 : 해당 학교의 행정사무를 총괄하는 사람
 - 아. 가목부터 사목까지의 규정에 따른 기관 외의 공공기관 : 개인정보 처리 관련 업무를 담당하는 부서의 장으로서 공공기관의 장이 지정하는 사람
2. 공공기관 외의 개인정보처리자의 경우는 다음 각 목의 어느 하나에 해당하는 사람
 - 가. 사업주 또는 대표자
 - 나. 임원(임원이 없는 경우에는 개인정보 처리 관련 업무를 담당하는 부서의 장)

개인정보 보호책임자는 개인정보 처리에 관한 전반적인 사항을 결정하고 이로 인한 제반 결과에 대하여 책임을 지는 자이므로 개인정보 수집·이용·제공 등 처리에 대하여 실질적인 권한을 가지고 있어야 하며 조직 내에서 어느 정도 독자적인 의사결정을 할 수 있는 지위에 있는 자이어야 한다.

특히 공공기관이 아닌 개인정보처리자의 경우 개인정보 보호책임자로 지정될 수 있는 자는 사업주 또는 대표자, 임원이거나 임원이 없는 경우에는 개인정보 처리 관련 업무를 담당하는 부서의 장이어야 한다. 여기서 임원이란 회사 경영 업무에 주요한 권한이 있고 경영에 책임을 지는 자로서 일반적으로 사장, 부사장, 상무, 전무, 이사, 감사 등으로 불리기도 한다. 임원의 범위를 정하고 있는 법률로는 「상법」, 「법인세법」 등이 있다. 예를 들어, 「상법」 상 임원에는 등기 이사 및 감사가 해당되며(제312조), 「법인세법」 상 임원은 법인의 회장·사장·부사장·이사장·대표이사·전무이사·상무이사 등 이사회 의 구성원 전원과 청산인, 합명회사·합자회사 및 유한회사의 업무집행사원 또는 이사, 감사, 기타 이에 준하는 자가 해당된다(제20조제1항제4호). 또한, 개인정보 처리 관련 업무를 담당하는 부서란 그 명칭과 관계없이 실제로 개인정보 처리와 관련된 업무를 담당하고 있는 부서이면 해당될 수 있으며, 반드시 개인정보 처리 관련 업무만을 수행하고 있을 필요는 없다.

한편, 개인정보처리자가 「소상공인 보호 및 지원에 관한 법률」 제2조에 따른 소상공인에 해당하는 경우에는 그 사업주 또는 대표자를 개인정보 보호책임자로 지정한 것으로 본다(영 제32조제3항). 소규모·영세 사업자의 경우 위의 자격요건에 따라 개인정보 보호책임자를 지정하여야 하는 것이 부담이 될 수 있는 점을 고려하여 예외를 인정한 것이다. 다만, 개인정보 보호책임자를 별도로 지정하는 것도 가능하므로(동항 단서 참고) 영 제32조제3항제2호나목에 따라 그 임원(임원이 없는 경우에는 개인정보 처리 관련 업무를 담당하는 부서의 장)을 별도로 개인정보 보호책임자로 지정할 수 있다.

참고 소상공인 요건(「소상공인 보호 및 지원에 관한 법률」 제2조 및 동법 시행령 제2조)

- 「중소기업기본법」 제2조제2항에 따른 소기업(小企業)일 것
(해당 기업이 영위하는 주된 업종의 평균매출액등이 「중소기업기본법 시행령」 [별표3] 기준을 충족할 것)
※ 식료품, 음료, 의복, 가족, 화학제품, 전자제품 등(120억 이하) / 농업, 담배, 섬유제품, 종이, 의료, 건설업 등(80억 이하) / 도매, 소매업, 정보통신업(50억 이하) / 폐기물 처리, 원료재생업, 부동산업, 과학 및 기술 서비스업, 예술, 스포츠 관련 서비스업 등(30억 이하) / 산업용 기계, 숙박, 교육, 보건, 사회복지 서비스업 등(10억 이하)
- 상시 근로자 수가 10명 미만일 것
- 업종별 상시 근로자 수 등이 광업·제조업·건설업 및 운수업의 경우 10명 미만, 그 밖의 업종의 경우 5명 미만일 것

3. 개인정보 보호책임자의 업무

개인정보 보호책임자는 개인정보의 처리에 관한 업무를 총괄해서 책임지는 자로서 다음 각

호의 업무를 수행한다. 개인정보 보호책임자의 이 같은 업무는 총괄책임자로서 지는 업무이므로, 개인정보 보호책임자는 분야별로 개인정보취급자를 두어 업무를 하게 할 수 있다.

개인정보 보호책임자의 업무 (제31조제2항, 영 제32조제1항)

1. 개인정보보호 계획의 수립 및 시행
2. 개인정보 처리 실태 및 관행의 정기적인 조사 및 개선
3. 개인정보 처리와 관련한 불만의 처리 및 피해 구제
4. 개인정보 유출 및 오용·남용 방지를 위한 내부통제시스템의 구축
5. 개인정보보호 교육 계획의 수립 및 시행
6. 개인정보파일의 보호 및 관리·감독
7. 법 제30조에 따른 개인정보 처리방침의 수립·변경 및 시행
8. 개인정보보호 관련 자료의 관리
9. 처리목적이 달성되거나 보유기간이 경과한 개인정보의 파기

4. 개인정보 보호책임자의 공개

개인정보처리자가 개인정보 보호책임자를 지정하거나 변경하는 경우 개인정보 보호책임자의 지정 및 변경 사실, 성명과 부서의 명칭, 전화번호 등 연락처를 개인정보 처리방침에 공개하여야 한다. 이 경우 개인정보처리자는 개인정보보호와 관련한 고충처리 및 상담을 실제로 처리할 수 있는 연락처를 공개하여야 하며, 개인정보 보호책임자와 개인정보보호 업무를 처리하는 담당자의 성명, 부서의 명칭, 전화번호 등 연락처를 함께 공개할 수 있다.

5. 개인정보 보호책임자의 권한과 의무

개인정보 보호책임자가 형식적으로 외부에 보여주기 위한 장치가 아닌 개인정보처리자의 내부관리체계를 강화하고 자율규제를 활성화하는 보다 실효성 있는 제도로 정착될 수 있도록 하기 위해 법은 개인정보 보호책임자에게 실질적인 권한과 의무를 부여하고 있다.

가 개인정보 보호책임자의 권한

개인정보 보호책임자는 자신의 업무를 수행하기 위하여 필요한 경우에는 개인정보의 처리 현황, 처리 체계 등에 대하여 수시로 조사하거나 관계 당사자로부터 보고를 받을 수 있다. 개인정보 보호책임자는 개인정보보호에 관하여 전사적인 책임을 지는 자이므로 소속 부서에 관계없이 조사를 하고 보고를 받을 수 있어야 한다.

나 개인정보 보호책임자의 의무

개인정보 보호책임자는 개인정보 보호와 관련하여 이 법 및 다른 관계 법령의 위반 사실을 알게 된 경우에는 즉시 개선조치를 하여야 하며, 필요하면 소속 기관 또는 단체의 장에게 개선조치를 보고하여야 한다. 여기서 이 법 및 다른 관계 법령이라 함은 「개인정보 보호법」 및 동법 시행령뿐만 아니라 「신용정보법」 및 동법 시행령·시행규칙 등 개인정보 보호와 관련되는 법령을 모두 포함하며, 소속 기관 또는 단체의 장이라 함은 그 개인정보 보호책임자가 속해 있는 해당 기관·단체의 장을 말한다.

다 개인정보 보호책임자의 신분보장

개인정보처리자는 개인정보 보호책임자가 자신의 업무를 수행함에 있어서 정당한 이유 없이 불이익을 주거나 받게 하여서는 아니 된다. 독일, 캐나다 등 다수 국가에서도 개인정보 보호책임자의 지정을 의무화하는 한편, 개인정보 보호책임자의 불이익 방지 및 신분보장 장치를 마련해 두고 있으며, 개인정보 보호책임자의 임무수행을 위하여 필요한 비용·인력 등을 지원하도록 법률로 명시하고 있다.

6. 교육과정의 개설·운영 등의 지원

보호위원회는 개인정보 보호책임자가 자신의 업무를 원활히 수행할 수 있도록 개인정보 보호책임자에 대한 교육과정을 개설·운영하는 등 필요한 지원을 할 수 있다. 개인정보 보호책임자에게 정부의 정책과 방침을 정확히 전달하고 개인정보 보호책임자가 조직 내에서 그 역할을 충실히 수행할 수 있도록 지원하기 위한 것이다.

보호위원회는 개인정보보호 관련 법령 및 제도의 내용, 개인정보 보호책임자의 업무수행에 필요한 사항, 그 밖에 개인정보처리자의 개인정보 보호를 위하여 필요한 사항 등에 관한 교육과정을 개설하여 운영할 수 있다(표준지침 제23조). 또한 보호위원회는 개인정보 보호책임자가 지리적·경제적 여건에 구애받지 않고 편리하게 교육을 받을 수 있도록 온라인 강좌를 개설하는 등 교육여건 조성을 위해 노력하여야 한다(표준지침 제24조제3항).

이에 보호위원회는 개인정보 보호 교육 지원을 위한 온라인 교육을 무료로 지원하고 있으며, 각 기관(기업)에서 자체적으로 교육을 수행할 수 있도록 개인정보 보호 교육 및 홍보 자료를 공개, 제공하고 있다. 또한, 외부강사를 초빙하여 교육을 진행할 수 있도록 개인정보 보호 전문강사단을 운영하고 있다(이와 관련하여 자세한 내용은 개인정보보호 포털 www.privacy.go.kr 참고).

7. 다른 법률과의 관계

「신용정보법」에 따른 신용정보 관리·보호인을 지정하였을 경우 별도의 개인정보 보호 책임자를 지정하지 않고 신용정보 관리·보호인이 개인정보 보호책임자를 대체할 수 있다. 다만, 신용정보관리·보호인은 「신용정보법」에 규정된 신용정보관리·보호인의 업무 외에도 이 법에 규정된 개인정보 보호책임자의 업무를 수행하여야 한다.

신용정보법	<p>제20조(신용정보 관리책임의 명확화 및 업무처리기록의 보존) ③ 신용정보회사, 본인신용정보관리회사, 채권추심회사, 신용정보집중기관 및 대통령령으로 정하는 신용정보제공·이용자는 제4항에 따른 업무를 하는 신용정보관리·보호인을 1명 이상 지정하여야 한다. 다만, 총자산, 종업원 수 등을 감안하여 대통령령으로 정하는 자는 신용정보관리·보호인을 임원(신용정보의 관리·보호 등을 총괄하는 지위에 있는 사람으로서 대통령령으로 정하는 사람을 포함한다)으로 하여야 한다.</p> <p>④ 제3항에 따른 신용정보관리·보호인은 다음 각 호의 업무를 수행한다.</p> <p>1. 개인신용정보의 경우에는 다음 각 목의 업무</p> <p>가. 「개인정보 보호법」 제31조제2항제1호부터 제5호까지의 업무</p> <p>나. 임직원 및 전속 모집인 등의 신용정보보호 관련 법령 및 규정 준수 여부 점검다. 그 밖의 신용정보의 관리 및 보호를 위하여 대통령령으로 정하는 업무</p> <p>2. 기업신용정보의 경우 다음 각 목의 업무</p> <p>가. 신용정보의 수집·보유·제공·삭제 등 관리 및 보호 계획의 수립 및 시행</p> <p>나. 신용정보의 수집·보유·제공·삭제 등 관리 및 보호 실태와 관행에 대한 정기적인 조사 및 개선</p> <p>다. 신용정보 열람 및 정정청구 등 신용정보주체의 권리행사 및 피해구제</p> <p>라. 신용정보 유출 등을 방지하기 위한 내부통제시스템의 구축 및 운영</p> <p>마. 임직원 및 전속 모집인 등에 대한 신용정보보호교육계획의 수립 및 시행</p> <p>바. 임직원 및 전속 모집인 등의 신용정보보호 관련 법령 및 규정 준수 여부 점검</p> <p>사. 그 밖에 신용정보의 관리 및 보호를 위하여 대통령령으로 정하는 업무</p> <p>⑤ 신용정보관리·보호인의 업무수행에 관하여는 「개인정보 보호법」 제31조제3항 및 제5항의 규정을 준용한다.</p> <p>⑥ 대통령령으로 정하는 신용정보회사등의 신용정보관리·보호인은 처리하는 개인신용정보의 관리 및 보호 실태를 대통령령으로 정하는 절차와 방법에 따라 정기적으로 점검하고, 그 결과를 금융위원회에 제출하여야 한다.</p> <p>⑦ 제3항에 따른 신용정보관리·보호인의 자격요건과 그 밖에 지정에 필요한 사항, 제6항에 따른 제출 방법에 대해서는 대통령령으로 정한다.</p> <p>⑧ 「금융지주회사법」 제48조의2제6항에 따라 선임된 고객정보관리인이 제6항의 자격요건에 해당하면 제3항에 따라 지정된 신용정보관리·보호인으로 본다.</p>
-------	---

8. 벌칙규정

위반행위	벌칙
개인정보 보호책임자 미지정 (제31조제1항 위반)	1천만원 이하 과태료 (제75조제4항제8호)

9. 질의 응답

Q 개인정보 보호책임자를 지정해야 한다는데, 어느 정도의 직급을 책임자로 지정하면 되는지 알고 싶다.

A 회사의 경우 개인정보 보호책임자로 지정될 수 있는 자는 사업주 또는 대표자, 임원이거나 임원이 없는 경우에는 개인정보 처리 관련 업무를 담당하는 부서의 장이어야 한다. 개인정보 보호책임자는 직급보다 조직 내에서 어느 정도의 독자적인 의사결정권이 있어야 한다는 점이 더 중요하다.

Q 개인정보 보호 업무를 담당하는 부서의 장을 개인정보 보호책임자로 지정하고 해당 임원의 전화번호·이메일을 개인정보 처리방침에 공개하였는데, 일반적인 상품·서비스 문의같이 사소한 상담까지도 모두 담당 임원의 전화로 걸려오고 있다. 어떻게 하면 좋은가?

A 반드시 개인정보 보호책임자의 직통 연락처를 기재하여야 하는 것은 아니며, 개인정보 보호와 관련한 고충처리 및 상담을 책임지고 실제로 처리할 수 있는 연락처를 공개하면 된다. 또한 실무를 맡고 있는 개인정보 취급자의 성명 및 연락처를 기재하여도 된다.

Q 별도의 직원은 없고 부인과 함께 점포를 운영하고 있는데, 우리 같은 소규모 개인사업자도 개인정보 보호책임자를 꼭 지정해야 하는가?

A 소규모 개인사업자의 경우에도 사업주나 대표자 또는 임원(임원이 없는 경우에는 개인정보 처리 관련 업무를 담당하는 부서의 장)을 개인정보 보호책임자로 지정하여야 한다. 다만 「소상공인 보호 및 지원에 관한 법률」 제2조에 따른 소상공인에 해당하는 자(「중소기업기본법」 제2조제2항에 해당하는 소기업 중, 상시 근로자 수가 광업·제조업·건설업 및 운수업은 10명 미만, 그 밖의 업종은 5명 미만인 경우)는 사업주나 대표자가 개인정보 보호책임자가 된다. 또한 개인정보 보호책임자를 별도로 지정하는 것도 가능하다.

제32조 | 개인정보파일의 등록 및 공개

법률

제32조(개인정보파일의 등록 및 공개) ① 공공기관의 장이 개인정보파일을 운용하는 경우에는 다음 각 호의 사항을 보호위원회에 등록하여야 한다. 등록된 사항이 변경된 경우에도 또한 같다.

1. 개인정보파일의 명칭
2. 개인정보파일의 운영 근거 및 목적
3. 개인정보파일에 기록되는 개인정보의 항목
4. 개인정보의 처리방법
5. 개인정보의 보유기간
6. 개인정보를 통상적 또는 반복적으로 제공하는 경우에는 그 제공받는 자
7. 그 밖에 대통령령으로 정하는 사항

② 다음 각 호의 어느 하나에 해당하는 개인정보파일에 대하여는 제1항을 적용하지 아니한다.

1. 국가 안전, 외교상 비밀, 그 밖에 국가의 중대한 이익에 관한 사항을 기록한 개인정보파일
2. 범죄의 수사, 공소의 제기 및 유지, 형 및 감호의 집행, 교정처분, 보호처분, 보안관찰처분과 출입국관리에 관한 사항을 기록한 개인정보파일
3. 「조세범처벌법」에 따른 범칙행위 조사 및 「관세법」에 따른 범칙행위 조사에 관한 사항을 기록한 개인정보파일
4. 공공기관의 내부적 업무처리만을 위하여 사용되는 개인정보파일
5. 다른 법령에 따라 비밀로 분류된 개인정보파일

③ 보호위원회는 필요하면 제1항에 따른 개인정보파일의 등록사항과 그 내용을 검토하여 해당 공공기관의 장에게 개선을 권고할 수 있다.

④ 보호위원회는 제1항에 따른 개인정보파일의 등록 현황을 누구든지 쉽게 열람할 수 있도록 공개하여야 한다.

⑤ 제1항에 따른 등록과 제4항에 따른 공개의 방법, 범위 및 절차에 관하여 필요한 사항은 대통령령으로 정한다.

⑥ 국회, 법원, 헌법재판소, 중앙선거관리위원회(그 소속 기관을 포함한다)의 개인정보파일 등록 및 공개에 관하여는 국회규칙, 대법원규칙, 헌법재판소규칙 및 중앙선거관리위원회규칙으로 정한다.

시행령

제33조(개인정보파일의 등록사항) 법 제32조제1항제7호에서 “대통령령으로 정하는 사항”이란 다음 각 호의 사항을 말한다.

1. 개인정보파일을 운용하는 공공기관의 명칭
2. 개인정보파일로 보유하고 있는 개인정보의 정보주체 수
3. 해당 공공기관에서 개인정보 처리 관련 업무를 담당하는 부서

4. 제41조에 따른 개인정보의 열람 요구를 접수·처리하는 부서
5. 개인정보파일의 개인정보 중 법 제35조제4항에 따라 열람을 제한하거나 거절할 수 있는 개인정보의 범위 및 제한 또는 거절 사유

제34조(개인정보파일의 등록 및 공개 등) ① 개인정보파일을 운용하는 공공기관의 장은 그 운용을 시작한 날부터 60일 이내에 보호위원회가 정하여 고시하는 바에 따라 보호위원회에 법 제32조제1항 및 이 영 제33조에 따른 등록사항(이하 “등록사항”이라 한다)의 등록을 신청하여야 한다. 등록 후 등록된 사항이 변경된 경우에도 또한 같다.

- ② 보호위원회는 법 제32조제4항에 따라 개인정보파일의 등록 현황을 인터넷 홈페이지에 게재해야 한다.
- ③ 보호위원회는 제1항에 따른 개인정보파일의 등록사항을 등록하거나 변경하는 업무를 전자적으로 처리할 수 있도록 시스템을 구축·운영할 수 있다.

개인정보 처리 방법에 관한 고시(보호위원회고시 제2020-7호)

제3조(개인정보보호 업무 관련 장부 및 문서 서식) ① 법 제18조제2항과 「개인정보 보호법 시행령」(이하 “영”이라 한다) 제15조에 따른 개인정보의 목적 외 이용 및 제3자 제공 대장은 별지 제1호서식과 같다.

- ② 법 제32조제1항과 영 제34조제1항에 따른 개인정보파일 등록 신청 및 변경 등록 신청은 별지 제2호서식의 개인정보파일 등록·변경등록 신청서에 따른다.

제49조(적용대상) 이 장의 적용대상은 다음과 같다.

1. 중앙행정기관(대통령 소속 기관과 국무총리 소속 기관을 포함한다) 및 그 소속 기관, 지방자치단체
2. 「국가인권위원회법」에 따른 국가인권위원회
3. 「공공기관의 운영에 관한 법률」에 따른 공공기관
4. 「지방공기업법」에 따른 지방공사 및 지방공단
5. 특별법에 의하여 설립된 특수법인
6. 「초·중등교육법」, 「고등교육법」 및 그 밖의 다른 법률에 따라 설치된 각급 학교

제50조(적용제외) 이 장은 다음 각 호의 어느 하나에 해당하는 개인정보파일에 관하여는 적용하지 아니한다.

1. 국회, 법원, 헌법재판소, 중앙선거관리위원회(그 소속기관을 포함한다)에서 관리하는 개인정보파일
2. 법 제32조제2항에 따라 적용이 제외되는 다음 각목의 개인정보파일
 - 가. 국가안전, 외교상 비밀, 그 밖에 국가의 중대한 이익에 관한 사항을 기록한 개인정보파일
 - 나. 범죄의 수사, 공소의 제기 및 유지, 형 및 감호의 집행, 교정처분, 보호처분, 보안관찰처분과 출입국 관리에 관한 사항을 기록한 개인정보파일

고시

표준지침

- 다. 「조세범처벌법」에 따른 범칙행위 조사 및 「관세법」에 따른 범칙행위 조사에 관한 사항을 기록한 개인정보파일
 - 라. 공공기관의 내부적 업무처리만을 위하여 사용되는 개인정보파일
 - 마. 다른 법령에 따라 비밀로 분류된 개인정보파일
3. 법 제58조제1항에 따라 적용이 제외되는 다음 각목의 개인정보파일
- 가. 공공기관이 처리하는 개인정보 중 「통계법」에 따라 수집되는 개인정보파일
 - 나. 국가안전보장과 관련된 정보 분석을 목적으로 수집 또는 제공 요청되는 개인정보파일
 - 다. 공중위생 등 공공의 안전과 안녕을 위하여 긴급히 필요한 경우로서 일시적으로 처리되는 개인정보파일
4. 영상정보처리기기를 통하여 처리되는 개인영상정보파일
5. 자료·물품 또는 금전의 송부, 회성 행사 수행 등의 목적만을 위하여 이용하는 경우로서 저장하거나 기록하지 않고 폐기할 목적으로 수집된 개인정보파일
6. 「금융실명거래 및 비밀보장에 관한 법률」에 따른 금융기관이 금융업무 취급을 위해 보유하는 개인정보파일

제51조(개인정보파일 등록 주체) ① 개인정보파일을 운용하는 공공기관의 개인정보 보호책임자는 그 현황을 보호위원회에 등록하여야 한다.

- ② 중앙행정기관, 광역자치단체, 특별자치시도, 기초자치단체는 보호위원회에 직접 등록하여야 한다.
- ③ 교육청 및 각급 학교 등은 교육부를 통하여 보호위원회에 등록하여야 한다.
- ④ 중앙행정기관 및 지방자치단체의 소속기관, 기타 공공기관은 상위 관리기관을 통하여 보호위원회에 등록하여야 한다.

제52조(개인정보파일 등록 및 변경 신청) ① 개인정보파일을 운용하는 공공기관의 개인정보취급자는 해당 공공기관의 개인정보 보호책임자에게 개인정보파일 등록을 신청하여야 한다.

② 개인정보파일 등록 신청 사항은 다음의 각 호와 같다. 신청은 「개인정보 보호법 고시」(이하 “고시”라 한다) 제3조제2항에 따른 별지 제2호서식의 ‘개인정보파일 등록·변경등록 신청서’를 활용할 수 있다.

- 1. 개인정보파일을 운용하는 공공기관의 명칭
- 2. 개인정보파일의 명칭
- 3. 개인정보파일의 운영 근거 및 목적
- 4. 개인정보파일에 기록되는 개인정보의 항목
- 5. 개인정보파일로 보유하고 있는 개인정보의 정보주체 수
- 6. 개인정보의 처리 방법
- 7. 개인정보의 보유 기간

8. 개인정보를 통상적 또는 반복적으로 제공하는 경우에는 그 제공받는 자
9. 해당 공공기관에서 개인정보 처리 관련 업무를 담당하는 부서
10. 개인정보의 열람 요구를 접수·처리하는 부서
11. 개인정보파일의 개인정보 중 법 제35조제4항에 따라 열람을 제한하거나 거절할 수 있는 개인정보의 범위 및 제한 또는 거절 사유
12. 법 제33조제1항에 따른 개인정보 영향평가를 받은 개인정보파일의 경우에는 그 영향평가의 결과

③ 개인정보취급자는 등록한 사항이 변경된 경우에는 고시 제3조제2항에 따른 별지 제2호서식의 ‘개인정보파일 등록·변경등록 신청서’를 활용하여 개인정보 보호책임자에게 변경을 신청하여야 한다.

제53조(개인정보파일 등록 및 변경 확인) ① 개인정보파일 등록 또는 변경 신청을 받은 개인정보 보호책임자는 등록·변경 사항을 검토하고 그 적정성을 판단한 후 보호위원회에 등록하여야 한다.

② 교육청 및 각급 학교 등의 개인정보 보호책임자는 교육부에 제1항에 따른 등록·변경 사항의 검토 및 적정성 판단을 요청한 후, 교육부의 확인을 받아 보호위원회에 등록하여야 한다.

③ 중앙행정기관 및 지방자치단체의 소속기관, 기타 공공기관은 상위 관리기관에 제1항에 따른 등록·변경 사항의 검토 및 적정성 판단을 요청한 후, 상위 관리기관의 확인을 받아 보호위원회에 등록하여야 한다.

④ 제1항부터 제3항의 등록은 60일 이내에 하여야 한다.

제54조(개인정보파일 표준목록 등록과 관리) ① 특별지방행정기관, 지방자치단체, 교육기관(학교 포함) 등 전국적으로 단일한 공통 업무를 집행하고 있는 기관은 각 중앙행정기관에서 제공하는 ‘개인정보파일 표준목록’에 따라 등록해야 한다.

② 전국 단일의 공통업무와 관련된 개인정보파일 표준목록은 해당 중앙부처에서 등록·관리해야 한다.

제55조(개인정보파일의 파기) ① 공공기관은 개인정보파일의 보유기간 경과, 처리 목적 달성 등 개인정보파일이 불필요하게 되었을 때에는 지체 없이 그 개인정보파일을 파기하여야 한다. 다만, 다른 법령에 따라 보존하여야 하는 경우에는 그러하지 아니하다.

② 공공기관은 개인정보파일의 보유기간, 처리 목적 등을 반영한 개인정보 파기계획을 수립·시행하여야 한다. 다만, 영 제30조제1항제1호에 따른 내부관리계획이 수립되어 있는 경우에는 내부 관리계획에 개인정보 파기계획을 포함하여 시행할 수 있다.

③ 개인정보취급자는 보유기간 경과, 처리 목적 달성 등 파기 사유가 발생한 개인정보파일을 선정하고, 별지 제4호 서식에 따른 개인정보파일 파기요청서

에 파기 대상 개인정보파일의 명칭, 파기방법 등을 기재하여 개인정보 보호 책임자의 승인을 받아 개인정보를 파기하여야 한다.

④ 개인정보 보호책임자는 개인정보 파기 시행 후 파기 결과를 확인하고 별지 제5호 서식에 따른 개인정보파일 파기 관리대장을 작성하여야 한다.

제56조(개인정보파일 등록 사실의 삭제) ① 개인정보취급자는 제55조에 따라 개인정보파일을 파기한 경우, 법 제32조에 따른 개인정보파일의 등록사실에 대한 삭제를 개인정보 보호책임자에게 요청해야 한다.

② 개인정보파일 등록의 삭제를 요청받은 개인정보 보호책임자는 그 사실을 확인하고, 지체 없이 등록 사실을 삭제한 후 그 사실을 보호위원회에 통보한다.

제57조(등록·파기에 대한 개선권고) ① 공공기관의 개인정보 보호책임자는 제53조제1항에 따라 검토한 개인정보파일이 과다하게 운용되고 있다고 판단되는 경우에는 개선을 권고할 수 있다.

② 교육청 및 각급 학교, 중앙행정기관 및 지방자치단체의 소속기관, 기타 공공기관의 개인정보 보호책임자는 제53조제2항 및 제53조제3항에 따라 검토한 개인정보파일이 과다하게 운용된다고 판단되거나, 등록되지 않은 파일이 있는 것으로 확인되는 경우에는 개선을 권고할 수 있다.

③ 보호위원회는 개인정보파일의 등록사항과 그 내용을 검토하고 다음 각 호의 어느 하나에 해당되는 경우에는 법 제32조제3항에 따라 해당 공공기관의 개인정보 보호책임자에게 개선을 권고할 수 있다.

1. 개인정보파일이 과다하게 운용된다고 판단되는 경우
2. 등록하지 않은 개인정보파일이 있는 경우
3. 개인정보파일 등록 사실이 삭제되었음에도 불구하고 개인정보파일을 계속 보유하고 있는 경우
4. 개인정보 영향평가를 받은 개인정보파일을 보유하고 있음에도 그 결과를 등록사항에 포함하지 않은 경우
5. 기타 법 제32조에 따른 개인정보파일의 등록 및 공개에 위반되는 사항이 있다고 판단되는 경우

④ 보호위원회는 제3항에 따라 개선을 권고한 경우에는 그 내용 및 결과에 대하여 개인정보 보호위원회의 심의·의결을 거쳐 공표할 수 있다.

⑤ 보호위원회는 공공기관의 개인정보파일 등록·파기 현황에 대한 점검을 실시할 수 있다.

제58조(개인정보파일대장 작성) 공공기관은 1개의 개인정보파일에 1개의 개인정보파일대장을 작성해야 한다.

제59조(개인정보파일 이용·제공 관리) 공공기관은 법 제18조제2항 각 호에 따라 제3자가 개인정보파일의 이용·제공을 요청한 경우에는 각각의 이용·제공 가능 여부를 확인하고 별지 제6호서식의 ‘개인정보 목적 외 이용·제공

대장'에 기록하여 관리해야 한다.

제60조(개인정보파일 보유기간의 산정) ① 보유기간은 전체 개인정보가 아닌 개별 개인정보의 수집부터 삭제까지의 생애주기로서 보유목적에 부합된 최소기간으로 산정하되, 개별 법령의 규정에 명시된 자료의 보존기간에 따라 산정해야 한다.

② 개별 법령에 구체적인 보유기간이 명시되어 있지 않은 경우에는 개인정보 보호책임자의 협의를 거쳐 기관장의 결재를 통하여 산정해야 한다. 다만, 보유기간은 별표 1의 개인정보파일 보유기간 책정 기준표에서 제시한 기준과 「공공기록물 관리에 관한 법률 시행령」에 따른 기록관리기준표를 상회할 수 없다.

③ 정책고객, 홈페이지 회원 등의 홍보 및 대국민서비스 목적의 외부고객 명부는 특별한 경우를 제외하고는 2년을 주기로 정보주체의 재동의 절차를 거쳐 동의한 경우에만 계속하여 보유할 수 있다.

제61조(개인정보파일 현황 공개 및 방법) ① 공공기관의 개인정보 보호책임자는 개인정보파일의 보유·과기현황을 주기적으로 조사하여 그 결과를 해당 공공기관의 개인정보 처리방침에 포함하여 관리해야 한다.

② 보호위원회는 개인정보파일 등록 현황을 누구든지 쉽게 열람할 수 있도록 공개하여야 한다.

③ 보호위원회는 전 공공기관의 개인정보파일 등록 및 삭제 현황을 종합하여 매년 공개해야 하며, 개인정보파일 현황 공개에 관한 업무를 전자적으로 처리하기 위하여 정보시스템을 구축·운영할 수 있다.

1. 개인정보파일 등록 의무

가 등록 의무자

공공기관의 장이 개인정보파일을 운용하는 경우에는 보호위원회에 그 사실을 등록하여야 한다. 등록된 사항에 변경이 있는 경우에도 역시 그 내용을 등록하여야 한다. 개인정보파일 등록은 공공기관만 부담하는 의무이며 민간 부문의 기업·단체 등은 개인정보파일 등록의무가 적용되지 않는다. 개인정보파일 등록 의무가 있는 공공기관은 구체적으로 다음과 같다(표준지침 제49조).

- ① 중앙행정기관(대통령 소속 기관과 국무총리 소속 기관을 포함한다) 및 그 소속 기관, 지방자치단체
- ② 「국가인권위원회법」에 따른 국가인권위원회
- ③ 「공공기관의 운영에 관한 법률」에 따른 공공기관

- ④ 「지방공기업법」에 따른 지방공사 및 지방공단
- ⑤ 특별법에 의하여 설립된 특수법인
- ⑥ 「초·중등교육법」, 「고등교육법」 및 그 밖의 다른 법률에 따라 설치된 각급 학교

개인정보파일 등록업무를 실제 수행하는 것은 해당 공공기관의 개인정보 보호책임자이다. 개인정보파일을 운용하는 공공기관의 개인정보 보호책임자는 그 현황을 보호위원회에 등록하여야 한다. 이 경우 중앙행정기관, 광역자치단체, 특별자치시도, 기초자치단체는 보호위원회에 직접 등록하고, 중앙행정기관 및 지방자치단체의 소속기관, 기타 공공기관은 상위관리기관을 통하여 보호위원회에 등록하여야 한다. 교육지원청 및 각급 학교 등은 교육부를 통하여 보호위원회에 등록하여야 한다(표준지침 제51조).

여기서 “통하여 등록한다.”는 의미는 상위기관에서 개인정보파일의 등록·변경 사항을 검토하고 그 적정성을 판단하여 의견을 제시하며, 등록은 해당 기관에서 자체적으로 수행하는 것을 의미한다.

나 등록 방법 및 절차

개인정보파일을 운용하는 공공기관의 개인정보취급자는 해당 공공기관의 개인정보 보호책임자에게 개인정보파일 등록을 신청하여야 한다. 이 때 등록 신청을 받은 개인정보 보호책임자는 등록·변경 사항을 검토하고 그 적정성을 판단한 후 보호위원회에 개인정보파일을 등록하여야 한다.

다만, 교육지원청 및 각급 학교 등의 개인정보 보호책임자는 교육부에 제1항에 따른 등록·변경 사항의 검토 및 적정성 판단을 요청한 후, 교육부의 확인을 받아 보호위원회에 등록하여야 한다. 또한 중앙행정기관 및 지방자치단체의 소속기관, 기타 공공기관은 상위 관리기관에 등록·변경 사항의 검토 및 적정성 판단을 요청한 후, 상위 관리기관의 확인을 받아 보호위원회에 등록하여야 한다.

다 등록 사항

공공기관의 장이 개인정보파일을 등록할 때에는 다음 각 호의 사항을 모두 등록하여야 한다(제32조제1항, 영 제33조). 또한 공공기관의 장이 법 제33조에 따라 해당 개인정보파일에 대하여 개인정보 영향평가를 실시한 경우에는 그 결과를 함께 첨부하여야 한다(제33조제4항).

파일 등록사항(제32조제1항, 영 제33조)

1. 개인정보파일의 명칭
2. 개인정보파일의 운영 근거 및 목적
3. 개인정보파일에 기록되는 개인정보의 항목
4. 개인정보의 처리방법
5. 개인정보의 보유기간
6. 개인정보를 통상적 또는 반복적으로 제공하는 경우에는 그 제공받는 자
7. 개인정보파일을 운영하는 공공기관의 명칭
8. 개인정보파일로 보유하고 있는 개인정보의 정보주체 수
9. 해당 공공기관에서 개인정보 처리 관련 업무를 담당하는 부서
10. 영 제41조에 따른 개인정보의 열람 요구를 접수·처리하는 부서
11. 개인정보파일의 개인정보 중 법 제35조제4항에 따라 열람을 제한하거나 거절할 수 있는 개인정보의 범위 및 제한 또는 거절 사유

라 등록 시한

개인정보파일을 운용하는 공공기관의 장은 그 운용을 시작한 날부터 60일 이내에 보호위원회에 등록하여야 한다. 등록 후 등록사항이 변경된 경우에도 또한 같다.

2. 개인정보파일 등록 제외

국가안보, 외교상 비밀 등 국가의 중대한 이익이나 범죄수사 등 공익 달성을 위한 개인정보파일은 이를 공개하지 않는 것이 보다 공익에 부합할 수 있다. 따라서 이러한 개인정보파일은 등록·공개 의무를 면제할 필요가 있다.

가 헌법기관의 개인정보파일

국회, 법원, 헌법재판소, 중앙선거관리위원회 및 그 소속 기관의 개인정보파일 등록 및 공개에 관하여는 국회규칙, 대법원규칙, 헌법재판소규칙 및 중앙선거관리위원회규칙으로 따로 정하도록 하고 있다.

이에 따라 국회, 법원, 헌법재판소, 중앙선거관리위원회 및 이들 기관의 소속기관에서 관리하는 개인정보파일(그 소속기관을 포함한다)에서 관리하는 개인정보파일에 대해서는 이 법 및 표준지침에 따른 등록·공개 의무가 적용되지 않는다.

나 법 제32조제2항에 따라 적용이 제외되는 개인정보파일

공공기관이 다음 각 호의 어느 하나에 해당하는 개인정보파일을 운영할 때에는 이를 보호 위원회에 등록하지 않아도 된다(제32조제2항).

등록면제 개인정보파일(제32조제2항)

1. 국가 안전, 외교상 비밀, 그 밖에 국가의 중대한 이익에 관한 사항을 기록한 개인정보파일
2. 범죄의 수사, 공소의 제기 및 유지, 형 및 감호의 집행, 교정처분, 보호처분, 보안관찰처 분과 출입국관리에 관한 사항을 기록한 개인정보파일
3. 「조세범처벌법」에 따른 범칙행위 조사 및 「관세법」에 따른 범칙행위 조사에 관한 사 항을 기록한 개인정보파일
4. 공공기관의 내부적 업무처리만을 위하여 사용되는 개인정보파일
5. 다른 법령에 따라 비밀로 분류된 개인정보파일

예시1 | 공공기관 내부 업무처리를 위한 개인정보파일

- 임직원 전화번호부, 비상연락망, 인사기록파일 등
- 공공요금 정산, 회의참석자 수당지급, 자문기구운영 등을 위한 개인정보파일

예시2 | 다른 법령에 따른 비밀 개인정보파일

「공공기록물 관리에 관한 법률」 제33조(비밀 기록물의 관리) ① 공공기관은 비밀 기록 물을 생산할 때에는 그 기록물의 원본에 비밀 보호기간 및 보존기간을 함께 정하여 보존기 간이 끝날 때까지 관리되도록 하여야 한다. 이 경우 보존기간은 비밀 보호기간 이상의 기간 으로 책정하여야 한다.

② 비밀 기록물의 원본은 대통령령으로 정하는 바에 따라 관할 기록물관리기관으로 이관하 여 보존하여야 한다.

「보안업무규정」 제4조(비밀의 구분) 비밀은 그 중요성과 가치의 정도에 따라 다음 각 호 와 같이 구분한다.

1. I 급비밀: 누설될 경우 대한민국과 외교관계가 단절되고 전쟁을 일으키며, 국가의 방위 계획·정보활동 및 국가방위에 반드시 필요한 과학과 기술의 개발을 위태롭게 하는 등의 우려가 있는 비밀
2. II 급비밀: 누설될 경우 국가안전보장에 막대한 지장을 끼칠 우려가 있는 비밀
3. III 급비밀: 누설될 경우 국가안전보장에 해를 끼칠 우려가 있는 비밀

다 법 제58조제1항에 따라 적용이 제외되는 개인정보파일

개인정보 보호를 지나치게 강조하게 되면, 헌법에서 보장하고 있는 다른 공익적 가치의 실현이 곤란한 경우가 있다. 이에 따라서 법 제58조제1항은 국가안전보장, 공중위생 등 다른 공익적 가치의 실현을 위해서 법률의 제3장부터 제8장까지의 적용을 제외하고 있다¹⁰⁾. 따라

10) 현행 「개인정보 보호법」 제58조제1항은 법률의 제3장부터 제7장까지의 적용을 제외하는 것으로 규정하고 있는데, 이는 입법 오류에 해당하여 향후 법률 개정을 통해 바로 잡을 예정이다.

* 524면, 526면 동일

서 아래의 경우에 해당하는 개인정보에 대해서는 개인정보파일 등록·공개 의무가 적용되지 않는다.

등록면제 개인정보파일(표준지침 제50조)

1. 공공기관이 처리하는 개인정보 중 「통계법」에 따라 수집되는 개인정보파일
2. 국가안전보장과 관련된 정보 분석을 목적으로 수집 또는 제공 요청되는 개인정보파일
3. 공중위생 등 공공의 안전과 안녕을 위하여 긴급히 필요한 경우로서 일시적으로 처리되는 개인정보파일

라 그 외에 등록 의무가 적용 제외되는 개인정보파일

공공기관에서 영상정보처리기를 통하여 촬영한 자료는 개인정보파일 등록·공개 의무에서 제외된다.

이 외에, 자료·물품 또는 금전의 송부, 1회성 행사 수행 등의 목적만을 위하여 운용하는 경우로서, 저장하거나 기록하지 않고 폐기할 목적으로 수집한 개인정보파일 역시 등록·공개 의무에서 제외된다.

예시 | 저장하거나 기록하지 않고 폐기할 목적으로 수집한 개인정보파일

- 공공기관이 개최하는 일회성 행사에 등록하는 참가자 명단

마지막으로, 「금융실명거래 및 비밀보장에 관한 법률」에 따른 금융기관 중 공공기관의 지위를 가지는 금융기관이 ‘금융업무 취급’을 위하여 보유하는 개인정보파일도 이 법에 따른 등록 의무 적용이 배제된다.

3. 개인정보파일 등록에 대한 개선권고

개인정보파일은 그 등록과정에서 등록사항에 대한 검토가 이루어지고, 흠결 또는 개선이 필요한 사항이 있는 경우에는 그 검토결과에 따라 개선조치가 이루어질 수 있어야 한다.

먼저, 각 공공기관의 개인정보 보호책임자는 해당 기관의 개인정보취급자가 개인정보파일 등록을 신청한 경우, 이를 검토하여 개선을 권고할 수 있다(표준지침 제57조제1항). 교육청 및 각급 학교, 중앙행정기관 및 지방자치단체의 소속기관, 기타 공공기관의 개인정보 보호책임자도 개인정보파일이 과다하게 운용된다고 판단되거나, 등록되지 않은 파일이 있는 것으로 확인되는 경우에는 개선을 권고할 수 있다.

그리고 보호위원회는 공공기관이 개인정보파일을 등록할 때 그 내용을 검토하여 등록사항을 흠결하였거나 그 내용이 부실하다고 판단될 때에는 해당 공공기관의 장에게 개선을 권고

할 수 있다(제32조제3항). 구체적으로 보호위원회가 개선을 권고할 수 있는 경우는 다음과 같다.

< 개인정보파일 등록시 개선 권고 사항 >

1. 개인정보파일이 과다하게 운용된다고 판단되는 경우
2. 등록하지 않은 개인정보파일이 있는 경우
3. 개인정보파일 등록 사실이 삭제되었음에도 불구하고 개인정보파일을 계속 보유하고 있는 경우
4. 개인정보 영향평가를 받은 개인정보파일을 보유하고 있음에도 그 결과를 등록사항에 포함시키지 않은 경우
5. 기타 법 제32조에 따른 개인정보파일의 등록 및 공개에 위반되는 사항이 있다고 판단되는 경우

경우에 따라서는 개인정보파일 등록에 대한 개선권고 사항을 일반 정보주체 등이 알 수 있도록 공개할 필요성이 있다. 이에 따라 보호위원회는 해당 공공기관의 장에게 개선을 권고한 경우, 그 내용 및 결과에 대하여 개인정보 보호위원회의 심의·의결을 거쳐 공표할 수 있도록 하고 있다(표준지침 제57조제4항).

4. 개인정보파일의 관리

공공기관은 개인정보파일에 대해 대장을 작성하여 관리할 필요가 있다. 이를 위해 공공기관은 1개의 개인정보파일에 1개의 개인정보파일대장을 작성하여 관리하여야 한다. 또한 공공기관은 법 제18조제2항에 따라 제3자가 개인정보파일의 이용·제공을 요청한 경우에는 각각의 이용·제공 가능 여부를 확인하고 ‘개인정보 목적외 이용·제공대장(표준지침 별지 제6호 서식)’에 기록하여 관리해야 한다.

5. 개인정보파일의 공개

등록 관리되고 있는 개인정보파일은 궁극적으로는 국민 개개인이 그 내역을 손쉽게 확인할 수 있도록 공개하는 것이 필요하다. 이를 통해 정보주체인 국민들은 자신에 관한 개인정보가 어떤 공공기관에서 어떠한 개인정보파일에 포함되어 어떻게 관리되고 있는지를 확인하고, 이를 통해 열람 및 정정 등을 요구할 수도 있다. 이에 따라 이 법은 개인정보파일의 공개를 명시하고 있다.

보호위원회는 개인정보파일의 등록 현황을 누구든지 쉽게 열람할 수 있도록 공개하여야 한다. 이를 위해 보호위원회는 개인정보파일의 등록 현황을 인터넷 홈페이지에 게재하여야 한다. 그리고 보호위원회는 개인정보파일의 등록사항을 등록하거나 변경하는 업무를 각 공공

기관의 개인정보 보호책임자 등이 손쉽게 처리할 수 있도록 하기 위하여 이를 전자적으로 처리할 수 있는 시스템을 구축·운영할 수 있다(영 제34조제3항).

현재 보호위원회는 ‘개인정보파일 등록·공개 시스템’을 ‘개인정보 보호 포털(www.privacy.go.kr)’에 구축·운영하고 있으며, 이를 통해 국민들은 각 공공기관이 등록한 개인정보파일의 등록사항을 열람할 수 있으며 각 공공기관은 개인정보파일 등록업무를 손쉽게 간편하게 수행할 수 있도록 지원하고 있다.

제32조의2 | 개인정보 보호 인증

법률

제32조의2(개인정보 보호 인증) ① 보호위원회는 개인정보처리자의 개인정보 처리 및 보호와 관련한 일련의 조치가 이 법에 부합하는지 등에 관하여 인증할 수 있다.

② 제1항에 따른 인증의 유효기간은 3년으로 한다.

③ 보호위원회는 다음 각 호의 어느 하나에 해당하는 경우에는 대통령령으로 정하는 바에 따라 제1항에 따른 인증을 취소할 수 있다. 다만, 제1호에 해당하는 경우에는 취소하여야 한다.

1. 거짓이나 그 밖의 부정한 방법으로 개인정보 보호 인증을 받은 경우
2. 제4항에 따른 사후관리를 거부 또는 방해한 경우
3. 제8항에 따른 인증기준에 미달하게 된 경우
4. 개인정보 보호 관련 법령을 위반하고 그 위반사유가 중대한 경우

④ 보호위원회는 개인정보 보호 인증의 실효성 유지를 위하여 연 1회 이상 사후관리를 실시하여야 한다.

⑤ 보호위원회는 대통령령으로 정하는 전문기관으로 하여금 제1항에 따른 인증, 제3항에 따른 인증 취소, 제4항에 따른 사후관리 및 제7항에 따른 인증 심사원 관리 업무를 수행하게 할 수 있다.

⑥ 제1항에 따른 인증을 받은 자는 대통령령으로 정하는 바에 따라 인증의 내용을 표시하거나 홍보할 수 있다.

⑦ 제1항에 따른 인증을 위하여 필요한 심사를 수행할 심사원의 자격 및 자격 취소 요건 등에 관하여는 전문성과 경력 및 그 밖에 필요한 사항을 고려하여 대통령령으로 정한다.

⑧ 그 밖에 개인정보 관리체계, 정보주체 권리보장, 안전성 확보조치가 이 법에 부합하는지 여부 등 제1항에 따른 인증의 기준·방법·절차 등 필요한 사항은 대통령령으로 정한다.

시행령

제34조의2(개인정보 보호 인증의 기준·방법·절차 등) ① 보호위원회는 제30조제1항 각 호의 사항 및 제48조의2제1항 각 호의 사항을 고려하여 개인정보 보호의 관리적·기술적·물리적 보호대책의 수립 등을 포함한 법 제32조의2 제1항에 따른 인증의 기준을 정하여 고시한다.

② 법 제32조의2제1항 따라 개인정보 보호의 인증을 받으려는 자(이하 이 조 및 제34조의3에서 “신청인”이라 한다)는 다음 각 호의 사항이 포함된 개인정보 보호 인증신청서(전자문서로 된 신청서를 포함한다)를 제34조의6에 따른 개인정보 보호 인증 전문기관(이하 “인증기관”이라 한다)에 제출하여야 한다.

1. 인증 대상 개인정보 처리시스템의 목록
2. 개인정보 보호 관리체계를 수립·운영하는 방법과 절차

3. 개인정보 보호 관리체계 및 보호대책 구현과 관련되는 문서 목록

③ 인증기관은 제2항에 따른 인증신청서를 받은 경우에는 신청인과 인증의 범위 및 일정 등에 관하여 협의하여야 한다.

④ 법 제32조의2제1항에 따른 개인정보 보호 인증심사는 제34조의8에 따른 개인정보 보호 인증심사원이 서면심사 또는 현장심사의 방법으로 실시한다.

⑤ 인증기관은 제4항에 따른 인증심사의 결과를 심의하기 위하여 정보보호에 관한 학식과 경험이 풍부한 사람을 위원으로 하는 인증위원회를 설치·운영하여야 한다.

⑥ 제1항부터 제5항까지에서 규정한 사항 외에 인증신청, 인증심사, 인증위원회의 설치·운영 및 인증서의 발급 등 개인정보 보호 인증에 필요한 세부 사항은 보호위원회가 정하여 고시한다.

제34조의3(개인정보 보호 인증의 수수료) ① 신청인은 인증기관에 개인정보 보호 인증 심사에 소요되는 수수료를 납부하여야 한다.

② 보호위원회는 개인정보 보호 인증 심사에 투입되는 인증 심사원의 수 및 인증심사에 필요한 일수 등을 고려하여 제1항에 따른 수수료 산정을 위한 구체적인 기준을 정하여 고시한다.

제34조의4(인증취소) ① 인증기관은 법 제32조의2제3항에 따라 개인정보 보호 인증을 취소하려는 경우에는 제34조의2제5항에 따른 인증위원회의 심의·의결을 거쳐야 한다.

② 보호위원회 또는 인증기관은 법 제32조의2제3항에 따라 인증을 취소한 경우에는 그 사실을 당사자에게 통보하고, 관보 또는 인증기관의 홈페이지에 공고하거나 게시해야 한다.

제34조의5(인증의 사후관리) ① 법 제32조의2제4항에 따른 사후관리 심사는 서면심사 또는 현장심사의 방법으로 실시한다.

② 인증기관은 제1항에 따른 사후관리를 실시한 결과 법 제32조의2제3항 각 호의 사유를 발견한 경우에는 제34조의2제5항에 따른 인증위원회의 심의를 거쳐 그 결과를 보호위원회에 제출해야 한다.

제34조의6(개인정보 보호 인증 전문기관) ① 법 제32조의2제5항에서 “대통령령으로 정하는 전문기관”이란 다음 각 호의 기관을 말한다.

1. 한국인터넷진흥원
2. 다음 각 목의 요건을 모두 충족하는 법인, 단체 또는 기관 중에서 보호위원회가 지정·고시하는 법인, 단체 또는 기관
 - 가. 제34조의8에 따른 개인정보 보호 인증심사원 5명 이상을 보유할 것
 - 나. 보호위원회가 실시하는 업무수행 요건·능력 심사에서 적합하다고 인정 받을 것

② 제1항제2호에 해당하는 법인, 단체 또는 기관의 지정과 그 지정의 취소에

필요한 세부기준 등은 보호위원회가 정하여 고시한다.

제34조의7(인증의 표시 및 홍보) 법 제32조의2제6항에 따라 인증을 받은 자가 인증 받은 내용을 표시하거나 홍보하려는 경우에는 보호위원회가 정하여 고시하는 개인정보 보호 인증표시를 사용할 수 있다. 이 경우 인증의 범위와 유효기간을 함께 표시해야 한다.

제34조의8(개인정보 보호 인증심사원의 자격 및 자격 취소 요건) ① 인증기관은 법 제32조의2제7항에 따라 개인정보 보호에 관한 전문지식을 갖춘 사람으로서 인증심사에 필요한 전문 교육과정을 이수하고 시험에 합격한 사람에게 개인정보 보호 인증심사원(이하 “인증심사원”이라 한다)의 자격을 부여한다. ② 인증기관은 법 제32조의2제7항에 따라 인증심사원이 다음 각 호의 어느 하나에 해당하는 경우 그 자격을 취소할 수 있다. 다만, 제1호에 해당하는 경우에는 자격을 취소하여야 한다.

1. 거짓이나 부정한 방법으로 인증심사원 자격을 취득한 경우
2. 개인정보 보호 인증 심사와 관련하여 금전, 금품, 이익 등을 부당하게 수수한 경우
3. 개인정보 보호 인증 심사 과정에서 취득한 정보를 누설하거나 정당한 사유 없이 업무상 목적 외의 용도로 사용한 경우

③ 제1항 및 제2항에 따른 전문 교육과정의 이수, 인증심사원 자격의 부여 및 취소 등에 관한 세부 사항은 보호위원회가 정하여 고시한다.

정보보호 및 개인정보보호 관리체계 인증 등에 관한 고시(보호위원회 고시 제 2020-8호)

제1조(목적) 이 고시는 「정보통신망 이용촉진 및 정보보호 등에 관한 법률」(이하 “정보통신망법”이라 한다) 제47조제3항·제4항, 같은 법 시행령 제47조부터 제53조의2까지의 규정 및 같은 법 시행규칙 제3조에 따른 정보보호 관리체계 인증과, 「개인정보 보호법」 제32조의2, 같은 법 시행령 제34조의2부터 제34조의8까지의 규정에 따른 개인정보보호 인증의 통합 운영에 필요한 사항을 정하는 것을 목적으로 한다.

제2조(용어의 정의) 이 고시에서 사용하는 용어의 정의는 다음 각 호와 같다.

1. “정보보호 및 개인정보보호 관리체계 인증”이란 인증 신청인의 정보보호 및 개인정보보호를 위한 일련의 조치와 활동이 인증기준에 적합함을 한국인터넷진흥원(이하 “인터넷진흥원”이라 한다) 또는 인증기관이 증명하는 것을 말한다.
2. “정보보호 관리체계 인증”이란 인증 신청인의 정보보호 관련 일련의 조치와 활동이 인증기준에 적합함을 인터넷진흥원 또는 인증기관이 증명하는 것을 말한다.
3. “인증기관”이란 인증에 관한 업무를 수행할 수 있도록 정보통신망법 제

고시

47조제6항, 「개인정보 보호법 시행령」 제34조의6제1항제2호 및 제2항에 따라 과학기술정보통신부장관과 개인정보 보호위원회(이하 “보호위원회” 라 한다)가 지정하는 기관을 말한다.

4. “심사기관” 이란 인증심사 업무를 수행할 수 있도록 정보통신망법 제47조제7항, 「개인정보 보호법 시행령」 제34조의6제1항제2호 및 제2항에 따라 과학기술정보통신부장관과 보호위원회가 지정하는 기관을 말한다.
5. “업무수행 요건·능력 심사” 란 인증기관 또는 심사기관으로 지정받고자 신청한 법인 또는 단체의 업무수행 요건·능력을 심사하는 것을 말한다.
6. “인증심사” 란 신청기관이 수립하여 운영하는 관리체계가 인증기준에 적합한지의 여부를 인터넷진흥원·인증기관 또는 심사기관(이하 “심사수행기관” 이라 한다)이 서면심사 및 현장심사의 방법으로 확인하는 것을 말한다.
7. “인증위원회” 란 인터넷진흥원 또는 인증기관의 장이 인증심사 결과 등을 심의·의결하기 위해 설치·운영하는 기구로서 위원장과 위원으로 구성된다.
8. “인증심사원” 이란 인터넷진흥원으로부터 인증심사를 수행할 수 있는 자격을 부여받고 인증심사를 수행하는 자를 말한다.
9. “최초심사” 란 처음으로 인증을 신청하거나 인증범위에 중요한 변경이 있어서 다시 인증을 신청한 때 실시하는 인증심사를 말한다.
10. “사후심사” 란 인증(인증이 갱신된 경우를 포함한다)을 받고난 후 매년 사후관리를 위하여 실시하는 인증심사를 말한다.
11. “갱신심사” 란 유효기간 만료로 유효기간 갱신을 위해 실시하는 인증심사를 말한다.

제3조(적용범위) 이 고시는 정보보호 및 개인정보보호 관리체계 인증, 정보보호 관리체계 인증에 공통으로 적용하되, 각 인증에 따로 적용되는 내용이 있는 경우 별도 조항으로 정한다.

제4조(협의회의 구성) ① 과학기술정보통신부장관과 보호위원회는 정보보호 및 개인정보보호 관리체계 인증 운영에 관한 정책 사항을 협의하기 위하여 정보보호 및 개인정보보호 관리체계 인증 협의회(이하 “협의회” 라 한다)를 운영한다.

② 협의회 위원은 과학기술정보통신부, 보호위원회 소속의 인증업무를 담당하는 부서의 장으로 한다.

③ 협의회 운영을 위하여 인터넷진흥원의 인증업무를 담당하는 부서의 장을 간사로 두며, 간사는 회의에 참석하여 발언할 수 있다.

제5조(협의회의 운영) ① 협의회는 정보보호 및 개인정보보호 관리체계 인증제도와 관련하여 다음 각 호의 사항을 협의한다.

1. 인증제도 연구 및 개선에 관한 사항
2. 인증제도 운영을 위한 제반사항 검토 및 품질관리에 관한 사항
3. 인증기관 및 심사기관의 지정·재지정 및 업무정지·지정 취소에 관한 사항
4. 인증기관 및 심사기관의 관리·감독에 관한 사항
5. 인증제도 운영에 따른 민원 처리 및 법적 분쟁에 관한 사항
6. 그 밖에 협의가 필요한 사항

② 협의회는 과학기술정보통신부장관 또는 보호위원회의 요구가 있거나 협의안건이 발생한 경우 개최할 수 있다.

③ 인터넷진흥원은 협의회 개최 및 제1항 각 호에 따른 협의회 운영 업무를 지원할 수 있다.

④ 협의회는 필요하다고 인정하는 때에는 관계기관의 공무원 및 임·직원, 그 밖의 전문가를 협의회에 참석하게 하여 그 의견을 들을 수 있다.

⑤ 협의회는 협의회의 운영을 위한 별도의 규정을 정할 수 있다.

제6조(지정공고) ① 과학기술정보통신부장관과 보호위원회는 인증기관 또는 심사기관을 지정할 필요가 있는 때에는 협의회에서 지정대상 기관의 수, 업무의 범위, 신청방법 등을 미리 협의하고, 관보 또는 인터넷 홈페이지에 20일 이상 공고하여야 한다.

② 제1항에 따라 인증기관 또는 심사기관으로 지정받으려는 자는 다음 각 호의 서류를 과학기술정보통신부장관과 보호위원회에 제출하여야 한다.

1. 별지 제1호서식의 인증기관·심사기관 지정 신청서
2. 별지 제2호서식의 인증심사 업무를 수행하는 직원 보유현황과 이를 증명할 수 있는 서류
3. 별표 1의 업무수행 요건·능력 심사 제출서류

③ 과학기술정보통신부장관과 보호위원회는 인증기관 또는 심사기관의 지정, 재지정, 사후관리 등에 따른 업무를 인터넷진흥원에 위탁할 수 있다.

제7조(지정기준 및 지정절차) ① 인증기관 또는 심사기관의 업무수행 요건·능력 심사에 관한 세부기준은 별표 2와 같다.

② 과학기술정보통신부장관과 보호위원회는 제6조제2항에 따라 인증기관 또는 심사기관의 지정 신청을 받은 때에는 제1항에 따른 업무수행 요건·능력을 심사한다.

③ 과학기술정보통신부장관과 보호위원회는 제2항에 따른 심사 결과를 바탕으로 협의하여 인증기관 또는 심사기관으로의 지정여부를 최종 결정한다.

④ 과학기술정보통신부장관과 보호위원회는 인증기관으로 지정된 신청기관에 별지 제3호서식 정보보호 및 개인정보보호 관리체계 인증기관 지정서를, 심사기관으로 지정된 신청기관에 별지 제4호서식 정보보호 및 개인정보보호 관리체계 심사기관 지정서를 발급한다.

제8조(인증기관 및 심사기관의 사후관리) ① 인증기관과 심사기관은 매년 1월 31일까지 다음 각 호의 서류를 작성하여 과학기술정보통신부장관과 보호위원회에 제출하여야 한다.

1. 별지 제5호서식의 인증실적 보고서(해당 시)
2. 별지 제6호서식의 인증심사실적 보고서(해당 시)

② 과학기술정보통신부장관과 보호위원회는 필요한 경우 인증기관 또는 심사기관이 지정기준에 적합한지 여부의 확인을 위해 자료요청 또는 현장실사를 할 수 있다.

제9조(인증기관 및 심사기관의 재지정) ① 인증기관 및 심사기관 지정의 유효기간은 3년이며 유효기간이 끝나기 전 6개월부터 끝나는 날까지 재지정을 신청할 수 있으며 제6조제2항 각 호의 서류를 과학기술정보통신부장관과 보호위원회에 제출하여야 한다. 이 경우 재지정의 신청에 대한 처리결과를 통지받을 때까지는 그 지정이 계속 유효한 것으로 본다.

② 과학기술정보통신부장관과 보호위원회는 제1항에 따른 재지정 신청을 받은 때에는 별표 2 업무수행 요건·능력 심사에 관한 세부기준에 따른 적합 여부를 심사하여 신청을 받은 날부터 3개월 이내에 그 결과를 신청기관에 통지하고, 인증기관 또는 심사기관으로 지정되는 신청기관에 제7조제4항의 지정서를 발급하여야 한다.

③ 인증기관 또는 심사기관이 재지정을 신청하지 않고 유효기간이 경과한 때에는 인증기관 또는 심사기관의 효력은 상실된다.

제10조(공정성 및 독립성 확보) 인증기관 및 심사기관은 인증심사의 공정성 및 독립성 확보를 위해 다음 각 호의 행위가 발생되지 않도록 노력하여야 한다.

1. 정보보호 및 개인정보보호 관리체계 구축과 관련된 컨설팅 업무를 수행하는 행위
2. 정당한 사유 없이 인증절차, 인증기준 등의 일부를 생략하는 행위
3. 조직의 이익 등을 위해 인증심사 결과에 영향을 주는 행위
4. 그 밖에 인증심사의 공정성 및 독립성을 훼손할 수 있는 행위

제11조(인증기관 및 심사기관의 지정취소 등) ① 인증기관 및 심사기관이 다음 각 호의 어느 하나에 해당하면 그 지정을 취소하거나 1년 이내의 기간을 정하여 해당 업무의 전부 또는 일부의 정지를 명할 수 있다. 다만, 제1호나 제2호에 해당하는 경우에는 그 지정을 취소하여야 한다.

1. 거짓이나 그 밖의 부정한 방법으로 인증기관 또는 심사기관의 지정을 받은 경우
2. 업무정지 기간 중에 인증 또는 인증심사를 한 경우
3. 정당한 사유 없이 인증 또는 인증심사를 하지 아니한 경우
4. 정보통신망법 제47조제11항을 위반하여 인증 또는 인증심사를 한 경우

5. 정보통신망법 제47조제12항에 따른 지정기준에 적합하지 아니하게 된 경우
 ② 지정취소 및 업무정지에 대해서는 「정보통신망 이용촉진 및 정보보호 등에 관한 법률 시행령(이하 “정보통신망법 시행령”이라 한다)」 제54조에 따른 지정취소 및 업무정지에 관한 행정처분의 기준을 따른다.

제12조(인증심사원의 자격 요건 등) 인증심사원은 심사원보, 심사원, 선임심사원으로 구분하며 등급별 자격 요건은 별표 3과 같다.

제13조(인증심사원 자격 신청) ① 인증심사원 자격을 신청하고자 하는 자는 별표 4의 인증심사원 자격 신청 요건을 갖추고 인터넷진흥원이 공고하는 신청기간 내에 별지 제7호 서식의 인증심사원 자격 신청서와 관련 서류를 제출하여야 한다.

② 인터넷진흥원은 제1항에 의해 제출한 신청서류가 자격 신청 요건에 적합한지를 검토하여야 한다.

③ 제2항에 따른 서류검토 결과 적합한 자는 인터넷진흥원이 시행하는 인증심사원 양성과정을 수료하여야 한다.

제14조(인증심사원 자격 발급 및 관리) ① 인터넷진흥원은 인증심사원 양성과정을 수료한 자에게 별지 제8호서식의 정보보호 및 개인정보보호 관리체계 인증심사원 자격 증명서를 발급하여야 한다.

② 인터넷진흥원은 인증심사원의 자격 증명서 발급, 심사원등급, 인증심사업무경력 등을 관리하여야 한다.

제15조(인증심사원 자격 유지 및 갱신) ① 인증심사원의 자격 유효기간은 자격을 부여 받은 날부터 3년으로 한다.

② 인증심사원은 자격유지를 위해 자격 유효기간 만료 전까지 인터넷진흥원이 인정하는 보수교육을 수료하여야 한다.

③ 인터넷진흥원은 자격 유효기간 동안 1회 이상의 인증심사를 참여한 인증심사원에 대하여 제2항의 보수교육 시간 중 일부를 이수한 것으로 인정할 수 있다.

④ 인터넷진흥원은 인증정보를 제공하는 홈페이지에 제2항의 보수교육 운영에 관한 세부내용을 공지하여야 한다.

⑤ 인터넷진흥원은 제2항의 요건을 충족한 인증심사원에 한하여 별지 제8호 서식의 정보보호 및 개인정보보호 관리체계 인증심사원 자격 증명서를 갱신하여 발급하고 자격 유효기간을 3년간 연장한다.

제16조(인증심사원 자격 취소) ① 인터넷진흥원은 다음 각 호의 어느 하나에 해당하는 사유를 발견한 경우 인증심사원의 자격을 취소할 수 있다.

1. 거짓이나 부정한 방법으로 인증심사원 자격을 부여 받은 경우
2. 제15조제2항에 따른 자격 유지 기준을 충족하지 못한 경우
3. 인증심사원으로서 객관적이고 공정한 인증심사를 수행하지 않은 경우

4. 인증심사 과정에서 취득한 정보 또는 서류를 관련 법령의 근거나 인증신청인의 동의 없이 누설 또는 유출하거나 업무목적 외에 이를 사용한 경우
5. 인증신청인으로부터 금전, 금품, 향응, 이익 등을 부당하게 수수하거나 요구한 경우

② 인터넷진흥원의 장은 제1항에 따른 자격 취소의 적합여부를 심의·의결하기 위하여 자격심의위원회를 개최하여야 하며, 자격심의위원회는 제29조의 인증위원회 위원 3인 이상을 포함하여 구성한다.

③ 제1항에 따른 자격 취소에 대하여 인증심사원은 30일 이내에 이의신청을 할 수 있다. 이 경우 인터넷진흥원은 해당 인증심사원의 자격을 제2항의 절차에 따라 재심의하여 처리결과를 통지하여야 한다.

제17조(신청인의 사전 준비사항) ① 정보보호 및 개인정보보호 관리체계 인증을 취득하고자 하는 자(이하 “신청인”이라 한다)는 인증을 신청하기 전에 인증기준에 따른 정보보호 및 개인정보보호 관리체계 또는 정보보호 관리체계를 구축하여 최소 2개월 이상 운영하여야 한다.

② 신청인은 인증심사를 위하여 다음 각 호의 사항을 인증심사 실시 전에 준비하여야 한다.

1. 인증심사를 위한 문서 및 증적자료
2. 인증심사 수행에 필요한 장소·시설·장비·기자재 등의 확보
3. 그 밖에 인증심사를 원활하게 수행하기 위하여 심사수행기관이 요구하는 사항

제18조(인증 신청 등) ① 신청인은 다음 각 호의 인증을 선택하여 신청할 수 있다.

1. 정보보호 및 개인정보보호 관리체계 인증
2. 정보보호 관리체계 인증

② 신청인은 제1항의 인증 선택에 따른 별지 제9호서식의 정보보호 및 개인정보보호 관리체계 인증 신청서를 심사수행기관에 제출하여야 한다.

③ 신청인은 인증범위 및 일정 등을 심사수행기관과 사전 협의하여 신청하여야 한다.

④ 심사수행기관은 제17조에 따른 신청인의 인증심사 사전준비사항을 확인할 수 있으며, 신청인의 준비가 미흡한 경우에는 신청인에 이를 보완할 것을 요구할 수 있다.

⑤ 심사수행기관은 인증범위의 변경이 필요한 경우에 이를 신청인과 협의하여 변경할 수 있다.

제19조(정보보호 관리체계 인증 의무대상자) ① 정보보호 관리체계 인증 의무대상자(이하 “의무대상자”라 한다)란 정보통신망법 제47조제2항, 같은 법 시행령 제49조에 해당하는 자를 말한다.

② 제1항에 해당하는 자 중 집적정보통신시설 사업자가 마련한 시설의 일부

를 임대하여 집적정보통신시설 사업을 하는 자에 대하여는 정보통신망법 시행령 제49조제2항의 기준을 준용한다.

③ 의무대상자는 제18조제1항제2호의 정보보호 관리체계 인증을 받아야 한다. 이때 의무대상자가 같은 항 제1호의 인증을 받은 경우에도 인증의무를 이행한 것으로 본다.

④ 의무대상자에 해당하는 자는 다음 해 8월 31일까지 인증을 받아야 한다.

제20조(인증심사의 일부 생략 신청 등) ① 제18조제1항제2호의 정보보호 관리체계 인증을 신청한 자가 다음 각 호의 어느 하나에 해당하는 인증을 받거나 정보보호 조치를 취한 경우 별표 5의 인증심사 일부 생략의 범위 내에서 인증심사의 일부를 생략할 수 있다.

1. 국제인증협력기구에 가입된 인정기관이 인정한 인증기관으로부터 받은 ISO/IEC 27001 인증

2. 「정보통신기반 보호법」 제9조에 따른 주요정보통신기반시설의 취약점 분석·평가

② 제1항에 따라 정보보호 관리체계 인증심사의 일부를 생략하려는 경우에는 다음 각 호의 요건을 모두 충족하여야 한다.

1. 해당 국제표준 정보보호 인증 또는 정보보호 조치의 범위가 정보보호 관리체계 인증의 범위와 일치할 것

2. 정보보호 관리체계 인증 신청 및 심사 시에 해당 국제표준 정보보호 인증이나 정보보호 조치가 유효하게 유지되고 있을 것

③ 제1항에 따른 인증심사 일부 생략을 신청하고자하는 자는 별지 제10호서식의 인증심사 일부 생략 신청서를 심사수행기관에 제출하여야 한다.

④ 심사수행기관은 별표 5의 인증심사 일부 생략의 범위를 생략하여 심사하고 인터넷진흥원 또는 인증기관이 인증을 부여할 때에는 그 사실을 인증서에 표기하여야 한다.

제21조(수수료의 산정) ① 인증 수수료는 별표 6의 인증 수수료 산정 및 심사원 보수 기준을 적용하여 산정한다.

② 심사수행기관은 제1항에 따라 산정된 인증 수수료를 공지하여야 한다.

③ 심사수행기관은 신청인이 다음 각 호에 해당하는 경우 수수료를 감면 또는 조정할 수 있다.

1. 「중소기업기본법」 제2조에 따른 중소기업에 해당되는 경우

2. 제20조에 따른 인증심사 일부 생략 신청을 하는 경우

3. 그 밖에 신청인과 협의하여 수수료 조정이 필요하다고 판단되는 경우

제22조(수수료의 납부) 신청인은 최초심사, 사후심사 및 갱신심사 신청 시 인증 수수료를 청구 받은 날부터 인증심사 시작일 이전까지 심사수행기관에 납부하여야 하며, 수수료를 납부하지 않은 경우 심사수행기관은 인증심사를 실시

하지 아니할 수 있다.

제23조(인증심사 기준) ① 인증기준은 별표 7과 같다. 다만, 제18조제1항제2호의 정보보호 관리체계 인증을 받는 경우 별표 7의 인증기준 중에서 “가. 관리체계 수립 및 운영”, “나. 보호대책 요구사항”의 기준을 적용한다.

② 심사수행기관은 신청인과 협의를 통해 별표 7의 인증기준 내에서 인증범위, 업무특성 등을 고려하여 인증심사 항목을 조정할 수 있다.

제24조(인증심사팀 구성) ① 심사수행기관은 인증심사 일정이 확정된 때에는 인터넷진흥원에 심사원 모집을 요청하여 인증심사팀을 구성하여야 한다.

② 인증심사팀 구성 시 신청인의 인증범위, 사업유형, 기술의 다양성 등을 고려하여 심사팀원을 구성하고 심사팀장은 심사수행기관 소속의 심사원 이상으로 선정하여야 한다.

③ 인증심사원은 신청인의 정보보호 또는 개인정보보호 컨설팅에 참여하였거나 소속직원 등 신청인과 이해관계를 가지는 경우 사전에 소명하여야 하며, 심사수행기관은 해당 심사원을 인증심사팀의 구성원에서 배제하여야 한다.

제25조(인증심사 방법 및 보완조치) ① 인증심사는 신청인을 방문하여 서면심사와 현장심사를 병행한다.

② 서면심사는 별표 7의 인증기준에 적합한지에 대하여 정보보호 및 개인정보보호 관리체계 구축·운영 관련 정책, 지침, 절차 및 이행의 증적자료 검토, 정보보호대책 및 개인정보 처리단계별 요구사항 적용 여부 확인 등의 방법으로 관리적 요소를 심사한다.

③ 현장심사는 서면심사의 결과와 기술적·물리적 보호대책 이행여부를 확인하기 위하여 담당자 면담, 관련 시스템 확인 및 취약점 점검 등의 방법으로 기술적 요소를 심사한다.

④ 심사수행기관은 인증심사에서 발견된 결함에 대해 심사종료 다음날부터 최대 100일(재조치 요구 60일 포함) 이내에 보완조치를 완료하도록 신청인에게 요청할 수 있다.

⑤ 심사수행기관은 인증위원회 심의결과에 따라 인증위원회 종료 다음날부터 30일 이내에 신청인에게 추가 보완조치를 요구할 수 있다.

⑥ 심사수행기관은 보완조치 결과를 확인하기 위하여 필요한 때에는 현장 확인을 할 수 있다.

제26조(심사중단) ① 심사수행기관은 다음 각 호의 사유가 발생한 경우에는 인증심사를 중단할 수 있다.

1. 신청인이 고의로 인증심사의 실시를 지연 또는 방해하거나 신청인의 귀책사유로 인하여 인증심사팀장이 인증심사를 계속 진행하기가 곤란하다고 판단하는 경우
2. 신청인이 제출한 관련 자료 등을 검토한 결과 인증심사를 받을 준비가 되

었다고 볼 수 없는 경우

3. 인증심사 후 제25조제4항에 따른 보완조치를 최대 100일(제조치 요구 60일 포함) 이내에 완료하지 않은 경우

4. 천재지변 및 경영환경 변화 등으로 인하여 인증심사 진행이 불가능하다고 판단되는 경우

② 심사수행기관은 제1항에 따라 인증심사를 중단하는 때에는 그 사유를 신청인에 서면으로 통보하여야 한다.

③ 심사수행기관은 제1항의 인증심사 중단 사유가 해소되거나 제36조에 따른 이의신청 처리결과에 따라 인증심사를 재개하거나 종결할 수 있다.

제27조(사후관리) ① 인증을 취득한 자는 인증서 유효기간 중 연 1회 이상 심사수행기관에 사후심사를 신청하여야 한다.

② 사후심사는 제5장 및 제6장을 준용하여 진행한다.

③ 인증 취득한 범위와 관련하여 침해사고 또는 개인정보 유출사고가 발생한 경우 인터넷진흥원은 필요에 따라 인증관련 항목의 보안향상을 위한 필요한 지원 등을 할 수 있다.

제28조(인증의 갱신) ① 인증을 취득한 자는 인증서 유효기간 만료 3개월 전에 갱신심사를 신청하여야 한다.

② 갱신심사는 제5장 및 제6장을 준용하여 진행한다.

③ 인증을 취득한 자가 제1항에 따른 인증의 갱신을 신청하지 않고 인증의 유효기간이 경과한 때에는 인증의 효력은 상실된다.

제29조(인증위원회의 구성) ① 인터넷진흥원 또는 인증기관의 장은 다음 각 호의 사항을 심의·의결하기 위하여 인증위원회를 설치·운영하여야 한다.

1. 최초심사 또는 갱신심사 결과가 인증기준에 적합한지 여부

2. 제35조제1항에 따른 인증의 취소에 관한 사항

3. 제36조에 따른 이의신청에 관한 사항

4. 그 밖에 정보보호 및 개인정보보호 관리체계 인증과 관련하여 위원장이 필요하다고 인정하는 사항

② 인증위원회는 35인 이내의 위원으로 구성하되, 위원은 정보보호 및 개인정보보호 관련 분야에 학식과 경험이 있는 자 중에서 인터넷진흥원 또는 인증기관의 장이 위촉하며, 위원장은 위원 중에서 호선한다.

③ 위원장은 인증위원회의 업무를 통할하며 위원회를 대표한다.

④ 인터넷진흥원 또는 인증기관의 장은 위원이 법령 또는 이 규정을 위반한 때에는 해당 위원을 해촉할 수 있다.

제30조(인증위원회의 운영) ① 인증위원회의 회의는 인터넷진흥원 또는 인증기관의 요구로 개최하되, 회의마다 위원장과 인증위원의 전문분야를 고려하여 6인 이상의 인증위원으로 구성한다. 단, 위원장이 부득이한 사유로 직무를

수행할 수 없는 경우 위원장이 사전에 지명한 위원이 위원장의 직무를 대행한다.

② 인터넷진흥원 또는 인증기관의 장은 인증위원회의 심의안건을 검토하여 위원회 개최 5일 전까지 인증위원회에 제출한다. 다만, 긴급한 경우나 부득이한 사유가 있는 경우에는 그러하지 아니하다.

③ 인증위원회 위원장은 제29조제1항의 각 호의 사항에 대한 심의·의결 결과를 인터넷진흥원 또는 인증기관의 장에게 제출한다.

④ 인증위원회는 심의를 위하여 필요하다고 인정되는 경우에는 인증심사에 참여한 인증심사원 또는 관련 전문가로부터 그에 관한 의견을 들을 수 있다.

⑤ 인터넷진흥원 또는 인증기관의 장은 인증위원회의 심의·의결 결과를 제출받은 때에는 신청인에게 결과를 통보하여야 한다.

제31조(제척·기피·회피) ① 인증위원회 위원은 신청인과 다음 각 호의 사항 중 어느 하나에 해당하는 때에는 심의·의결에 관여할 수 없다.

1. 위원 본인과 직접적인 이해관계가 있는 사항
2. 위원 본인과 친족관계에 있거나 있었던 자와 관련된 사항
3. 위원이 되기 전에 감사·수사 또는 조사에 관여한 사항

② 위원에게 심의·의결의 공정성을 기대하기 어려운 사정이 있는 경우 신청인은 기피신청을 할 수 있고, 위원회는 의결로 이를 결정한다.

③ 위원은 제척사유 또는 기피사유에 해당하는 경우에는 자기 스스로 심의·의결을 회피할 수 있다.

제32조(인증서의 발급 등) ① 인터넷진흥원 또는 인증기관의 장은 인증위원회에서 인증적합으로 판정된 경우 그 결과에 따라 신청인에게 별지 제11호서식의 정보보호 및 개인정보보호 관리체계 인증서 또는 별지 제12호서식의 정보보호 관리체계 인증서를 발급하여야 한다.

② 인증서 발급 시 인증번호는 별표 8의 인증의 표시를 따른다.

③ 제1항에 따른 인증서의 유효기간은 3년으로 한다.

제33조(인증서 관리 및 재발급) ① 인터넷진흥원 또는 인증기관은 발급된 인증서의 인증번호, 발급일, 유효기간 등 인증서를 관리하여야 한다.

② 인증을 취득한 자는 인증서의 분실 등으로 인해 재발급을 받고자 할 경우 별지 제13호서식의 인증서 재발급 신청서를 인터넷진흥원 또는 인증기관에 제출하여야 한다.

③ 인증을 취득한 자가 주소, 업체명 등 인증서 기재사항의 변경을 요청하고자 하는 경우 별지 제14호서식의 인증서 변경 신청서를 인터넷진흥원 또는 인증기관에 제출하여야 한다.

제34조(인증의 표시 및 홍보) ① 「개인정보 보호법 시행령」 제34조의7 및 정보통신망법 시행령 제52조에 따른 인증의 표시는 별표 8과 같다.

② 제1항에 따른 인증의 표시를 사용하는 경우에는 인증범위 및 유효기간을

함께 표시하여야 한다.

③ 인터넷진흥원은 인증정보를 제공하는 홈페이지를 통해 인증현황을 공개하여야 한다.

제35조(인증의 취소) ① 인터넷진흥원 또는 인증기관은 다음 각 호의 사유를 발견한 때는 인증위원회 심의·의결을 거쳐 인증을 취소할 수 있다.

1. 거짓 혹은 부정한 방법으로 인증을 취득한 경우
2. 제23조에 따른 인증기준에 미달하게 된 경우
3. 인증을 취득한 자가 제27조제1항에 따른 사후심사 또는 제28조제1항에 따른 갱신심사를 받지 않았거나 제25조제4항에 따른 보완조치를 하지 않은 경우
4. 인증 받은 내용을 홍보하면서 제34조제2항에 따른 인증범위 및 유효기간을 허위로 표기하거나 누락한 경우
5. 인증을 취득한 자가 제27조 및 제28조에 따른 사후관리를 거부 또는 방해하는 경우
6. 개인정보보호 관련 법령을 위반하고 그 위반사유가 중대한 경우

② 인터넷진흥원 또는 인증기관은 제1항에 따라 인증을 취소한 경우에 그 결과를 통지하고, 제32조에 따라 발급한 인증서를 회수한다.

제36조(이의신청) ① 신청인 또는 인증을 취득한 자가 인증심사 결과 또는 인증 취소처분에 관하여 이의가 있는 때에는 그 결과를 통보받은 날부터 15일 이내에 별지 제15호서식의 이의신청서를 인터넷진흥원 또는 인증기관에 제출하여야 한다.

② 인터넷진흥원 또는 인증기관은 제1항에 따른 이의신청이 이유가 있다고 인정되는 경우에는 인증위원회에 재심의를 요청할 수 있다.

③ 인터넷진흥원 또는 인증기관은 이의신청에 대한 처리결과를 신청인 또는 인증을 취득한 자에 통지하여야 한다.

제37조(비밀유지 등) ① 인터넷진흥원, 인증기관, 심사기관, 인증위원회 위원, 인증심사원 등 인증심사 업무에 종사하는 자 또는 종사하였던 자는 정당한 권한 없이 또는 허용된 권한을 초과하여 업무상 지득한 비밀에 관한 정보를 누설하거나 이를 업무 목적 이외에 사용하여서는 아니 된다.

② 인터넷진흥원, 인증기관, 심사기관, 인증위원회 위원, 인증심사원 등 인증심사 업무에 종사하는 자 또는 종사하였던 자는 인증에 관련하여 일체의 금전, 금품, 이익 등을 부당하게 수수하여서는 아니 된다.

제38조(업무 지침 등) 인터넷진흥원, 인증기관 또는 심사기관은 인증 또는 심사 업무 수행을 위해 필요한 경우 법령의 범위 내에서 인증 또는 심사업무에 관한 지침을 마련하여 시행할 수 있다.

제39조(재검토 기한) 과학기술정보통신부장관과 보호위원회는 「행정규제기본

법」 및 「훈령·예규 등의 발령 및 관리에 관한 규정」에 따라 이 고시에 대하여 2019년 1월 1일을 기준으로 매3년이 되는 시점(매 3년째의 12월 31일 까지를 말한다)마다 그 타당성을 검토하여 개선 등의 조치를 하여야 한다.

1. 정보보호 및 개인정보보호 관리체계 인증제도(ISMS-P)의 의의

보호위원회는 개인정보처리자의 개인정보 처리 및 보호와 관련한 일련의 조치가 이 법에 부합하는지 등에 관하여 인증할 수 있다(제32조의2제1항).

특히, 제32조의2에 따른 개인정보보호 관리체계 인증 제도(PIMS, Personal Information Management System)는 2018년 11월부터 과학기술정보통신부에서 별도로 운영하던 「정보통신망법」 제47조에 따른 정보보호 관리체계 인증제도(ISMS, Information Security Management System)와 통합되어 정보보호 및 개인정보보호 관리체계 인증제도(ISMS-P)로 개편되어 운영되고 있다.

2. 인증제도 실행 체계

가 인증기관

정보보호 및 개인정보 보호인증 전문기관(이하 ‘인증기관’)이란 한국인터넷진흥원(KISA) 또는 인증심사원을 5명 이상을 보유하고 업무수행 요건·능력 심사에서 적합하다고 인정받은 법인, 단체 또는 기관으로서 보호위원회 및 과학기술정보통신부장관이 지정하는 법인, 단체 또는 기관을 말한다(영 제34조의6, 「정보보호 및 개인정보보호 관리체계 인증 등에 관한 고시」 별표 2).

인증기관은 심사팀을 구성하여 신청기관이 수립·운영하는 정보보호 및 개인정보보호 관리체계를 인증기준에 따라 심사하고, 심사기간에 발견된 결함사항의 보완조치 여부를 확인하는 한편, 인증심사 결과의 심의, 인증서 발급·관리, 인증의 사후관리, 인증위원회 운영 등 업무를 담당한다. 또한 이들 업무 중 인증심사 업무만 수행하는 기관을 심사기관이라 한다. 한국인터넷진흥원은 인증기관의 업무와 인증협의회 운영 지원, 인증기관 및 심사기관 지정 지원, 인증심사원 양성 및 자격관리 등의 업무를 수행한다.

나 인증위원회

인증위원회는 인증심사 결과(최초심사 또는 갱신심사결과)가 인증기준에 적합한지 여부,

인증취소에 관한 사항, 이의신청에 관한 사항 등을 심의·의결한다(「정보보호 및 개인정보 보호 관리체계 인증 등에 관한 고시」 제29조제1항).

인증위원회는 정보보호 및 개인정보보호 관련 분야에 학식과 경험이 있는 자 중에서 한국인터넷진흥원 또는 인증기관의 장이 위촉한 35명 이내의 위원으로 구성하여 운영하며, 위원장은 위원 중에서 호선한다(「정보보호 및 개인정보보호 관리체계 인증 등에 관한 고시」 제29조제2항).

다 인증심사원

인증심사원은 한국인터넷진흥원으로부터 자격을 부여 받고 인증심사를 수행하는 자를 말한다. 인증심사원은 인증심사 수행능력에 따라 심사원보, 심사원, 선임심사원으로 구분된다. 인증심사원의 등급별 자격요건은 다음과 같다(「정보보호 및 개인정보보호 관리체계 인증 등에 관한 고시」 별표 3). 한편, 한국인터넷진흥원은 매년 선임심사원 중 심사능력이 우수하고 참여율이 높은 심사원을 책임심사원으로 지정하고 해당 심사원에 그 결과를 안내할 수 있다.

구 분	자격 기준
심사원보	· 인증심사원 자격 신청 요건을 만족하는 자로서 인터넷진흥원이 수행하는 인증심사원 양성과정 통과하여 자격을 취득한 자
심사원	· 심사원보 자격 취득자로서 인증심사에 4회 이상 참여하고 심사일수의 합이 20일 이상인 자
선임 심사원	· 심사원 자격 취득자로서 정보보호 및 개인정보보호 관리체계 인증심사를 3회 이상 참여하고 심사일수의 합이 15일 이상인 자

※ 한국인터넷진흥원은 인증심사원의 인증심사 능력에 따라 매년 책임심사원을 지정할 수 있다.

인증심사원 신청을 하기 위해서는 정보보호 및 개인정보보호에 관한 전문지식을 갖춘 사람으로서 기본요건 또는 경력 대체 요건을 갖춘 자가 신청할 수 있다.

라 신청기관

신청기관은 정보보호 및 개인정보보호 활동의 체계적이고 지속적인 관리여부를 객관적으로 검증 받기 위하여 정보보호 및 개인정보보호 관리체계 인증을 신청하는 자를 말한다.

신청기관은 정보보호 및 개인정보보호 관리체계 인증을 신청하기 전에 인증기준에 따른 정보보호 및 개인정보보호 관리체계를 구축하여 반드시 최소 2개월 이상 운영하여야 한다(「정보보호 및 개인정보보호 관리체계 인증 등에 관한 고시」 제17조제1항).

< 정보보호 및 개인정보 보호 관리체계 담당기관별 책임 및 역할 >

담당 기관	책임 및 역할
인증협의회 (개인정보보호위원회, 과학기술정보통신부)	<ul style="list-style-type: none"> • 인증제도 연구 및 개선에 관한 사항 • 인증제도 운영을 위한 제반사항 검토 및 품질관리에 관한 사항 • 인증기관 및 심사기관의 지정·재지정 및 업무정지·지정 취소에 관한 사항 • 인증기관 및 심사기관의 관리·감독에 관한 사항 • 인증제도 운영에 따른 민원 처리 및 법적 분쟁에 관한 사항 • 그 밖에 협의회가 필요한 사항
한국인터넷진흥원(KISA)	<ul style="list-style-type: none"> • 인증협의회 운영 지원 • 인증기관 및 심사기관 지정, 재지정, 사후관리 업무 지원 • 제도 운영 및 인증품질관리 • 신규·특수 분야 인증심사 • 인증심사원 양성 및 관리 • 인증위원회 구성·운영 • 인증서 부여 및 인증마크 발급, 관리
인증기관	<ul style="list-style-type: none"> • 인증심사 신청 접수 • 인증심사 수행 • 인증심사팀 구성·운영 • 인증위원회 구성·운영 • 인증서 부여 및 인증마크 발급
심사기관	<ul style="list-style-type: none"> • 인증심사 신청 접수 • 인증심사 수행 • 인증심사팀 구성·운영
인증위원회	<ul style="list-style-type: none"> • 인증심사 결과 심의·의결 • 이의신청 사항에 대한 심의·의결 • 인증 취소에 대한 심의·의결
인증심사원	<ul style="list-style-type: none"> • 인증심사 실시 • 인증심사 결과보고서 작성
신청기관	<ul style="list-style-type: none"> • 인증심사 신청, 인증 취득 및 관리체계 유지관리

3. 인증심사 대상

가 인증의 유형

인증을 취득하고자 하는 신청기관은 다음의 인증 유형을 선택하여 신청할 수 있다(「정보보호 및 개인정보보호 관리체계 인증 등에 관한 고시」 제18조제1항).

- ① 정보보호 및 개인정보보호 관리체계 인증
- ② 정보보호 관리체계 인증

②유형은 정보통신망법 제47조제2항에 따라 정보보호 관리체계 인증을 의무적으로 받아야 하는 기관, 개인정보를 보유하지 않거나 개인정보 흐름의 보호가 불필요한 조직 등에 적합한 인증이라 할 수 있으므로, 이하에서는 ①유형의 인증을 중심으로 설명하도록 한다.

나 인증기준

정보보호 및 개인정보보호 관리체계 인증기준은 관리체계 수립 및 운영(16항목), 보호대책 요구사항(64항목), 개인정보 처리단계별 요구사항(22항목) 총 3개 분야 102개의 심사항목으로 구성되어 있다(자세한 인증기준은 「정보보호 및 개인정보보호 관리체계 인증 등에 관한 고시」 별표 7 참조). 한편, 2018년 11월 정보보호 및 개인정보보호 관리체계 인증으로 통합되면서 종전 개인정보보호 관리체계 인증의 신청기관 유형별(공공기관, 대기업·정보통신서비스 제공자, 중소기업, 소상공인) 인증기준은 폐지되었다.



4. 인증 절차

정보보호 및 개인정보 보호 관리체계 인증은 ① 준비단계 ② 심사단계 ③ 인증단계 ④ 사후 관리 단계로 이루어진다.

- ① 준비단계 : 인증 신청서 접수, 예비점검, 계약 협의 및 체결
- ② 심사단계 : 인증기준 적합 여부에 대한 서면 및 현장 심사
- ③ 인증단계 : 인증심사의 결과를 근거한 인증 적합성 심의
- ④ 사후관리단계 : 인증취득 후 매년 유지 상태에 대한 점검

가 준비단계

1) 구축 및 운영

신청기관은 인증신청서를 제출하기 전에 인증기준에 따라 정보보호 및 개인정보보호 관리체계를 구축하고 최소 2개월 이상 운영해 왔다는 증빙 자료를 준비해야 한다. 특히 신청기관은 인증 받고자 하는 인증범위를 정할 때 정보보호 및 개인정보 관련 업무를 상세하게 분석하여 정보서비스 및 Life-Cycle(수집·보유·이용·제공·폐기)에 따른 흐름을 고려하여 증적을 준비하는 한편, 해당 증적에는 모든 서비스, 인력 등 관련 내용이 포함되어야 한다.

인증 받고자 하는 인증범위는 이용자 중심의 대외 서비스만 포함할 것인지 임직원이 이용하는 내부 서비스까지도 포함할 것인지에 대해서도 고려하여 결정하여야 한다.

2) 인증심사 신청 및 접수

정보보호 및 개인정보보호 관리체계 인증을 신청하려는 자는 다음의 신청서류를 심사수행기관에 제출한다.

- ① 인증신청공문
- ② 정보보호 및 개인정보보호 관리체계 인증신청서
- ③ 정보보호 및 개인정보보호 관리체계 명세서
- ④ 정보보호 및 개인정보보호 관리체계 인증범위서
- ⑤ 법인등기부등본
- ⑥ 인증신청기관이 인증수수료 할인 대상인 경우 이를 증빙할 수 있는 서류

※ 신청서 및 명세서 양식은 홈페이지(<https://isms-p.kisa.or.kr>) 참조

인증신청은 방문접수 또는 등기우편으로 신청할 수 있으며, 신청 서류의 미비로 인증기관의 보완요청이 있을 경우 신청서류를 재구비하여 제출하여야 한다.

인증심사 신청부터 인증심사까지 예비점검, 계약, 심사원 모집 등 업무처리를 위한 기간이 필요하므로 희망심사일 기준 최소 8주전에 신청하도록 한다.

특히 정보보호 및 개인정보보호 관리체계 인증제도와 관련하여 한국인터넷진흥원(KISA) 홈페이지(<https://isms-p.kisa.or.kr>)로 안내하고 있으며, 이메일(isms-p@kisa.or.kr)을 통하여 구체적인 상담이 가능하다.

3) 예비 점검

예비점검이란 한국인터넷진흥원·인증기관 또는 심사기관(이하 “심사수행기관”이라 한다)의 심사팀장이 신청기관을 방문하여 인증범위 내 정보시스템의 규모, 정보서비스흐름도, 위험분석보고서, 대책명세서 등 인증심사에 필요한 기초자료 구비 유무, 인증심사 준비상태 및 운영여부를 확인하는 것을 말한다.

예비점검 기간에 신청기관의 정보보호 및 개인정보보호 관리체계 운영상황을 확인하고 인증심사 가능여부를 판단하여 심사일정을 조정한다. 특히 신청기관의 담당자는 인증범위의 설명과 증적자료를 확인할 수 있도록 협조하여야 한다. 또한 심사수행기관의 심사팀장은 신청기관의 정보보호 최고 책임자(CISO, Chief Information Security Officer) 및 개인정보보호책임자(CPO, Chief Privacy Officer) 또는 담당자와 예비점검 결과를 공유하고, 인증범위를 고려하여 심사일정을 확정한다.

4) 계약 및 수수료 납부

심사수행기관은 신청기관과 인증의 범위, 심사 기간, 심사 인원, 심사팀 구성, 인증 수수료(홈페이지 참고) 등을 협의하여 정보보호 및 개인정보보호 관리체계 인증심사 계약을 체결한다.

신청기관은 인증심사계약이 완료되면 계약에 따라 정해진 심사수수료를 인증심사 시작일 이전까지 납부하여야 한다. 신청기관은 최초심사, 사후심사 및 갱신심사 신청 시 수수료를 납부하여야 하며, 수수료를 납부하지 않은 경우에 심사수행기관은 인증심사를 실시하지 아니할 수 있다(「정보보호 및 개인정보보호 관리체계 인증 등에 관한 고시」 제22조).

인증심사 수수료는 신청기관이 심사수행기관에 납부하는 비용으로 인증심사 신청접수 및 계약, 예비점검, 심사원 자문료 등에 소요되는 제비용을 의미한다. 인증심사 수수료는 직접인건비, 직접경비, 제경비, 기술료의 합으로 산정한다.

나 심사단계

1) 인증심사

심사수행기관은 인증심사 계약을 체결한 때에는 인증심사팀을 구성하여야 한다. 인증심사팀 구성시 심사팀장은 심사수행기관 소속의 심사원 이상으로 선정하여야 한다. 한편 인증심사원은 신청기관의 정보보호 및 개인정보보호 관리체계 인증을 위한 컨설팅에 참여하였거나 소속직원 등 신청기관과 이해관계를 가지는 경우 사전에 소명하여야 하며, 심사수행기관은 해당 심사원을 인증심사팀의 구성원에서 배제하여야 한다(「정보보호 및 개인정보보호 관리체계 인증 등에 관한 고시」 제24조).

인증심사는 정보보호 및 개인정보보호 관리체계 수립 및 운영, 보호대책, 개인정보 처리 단계별 요구사항으로 구성된 관리체계의 인증기준을 신청기관이 적절히 이행하고 있는지를 심사하는 것으로, 신청기관을 방문하여 서면심사와 현장심사를 병행하는 방법으로 진행된다.

서면심사는 인증기준에 적합한지에 대하여 정보보호 및 개인정보보호 관리체계 구축·운영 관련 정책, 지침, 절차 및 이행의 증빙 자료 검토, 정보보호대책 및 개인정보 처리단계별 요구사항 적용 여부 확인 등의 방법으로 관리적 요소를 심사한다(「정보보호 및 개인정보보호 관리체계 인증 등에 관한 고시」 제25조제2항).

현장심사는 서면심사의 결과와 기술적·물리적 보호대책 이행여부를 확인하기 위하여 담당자 면담, 관련 시스템 확인 및 취약점 점검 등의 방법으로 기술적 요소를 심사한다(「정보보호 및 개인정보보호 관리체계 인증 등에 관한 고시」 제25조제3항). 심사수행기관은 인증심사 후 서면심사 및 현장심사를 통하여 도출된 결함을 정리한 보고서를 작성하여 신청기관에게 보완조치를 완료할 것을 요청하여야 한다.

2) 인증심사 보완조치 제출

신청기관은 보완조치 요청을 받은 날로부터 40일 이내 보완조치를 하고 보완조치 사항에 대해 보완조치 내역서를 작성하여 심사수행기관에 제출해야 한다. 인증기관은 제출한 보완조치 결과가 미흡하다고 판단하거나, 신청기관 스스로 보완조치 기간이 추가로 필요하다고 판단한 경우 공문을 통해 최대 60일까지(재조치 기간 포함) 보완조치 기간을 연장할 수 있다. 보완조치 기한 연장 시 보완조치요약서 및 개선된 결함사항에 대한 보완조치 내역서를 공문과 같이 제출하여야 한다. 총 100일의 보완조치 기간은 심사팀장이 보완조치 결과를 확인하기 위한 이행점검까지 끝낸 시점까지를 포함한다.

심사수행기관은 신청기관의 보완조치 결과를 문서 및 현장확인을 통해 확인하며, 보완조치 확인결과를 보완조치 완료확인서에 서명 날인하는 것으로 보완조치 확인을 마무리한다. 보완조치 내역은 조치 전·후의 내용을 확인할 수 있도록 작성해야 한다.

3) 인증심사의 중단

인증심사 수행기관은 다음의 상황으로 인하여 인증심사 진행이 불가능하다고 판단되는 경우 인증심사를 중단할 수 있다(「정보보호 및 개인정보보호 관리체계 인증 등에 관한 고시」 제26조).

- ① 신청기관이 고의로 인증심사의 실시를 지연 또는 방해하거나 신청기관의 귀책사유로 인하여 인증심사를 계속 진행하기가 곤란하다고 인정되는 경우
- ② 신청기관이 제출한 관련 자료 등을 검토한 결과 인증 준비가 되었다고 볼 수 없는 경우
- ③ 인증심사 후 보완 조치를 최대 100일(재조치 요구 60일 포함) 이내에 완료하지 않은 경우
- ④ 천재지변 및 경영환경 변화 등으로 인하여 인증심사 진행이 불가능하다고 판단되는 경우

다 인증단계

1) 인증위원회 심의 · 의결

최초 또는 갱신심사의 경우 보완조치가 완료된 기관에 대하여 심사수행기관은 인증심사팀이 수행한 심사결과에 대한 객관성과 공정성 확보 및 일정 수준 이상의 품질 확보를 위하여 한국인터넷진흥원 또는 인증기관의 장이 구성·운영하는 인증위원회에 “인증심사 결과보고서”를 작성하여 인증위원회 안건으로 상정한다.

인증위원회는 한국인터넷진흥원 또는 인증기관의 요구로 개최되며 인증심사 기간에 발견된 문제점에 대한 판단의 적합성과 보완조치 확인의 적절성을 검토하여 인증적합 여부를 심의하며, 심사수행기관은 심의 결과에 따라 인증위원회 종료 다음 날부터 30일 이내의 보완조치를 요구할 수 있다(「정보보호 및 개인정보보호 관리체계 인증 등에 관한 고시」 제25조제5항).

보완조치사항을 전달받은 신청기관은 해당사항의 보완 완료 후 심사팀장에게 수정된 “보완조치 내역서”를 제출하고 다음 회기 인증위원회에 상정하여 최종 인증부여 여부를 의결받아야 한다. 인증위원회에서 의결이 완료되면 인증위원장은 인증심의 결과서와 심의의견서를 인증기관에 제출한다.

인증의 효력은 3년이다(제32조의2제2항).

2) 인증결과 통보

한국인터넷진흥원 또는 인증기관의 장은 인증위원회의 심의·의결 결과를 신청기관에 통보하고 정보보호 및 개인정보보호 관리체계 인증기준에 적합한 경우 인증서를 발급하며, 부적합 통보를 받은 신청기관은 통보받은 날로부터 15일 이내에 이의신청을 할 수 있다(「정보보호 및 개인정보보호 관리체계 인증 등에 관한 고시」 제32조제1항, 제36조제1항).

인증취득기관은 정보보호 및 개인정보보호 관리체계 인증 유효기간 동안 정보보호 및 개인정보보호 관리체계를 지속적으로 유지하고 관리하여야 한다.

라 사후관리 단계

1) 사후심사

사후심사란 인증을 받거나 인증이 갱신된 후 매년 사후관리를 위하여 실시하는 인증심사를 말한다(「정보보호 및 개인정보보호 관리체계 인증 등에 관한 고시」 제2조제10호). 사후심사는 인증발급일 기준으로 매 1년 이전에 인증심사 완료 및 유지공문을 받아야 하며, 매 1년 내 인증유지공문을 받지 못할 시 인증이 취소될 수 있다.

한편, 인증 취득한 범위와 관련하여 침해사고 또는 개인정보 유출사고가 발생한 경우 한국인터넷진흥원은 필요에 따라 인증관련 보안향상을 위한 필요한 지원 등을 할 수 있다(「정보보호 및 개인정보보호 관리체계 인증 등에 관한 고시」 제27조제3항).

2) 갱신심사

정보보호 및 개인정보보호 관리체계 인증의 유효기간은 3년이므로 인증취득기관이 인증의 효력을 연장하고자 하는 경우 갱신심사를 신청하여 심사수행기관의 심사를 받아 인증을 갱신하여야 한다. 갱신심사 신청은 인증서 유효기간 만료 3개월 전까지 하여야 한다. 만일 인증취득기간이 인증의 갱신을 신청하지 않고 인증의 유효기간을 경과한 때에는 인증의 효력은 상실된다(「정보보호 및 개인정보보호 관리체계 인증 등에 관한 고시」 제28조).

5. 인증의 표시 및 홍보

정보보호 및 개인정보보호 관리체계 인증을 받은 자는 인증 취득 사실을 홍보할 수 있으며, 인증 표시를 사용할 수 있다(인증표시의 구체적인 사용 방법과 인증명판 제작방법 등에 대해서는 정보보호 및 개인정보보호 관리체계 인증 등에 관한 고시 별표 8 이하 참고). 한국인터넷진흥원은 인증정보를 제공하는 홈페이지(<https://isms-p.kisa.or.kr>)를 통해 인증현황을 공개하여야 한다(「정보보호 및 개인정보보호 관리체계 인증 등에 관한 고시」 제34조제3항).

정보보호 및 개인정보보호 관리체계 인증	정보보호 관리체계 인증
<div style="text-align: center;">  </div> <p>유효기간 :</p> <p>인증범위 :</p> <p>※ 심사 생략 범위 :</p>	<div style="text-align: center;">  </div> <p>유효기간 :</p> <p>인증범위 :</p> <p>※ 심사 생략 범위 :</p>

정보보호 및 개인정보보호 관리체계 인증 취득 사실의 홍보는 정보보호 및 개인정보보호 관리체계 인증서를 발급받은 날부터 효력이 유지되는 동안에만 사용이 가능하다. 또한 인증을 취득한 자는 인증의 사실을 과장되거나 불명확한 표현을 사용하여 광고할 수 없다. 한편 인증이 취소된 경우에는 인증에 대한 홍보, 정보보호 및 개인정보보호 관리체계 인증서 사용을 중지하여야 한다. 또한, 인증 표시를 사용하는 경우 유효기간, 인증범위, 인증 심사 생략 범위를 함께 표시하여야 한다.

6. 인증취소

한국인터넷진흥원 또는 인증기관은 다음 각 호의 사유를 발견한 때는 인증위원회의 심의·의결을 거쳐 인증을 취소할 수 있다(「정보보호 및 개인정보보호 관리체계 인증 등에 관한 고시」 제35조).

인증취소 사유(고시 제35조제1항)

1. 거짓 혹은 부정한 방법으로 인증을 취득한 경우
2. 인증기준에 미달하게 된 경우
3. 인증 취득기관이 제27조제1항에 따른 사후심사 또는 제28조제1항에 따른 갱신심사를 받지 않았거나 제25조제4항에 따른 보완조치를 하지 않은 경우
4. 인증 받은 내용을 홍보하면서 제34조제2항에 따른 인증범위 및 유효기간을 허위로 표기하거나 누락한 경우
5. 인증을 취득한 기관이 제27조 및 제28조에 따른 사후관리를 거부 또는 방해하는 경우
6. 개인정보보호 관련 법령을 위반하고 그 위반사유가 중대한 경우

한국인터넷진흥원 또는 인증기관은 인증을 취소한 경우에 인증취득기관에 통지하고, 「정보보호 및 개인정보보호 관리체계 인증 등에 관한 고시」 제32조에 따라 발급한 인증서를 회수한다. 인증취득기관은 인증 취소처분에 관하여 이의가 있는 때에는 그 결과를 통보받은 날로부터 15일 이내에 한국인터넷진흥원 또는 인증기관에 이의신청을 할 수 있다(「정보보호 및 개인정보보호 관리체계 인증 등에 관한 고시」 제36조제1항).

7. 질의응답

Q 서비스별로 ISMS 인증과 ISMS-P 인증을 나누어 받는 기업의 사례는?

A 동일한 관리체계 내에서 일부 서비스는 개인정보 흐름을 포함하고 일부 서비스는 개인정보 흐름을 포함하지 않고 인증을 받는 경우가 해당함. 예를 들어 은행이 인터넷뱅킹서비스와 금고서비스를 인증 받고자 하는데, 인터넷뱅킹서비스만 개인정보 흐름을 포함하여 인증을 받고자 하는 경우 인터넷뱅킹서비스는 ISMS-P 인증, 금고서비스는 ISMS 인증으로 나누어 받을 수 있음.

Q ISMS 인증과 ISMS-P 인증을 나누어 받고자 하는데, 반드시 신청을 같이 해야만 하는지?

A 기업(기관)의 선택에 따라 두 개의 인증을 같이 신청할 수도 있고 다른 시기에 개별로 신청할 수도 있음. 다만, 같이 신청하는 경우 수수료, 중복심사 부담 완화 등 이점이 있음.

8. 벌칙규정

위반행위	벌칙
인증을 받지 아니하였음에도 거짓으로 인증의 내용을 표시하거나 홍보한자 (제32조의2제6항 위반)	3천만원 이하의 과태료 (제75조제2항제7호의3)

제33조 | 개인정보 영향평가

법률

제33조(개인정보 영향평가) ① 공공기관의 장은 대통령령으로 정하는 기준에 해당하는 개인정보파일의 운용으로 인하여 정보주체의 개인정보 침해가 우려되는 경우에는 그 위험요인의 분석과 개선 사항 도출을 위한 평가(이하 “영향평가”라 한다)를 하고 그 결과를 보호위원회에 제출하여야 한다. 이 경우 공공기관의 장은 영향평가를 보호위원회가 지정하는 기관(이하 “평가기관”이라 한다) 중에서 의뢰하여야 한다.

② 영향평가를 하는 경우에는 다음 각 호의 사항을 고려하여야 한다.

1. 처리하는 개인정보의 수
2. 개인정보의 제3자 제공 여부
3. 정보주체의 권리를 해할 가능성 및 그 위험 정도
4. 그 밖에 대통령령으로 정한 사항

③ 보호위원회는 제1항에 따라 제출받은 영향평가 결과에 대하여 의견을 제시할 수 있다.

④ 공공기관의 장은 제1항에 따라 영향평가를 한 개인정보파일을 제32조제1항에 따라 등록할 때에는 영향평가 결과를 함께 첨부하여야 한다.

⑤ 보호위원회는 영향평가의 활성화를 위하여 관계 전문가의 육성, 영향평가 기준의 개발·보급 등 필요한 조치를 마련하여야 한다.

⑥ 제1항에 따른 평가기관의 지정기준 및 지정취소, 평가기준, 영향평가의 방법·절차 등에 관하여 필요한 사항은 대통령령으로 정한다.

⑦ 국회, 법원, 헌법재판소, 중앙선거관리위원회(그 소속 기관을 포함한다)의 영향평가에 관한 사항은 국회규칙, 대법원규칙, 헌법재판소규칙 및 중앙선거관리위원회규칙으로 정하는 바에 따른다.

⑧ 공공기관 외의 개인정보처리자는 개인정보파일 운용으로 인하여 정보주체의 개인정보 침해가 우려되는 경우에는 영향평가를 하기 위하여 적극 노력하여야 한다.

시행령

제35조(개인정보 영향평가의 대상) 법 제33조제1항에서 “대통령령으로 정하는 기준에 해당하는 개인정보파일”이란 개인정보를 전자적으로 처리할 수 있는 개인정보파일로서 다음 각 호의 어느 하나에 해당하는 개인정보파일을 말한다.

1. 구축·운용 또는 변경하려는 개인정보파일로서 5만명 이상의 정보주체에 관한 민감정보 또는 고유식별정보의 처리가 수반되는 개인정보파일
2. 구축·운용하고 있는 개인정보파일을 해당 공공기관 내부 또는 외부에서 구축·운용하고 있는 다른 개인정보파일과 연계하려는 경우로서 연계 결과 50만명 이상의 정보주체에 관한 개인정보가 포함되는 개인정보파일

3. 구축·운영 또는 변경하려는 개인정보파일로서 100만명 이상의 정보주체에 관한 개인정보파일
4. 법 제33조제1항에 따른 개인정보 영향평가(이하 “영향평가”라 한다)를 받은 후에 개인정보 검색체계 등 개인정보파일의 운용체계를 변경하려는 경우 그 개인정보파일. 이 경우 영향평가 대상은 변경된 부분으로 한정한다.

제36조(영향평가 시 고려사항) 법 제33조제2항제4호에서 “대통령령으로 정한 사항”이란 다음 각 호의 사항을 말한다.

1. 민감정보 또는 고유식별정보의 처리 여부
2. 개인정보 보유기간

제37조(평가기관의 지정 및 지정취소) ① 보호위원회는 법 제33조제1항 후단에 따라 다음 각 호의 요건을 모두 갖춘 법인을 개인정보 영향평가기관(이하 “평가기관”이라 한다)으로 지정할 수 있다.

1. 최근 5년간 다음 각 목의 어느 하나에 해당하는 업무 수행의 대가로 받은 금액의 합계액이 2억 원 이상인 법인
 - 가. 영향평가 업무 또는 이와 유사한 업무
 - 나. 「전자정부법」 제2조제13호에 따른 정보시스템(정보보호시스템을 포함한다)의 구축 업무 중 정보보호컨설팅 업무(전자적 침해행위에 대비하기 위한 정보시스템의 분석·평가와 이에 기초한 정보 보호 대책의 제시 업무를 말한다. 이하 같다)
 - 다. 「전자정부법」 제2조제14호에 따른 정보시스템 감리 업무 중 정보보호컨설팅 업무
 - 라. 「정보보호산업의 진흥에 관한 법률」 제2조제2호에 따른 정보보호산업에 해당하는 업무 중 정보보호컨설팅 업무
 - 마. 「정보보호산업의 진흥에 관한 법률」 제23조제1항제1호 및 제2호에 따른 업무

2. 별표 1의2에 따른 전문인력을 10명 이상 상시 고용하고 있는 법인

3. 다음 각 목의 사무실 및 설비를 갖춘 법인

- 가. 신원 확인 및 출입 통제를 위한 설비를 갖춘 사무실
- 나. 기록 및 자료의 안전한 관리를 위한 설비

② 평가기관으로 지정받으려는 자는 보호위원회가 정하여 고시하는 평가기관 지정신청서에 다음 각 호의 서류를 첨부하여 보호위원회에 제출해야 한다.

1. 정관
2. 대표자의 성명
3. 제1항제2호에 따른 전문인력의 자격을 증명할 수 있는 서류
4. 그 밖에 보호위원회가 정하여 고시하는 서류

③ 제2항에 따라 평가기관 지정신청서를 제출받은 보호위원회는 「전자정부

법」 제36조제1항에 따른 행정정보의 공동이용을 통하여 다음 각 호의 서류를 확인해야 한다. 다만, 신청인이 제2호의 확인에 동의하지 않는 경우에는 신청인에게 그 서류를 첨부하게 해야 한다.

1. 법인 등기사항증명서
2. 「출입국관리법」 제88조제2항에 따른 외국인등록 사실증명(외국인인 경우만 해당한다)

④ 보호위원회는 제1항에 따라 평가기관을 지정한 경우에는 지체 없이 평가기관 지정서를 발급하고, 다음 각 호의 사항을 관보에 고시해야 한다. 고시된 사항이 변경된 경우에도 또한 같다.

1. 평가기관의 명칭·주소 및 전화번호와 대표자의 성명
2. 지정 시 조건을 붙이는 경우 그 조건의 내용

⑤ 보호위원회는 제1항에 따라 지정된 평가기관이 다음 각 호의 어느 하나에 해당하는 경우에는 평가기관의 지정을 취소할 수 있다. 다만, 제1호 또는 제2호에 해당하는 경우에는 평가기관의 지정을 취소해야 한다.

1. 거짓이나 그 밖의 부정한 방법으로 평가기관의 지정을 받은 경우
2. 지정된 평가기관 스스로 지정취소를 원하는 경우나 폐업한 경우
3. 제1항에 따른 지정요건을 충족하지 못하게 된 경우
4. 제6항에 따른 신고의무를 이행하지 아니한 경우
5. 고의 또는 중대한 과실로 영향평가 업무를 부실하게 수행하여 그 업무를 적정하게 수행할 수 없다고 인정되는 경우
6. 그 밖에 법 또는 이 영에 따른 의무를 위반한 경우

⑥ 제1항에 따라 지정된 평가기관은 지정된 후 다음 각 호의 어느 하나에 해당하는 사유가 발생한 경우에는 보호위원회가 정하여 고시하는 바에 따라 그 사유가 발생한 날부터 14일 이내에 보호위원회에 신고해야 한다. 다만, 제3호에 해당하는 경우에는 그 사유가 발생한 날부터 60일 이내에 신고해야 한다.

1. 제1항 각 호의 어느 하나에 해당하는 사항이 변경된 경우
2. 제4항제1호에 해당하는 사항이 변경된 경우
3. 평가기관을 양도·양수하거나 합병하는 등의 사유가 발생한 경우

⑦ 보호위원회는 제5항에 따라 평가기관의 지정을 취소하려는 경우에는 청문을 해야 한다.

제38조(영향평가의 평가기준 등) ① 법 제33조제6항에 따른 영향평가의 평가기준은 다음 각 호와 같다.

1. 해당 개인정보파일에 포함되는 개인정보의 종류·성질, 정보주체의 수 및 그에 따른 개인정보 침해의 가능성
2. 법 제24조제3항, 제25조제6항 및 제29조에 따른 안전성 확보 조치의 수준 및 이에 따른 개인정보 침해의 가능성

3. 개인정보 침해의 위험요인별 조치 여부
 4. 그 밖에 법 및 이 영에 따라 필요한 조치 또는 의무 위반 요소에 관한 사항
- ② 법 제33조제1항에 따라 영향평가를 의뢰받은 평가기관은 제1항의 평가기준에 따라 개인정보파일의 운용으로 인한 개인정보 침해의 위험요인을 분석·평가한 후 다음 각 호의 사항이 포함된 평가 결과를 영향평가서로 작성하여 해당 공공기관의 장에게 보내야 하며, 공공기관의 장은 제35조 각 호에 해당하는 개인정보파일을 구축·운용 또는 변경하기 전에 그 영향평가서를 보호위원회에 제출(영향평가서에 제3호에 따른 개선 필요 사항이 포함된 경우에는 그에 대한 조치 내용을 포함한다)해야 한다.
1. 개인정보파일 운용과 관련된 사업의 개요 및 개인정보파일 운용의 목적
 2. 영향평가 대상 개인정보파일의 개요
 3. 평가기준에 따른 개인정보 침해의 위험요인에 대한 분석·평가 및 개선이 필요한 사항
 4. 영향평가 수행 인력 및 비용
- ③ 보호위원회는 법 및 이 영에서 정한 사항 외에 평가기관의 지정 및 영향평가의 절차 등에 관한 세부 기준을 정하여 고시할 수 있다.

개인정보 처리 방법에 관한 고시(보호위원회 고시 제2020-7호)

제3조(개인정보 보호업무 관련 장부 및 문서 서식)

- ③ 영 제37조제2항에 따라 개인정보 영향평가기관의 지정을 신청하려는 자는 별지 제3호서식의 개인정보 영향평가기관 지정신청서에 다음 각 호의 서류(전자문서를 포함한다)를 첨부하여 개인정보 보호위원회에 제출하여야 한다.
1. 영 제37조제2항제1호부터 제3호까지의 규정에 따른 서류
 2. 영 제37조제2항제4호에 따른 다음 각 목의 서류
 - 가. 별지 제4호서식의 개인정보 영향평가 수행인력 보유 현황
 - 나. 별지 제5호서식의 개인정보 영향평가 수행 관련 사무실 및 설비 보유 현황
 - 다. 영 제37조제1항제1호의 사실을 증명할 수 있는 서류 등 개인정보 보호위원회가 정하는 서류
 3. 「출입국관리법」 제88조제2항에 따른 외국인등록 사실증명(영 제37조제3항 각 호 외의 부분 단서에 해당하는 경우에만 첨부한다)
- ④ 법 제33조제1항과 영 제37조제4항에 따른 개인정보 영향평가기관 지정서는 별지 제6호서식과 같다.
- ⑤ 법 제33조제6항과 영 제37조제6항에 따른 신고는 별지 제7호서식의 개인정보 영향평가기관 변경사항 신고서에 따른다.

개인정보 영향평가에 관한 고시(보호위원회 고시 제2020-4호)

제1조(목적) 이 고시는 「개인정보 보호법」(이하 “법”이라 한다) 제33조와

고시

「개인정보 보호법 시행령」(이하 “영”이라 한다) 제38조에 따른 평가기관의 지정 및 영향평가의 절차 등에 관한 세부기준을 정함을 목적으로 한다.

제2조(용어의 정의) 이 고시에서 사용하는 용어의 정의는 다음과 각 호와 같다.

1. “개인정보 영향평가(이하 “영향평가”라 한다)”란 법 제33조제1항에 따라 공공기관의 장이 영 제35조에 해당하는 개인정보파일의 운용으로 인하여 정보주체의 개인정보 침해가 우려되는 경우에 그 위험요인의 분석과 개선 사항 도출을 위한 평가를 말한다.
2. “대상기관”이란 영 제35조에 해당하는 개인정보파일을 구축·운용, 변경 또는 연계하려는 공공기관을 말한다.
3. “개인정보 영향평가기관(이하 “평가기관”이라 한다)”이란 영 제37조제1항 각 호의 요건을 모두 갖춘 법인으로서 공공기관의 영향평가를 수행하기 위하여 개인정보 보호위원회(이하 “보호위원회”라 한다)가 지정한 기관을 말한다.
4. “대상시스템”이란 영 제35조에 해당하는 개인정보파일을 구축·운용, 변경 또는 연계하려는 정보시스템을 말한다.
5. “개인정보 영향평가 관련 분야 수행실적(이하 “영향평가 관련 분야 수행실적”이라 한다)”이란 영 제37조제1항제1호에 따른 영향평가 업무 또는 이와 유사한 업무, 정보보호 컨설팅 업무 등을 수행한 실적을 말한다.

제3조(평가기관 지정절차) ① 영 제37조에 따른 평가기관의 지정절차는 지정신청 공고, 지정신청 서류 접수 및 검토, 현장실사, 종합심사의 순으로 진행된다.

② 보호위원회는 평가기관으로 지정받으려는 자가 지정 신청을 할 수 있도록 관보 등을 통해 15일 이상 지정신청공고를 하여야 한다.

③ 평가기관으로 지정받으려는 자는 「개인정보 보호법 시행규칙」(이하 “규칙”이라 한다) 별지 제3호서식의 “개인정보 영향평가기관 지정신청서”와 함께 다음 각 호의 서류를 보호위원회에 제출한다.

1. 별지 제1호서식의 개인정보 영향평가 수행실적 명세서
2. 별지 제2호서식의 개인정보 영향평가 수행실적물 관리카드
3. 별지 제3호서식의 개인정보 영향평가 수행인력의 경력 및 실적 증명서
4. 별지 제4호서식의 개인정보 영향평가 수행인력 관리카드
5. 별지 제5호서식의 개인정보 영향평가 수행능력 세부 심사자료
6. 별지 제6호서식의 개인정보 영향평가 관련 기술자산 보유목록

④ 보호위원회는 제3항에 따른 평가기관 지정신청을 받은 경우 지정기준의 적합여부를 심사하기 위하여 평가기관 지정심사위원회(이하 “지정심사위원회”라 한다)를 구성·운영한다.

⑤ 보호위원회는 지정심사위원회의 심사결과를 검증한 후 평가기관 지정을 확정한다.

⑥ 평가기관의 유효기간은 보호위원회가 평가기관으로 지정한 날로부터 3년으로 한다.

⑦ 평가기관의 유효기간을 연장하고자 하는 자는 유효기간 만료일 3개월 전까지 제3조제3항에 따른 서류를 보호위원회에 제출해야 한다.

제4조(지정심사위원회의 구성 및 운영) ① 제3조에 따른 지정심사위원회는 다음 각 호의 자격을 가진 자 중에서 보호위원회가 위촉하는 5인 이상 15인 이내의 위원으로 구성한다.

1. 「고등교육법」 제2조제1호·제2호 또는 제5호에 따른 학교나 공인된 연구기관에서 조교수 이상의 직 또는 이에 상당하는 직에 있거나 있었던 자로 개인정보 보호 연구경력이 8년 이상인 사람
2. 개인정보 보호 관련 업체, 기관 또는 단체(협회, 조합)에서 8년 이상 개인정보 보호 업무에 종사한 사람
3. 그 밖에 개인정보 보호에 관한 학식과 경험이 풍부한 사람

② 지정심사위원회는 영 제37조제1항에 따른 신청한 법인의 자격 및 업무수행능력 등을 검토한다.

③ 지정심사위원회의 위원 임기는 3년으로 하되, 연임할 수 있다.

④ 지정심사위원회의 회의는 필요에 따라 보호위원회가 소집한다.

제5조(영향평가 수행인력 자격) ① 영향평가 수행인력은 다음 각 호와 같이 일반수행인력과 고급수행인력으로 구분할 수 있다.

1. 일반수행인력의 자격은 다음 각 목과 같다.

가. 영 제37조제1항제2호의 전문인력 자격을 갖춘 사람

나. 한국CPO포럼이 시행하는 개인정보관리사 자격을 취득한 후 1년 이상 개인정보 영향평가 관련 분야 수행실적이 있는 사람

2. 고급수행인력의 자격은 다음 각 목과 같다.

가. 제1호의 일반수행인력의 자격을 갖춘 후 5년 이상의 영향평가 관련 분야 수행실적이 있는 사람

나. 관련 분야 박사학위를 취득한 후 3년 이상의 영향평가 관련 분야 수행실적이 있는 사람

다. 「국가기술자격법 시행규칙」 제3조에 따른 정보관리기술사, 컴퓨터시스템응용기술사, 정보통신기술사 자격을 취득한 후 3년 이상의 영향평가 관련 분야 수행실적이 있는 사람

② 제1항에 따른 영향평가 수행인력은 제6조제2항에 따른 전문교육을 이수하고 제6조제3항에 따른 전문인력 인증서를 받은 경우에 영향평가를 수행할 수 있다.

제6조(영향평가 전문교육의 운영 및 실시) ① 보호위원회는 영향평가 전문인력 양성을 위한 세부 교육계획 수립 및 교육 운영 등의 업무를 효율적으로 추진하기 위하여 한국인터넷진흥원을 전문교육기관으로 지정한다.

② 전문교육기관의 장은 영향평가 전문인력 양성을 위한 세부 교육계획을 수립하여 전문교육 등을 실시하여야 한다.

③ 전문교육기관의 장은 전문교육 이수자에 대한 평가를 실시하고 그 결과에 따라 개인정보 영향평가 전문인력 인증서를 교부한다.

④ 전문교육기관의 장은 다음 각 호의 1에 해당되는 경우에는 제3항에 따른 전문인력 인증서를 교부받은 자에 대한 계속교육을 실시하여야 하며, 이수 여부에 따라 전문인력 인증서를 갱신하여 교부한다.

1. 인증서를 교부받은 후 매 2년이 경과한 경우
2. 법령 또는 평가기준 등의 개정에 따른 변경사항이 발생하여 교육의 실시가 필요하다고 판단되는 경우

⑤ 제3항 또는 제4항에 따라 전문인력 인증서를 교부받은 자가 전문교육기관의 장이 정하는 기간 내에 제4항의 계속교육을 이수하지 아니하여 인증서를 갱신하지 못한 경우 기존 인증서의 효력은 정지된다.

제7조(영향평가 수행능력심사의 세부평가 및 지정기준) ① 평가기관의 영향평가 수행능력심사의 세부평가기준은 별표 1과 같다.

② 보호위원회는 영향평가 수행능력심사 세부평가기준에 따른 심사결과가 총점 75점 이상인 경우 신청한 법인을 평가기관으로 지정한다.

③ 평가기관의 유효기간을 연장하고자 하는 자에 대한 세부평가기준은 별표 2와 같다.

제8조(사후관리) ① 보호위원회는 평가기관이 영 제37조제1항의 평가기관 지정요건을 충족하는 지 여부와 영 제37조제6항에 따른 변경사항을 확인하기 위하여 현장실사, 관련 자료제출 요구 등을 할 수 있다.

② 평가기관은 다음 각 호를 포함한 보호대책을 별표 3과 같이 수립·시행하여야 하며, 보호위원회는 그에 대한 준수여부를 점검할 수 있다.

1. 영향평가 수행구역 및 설비에 대한 보호대책
2. 영향평가 수행 인력에 대한 보호대책
3. 문서 및 전산자료에 대한 보호대책
4. 일반 관리적 보호대책

③ 보호위원회는 평가기관이 영 제37조제5항제3호부터 제6호까지의 규정에 해당하는 경우에는 지정취소 이전에 시정 및 보완을 요구할 수 있다.

제9조(평가절차) 대상기관은 다음 각 호와 같이 사전 준비, 영향평가 수행, 이행 단계로 영향평가를 수행한다.

1. 사전 준비 단계에서는 영향평가 사업계획을 수립하여 예산을 확보하고 평가기관을 선정한다.
2. 영향평가 수행 단계에서는 평가기관이 개인정보 침해요인을 분석하고 개선계획을 수립하여 영향평가서를 작성한다.

3. 이행 단계에서는 영향평가서의 침해요인에 대한 개선계획이 반영되는 가
를 점검한다.

제9조의2(영향평가 수행) ① 개인정보파일을 구축·운영 또는 변경하고자 하는
공공기관의 장은 별표 4의 필요한 사항이 반영될 수 있도록 설계완료 전에
영향평가를 수행하여야 한다.

② 공공기관의 장이 개인정보파일을 구축·운영 또는 변경하고자 할 때에는
제1항의 영향평가 결과를 반영한 조치를 이행하고 그 결과를 보호위원회에
제출하여야 한다.

제9조의3(영향평가 개선계획 반영여부의 확인) 공공기관의 장은 개인정보 영향
평가 수행 후, 영향평가 개선계획의 반영여부를 정보시스템 감리 시 확인하
여야 한다. 단, 감리를 수행하지 않은 경우에는 정보시스템 테스트단계에서
영향평가 개선계획의 반영여부를 확인하여야 한다.

제10조(평가영역 및 평가분야) 영 제38조제1항의 영향평가기준에 따른 평가영
역은 별표 4와 같다. 다만, 대상기관이 1년 이내에 다른 정보시스템의 영향평
가를 받은 경우에는 대상기관의 개인정보 보호 관리체계에 대한 평가는 생략
할 수 있다.

제11조(평가항목) ① 평가기관은 별표 4에 따라 적합한 평가항목을 선정하여
영향평가를 수행하여야 한다. 다만, 대상기관이 1년 이내에 이미 평가받은
항목은 그 변경이 없는 때에는 평가항목에서 제외된다.

② 별표 4에 명시되지 않은 특화된 IT기술을 적용하는 경우에는 해당 기술이
개인정보 보호에 미치는 영향에 대한 평가항목을 개발하여 영향평가 시 반영
하여야 한다.

제12조(영향평가서의 제출) 영 제38조제2항에 따라 영향평가서를 제출받은 대
상기관의 장은 2개월 이내에 평가결과에 대한 내부승인 절차를 거쳐 영향평
가서를 보호위원회에 제출하여야 한다.

제13조(영향평가 수행안내서) 보호위원회는 영향평가에 필요한 세부기준 및 절
차, 평가항목 등을 구체화하는 “영향평가 수행안내서”를 마련하여 제공할
수 있다.

제14조(영향평가 개선사항 이행) 영 제38조제2항에 따라 영향평가서를 제출받
은 공공기관의 장은 개선사항으로 지적된 부분에 대한 이행계획 등을 별지
제8호서식에 따라 영향평가서를 제출받은 날로부터 1년 이내에 보호위원회
에 제출하여야 한다.

제15조(재검토 기한) 보호위원회는 「훈령·예규 등의 발령 및 관리에 관한 규
정」에 따라 이 고시에 대하여 2020년 8월 11일을 기준으로 매 3년이 되는
시점(매 3년째의 8월 10일까지를 말한다)마다 그 타당성을 검토하여 개선 등
의 조치를 하여야 한다.

개인정보파일을 새로 구축하거나 변경하고자 하는 때에는 미리 해당 파일의 내용에 법령 위반 소지는 없는지 또는 해당 파일에 사생활 침해 위험이 잠재되어 있지는 않는지 등을 미리 조사·평가하게 하는 것이 개인정보파일에 대한 정보주체의 신뢰를 확보하고 개인정보 피해를 예방하는 길이 된다.

1. 개인정보 영향평가의 의의

‘개인정보 영향평가’ (PIA, Privacy Impact Assessment)란 개인정보 수집·활용이 수반되는 사업 추진시 개인정보 오남용으로 인한 프라이버시 침해 위험이 잠재되어 있지 않는지를 조사·예측·검토하고 개선하는 제도이다.

법 제33조는 개인정보 영향평가를 ‘개인정보파일의 운용으로 인하여 정보주체의 개인정보 침해가 우려되는 경우에 그 위험요인을 분석하고 개선사항을 도출하기 위한 평가’라고 정의하고 있다(제1항).

개인정보 영향평가제도의 목적은 평가대상 시스템 활용에 따른 잠재적 위험을 평가하여 개인정보 침해에 따른 피해를 줄일 수 있는지를 미리 검토·반영하는 것이다.

미국은 「전자정부법」 제208조에 전자정부 구현 과정에서 개인정보 및 프라이버시 보호를 위하여 개인정보 영향평가를 명문화 하였고, 캐나다도 2002년부터 공공부문에 대한 개인정보 영향평가를 의무화하고 있다. 유럽 연합(EU) 또한 「일반 개인정보 보호법」(GDPR) 제35조에 개인정보 영향평가를 명문화하면서 일정한 경우 공공·민간부문에 대한 개인정보 영향평가를 의무화하고 있다. 그밖에 뉴질랜드·홍콩·호주 등에서도 공공·민간부문에 대하여 개인정보 영향평가를 권장하고 있다.

< 국가별 PIA제도 비교 >

구 분	미 국	캐나다	EU	뉴질랜드
시행대상	연방정부기관	연방정부기관 및 일부 지방정부	민간·공공	민간·공공 자율
관련근거	전자정부법(2002), 관리예산처 지침	개인정보 영향평가 지침	일반 개인정보 보호법(GDPR)	개인정보 영향평가 지침
평가주체	사업 수행기관 (자체평가)	사업 수행기관 (자체평가)	사업 수행기관 (자체평가)	외부평가 중심
감독 및 평가결과 제출처	관리예산처	프라이버시 감독관	개인정보 감독기구	-
강제성 유무	의무사항	-	-	권고사항

구 분	미 국	캐나다	EU	뉴질랜드
평가결과 활용	웹사이트, 관보, 그 밖의 다른 수단으로 공개	웹사이트, 책자를 통해 두 개 이상의 공식 언어로 요약해 공개	-	-

2. 영향평가 대상 개인정보파일

공공부문의 경우 전자정부 추진으로 개인정보를 대량으로 시스템화하여 상호 연동하는 등 개인정보 침해 우려가 높으므로 행정정보 공유 및 전자정부 추진사업의 신뢰성을 제고하기 위하여 영향평가를 의무화하고 있다.

다만, 공공기관이 구축·운영·변경하는 모든 개인정보파일에 대하여 영향평가를 수행하게 하는 것은 예산 낭비를 초래할 수 있으므로 각 호에 해당하는 개인정보파일에 한하여 영향평가를 의무화하고 있다.

영향평가 대상 개인정보파일(영 제35조)

1. 민감정보 또는 고유식별정보의 처리가 수반되는 개인정보파일 : 구축·운영 또는 변경하려는 개인정보파일에 5만명 이상의 정보주체에 관한 개인정보가 포함된 경우
2. 다른 개인정보파일과 연계하려는 경우 : 해당 공공기관 내부 또는 외부에서 구축·운영하고 있는 다른 개인정보파일과 연계한 결과 50만명 이상의 정보주체에 관한 개인정보가 포함된 경우
3. 일반적인 개인정보 파일 : 구축·운영 또는 변경하려는 개인정보파일에 100만명 이상의 정보주체에 관한 개인정보가 포함된 경우
4. 영향평가를 받은 후 개인정보 검색 체계 등 개인정보파일의 운용 체계를 변경하려는 경우 : 해당 개인정보파일 중 변경된 부분

한편, 현 시점 기준으로 영 제35조에 따른 영향평가 대상은 아니나 가까운 시점(1년 이내)에 정보주체의 수가 동조의 기준을 초과할 것이 확실한 경우 영향평가를 수행할 수 있다.

3. 영향평가의 수행방법 등

공공기관의 장이 개인정보 영향평가를 수행하고자 하는 경우에는 보호위원회가 지정하는 평가기관 중에서 의뢰하여야 한다. 평가기관이란 영향평가 수행에 필요한 업무수행실적, 전문인력, 안전한 사무실·설비 등의 지정요건을 갖춘 법인으로 지정절차를 거쳐 보호위원회가 평가기관으로 지정한 기관을 말한다(「개인정보 영향평가에 관한 고시」 제2조제3호 참고). 영향평가를 하는 경우에는 다음 각 호의 사항을 고려하여야 한다.

영향평가지 고려사항(제33조제2항, 영 제36조)

1. 처리하는 개인정보의 수
2. 개인정보의 제3자 제공 여부
3. 정보주체의 권리를 해할 가능성 및 그 위험 정도
4. 민감정보 또는 고유식별정보의 처리 여부
5. 개인정보 보유기간

영향평가 시 평가기관은 평가기준에 따라 주관적인 견해를 배제하여 객관적인 평가를 수행하여야 하며, 영향평가서를 작성할 때에는 신의에 따라 성실하게 개인정보 영향평가를 수행하고 거짓으로 영향평가서를 작성하여서는 안 된다. 또한, 평가기관은 다른 법인(업체)에게 평가기관의 상호를 사용하여 개인정보 영향평가를 수행하도록 하여서는 아니 된다.

4. 개인정보 영향평가 결과의 활용

공공기관의 장이 개인정보 영향평가를 수행한 때에는 그 결과를 보호위원회에 제출하여야 한다(제1항). 이 경우 보호위원회는 제출받은 영향평가 결과에 대하여 의견이 있을 때에는 해당 공공기관에 의견을 제시할 수 있다(제3항). 또한 공공기관의 장은 보호위원회에 개인정보파일을 등록할 때에는 개인정보 영향평가 결과도 함께 첨부하여야 한다(제4항).

5. 영향평가 활성화 기반 마련

가 전문가 육성 등 활성화 기반 마련

보호위원회는 영향평가의 활성화를 위하여 관계 전문가의 육성, 영향평가 기준의 개발·보급 등 필요한 조치를 마련하여야 한다.

나 개인정보 영향평가기관의 지정 및 지정취소

1) 평가기관 지정요건

보호위원회는 다음 각 호의 요건을 모두 갖춘 법인을 개인정보 영향평가기관으로 지정할 수 있다. 여기서 지정은 사실상 ‘허가’의 의미를 갖는다. 즉 다음 각 호의 모든 요건을 갖춘 법인의 신청이 있으면 무조건 지정을 해야 하는 것이 아니라 시장 수요 등을 고려하여 지정 여부를 결정할 수 있다.

보호위원회로부터 평가기관으로 지정받기 위한 요건은 다음 각 호와 같다.

평가기관 지정요건(영 제37조제1항)

1. 최근 5년간 다음 각 목의 어느 하나에 해당하는 업무 수행의 대가로 받은 금액의 합계액이 2억원 이상인 법인
 - 가. 영향평가 업무 또는 이와 유사한 업무
 - 나. 「전자정부법」 제2조제13호에 따른 정보시스템(정보보호시스템을 포함한다)의 구축 업무 중 정보보호컨설팅 업무(전자적 침해행위에 대비하기 위한 정보시스템의 분석·평가와 이에 기초한 정보보호 대책의 제시 업무를 말한다. 이하 같다)
 - 다. 「전자정부법」 제2조제14호에 따른 정보시스템 감리 업무 중 정보보호컨설팅 업무
 - 라. 「정보보호산업의 진흥에 관한 법률」 제2조제2호에 따른 정보보호산업에 해당하는 업무 중 정보보호컨설팅 업무
 - 마. 「정보보호산업의 진흥에 관한 법률」 제23조제1항제1호 및 제2호에 따른 업무
2. 별표 1에 따른 전문인력을 10명 이상 상시 고용하고 있는 법인
3. 다음 각 목의 사무실 및 설비를 갖춘 법인
 - 가. 신원 확인 및 출입 통제를 위한 설비를 갖춘 사무실
 - 나. 기록 및 자료의 안전한 관리를 위한 설비

개인정보 영향평가 업무란 개인정보를 활용하는 새로운 정보시스템 도입이나 개인정보 취급이 수반되는 기존 정보시스템의 중대한 변경 시 동 시스템의 구축·운영·변경 등이 프라이버시에 미치는 영향에 대하여 사전에 조사·예측·검토하여 개선방안을 도출하는 업무를 말한다.

정보보호컨설팅 업무란 정보보호 관리체계 점검, 정보자산의 취약점 분석 등을 통해 비밀성, 무결성, 가용성 등을 확보하도록 지원하는 업무로 「전자정부법」 제2조제13호에 따른 정보시스템(정보보호시스템을 포함한다)의 구축업무 중 정보보호컨설팅 업무로 전자적 침해행위에 대비하기 위한 정보시스템의 분석·평가와 이에 기초한 정보 보호 대책의 제시 업무, 「전자정부법」 제2조제14호에 따른 정보시스템 감리 업무 중 정보보호컨설팅 업무, 「정보보호산업의 진흥에 관한 법률」 제2조제2호에 따른 정보보호산업에 해당하는 업무 중 정보보호컨설팅업무, 동법 제23조제1항제1호 및 제2호에 따른 업무가 포함된다.

정보시스템감리업무란 발주자와 사업자 등의 이해관계로부터 독립된 자가 정보시스템의 효율성을 향상시키고 안전성을 확보하기 위하여 제3자의 관점에서 정보시스템의 구축 및 운영 등에 관한 사항을 종합적으로 점검하고 문제점을 개선하도록 하는 업무를 말한다.

평가기관이 보유해야 하는 전문인력은 일반수행인력과 고급수행인력으로 구분되는데, 일반수행인력으로는 다음과 같은 자가 해당된다(「개인정보 영향평가에 관한 고시」 제5조).

- 한국인터넷진흥원이 시행하는 정보보호전문가(SIS) 자격을 취득한 후 1년 이상 개인정보 영향평가 관련 분야에서 업무를 수행한 경력이 있는 사람

정보보호전문가(SIS: Specialist for Information Security)는 한국인터넷진흥원에서 주관하는 자격증으로서, 정보보호 분야의 전문기술 및 실무경험을 갖춘 능력을 검정하고 정보보호 전문인력의 수요에 대응하기 위해 개발·시행된 자격제도이다.

※ 정보보호전문가(SIS) 자격증은 2013년 폐지되었고 기존 취득자에 한하여 적용된다.

- 「전자정부법」 제60조에 따른 감리원(ISA) 자격을 취득한 후 1년 이상 개인정보 영향평가 관련 분야에서 업무를 수행한 경력이 있는 사람

정보시스템감리사(ISA : Information Systems Auditor)는 한국정보화진흥원에서 주관하는 자격증으로 국가 주요 정보사업에 대한 감리체계의 확립과 실제 감리작업을 수행할 수 있는 전문인력을 양성하기 위하여 도입 실시되는 국가공인 민간자격증이다.

- 「국가기술자격법」에 따른 정보통신 직무분야의 국가기술자격 중 정보관리기술사, 컴퓨터시스템응용기술사, 정보통신기술사, 전자계산기조직응용기사, 정보처리기사 또는 정보통신기사 기술자격을 취득한 후 1년 이상 개인정보 영향평가 관련 분야에서 업무를 수행한 경력이 있는 사람

「국가기술자격법 시행규칙」 제3조에 따른 전자계산기조직응용기사·정보관리기술사·정보처리기사·컴퓨터시스템응용기술사·정보통신기술사·정보통신기사 자격을 취득한 자로서, 개인정보 취급 정보시스템을 개발·운영·유지·보수 등을 통해 안전하게 관리하는 업무를 수행한다.

- 국제정보시스템감사통제협회의 공인정보시스템감사사(CISA) 자격을 취득한 후 1년 이상 개인정보 영향평가 관련 분야에서 업무를 수행한 경력이 있는 사람

공인정보시스템감사사(CISA : Certified Information Systems Auditor)는 정보시스템감사통제협회(ISACA)에서 일정한 자격 요건을 갖춘 사람들에게 부여하는 ‘정보시스템 지배, 통제, 보안 및 감사 분야의 공인 전문 자격증’으로 경영 전략과 조직관리, 정보시스템 기반 기술, 정보시스템 보안 및 위험관리, 정보시스템 개발 및 프로젝트 관리, BPR과 전자상거래 등의 분야에 대한 체계적인 지식과 실무 경험을 보유하고 있다고 볼 수 있다.

- 국제정보시스템보안자격협회의 공인정보시스템보호전문가(CISSP) 자격을 취득한 후 1년 이상 개인정보 영향평가 관련 분야에서 업무를 수행한 경력이 있는 사람

공인정보시스템보호전문가(CISSP : Certified Information Systems Security Professional)는 ISC2(International Information Systems Security Certification Consortium)에서 주관하는 자격증으로 이 자격증을 취득한 자는 기업이 견고한 보안 수행을 구현하고, 위험분석을 수행하고, 필요한 대책을 파악하고, 그리고 전체 조직이 시설, 네트워크, 시스템, 그리고 정보를 보호하는 작업을 도와줄 수 있는 기술적 능력, 지식, 경험을 가진 자라고 볼 수 있다.

- 개인정보보호와 관련된 자격으로서 보호위원회가 정하는 자격을 취득한 후 1년 이상 개인정보 영향평가 관련 분야에서 업무를 수행한 경력이 있는 사람

“개인정보 영향평가 관련 분야에서 업무를 수행한 경력이 있는 사람”이란 공공기관, 법인 및 단체 등의 임직원으로 개인정보보호를 위한 공통기반기술(암호기술, 인증기술 등을 말한다), 시스템·네트워크 보호(시스템 보호, 해킹·바이러스 대응, 네트워크 보호 등을 말한다) 또는 응용서비스 보호(전자거래 보호, 응용서비스 보호, 정보보호 표준화 등을 말한다)에 해당되는 분야에서 계획, 분석, 설계, 개발, 운영, 유지·보수, 감리, 컨설팅 또는 연구·개발 업무 등을 수행한 경력이 있는 사람을 말한다.

- 한국CPO포럼이 시행하는 개인정보관리사(CPPG) 자격을 취득한 후 1년 이상 개인정보 영향평가 관련 분야에서 업무를 수행한 실적이 있는 사람

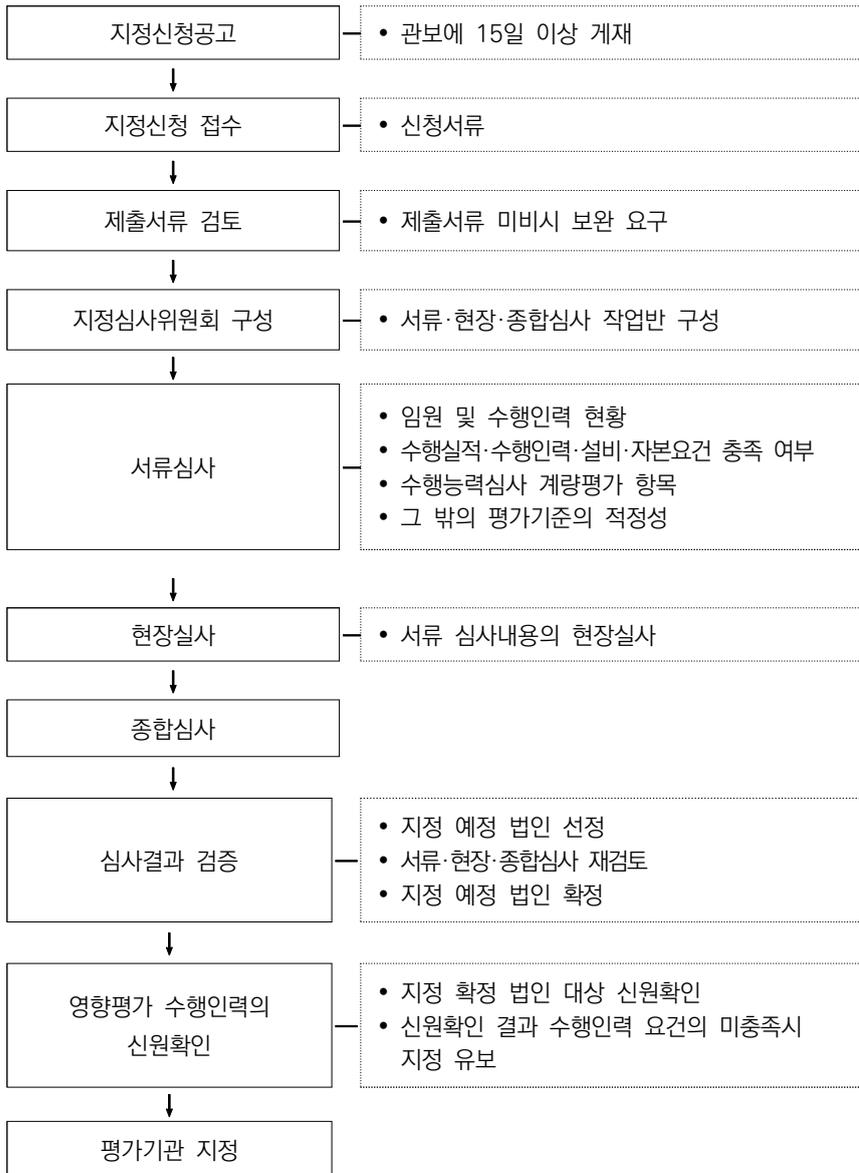
개인정보관리사(CPPG)는 개인정보보호 정책 및 대처 방법론에 대한 지식 및 능력을 검정하기 위해 개발·시행된 자격제도로써 한국CPO포럼이 주관하는 자격증이다.

고급수행인력의 자격은 ① 일반수행인력의 자격을 갖춘 후 5년 이상의 영향평가 관련 분야 수행 실적이 있는 사람 ② 관련 분야 박사학위를 취득한 후 3년 이상의 영향평가 관련 분야 수행 실적이 있는 사람 ③ 「국가기술자격법 시행규칙」 제3조에 따른 정보관리기술사·컴퓨터시스템응용기술사·정보통신기술사자격을 취득한 후 3년 이상의 영향평가 관련 분야 수행실적이 있는 사람이 해당된다.

한편 영향평가 수행 인력은 전문교육기관인 한국인터넷진흥원의 전문교육을 이수하여야 하며, 전문교육 이수자에 대한 평가 결과에 따라 부여되는 개인정보 영향평가 전문인력 인증서를 받은 경우에 한하여 영향평가를 수행할 수 있다(「개인정보 영향평가에 관한 고시」 제5조제2항, 제6조).

2) 평가기관 지정 절차

< 개인정보 영향평가기관 지정절차 >



① 지정신청

보호위원회는 관보에 지정신청 공고에 대한 사항을 15일 이상 게재하여야 한다. 공고내용은 지정 신청 목적, 지정 기준, 지정 절차, 신청 서류, 신청방법, 접수 시기 및 문의처 등 접수에 필요한 안내사항을 포함한다(「개인정보 영향평가에 관한 고시」 제3조제2항).

평가기관으로 지정을 받으려는 자는 평가기관 지정신청서(「개인정보 처리방침에 관한 고시」 제3조제3항 별지 제3호 서식)에 정관, 대표자의 성명, 전문인력의 자격을 증명할 수 있는 서류(전자문서를 포함한다)와 「개인정보 처리방침에 관한 고시」와 「개인정보 영향 평가에 관한 고시」에 따른 제출서류를 첨부하여 보호위원회에 제출하여야 한다.

< 고시에서 정하는 서류 >

「개인정보 처리방침에 관한 고시」에 따른 제출서류	「개인정보 영향평가에 관한 고시」에 따른 제출서류
<ul style="list-style-type: none"> ① 개인정보 영향평가 수행인력 보유현황 ② 개인정보 영향평가 수행 관련 사무실 및 설비 보유현황 	<ul style="list-style-type: none"> ① 개인정보 영향평가 수행실적 명세서 ② 개인정보 영향평가 수행실적물 관리카드 ③ 개인정보 영향평가 수행인력의 경력 및 실적 증명서 ④ 개인정보 영향평가 수행인력 관리카드 ⑤ 개인정보 영향평가 수행능력 세부 심사자료 ⑥ 개인정보 영향평가 관련 기술자산 보유목록

② 지정신청서 접수 및 확인

지정 신청서류는 우편 또는 방문을 통해 접수하도록 한다. 보호위원회는 신청법인의 제출서류가 미비한 경우 보완을 요구할 수 있으며, 이에 응하지 않을 경우 접수를 반려할 수 있다. 평가기관 지정신청서를 제출받은 보호위원회는 「전자정부법」 제36조제1항에 따른 행정정보의 공동이용을 통하여 다음 각 호의 서류를 확인하여야 한다. 다만, 신청인이 제2호의 확인에 동의하지 아니하는 경우에는 신청인에게 그 서류를 첨부하도록 하여야 한다.

지정신청서 접수시 확인서류(영 제37조제3항)

1. 법인 등기사항증명서
2. 「출입국관리법」 제88조제2항에 따른 외국인등록 사실증명(외국인인 경우만 해당한다)

③ 지정심사위원회 구성·운영

보호위원회는 평가기관 지정신청을 받은 경우 지정기준의 적합여부를 심사하기 위하여 평가기관 지정심사위원회를 구성·운영한다(「개인정보 영향평가에 관한 고시」 제3조제4항). 지정심사위원회는 지정심사에 대한 투명성, 공정성, 신뢰성 등을 확보하기 위해 다음의 자격기준에 적합한 5인 이상 15인 이내의 심사위원을 구성·위촉하며, 지정심사위원의 임기는 3년으로 연임할 수 있다(「개인정보 영향평가에 관한 고시」 제4조).

- 「고등교육법」 제2조제1호·제2호 또는 제5호에 따른 대학, 산업대학, 방송대학·통신

대학·방송통신대학 및 사이버대학(이하 “원격대학” 이라 한다)이나 공인된 연구기관에서 조교수 이상의 직 또는 이에 상당하는 직에 있거나 있었던 자로 개인정보 보호 연구경력이 8년 이상인 사람

- 개인정보 보호 관련 업체, 기관 혹은 단체(협회, 조합)에서 8년 이상 개인정보 보호 업무에 근무한 사람
- 그 밖에 개인정보 보호에 관한 학식과 경험이 풍부한 사람

보호위원회는 지정심사위원회의 회의를 매년 정기적으로 개최하되, 지정심사위원회의 의결이 필요할 때에는 수시로 소집할 수 있다.

지정심사위원회는 심사에 대한 공정성 및 신뢰성 확보를 위해 학자, 연구자, 실무자, 유관기관 전문가들을 위원으로 구성되며, 서류심사·현장실사·종합심사에 대한 종합적인 사항을 검증한다. 지정심사위원회는 신청서류를 중심으로 평가기관의 적격 여부, 수행실적·수행인력·자본·설비 등의 지정요건 충족 여부 등을 심사하는데, 필요시 현장실사를 통해 적정성 및 준수여부 등 확인·점검할 수 있다. 지정심사위원회는 서류심사와 현장실사 결과를 종합하여 책임자의 자질 및 경험, 업체의 컨설팅 방법론 등 업무수행능력 요건 등을 심사한다.

④ 평가기관의 영향평가 수행능력 심사

지정심사위원회는 세부평가기준에 따라 평가기관이 지정신청시 제출한 서류를 심사하고, 보호위원회는 신청법인의 객관적인 업무수행능력이 총점 75점 이상을 취득한 기관을 대상으로 현장실사·종합심사를 거쳐 평가기관으로 지정한다. 영향평가 수행능력 심사 세부평가기준은 정량평가(60점)와 정성평가(40점)로 구분되며, 총점 100점을 기준으로 정량·정성적 측면에서 ① 경험 ② 전문성 ③ 신뢰도 ④ 영향평가 수행역량으로 평가항목을 구성하여 세부평가기준에 따라 평가한다.

< 개인정보 영향평가 수행능력심사 세부평가기준 >

구분	평가항목	세부평가항목	배점	평가지표	세부 평가 기준
I. 정량평가(60)	1.경험(25)	최근 5년간 영향평가 관련 분야 수행실적	15	계약금액 총액	<ul style="list-style-type: none"> • 5억원 이상: 배점의 100% • 5억원 미만: 배점의 x% ※ $x = (\text{계약금액총액}/5\text{억원}) \times 100$
		최근 2년간 계약금액 1천만원 이상의 영향평가 관련 분야 수행실적	10	수행건수	<ul style="list-style-type: none"> • 5건 이상: 배점의 100% • 5건 미만: 배점의 x% ※ $x = (\text{수행건수}/5\text{건}) \times 100$

	2.전문성 (25)	고급수행인력의 수	15	인원수	• 인원수 × 1점(최대 15점)
		개인정보 영향평가 전문교육 인증시험 합격자 수	10	비율	• 배점 × (개인정보보호 전문교육 인증시험 합격자 수/ 전체 평가기관 인증시험 평균 합격자 수*) ※ 평가기관 인증시험 합격자수 평균
	3. 신뢰도 (10)	신용평가등급	10	등급	• 신용평가 등급에 근거하여 평가 ※ 「개인정보 영향평가에 관한 고시」 별표1의 붙임기준
II. 정성 평가 (40)	영향평가 수행역량 (40)	영향평가 수행실적의 질적 평가	20	비계량	• 영향평가 품질제고 활동 • 영향평가 수행 대상기관 • 영향평가 수행방법의 우수성
		영향평가 수행인력의 자질 및 경험	10	비계량	※ 신청서류, 현장실사 등을 통해 평가
		지정신청법인의 자체 개인정보영향평가대책	10	비계량	• 위험분석의 타당성 • 개인정보영향평가의 적절성 • 개인정보영향평가의 실효성
III. 기타		「벤처기업육성에 관한 특별조치법」 제25조에 따라 벤처기업으로 확인을 받은 기업	가점	확인여부	※ 벤처 확인기업: 가점 5점
		지방소재(수도권제외) 기업	가점	확인여부	※ 본사 위치가 수도권을 제외한 지방에 위치하는 경우 : 가점 5점
		최근 3년간 조달법령에 따라 부정당업자로 지정되어 입찰참가가 제한을 받은 기간	감점	입찰참가 제한월수	※ 제한월수 1월당: 감점 0.5점

비 고

1. 위 표 각 세부 평가항목별 점수는 소수점 이하 둘째 자리에서 반올림한다.
2. 세부 평가기준 중 신뢰도 항목은 기업신용평가서 제출로 대체할 수 있으며 이에 대한 배점기준은 [붙임] 신용평가등급에 의한 평가기준에 따른다.
3. '최근'의 기산일은 지정공고일자를 기준으로 한다.

⑤ 지정서 교부 및 고시

보호위원회는 지정심사위원회의 심사결과를 검증하고 수행인력의 신원확인을 거쳐 최종적으로 평가기관을 지정한 경우에는 지체 없이 평가기관 지정서를 교부하고, ① 평가기관의 명칭, 주소 및 전화번호와 대표자의 성명과 ② 지정 시 조건을 붙이는 경우 그 조건의 내용을 관보에 고시하여야 한다. 해당 사항이 변경된 경우에도 또한 같다.

⑥ 평가기관 지정 취소

보호위원회는 지정된 평가기관이 다음 각 호의 어느 하나에 해당하는 경우에는 평가기

관의 지정을 취소할 수 있다. 다만, 제1호 또는 제2호에 해당하는 경우에는 평가기관의 지정을 취소하여야 한다. 보호위원회가 평가기관 지정을 취소하려는 경우에는 청문을 실시하여야 한다.

평가기관 지정취소 사유(영 제37조제5항)

1. 거짓이나 그 밖의 부정한 방법으로 평가기관의 지정을 받은 경우
2. 지정된 평가기관 스스로 지정의 취소를 원하는 경우나 폐업한 경우
3. 지정요건(영 제27조제1항)에 충족하지 못하게 된 경우
4. 지정요건 변경 등의 신고의무(영 제37조제6항)를 이행하지 아니한 경우
5. 고의 또는 중대한 과실로 영향평가 업무를 부실하게 수행하여 그 업무를 적정하게 수행할 수 없다고 인정되는 경우
6. 그 밖에 법 또는 이 영에 따른 의무를 위반한 경우

⑦ 지정요건 등 변경 신고의무

지정된 평가기관은 지정된 후 다음 각 호의 어느 하나에 해당하는 사유가 발생한 경우에는 그 사유가 발생한 날부터 14일 이내에 개인정보영향평가기관 변경사항 신고서(개인정보 처리방침에 관한 고시 제3조제5항, 별지 제7호 서식)로 보호위원회에 신고하여야 한다. 다만, 제3호에 해당하는 경우에는 그 사유가 발생한 날부터 60일 이내에 신고하여야 한다.

변경신고 등의 사유(영 제37조제6항)

1. 제1항 각 호(평가기관 지정요건)의 어느 하나에 해당하는 사항이 변경된 경우
2. 제4항제1호(평가기관 명칭, 주소, 전화번호, 대표자)에 해당하는 사항이 변경된 경우
3. 평가기관을 양도·양수하거나 합병하는 등의 사유가 발생한 경우

개인정보 영향평가는 상당한 수준의 경험과 전문성을 필요로 하므로 적정 수준의 시설·인력기준을 갖춘 기관으로 하여금 영향평가를 수행할 수 있도록 하기 위하여 지정절차를 마련하고 있다. 따라서 적정수준의 개인정보 영향평가를 지속적으로 수행하기 위해서 보호위원회로 하여금 거짓이나 부정한 방법으로 지정을 받거나, 지정 후 지정기준에 부합되지 않는 경우에 지정된 평가기관의 지정을 취소하도록 하고 있다. 한편으로는 평가기관의 전문성을 강화하고 부실평가 업무수행을 방지하기 위하여 평가기관으로 하여금 지정된 후 인력 변동, 휴업·폐업, 양도·양수, 합병 등의 변동사항이 있는 경우 신고하도록 하고 있다.

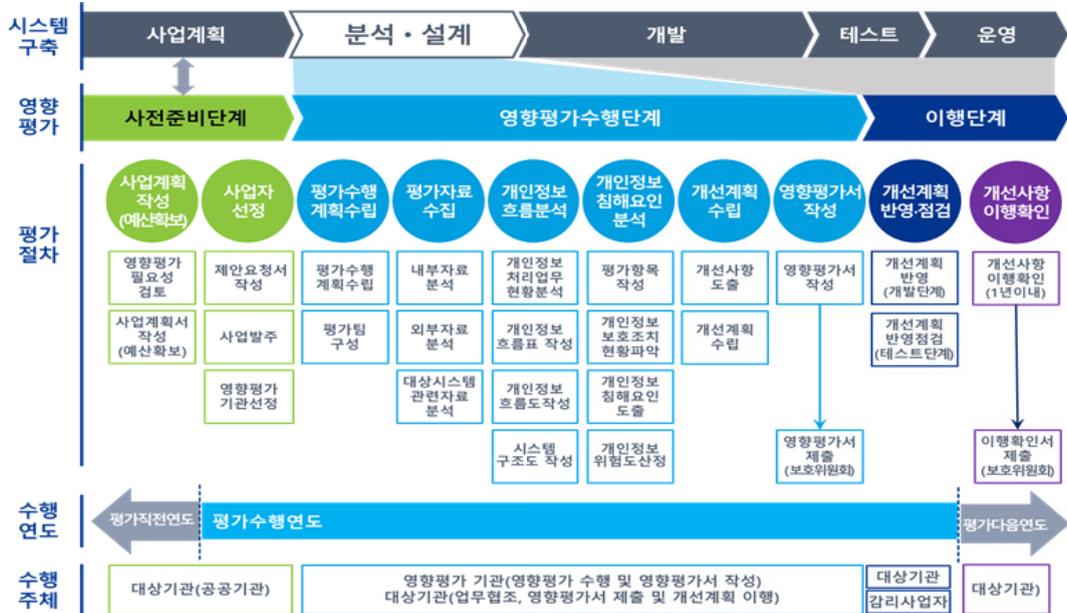
3) 개인정보 영향평가의 절차

영향평가는 개인정보파일을 구축·운영 또는 변경하거나 연계하려는 경우 발생할 수

있는 개인정보의 침해요인을 사전에 분석하여 개선하도록 하는 것이므로, 대상 공공기관이 개인정보처리시스템을 신규로 구축하거나 기존 시스템을 변경하려는 경우 대상 시스템의 설계 완료 전에 영향평가를 수행하여야 한다.

이 경우 영향평가 대상기관은 사전 준비, 영향평가 수행, 이행 단계로 영향평가를 수행한다(「개인정보 영향평가에 관한 고시」 제9조).

〈 개인정보 영향평가 절차 〉



① 사전 준비 단계

사전 준비 단계는 사업계획의 작성, 영향평가 기관 선정 순으로 진행된다. 사업계획의 작성 단계에서는 정보화사업을 추진하는 과정에서 개인정보의 신규 수집·이용·연계 또는 처리절차상 변경 등이 발생하는지에 대해 영향평가 필요성 검토서 작성을 통해 영향평가 필요성을 판단하고, 영향평가 사업계획서(예산확보 관련 내용 포함)를 작성한다. 한편, 영향평가 기관 선정은 보호위원회가 지정한 영향평가기관 중에서 선정해야 한다.

② 영향평가 수행 단계

영향평가 수행 단계는 영향평가 수행계획 수립, 평가자료 수집, 개인정보 흐름 분석, 개인정보 침해요인 분석, 개선계획 수립, 영향평가서 작성 순으로 진행된다.

영향평가 수행계획 수립 단계에서는 효율적인 영향평가 수행을 위하여 사업 주관부서가 영향평가팀을 구성하여 영향평가 수행계획을 수립한다. 한편, 수립한 계획서는 착수회

의를 통해 영향평가팀은 물론 당해 사업과 관련하여 협조가 필요한 유관 부서, 외부기관, 외부 전문가 등과 공유해야 한다.

< 영향평가 수행계획서 작성 예시 >

목적	주요 내용	참고자료
1. 평가 목적	• 영향평가 수행 필요성 및 추진 배경 등	• 필요성 검토 질문서
2. 평가 대상	• 평가대상이 되는 정보화사업(정보시스템)명칭 기술	• 제안요청서(RFP), 사업계획서 등
3. 평가 주체	• 영향평가팀 구성 현황	• 영향평가팀 구성 및 운영 계획서
4. 평가 기간	• 영향평가 착수시점부터 완료시점까지의 평가기간을 산정하여 기술	• 영향평가기관 선정 단계에서 산출물 및 협의내용, 영향평가 수행안내서 참고
5. 평가절차 (방법)	• 영향평가 수행안내서 등을 참조하여 평가 절차 및 단계별 주요 수행사항 및 기간 등 기술	
6. 주요 평가사항	• 중점적으로 평가되어야 하는 사항 기술	
7. 평가기준 및 평가항목	• 영향평가 수행안내서에서 표준적으로 요구되는 평가항목(표)과 해당 사업의 특정 IT 기술 활용 여부 확인 ※ 부록으로 영향평가 목록 첨부	
8. 자료수집 및 분석계획	• 영향평가 수행 시 분석하여야 하는 관련 참고자료를 확인하여 해당 기관과 관련있는 자료 파악	• 개인정보 관련 정책, 법규 검토 단계의 산출물 참조
9. 평가결과의 정리	• 영향평가 결과로 도출된 산출물(보고서)과 이를 활용하여 당해 사업에 적용하기 위한 방안 등 기술	• 영향평가팀 회의 내용 등 참조
10. 품질관리 방안	• 영향평가 결과의 품질 보장을 위한 상세 방안 기술	• 영향평가 품질검토 체크리스트 등 참고

평가자료의 수집 단계에서는 평가 대상사업 및 개인정보 보호 관련 내·외부 정책환경을 분석하기 위하여 개인정보 보호 관련 법규 및 상위기관의 지침과 해당기관의 내부 규정현황을 파악하고, 당해 사업을 이해하고 분석하기 위해 필요한 자료 등의 취합·분석이 이루어진다.

< 분석 자료 >

항목	수집 목적	수집 대상 자료
내부 정책 자료	• 기관 내부의 개인정보 보호체계, 규정, 조직 현황 등을 분석	• 기관 내 개인정보 보호 규정 • 기관 내 정보보안 관련 규정 • 기관 내 직제표 등
	• 개인정보취급자(정보시스템 운영자, 처리자자 등), 위탁 업체 등에 대한 내부 규정 및 관리·교육체계 확인	• 개인정보 관련 조직 내 업무 분장표 및 직급별 권한 • 정보시스템의 접근권한에 대한 내부 규정 • 위탁업체 관리 규정 등 • 시스템 운영자 및 정보취급자에 대한 교육계획

항목	수집 목적	수집 대상 자료
외부 정책 자료	• 개인정보 보호 정책환경 분석	• 개인정보 보호법, 관련 지침 등 • 개인정보 보호 기본계획 등
	• 영향평가 대상사업의 특수성을 반영한 정책 환경 분석	• 평가대상사업의 추진 근거 법률 및 개인정보 보호 관련 법령
대상시스템 설명 자료	• 정보시스템을 통해 수집되는 개인정보의 양과 범위가 해당 사업 수행을 위해 적절한지 파악	• 사업 수행 계획서, 요건 정의서 • 제안서, 업무기능분해도 • 업무흐름도, 화면설계서
	• 정보시스템의 외부연계 여부 검토	• 위탁 계획서, 연계 계획서 • 인터페이스 정의서 • 메뉴 구조도
	• 시스템 구조와 연계된 개인정보 보호 기술 현황 파악	• 침입차단시스템 등 보안 시스템 구조도 • 인터페이스 정의서

개인정보 흐름 분석이란 대상사업에서 처리되는 개인정보 흐름에 대한 파악을 위해 정보시스템 내 개인정보 흐름을 분석하는 작업을 말한다. 개인정보 흐름 분석 단계에서는 대상시스템을 면밀히 분석하고 업무를 정의하여 해당 사업을 통해 처리되는 업무 중 개인정보 취급이 수반되는 업무를 도출하여 평가범위를 명확히 한다.

개인정보의 침해요인 분석 단계에서는 개인정보의 흐름에 따른 개인정보 조치사항 및 계획 등을 파악하고 개인정보 침해 위험성을 도출한다.

개선계획 수립 단계에서는 개인정보 침해 요인별 위험도 분석에 기반하여, 위험요소를 제거하거나 최소화하기 위한 개선방안을 도출하고 개선계획을 수립하며, 위험정도에 따라 단기, 중·장기적인 개선방안을 제시할 수 있다.

영향평가서 작성 단계에서는 영향평가 추진경과 및 중간산출물 등의 내용을 정리하고 도출된 위험요소 및 개선계획 등 최종산출물을 모두 취합하여 작성한다.

③ 영향평가 이행 단계

영향평가 이행단계는 개선사항 반영여부 점검, 개선사항 이행 확인 순으로 진행한다.

개선사항 반영여부 점검 단계는 분석 및 설계단계에서 수행한 영향평가 개선계획의 반영 여부를 개인정보파일 및 개인정보처리시스템의 구축 및 운영 전에 확인하는 단계이다.

개선사항 이행 확인 단계는 영향평가 시 도출된 개선계획이 예정대로 수행이 되고 있는지 여부를 점검하는 단계이다. 평가기관으로부터 영향평가서를 제출받은 공공기관의 장은 개선사항 이행 현황을 영향평가서를 제출받은 날로부터 1년 이내에 보호위원회에 제출하여야 한다(「개인정보 영향평가에 관한 고시」 제14조).

4) 영향평가 기준

평가기관이 개인정보 영향평가를 할 때에는 다음 각 호의 평가기준에 따라서 하여야 한다. 아래에서 보는 바와 같이 평가기관은 처리되는 개인정보의 종류·성질, 데이터의 양(규모), 시스템 환경, 침해 위험 등을 종합적으로 고려하여야 한다.

평가기준(영 제38조제1항)

1. 해당 공공기관에서 처리하는 개인정보의 종류·성질 및 정보주체의 수 및 그에 따른 개인정보 침해의 가능성
2. 법 제24조제3항, 법 제25조제6항 및 법 제29조에 따른 안전성 확보 조치의 수준 및 이에 따른 개인정보 침해의 가능성
3. 개인정보 침해의 위험요인별 조치 여부
4. 그 밖에 법 및 이 영에 따른 필요적 조치 또는 의무 위반 요소에 관한 사항

평가기관은 아래의 표에 따라 적합한 평가항목을 선정하여 영향평가를 수행하여야 한다 (「개인정보 영향평가에 관한 고시」 제10조, 제11조).

<개인정보 영향평가의 평가영역 및 평가분야>

평가 영역	평가 분야	세부 분야
I. 대상기관 개인정보 보호 관리체계	1. 개인정보 보호 조직	개인정보 보호책임자의 지정
		개인정보 보호책임자 역할수행
	2. 개인정보 보호 계획	내부관리계획 수립
		개인정보 보호 연간계획 수립
3. 개인정보 침해대응	침해사고 신고 방법 안내	
	유출사고 대응	
4. 정보주체 권리보장	정보주체 권리보장 절차 수립	
	정보주체 권리보장 방법 안내	
II. 대상시스템의 개인정보 보호 관리체계	5. 개인정보취급자 관리	개인정보취급자 지정
		개인정보취급자 관리·감독
	6. 개인정보파일 관리	개인정보파일대장 관리
개인정보파일 등록		
7. 개인정보처리방침	개인정보처리방침의 공개	
	개인정보처리방침의 작성	
III. 개인정보 보호 처리단계별 보호조치	8. 수집	개인정보 수집의 적합성
		동의 받는 방법의 적절성
	9. 보유	보유기간 산정
		개인정보 제공의 적합성
	10. 이용·제공	목적 외 이용·제공 제한
		제공시 안전성 확보
11. 위탁	위탁사실 공개	
	위탁 계약	
	수탁사 관리·감독	

평가 영역	평가 분야	세부 분야
IV. 대상시스템의 기술적 보호조치	12. 파기	파기 계획 수립
		분리보관 계획 수립
		파기대장 작성
	13. 접근권한 관리	계정 관리
		인증 관리
		권한 관리
	14. 접근통제	접근통제 조치
		인터넷 홈페이지 보호조치
		업무용 모바일기기 보호조치
	15. 개인정보의 암호화	저장시 암호화
		전송시 암호화
	16. 접속기록의 보관 및 점검	접속기록 보관
		접속기록 점검
		접속기록 보관 및 백업
	17. 악성프로그램 등 방지	백신 설치 및 운영
		보안업데이트 적용
	18. 물리적 접근방지	출입통제 절차 수립
		반출·입 통제 절차 수립
	19. 개인정보의 파기	안전한 파기
	20. 기타 기술적 보호조치	개발 환경 통제
		개인정보처리화면 보안
출력시 보호조치		
21.개인정보처리구역보호	보호구역지정	
V. 특정 IT기술 활용시 개인정보 보호	22. CCTV	CCTV 설치시 의견수렴
		CCTV 설치 안내
		CCTV 사용 제한
		CCTV 설치 및 관리에 대한 위탁
	23. RFID	RFID 이용자 안내
		RFID 태그부착 및 제거
	24. 바이오정보	원본정보 보관시 보호조치
	25. 위치정보	개인위치정보 수집 동의
		개인위치정보 제공시 안내사항

평가기관은 개인정보를 취급하는 정보시스템이 안전성을 확보하고, 영향평가 시 모든 침해요인을 도출하여 개선할 수 있도록 필요한 평가항목을 선정하고, 그에 따라 개선방안을 제시하여야 한다. 단, 동일 대상기관이 같은 해에 여러 영향평가를 수행할 경우, 중복된 평가내용에 대해서는 이전의 평가결과로 대체할 수 있다.

예를 들어 OO기관이 A시스템의 영향평가(평가 완료)와 B시스템의 영향평가(평가 개시)를 같은 해에 진행하게 되어, 평가영역 및 평가분야(대상기관의 개인정보보호 관리체계)의 변화가 없을 경우 먼저 수행한 A시스템의 영향평가에서 도출된 결과내용을 B시스템의 영향평가시스템에 사용하여 중복평가를 하지 않도록 한다.

특정 IT기술 활용시 개인정보 보호에 대한 평가영역에서는 CCTV, RFID, 바이오 정보, 위치정보로 구분하여 평가항목을 구성하여 평가하도록 한다. 그러나 각각의 특정 IT기술은 그 특성에 따라 개인정보의 침해요인도 다를 수 있으므로 차별화된 평가항목을 도출하여야 한다. 표에 명시된 특정 IT기술 외에 활용하려는 IT기술이 있는 경우에는 해당 IT기술의 특성을 충분히 고려한 평가항목을 개발하여 적용하고, 그에 따른 침해요인의 분석결과를 바탕으로 개선방안을 도출하여야 한다.

5) 영향평가서 작성·송부·제출 등

공공기관으로부터 영향평가의 의뢰를 받은 평가기관은 평가기준에 따라 개인정보파일의 운영으로 인한 개인정보 침해의 위험요인을 분석·평가한 후 단계별 결과물을 포함한 영향평가서로 작성하여 대상기관의 장으로부터 승인을 받아 해당 공공기관의 장에게 송부하여야 한다. 영향평가서에는 개인정보파일의 운용과 관련된 사업의 개요 및 개인정보파일 운용의 목적, 영향평가 대상 개인정보파일의 개요, 평가기준에 따른 개인정보 침해의 위험요인에 대한 분석·평가 및 개선이 필요한 사항, 영향평가 수행 인력 및 예산이 포함되어야 한다.

또한 평가기관은 대상기관과의 계약 해지 및 평가 완료 후에는 평가수행을 위해 대상기관이 제공한 서류, 도구, 장비 등 일체를 대상기관의 장에게 반환하여야 하며, 반환이 불가능한 경우에는 대상기관의 승인 하에 관련 자료 등을 안전하게 파기하여야 한다.

평가기관으로부터 영향평가서를 송부 받은 공공기관의 장은 개인정보파일의 구축·운영에 앞서 해당 영향평가서를 보호위원회에 제출하여야 한다. 만약 영향평가서에 개선 필요 사항이 포함된 경우에는 그에 대한 조치 내용도 포함하여야 한다.

6) 사후관리

보호위원회는 평가기관 지정 후 인력변동, 휴업·폐업, 양도·양수, 합병 등으로 인한 변동사항이 있는지 여부와 평가기관이 심사 당시의 평가기준에 적합한지 여부를 확인할 수 있으며, 이를 위하여 현장실사, 관련 자료 등의 제출을 요구할 수 있다.

또한, 평가기관은 영향평가 수행구역 및 설비에 대한 보호대책, 영향평가 수행 인원에 대한 보호대책, 문서 및 전산자료에 대한 보호대책, 그 밖에 일반 관리적 보호대책을 수립·시행하여야 하며, 보호위원회는 그 준수여부를 감독할 수 있다.

< 개인정보 영향평가기관 보호대책의 주요 내용 >

항 목	주 요 내 용
I. 영향평가 수행구역 및 설비에 대한 보호대책	<ol style="list-style-type: none"> 영향평가를 수행하는 구역을 지정하여야 한다. 이 구역은 해당 영향평가 수행인력이 아닌 자의 출입이 제한되어야 한다. 영향평가 분석자료를 처리·전송·저장하는 정보통신망에 대하여 위험분석에 따른 통제대책을 강구하여야 한다. 이 경우 노트북 컴퓨터, 그 밖에 휴대용 정보처리기기에 대한 통제대책을 포함하여야 한다.
II. 영향평가 수행인원에 대한 보호대책	<ol style="list-style-type: none"> 영향평가 수행인력이 관계법령에 따르는 비밀유지의무를 포함한 제반의무를 숙지하고 이의 준수를 약속하는 내용의 서약서를 작성하는 지침과 절차를 마련하여야 한다. 영향평가 수행인력을 채용할 때의 적격 심사와 퇴직할 때의 퇴직자 관리를 위한 지침과 절차를 마련하여야 한다. 영향평가 수행인력이 평가기관의 보안대책을 위반하는 경우의 제재 및 처리에 관한 내부규정을 마련하여야 한다. 영향평가 수행인력을 포함한 임직원이 정기적으로 업체 내부 및 외부의 개인정보 영향평가 교육을 받을 수 있도록 하여야 한다.
III. 문서 및 전산 자료에 대한 보호대책	<ol style="list-style-type: none"> 영향평가 분석자료(부수자료를 포함한다)를 보호하기 위하여 법 제12조의 표준개인정보보호지침에 따른 보안대책을 마련하여야 한다. 영향평가 수행인력이 아닌 자는 영향평가 분석자료에 접근·열람하거나 편집·반출·폐기하지 못하도록 통제대책을 강구하여야 한다. 정보통신망을 통하여 처리·전송·저장하는 영향평가 분석자료에 대하여 위험분석에 따른 통제대책을 강구하여야 한다. 서면, 도면, 마이크로필름·전산출력물 등 출력물 형태의 영향평가 분석자료에 대한 보관·복사·배포·파기 등에 관한 통제대책을 강구하여야 한다.
IV. 일반 관리대책	<ol style="list-style-type: none"> 영향평가에 관한 평가기관의 기본방침을 대표자가 서면으로 공표하고 영향평가 수행인력을 포함한 임직원이 이를 숙지하여야 한다. 영향평가업무에 대한 위험분석 및 통제대책의 관리·운영실태를 주기적으로 점검·평가하여야 한다.

7) 영향평가 수행안내서

보호위원회는 영향평가에 관한 일반적인 개요, 영향평가에 필요한 세부기준 및 절차, 평가항목 등을 구체화하는 영향평가 수행안내서를 마련하여 제공할 수 있다(영향평가 수행안내서는 개인정보 보호 종합포털(www.privacy.go.kr)에서 다운로드 가능하다).

6. 헌법기관 등에 대한 특칙

가 헌법기관의 영향평가

국회, 법원, 헌법재판소, 중앙선거관리위원회(그 소속 기관을 포함한다)의 영향평가에 관한 사항은 국회규칙, 대법원규칙, 헌법재판소규칙 및 중앙선거관리위원회규칙으로 정하는 바에 따른다.

이들 헌법기관도 공공기관에 포함되기 때문에 개인정보파일을 구축·운용 또는 변경하려고 하는 경우에는 영향평가를 실시하여야 하나 권력분립 원칙에 따라 이들 기관의 영향평가에 관한 사항은 해당 기관의 규칙으로 정하도록 하였다.

나 민간기관의 영향평가

공공기관 외의 개인정보처리자는 개인정보파일 운용으로 인하여 정보주체의 개인정보 침해가 우려되는 경우에는 영향평가를 하기 위하여 적극 노력하여야 한다.

민간부문의 경우 개인정보 취급 양상이 분야별로 다양하여 일률적인 기준으로 개인정보 영향평가의 필요성이나 실효성을 판단하기 곤란하고 비용도 만만치 않기 때문에 자율적으로 시행하도록 하였다.

민간기관이 자율적 판단에 따라 개인정보 영향평가를 받고자 할 경우, 보호위원회가 지정하는 평가기관에 의뢰할 수 있다.

제34조 | 개인정보 유출 통지 등

법률

제34조(개인정보 유출 통지 등) ① 개인정보처리자는 개인정보가 유출되었음을 알게 되었을 때에는 지체 없이 해당 정보주체에게 다음 각 호의 사실을 알려야 한다.

1. 유출된 개인정보의 항목
2. 유출된 시점과 그 경위
3. 유출로 인하여 발생할 수 있는 피해를 최소화하기 위하여 정보주체가 할 수 있는 방법 등에 관한 정보
4. 개인정보처리자의 대응조치 및 피해 구제절차
5. 정보주체에게 피해가 발생한 경우 신고 등을 접수할 수 있는 담당부서 및 연락처

② 개인정보처리자는 개인정보가 유출된 경우 그 피해를 최소화하기 위한 대책을 마련하고 필요한 조치를 하여야 한다.

③ 개인정보처리자는 대통령령으로 정한 규모 이상의 개인정보가 유출된 경우에는 제1항에 따른 통지 및 제2항에 따른 조치 결과를 지체 없이 보호위원회 또는 대통령령으로 정하는 전문기관에 신고하여야 한다. 이 경우 보호위원회 또는 대통령령으로 정하는 전문기관은 피해 확산방지, 피해 복구 등을 위한 기술을 지원할 수 있다.

④ 제1항에 따른 통지의 시기, 방법 및 절차 등에 관하여 필요한 사항은 대통령령으로 정한다.

시행령

제39조(개인정보 유출 신고의 범위 및 기관) ① 법 제34조제3항 전단에서 “대통령령으로 정한 규모 이상의 개인정보”란 1천명 이상의 정보주체에 관한 개인정보를 말한다.

② 법 제34조제3항 전단 및 후단에서 “대통령령으로 정하는 전문기관”이란 각각 한국인터넷진흥원을 말한다.

제40조(개인정보 유출 통지의 방법 및 절차) ① 개인정보처리자는 개인정보가 유출되었음을 알게 되었을 때에는 서면등의 방법으로 지체 없이 법 제34조제1항 각 호의 사항을 정보주체에게 알려야 한다. 다만, 유출된 개인정보의 확산 및 추가 유출을 방지하기 위하여 접속경로의 차단, 취약점 점검·보완, 유출된 개인정보의 삭제 등 긴급한 조치가 필요한 경우에는 그 조치를 한 후 지체 없이 정보주체에게 알릴 수 있다.

② 제1항에도 불구하고 개인정보처리자는 같은 항 본문에 따라 개인정보가 유출되었음을 알게 되었을 때나 같은 항 단서에 따라 유출 사실을 알고 긴급한 조치를 한 후에도 법 제34조제1항제1호 및 제2호의 구체적인 유출 내용을 확인하지 못한 경우에는 먼저 개인정보가 유출된 사실과 유

출이 확인된 사항만을 서면등의 방법으로 먼저 알리고 나중에 확인되는 사항을 추가로 알릴 수 있다.

③ 제1항과 제2항에도 불구하고 법 제34조제3항 및 이 영 제39조제1항에 따라 1천명 이상의 정보주체에 관한 개인정보가 유출된 경우에는 서면등의 방법과 함께 인터넷 홈페이지에 정보주체가 알아보기 쉽도록 법 제34조제1항 각 호의 사항을 7일 이상 게재하여야 한다. 다만, 인터넷 홈페이지를 운영하지 아니하는 개인정보처리자의 경우에는 서면등의 방법과 함께 사업장등의 보기 쉬운 장소에 법 제34조제1항 각 호의 사항을 7일 이상 게시하여야 한다.

제25조(개인정보의 유출) 개인정보의 유출은 법령이나 개인정보처리자의 자유로운 의사에 의하지 않고, 정보주체의 개인정보에 대하여 개인정보처리자가 통제를 상실하거나 권한 없는 자의 접근을 허용한 것으로서 다음 각 호의 어느 하나에 해당하는 경우를 말한다.

1. 개인정보가 포함된 서면, 이동식 저장장치, 휴대용 컴퓨터 등을 분실하거나 도난당한 경우
2. 개인정보가 저장된 데이터베이스 등 개인정보처리시스템에 정상적인 권한이 없는 자가 접근한 경우
3. 개인정보처리자의 고의 또는 과실로 인해 개인정보가 포함된 파일 또는 종이문서, 기타 저장 매체가 권한이 없는 자에게 잘못 전달된 경우
4. 기타 권한이 없는 자에게 개인정보가 전달된 경우

제26조(유출 통지시기 및 항목) ① 개인정보처리자는 개인정보가 유출되었음을 알게 된 때에는 정당한 사유가 없는 한 5일 이내에 해당 정보주체에게 다음 각 호의 사항을 알려야 한다. 다만 유출된 개인정보의 확산 및 추가 유출을 방지하기 위하여 접속경로의 차단, 취약점 점검·보완, 유출된 개인정보의 삭제 등 긴급한 조치가 필요한 경우에는 그 조치를 한 후 그로부터 5일 이내에 정보주체에게 알릴 수 있다.

1. 유출된 개인정보의 항목
 2. 유출된 시점과 그 경위
 3. 유출로 인하여 발생할 수 있는 피해를 최소화하기 위하여 정보주체가 할 수 있는 방법 등에 관한 정보
 4. 개인정보처리자의 대응조치 및 피해구제절차
 5. 정보주체에게 피해가 발생한 경우 신고 등을 접수할 수 있는 담당부서 및 연락처
- ② 개인정보처리자는 제1항 각 호의 사항을 모두 확인하기 어려운 경우에는 정보주체에게 다음 각 호의 사실만을 우선 알리고, 추후 확인되는 즉시 알릴 수 있다.

1. 정보주체에게 유출이 발생한 사실

2. 제1항의 통지항목 중 확인된 사항

③ 개인정보처리자는 개인정보 유출 사고를 인지하지 못해 유출 사고가 발생한 시점으로부터 5일 이내에 해당 정보주체에게 개인정보 유출 통지를 하지 아니한 경우에는 실제 유출 사고를 알게 된 시점을 입증하여야 한다.

제27조(유출 통지방법) ① 개인정보처리자는 정보주체에게 제26조제1항 각 호의 사항을 통지할 때에는 서면, 전자우편, 모사전송, 전화, 휴대전화 문자전송 또는 이와 유사한 방법을 통하여 지체 없이 정보주체에게 알려야 한다.

② 개인정보처리자는 제1항의 통지방법과 동시에, 홈페이지 등을 통하여 제26조제1항 각 호의 사항을 공개할 수 있다.

제28조(개인정보 유출신고 등) ① 개인정보처리자는 1천명 이상의 정보주체에 관한 개인정보가 유출된 경우에는 정보주체에 대한 통지 및 조치결과를 5일 이내에 보호위원회 또는 영 제39조제2항의 전문기관에게 신고하여야 한다.

② 제1항에 따른 신고는 별지 제1호서식에 따른 개인정보 유출신고서를 통하여 하여야 한다.

③ 개인정보처리자는 전자우편, 팩스 또는 영 제39조제2항에 따른 전문기관의 인터넷 사이트를 통하여 유출신고를 할 시간적 여유가 없거나 그밖에 특별한 사정이 있는 때에는 먼저 전화를 통하여 제26조제1항의 사항을 신고한 후, 별지 제1호서식에 따른 개인정보 유출신고서를 제출할 수 있다.

④ 개인정보처리자는 1천명 이상의 정보주체에 관한 개인정보가 유출된 경우에는 제26조제1항에 따른 통지와 함께 인터넷 홈페이지 등에 정보주체가 알아보기 쉽도록 제26조제1항 각 호의 사항을 7일 이상 게재하여야 한다.

제29조(개인정보 유출 사고 대응 매뉴얼 등) ① 다음 각 호의 어느 하나에 해당하는 개인정보처리자는 유출 사고 발생 시 신속한 대응을 통해 피해 발생을 최소화하기 위해 「개인정보 유출 사고 대응 매뉴얼」을 마련하여야 한다.

1. 법 제2조제6호에 따른 공공기관

2. 그 밖에 1천명 이상의 정보주체에 관한 개인정보를 처리하는 개인정보처리자

② 제1항에 따른 개인정보 유출 사고 대응 매뉴얼에는 유출 통지·조치 절차, 영업점·인터넷회선 확충 등 고객 민원 대응조치, 현장 혼잡 최소화 조치, 고객불안 해소조치, 피해자 구제조치 등을 포함하여야 한다.

③ 개인정보처리자는 개인정보 유출에 따른 피해복구 조치 등을 수행함에 있어 정보주체의 불편과 경제적 부담을 최소화할 수 있도록 노력하여야 한다.

개인정보 특히 디지털화된 개인정보는 정보주체가 유출 여부를 알기 어려우며, 한번 유출된 개인정보는 다시 제2, 제3의 피해로 전이될 가능성이 크다.

예를 들어 유출된 개인정보를 이용한 인터넷 명의도용, 전화사기(보이스피싱), 스팸발송 등 다양한 피해로 확산될 위험이 크다. 따라서 이 법은 개인정보 유출로 인한 피해를 사

전에 방지하고 정보주체로 하여금 유출에 대응할 수 있도록 하기 위해 정보주체에 대한 통지 및 관련 기관으로 신고 의무를 부여하고 있다.

1. 개인정보 유출 통지의무

가 통지의무의 발생

개인정보가 유출되었음을 알게 되었을 때 통지 의무가 발생한다. ‘유출’이란 고의·과실 여부를 불문하고 개인정보처리자의 관리 범위를 벗어나 개인정보가 외부에 공개, 제공, 누출, 누설된 모든 상태를 말한다. 즉 ‘개인정보 유출’은 법령이나 개인정보처리자의 자유로운 의사에 의하지 않고, 개인정보처리자가 정보주체의 개인정보에 대한 통제 상실 또는 권한 없는 자의 접근을 허용하는 것으로 ① 개인정보가 포함된 서면, 이동식 저장장치, 휴대용 컴퓨터 등을 분실하거나 도난당한 경우 ② 개인정보가 저장된 데이터베이스 등 개인정보처리시스템에 정상적인 권한이 없는 자가 접근한 경우 ③ 개인정보처리자의 고의 또는 과실로 인해 개인정보가 포함된 파일 또는 종이문서, 그 밖의 저장매체가 권한이 없는 자에게 잘못 전달된 경우 ④ 그 밖에 권한이 없는 자에게 개인정보가 전달된 경우를 말한다(표준지침 제25조).

즉 개인정보가 해당 개인정보처리자의 관리·통제권을 벗어나 당해 개인정보를 모르는 제3자가 그 내용을 알 수 있는 상태에 이르게 되면 개인정보가 유출된 것이다. 이때 제3자가 개인정보의 내용을 취득하여야만 유출되었다고 보는 것은 아니며, 일반적 수준의 제3자가 해당 정보를 알 수 있는 상태에 이르렀다면 개인정보가 유출된 것이다.

참고 개인정보 유출의 의미에 대한 판례

주식회사 A는 피고 주식회사 B의 서버와 연동하는 사이트의 시스템이 제대로 작동하는지를 점검하기 위하여, 피고 B의 CP(Contents Provider)인 주식회사 C로부터 서버와 연동할 수 있는 C의 아이디와 비밀번호인 ‘○○○○○○’를 임시로 부여받은 사실, A는 위 아이디와 비밀번호를 이용하여 2G 서버와 연동하는 시스템이 성공적으로 구축되었음을 확인하였지만, 그 시스템 점검 후에도 사이트에서 위 아이디와 비밀번호를 삭제하지 아니하여 엠샵 사이트와 2G 서버가 계속 연동하고 있었으나, 원고들의 휴대폰번호가 사이트의 ‘폰정보 조회’ 페이지에 입력되어 피고 A의 서버로부터 사이트로 위와 같은 개인정보가 전송되었음이 확인되지 않은 사안에서, 대법원은 「정보통신망 이용촉진 및 정보보호 등에 관한 법률」로 보호되는 개인정보의 누출이란 개인정보가 해당 정보통신서비스 제공자의 관리·통제권을 벗어나 제3자가 그 내용을 알 수 있는 상태에 이르게 된 것을 의미하는바, 어느 개인정보가 정보통신서비스 제공자의 관리·통제 하에 있고 개인정보가 제3자에게 실제 열람되거나 접근되지 아니한 상태라면, 정보통신서비스 제공자의 기술적·관리적 보호조치에 미흡한 점이 있어서 제3자가 인터넷상 특정 사이트를 통해 정보통신서비스 제공자가 보관하고 있는 개인정보에 접근할 수 있는 상태에 놓여 있었다고 하더라도 그것만으로 바로 개인정보가 정보통신서비스 제공자의 관리·통제권을 벗어나 제3자가 내용을 알 수 있는 상태에 이르렀다고 할 수는 없다.”고 판시하였다(대법원 2014. 5. 16. 선고 2011다24555 판결).

유출된 개인정보의 수량, 종류, 시기 등은 따지지 않는다. 따라서 단 1건의 개인정보가 유출되었더라도 해당 정보주체에게 그 사실을 통지해야 한다. 유출된 개인정보가 암호화되어 있는 때에는 통지의무를 면제하고 있는 나라(미국 등)도 있지만 우리나라에서는 그와 같은 예외를 인정하고 있지 않다.

개인정보의 유출 사실을 ‘알게 되었을 때’ 이므로, 유출사실이 일어났다고 해서 바로 통지의무가 발생하는 것은 아니며, 유출 사실을 개인정보처리자가 인지한 시점에서 유출통지의무가 발생한다. 이 경우 개인정보처리자가 유출사실을 확신할 것까지는 요하지 않으며, 개인정보가 개인정보처리자의 관리·통제권을 벗어나 제3자가 그 개인정보를 알 수 있는 상태에 이르렀다는 사실을 알게 되었을 때도 이에 해당한다.

나 통지 사항

개인정보처리자는 정보주체가 개인정보 유출사실을 정확히 인지하고 적절히 대처할 수 있도록 다음 각 호의 사실을 알려야 한다.

개인정보 유출 통지사항(제34조제1항)

1. 유출된 개인정보의 항목
2. 유출된 시점과 그 경위
3. 유출로 인하여 발생할 수 있는 피해를 최소화하기 위하여 정보주체가 할 수 있는 방법 등에 관한 정보
4. 개인정보처리자의 대응조치 및 피해 구제절차
5. 정보주체에게 피해가 발생한 경우 신고 등을 접수할 수 있는 담당부서 및 연락처

다 통지 시기

‘유출되었음을 알게 되었을 때’에 지체없이 통지하여야 한다. 여기서 ‘지체없이’란 알게 된 날로부터 근무일 기준 ‘5일 이내’를 의미한다. 따라서 최초로 개인정보 유출사실을 발견한 때로부터 유출현황, 사건경위, 잠정원인 등을 파악하는데 소요되는 시간을 고려하여 정당한 사유가 없는 한 5일 이내에 통지하여야 한다(표준지침 제26조제1항 본문). 여기서 정당한 사유란 개인정보 유출과 관련하여 수사기관의 비공개 요청이 있는 경우, 단전, 홍수, 폭설 등의 천재지변으로 인해 5일 이내 통지가 불가능한 경우 등을 말한다. 한편 개인정보 유출 사고를 인지하지 못해 유출 사고 발생시점으로부터 5일 이내에 해당 정보주체에게 개인정보 유출 통지를 하지 아니한 경우에는 개인정보처리자는 실제 유출 사고를 알게 된 시점을 입증하여야 한다(표준지침 제26조제3항).

다만, 유출된 개인정보의 확산 및 추가 유출을 방지하기 위하여 접속경로의 차단, 취약점

점검·보완, 유출된 개인정보의 삭제 등 긴급한 조치가 필요한 경우에는 해당 조치를 취한 후 지체 없이, 즉 그로부터 5일 이내에 정보주체에게 알릴 수 있다(영 제40조제1항 단서, 표준지침 제26조제1항 단서).

라 통지 방법

통지는 서면등의 방법으로 하여야 한다(영 제40조제1항 본문). 즉 서면, 전자우편, 팩스, 전화, 문자전송 또는 이에 상당하는 방법을 이용한 개별적 통지 방법이면 된다. 그러나 웹사이트 게재, 관보 고시 등과 같은 집단적인 공시만으로는 정보주체에게 유출 사실을 알린 것이라고 볼 수 없다.

마 확인사실의 우선통지

개인정보의 유출을 알게 된 때 또는 유출사실을 알고 긴급한 조치를 취한 후에도 유출된 개인정보의 항목, 유출 시점 및 그 경위의 구체적인 내용을 확인하지 못한 경우에는 먼저 개인정보가 유출된 사실과 유출이 확인된 사항만을 서면등의 방법으로 먼저 알리고 추후 확인되는 사항을 추가로 알릴 수 있다(영 제40조제2항, 표준지침 제26조제2항).

2. 인터넷 홈페이지 게시

1천명 이상의 정보주체에 관한 개인정보가 유출된 경우에는 서면등의 방법과 함께 인터넷 홈페이지에 정보주체가 알아보기 쉽도록 7일 이상 법 제34조제1항 각 호의 사항(유출 통지 사항)을 게재하여야 한다. 다만, 인터넷 홈페이지를 운영하지 않는 개인정보처리자의 경우에는 서면등의 방법과 함께 사업장등의 보기 쉬운 장소에 법 제34조제1항 각 호의 사항을 게시하면 된다(영 제40조제3항).

3. 피해 최소화 등의 조치의무

개인정보처리자는 개인정보가 유출된 경우 그 피해를 최소화하기 위한 대책을 마련하고 필요한 조치를 하여야 한다. 시스템 일시정지, 암호 등의 변경, 유출 원인 분석, 기술적 보안조치 강화, 시스템 변경, 기술지원 의뢰 및 복구 등과 같은 임시 대응조치에서부터 유사 사고 발생 방지대책 수립 및 시행 등과 같은 장래의 피해 예방조치도 강구되어야 한다. 우선적으로 개인정보 유출사실을 지체없이 피해고객에게 통지하고, 피해고객으로부터 개인정보 유출로 인한 피해 현황을 접수받을 수 있는 창구를 마련해야 한다. 또한 신속하고 적절한 피해확산을 방지하고 피해를 복구하기 위하여 개인정보 유출을 야기한 직·간접적

인 사고발생 원인을 즉시 제거하고, 미비한 기술적·관리적·물리적 보호조치를 보완하며, 유출된 개인정보의 악용 또는 도용을 막을 수 있는 대책 마련 등의 조치를 취해야 한다.

특히, 공공기관 또는 1천명 이상의 정보주체에 관한 개인정보를 처리하는 개인정보처리자는 유출사고 발생시 신속한 대응을 통해 피해 발생을 최소화하기 위해 ‘개인정보 유출 사고 대응 매뉴얼’을 마련하여야 한다(표준지침 제29조제1항). 개인정보유출 사고 대응 매뉴얼에는 유출통지·조회 절차, 영업점·인터넷회선 확충 등 고객민원 대응조치, 현장 혼잡 최소화 조치, 고객불안 해소조치, 피해자 구제조치 등을 포함하여야 한다(표준지침 제29조제2항).

한편 개인정보처리자는 개인정보유출에 따른 피해복구 조치 등을 수행함에 있어 정보주체의 불편과 경제적 부담을 최소화할 수 있도록 노력하여야 한다(표준지침 제29조제3항).

4. 개인정보 유출 신고의무

일정 규모 이상의 대량 개인정보 유출이 발생한 경우에는 이를 단순히 정보주체에게 통지하는 것만으로는 부족하며, 이를 정부 및 관계 전문기관에 알림으로써 체계적·조직적 대응을 할 필요가 있다. 이에 따라 이 법은 ‘1천명 이상’의 정보주체의 개인정보가 유출된 경우에는 정보주체에 대한 통지의무와 더불어, 통지 결과 및 조치 결과를 지체없이 보호위원회 또는 전문기관에 신고하도록 하였다. 여기서 ‘지체 없이’란 5일 이내를 의미한다.

이 법은 개인정보 유출신고를 접수할 전문기관으로서 한국인터넷진흥원을 지정하고 있다(영 제39조제2항). 개인정보유출신고는 ‘개인정보 유출신고서’ (표준지침 별지 제1호 서식)를 통하여 신고하여야 한다(표준지침 제28조제1항). 다만 전자우편, 팩스 또는 인터넷 사이트를 통하여 유출신고를 할 시간적 여유가 없거나 그 밖에 특별한 사정이 있는 때에는 전화를 통하여 먼저 신고한 후 ‘개인정보 유출신고서’를 제출할 수 있다(표준지침 제28조제2항). 보호위원회 또는 전문기관은 유출신고가 접수된 경우에는 피해 확산방지, 피해 복구 등을 위한 기술을 지원할 수 있다.

< 개인정보 유출신고 >

신고기관	보호위원회(개인정보보호 종합포털)/한국인터넷진흥원
신고시기	5일 이내(정보주체에 대한 통지 및 조치결과 신고)
신고내용	기관명, 통지여부, 유출된 개인정보 항목·규모, 유출시점·경위, 유출피해 최소화 대책·조치 및 결과, 정보주체가 할 수 있는 피해 최소화 방법 및 구제조치, 담당부서, 담당자 및 연락처 등
신고방법	전자우편, 팩스 인터넷사이트(개인정보보호종합포털, www.privacy.go.kr)를 통해 유출사고 신고 및 신고서 제출, 시간적 여유가 없거나 특별한 사정이 있는 경우: 전화를 통하여 통지내용을 신고한 후, 유출 신고서를 제출할 수 있음

5. 다른 법률과의 관계

「신용정보법」은 ‘개인정보 유출통지 및 신고의무’와 관련하여 업무 목적 외로 개인 신용정보가 누설된 경우 통지 신고에 대하여 별도로 규정하고 있다(「신용정보법」 제39조의4). 이에 따라 신용정보회사등은 개인신용정보가 업무 목적 외로 누설되었음을 알게 된 때에 신용정보주체에게 통지하여야 하고, 1만명 이상 신용정보주체의 개인신용정보가 누설된 때에는 피해최소화 등 조치결과를 금융위원회 또는 금융감독원에 신고하여야 한다. 이 경우 신용정보주체에 대한 통지사항은 「개인정보 보호법」상 통지사항이 준용된다. 한편, 상거래 기업 및 법인은 보호위원회 또는 한국인터넷진흥원에 조치결과를 신고하여야 한다.

신용정보법	<p>제39조의4(개인신용정보 누설통지 등) ① 신용정보회사등은 개인신용정보가 업무 목적 외로 누설되었음을 알게 된 때에는 지체 없이 해당 신용정보주체에게 통지하여야 한다. 이 경우 통지하여야 할 사항은 「개인정보 보호법」 제34조제1항 각 호의 사항을 준용한다.</p> <ol style="list-style-type: none"> 1. 삭제 <2020. 2. 4.> 2. 삭제 <2020. 2. 4.> 3. 삭제 <2020. 2. 4.> 4. 삭제 <2020. 2. 4.> 5. 삭제 <2020. 2. 4.> <p>② 신용정보회사등은 개인신용정보가 누설된 경우 그 피해를 최소화하기 위한 대책을 마련하고 필요한 조치를 하여야 한다.</p> <p>③ 신용정보회사등은 대통령령으로 정하는 규모 이상의 개인신용정보가 누설된 경우 제1항에 따른 통지 및 제2항에 따른 조치결과를 지체 없이 금융위원회 또는 대통령령으로 정하는 기관(이하 이 조에서 “금융위원회등”이라 한다)에 신고하여야 한다. 이 경우 금융위원회등은 피해 확산 방지, 피해 복구 등을 위한 기술을 지원할 수 있다.</p> <p>④ 제3항에도 불구하고 제45조의3제1항에 따른 상거래기업 및 법인은 보호위원회 또는 대통령령으로 정하는 기관(이하 이 조에서 “보호위원회등”이라 한다)에 신고하여야 한다.</p> <p>⑤ 금융위원회등은 제3항에 따른 신고를 받은 때에는 이를 개인정보 보호위원회에 알려야 한다.</p> <p>⑥ 금융위원회등 또는 보호위원회등은 제2항에 따라 신용정보회사등이 행한 조치에 대하여 조사할 수 있으며, 그 조치가 미흡하다고 판단되는 경우 금융위원회 또는 보호위원회는 시정을 요구할 수 있다.</p> <p>⑦ 제1항에 따른 통지의 시기, 방법 및 절차 등에 필요한 사항은 대통령령으로 정한다.</p>
-------	---

6. 가명정보의 적용 제외

제34조제1항은 가명정보가 유출된 경우에는 적용되지 않는다(제28조의7).

7. 벌칙규정

위반행위	벌칙
개인정보 유출 통지사항을 알리지 아니한 자 (제34조제1항 위반)	3천만원 이하의 과태료 (제75조제2항제8호)
조치 결과의 신고를 하지 아니한 자 (제34조제3항 위반)	3천만원 이하의 과태료 (제75조제2항제9호)

8. 질의응답

Q 여러 명의 민원인에게 동일한 내용의 공문발송시 수신자 각자의 개인정보가 포함되는데 이러한 경우도 개인정보 유출에 해당되는지 여부

A 공문 수신자의 성명과 주소는 특정 개인을 식별할 수 있는 개인정보에 해당, 수신자별로 공문발송이 이루어 지도록 처리를 하여야 할 것이며 회원 대상으로 단체메일을 발송하는 과정에서 수신자의 이름과 메일주소, 첨부파일 상의 개인정보가 공개된 경우에는 「개인정보 보호법」 상의 개인정보 유출에 해당

Q 개인정보 유출이 발생하였으나 정보주체의 연락처 정보가 없어 유출통지가 어려운 경우에는 어떻게 해야 하는가?

A 연락처가 없어 정보주체에게 유출통지가 어려운 경우에는 시행령 제28조제2항 및 제31조제2항, 제3항을 준용하여 인터넷 홈페이지에 지속적으로 게재하거나 정보주체가 알아보기 쉬운 장소에 게시하는 등의 방법을 통하여 유출사실을 공개할 필요가 있다.

제34조의 2 | 과징금의 부과 등

법률

- 제34조의2(과징금의 부과 등)** ① 보호위원회는 개인정보처리자가 처리하는 주민등록번호가 분실·도난·유출·위조·변조 또는 훼손된 경우에는 5억원 이하의 과징금을 부과·징수할 수 있다. 다만, 주민등록번호가 분실·도난·유출·위조·변조 또는 훼손되지 아니하도록 개인정보처리자가 제24조제3항에 따른 안전성 확보에 필요한 조치를 다한 경우에는 그러하지 아니하다.
- ② 보호위원회는 제1항에 따른 과징금을 부과하는 경우에는 다음 각 호의 사항을 고려하여야 한다.
1. 제24조제3항에 따른 안전성 확보에 필요한 조치 이행 노력 정도
 2. 분실·도난·유출·위조·변조 또는 훼손된 주민등록번호의 정도
 3. 피해확산 방지를 위한 후속조치 이행 여부
- ③ 보호위원회는 제1항에 따른 과징금을 내야 할 자가 납부기한까지 내지 아니하면 납부기한의 다음 날부터 과징금을 낸 날의 전날까지의 기간에 대하여 내지 아니한 과징금의 연 100분의 6의 범위에서 대통령령으로 정하는 가산금을 징수한다. 이 경우 가산금을 징수하는 기간은 60개월을 초과하지 못한다.
- ④ 보호위원회는 제1항에 따른 과징금을 내야 할 자가 납부기한까지 내지 아니하면 기간을 정하여 독촉을 하고, 그 지정한 기간 내에 과징금 및 제2항에 따른 가산금을 내지 아니하면 국세 체납처분의 예에 따라 징수한다.
- ⑤ 과징금의 부과·징수에 관하여 그 밖에 필요한 사항은 대통령령으로 정한다.

시행령

- 제40조의2 (과징금의 부과기준 등)** ① 법 제34조의2제1항에 따른 과징금의 부과기준은 별표 1의3과 같다.
- ② 보호위원회는 법 제34조의2제1항에 따라 과징금을 부과하려는 경우에는 위반사실, 부과금액, 이의제기 방법 및 이의제기 기간 등을 명시하여 이를 납부할 것을 과징금 부과대상자에게 서면으로 통지해야 한다.
- ③ 제2항에 따라 통지를 받은 자는 통지를 받은 날부터 30일 이내에 보호위원회가 정하는 수납기관에 과징금을 납부하여야 한다. 다만, 천재지변이나 그 밖에 부득이한 사유로 인하여 그 기간 내에 과징금을 납부할 수 없는 경우에는 그 사유가 없어진 날부터 7일 이내에 납부해야 한다.
- ④ 법 제34조의2제3항 전단에서 “대통령령으로 정하는 가산금”이란 납부기한의 다음 날부터 과징금을 낸 날의 전날까지의 기간에 대하여 매 1개월이 지날 때마다 내지 아니한 과징금의 1천분의 5에 상당하는 금액을 가산한 금액을 말한다.

주민등록번호는 금융거래, 공공서비스와 같은 중요한 법적 거래나 서비스 이용과 관련하여 본인확인 등을 위해 활용된다. 주민등록번호의 경우 유출 내지 오·남용 사건이 발생하는 경우 해당 정보주체에게 회복하기 어려운 피해가 발생할 가능성이 있다. 이러한 주민등록번호의 중요성 등을 고려하여 「개인정보 보호법」은 법률·대통령령·국회규칙·대법원규칙·헌법재판소규칙·중앙선거관리위원회규칙 및 감사원규칙에서 구체적으로 주민등록번호의 처리를 요구하거나 허용한 경우, 정보주체 또는 제3자의 급박한 생명, 신체, 재산의 이익을 위하여 명백히 필요하다고 인정되는 경우로 제한하는 한편(제24조의2), 개인정보처리자가 처리하는 주민등록번호가 분실·도난·유출·위조·변조 또는 훼손된 경우 과징금을 부과할 수 있도록 규정하였다(제34조의2).

1. 과징금 부과 내용

보호위원회는 ‘개인정보처리자’가 처리하는 ‘주민등록번호’가 ‘분실·도난·유출·위조·변조 또는 훼손된 경우’에는 5억원 이하의 과징금을 부과·징수할 수 있다. 다만, 개인정보처리자가 주민등록번호가 분실·도난·유출·위조·변조 또는 훼손되지 아니하도록 제24조제3항에 따른 안전성 확보에 필요한 조치를 다한 경우에는 과징금을 부과·징수하지 아니할 수 있다.

한편, 보호위원회는 과징금을 부과하는 경우 ① 개인정보처리자가 안전성 확보에 필요한 조치 이행 노력 정도 ② 분실·도난·유출·위조·변조 또는 훼손된 주민등록번호의 정도 ③ 피해확산 방지를 위한 후속조치 이행 여부를 고려하여야 한다.

2. 과징금의 부과 절차 및 기준

보호위원회는 법 제34조의2제1항에 따라 과징금을 부과하려는 경우에는 위반사실, 부과금액, 이의제기 방법 및 이의제기 기간 등을 명시하여 이를 납부할 것을 과징금 부과대상자에게 서면으로 통지하여야 한다(영 제40조의2제2항).

과징금 부과 통지를 받은 자는 통지를 받은 날부터 30일 이내에 보호위원회가 정하는 수납기관에 과징금을 납부하여야 한다. 다만, 천재지변이나 그 밖에 부득이한 사유로 인하여 그 기간 내에 과징금을 납부할 수 없는 경우에는 그 사유가 없어진 날부터 7일 이내에 납부하여야 한다(영 제40조의2제3항).

보호위원회는 과징금을 내야 할 자가 납부기한까지 내지 아니하면 납부기한의 다음 날부터 과징금을 낸 날의 전날까지의 기간에 대하여 내지 아니한 과징금의 연 100분의 6의 범위에서 대통령령으로 정하는 가산금을 징수한다. “대통령령으로 정하는 가산금”이란 납부기한

의 다음 날부터 과징금을 낸 날의 전날까지의 기간에 대하여 매 1개월이 지날 때마다 내지 아니한 과징금의 1천분의 5에 상당하는 금액을 가산한 금액을 말한다(영 제40조의2제4항). 한편 가산금을 징수하는 기간은 60개월을 초과하지 아니한다.

구체적인 과징금 부과 기준은 다음 표와 같다.

<과징금의 부과기준(영 제40조의2제1항, 별표 1의3)>

1. 과징금 부과 여부의 결정

과징금은 법 제34조의2제2항 각 호의 사항과 위반행위의 내용 등을 종합적으로 고려하여 그 부과 여부를 결정한다. 다만, 법 제24조제3항에 따른 안전성 확보에 필요한 조치를 다한 경우에는 과징금을 부과하지 아니한다.

2. 과징금의 산정기준

과징금은 법 제34조의2제2항 각 호의 사항과 이에 영향을 미치는 사항을 종합적으로 고려하여 산정하되, 가목의 위반 정도에 따른 산정기준액에 나목의 안전성 확보에 필요한 조치 이행 노력 정도 등에 따른 조정(이하 “1차 조정”이라 한다), 다목의 위반행위의 기간 및 횟수 등에 따른 조정(이하 “2차 조정”이라 한다)을 거쳐 라목에 따라 부과과징금을 산정한다. 다만, 산정된 과징금이 5억원을 초과하는 경우에는 5억원으로 한다.

가. 기본 산정기준

위반 정도	산정기준액	비 고
매우 중대한 위반행위	3억 5천만원	고의 또는 중과실로 인하여 10만건 이상의 주민등록번호가 분실·도난·유출·변조 또는 훼손(이하 “분실등”이라 한다)된 경우를 말한다.
중대한 위반행위	2억 3천만원	고의 또는 중과실로 인하여 10만건 미만의 주민등록번호가 분실등이 된 경우 및 경과실로 인하여 10만건 이상의 주민등록번호가 분실등이 된 경우를 말한다.
일반 위반행위	1억원	경과실로 인하여 10만건 미만의 주민등록번호가 분실등이 된 경우를 말한다.

나. 1차 조정

법 제24조제3항에 따른 안전성 확보에 필요한 조치 이행 노력 정도, 피해를 최소화하기 위한 대책 마련 등 피해확산 방지를 위한 후속조치 이행 여부를 고려하여 산정기준액의 100분의 50의 범위에서 가중하거나 감경한다.

다. 2차 조정

위반행위의 기간 및 횟수, 위반 행위에 대한 조사 협조 여부, 위반행위에 따른 추가적 피해 발생 여부, 평소 개인정보보호를 위한 노력 정도 등을 종합적으로 고려하여 1차 조정된 금액의 100분의 50의 범위에서 가중하거나 감경한다.

라. 부과과징금의 산정

개인정보처리자의 현실적 부담능력이나 그 위반행위가 미치는 효과, 위반행위로 인하여 취득한 이익의 규모 등을 고려하여 볼 때 과중하다고 인정되는 경우에는 2차 조정된 금액의 100분의 50의 범위에서 감액하여 부과과징금으로 정할 수 있다.

제5장

정보주체의 권리 보장

제35조	개인정보의 열람
제36조	개인정보의 정정·삭제
제37조	개인정보의 처리정지 등
제38조	권리행사의 방법 및 절차
제39조	손해배상책임
제39조의2	법정손해배상의 청구



제35조 | 개인정보의 열람

법률

제35조(개인정보의 열람) ① 정보주체는 개인정보처리자가 처리하는 자신의 개인정보에 대한 열람을 해당 개인정보처리자에게 요구할 수 있다.

② 제1항에도 불구하고 정보주체가 자신의 개인정보에 대한 열람을 공공기관에 요구하고자 할 때에는 공공기관에 직접 열람을 요구하거나 대통령령으로 정하는 바에 따라 보호위원회를 통하여 열람을 요구할 수 있다.

③ 개인정보처리자는 제1항 및 제2항에 따른 열람을 요구받았을 때에는 대통령령으로 정하는 기간 내에 정보주체가 해당 개인정보를 열람할 수 있도록 하여야 한다. 이 경우 해당 기간 내에 열람할 수 없는 정당한 사유가 있을 때에는 정보주체에게 그 사유를 알리고 열람을 연기할 수 있으며, 그 사유가 소멸하면 지체 없이 열람하게 하여야 한다.

④ 개인정보처리자는 다음 각 호의 어느 하나에 해당하는 경우에는 정보주체에게 그 사유를 알리고 열람을 제한하거나 거절할 수 있다.

1. 법률에 따라 열람이 금지되거나 제한되는 경우
2. 다른 사람의 생명·신체를 해할 우려가 있거나 다른 사람의 재산과 그 밖의 이익을 부당하게 침해할 우려가 있는 경우
3. 공공기관이 다음 각 목의 어느 하나에 해당하는 업무를 수행할 때 중대한 지장을 초래하는 경우
 - 가. 조세의 부과·징수 또는 환급에 관한 업무
 - 나. 「초·중등교육법」 및 「고등교육법」에 따른 각급 학교, 「평생교육법」에 따른 평생교육시설, 그 밖의 다른 법률에 따라 설치된 고등교육기관에서의 성적 평가 또는 입학자 선발에 관한 업무
 - 다. 학력·기능 및 채용에 관한 시험, 자격 심사에 관한 업무
 - 라. 보상금·급부금 산정 등에 대하여 진행 중인 평가 또는 판단에 관한 업무
 - 마. 다른 법률에 따라 진행 중인 감사 및 조사에 관한 업무
- ⑤ 제1항부터 제4항까지의 규정에 따른 열람 요구, 열람 제한, 통지 등의 방법 및 절차에 관하여 필요한 사항은 대통령령으로 정한다.

시행령

제41조(개인정보의 열람절차 등) ① 정보주체는 법 제35조제1항에 따라 자신의 개인정보에 대한 열람을 요구하려면 다음 각 호의 사항 중 열람하려는 사항을 개인정보처리자가 마련한 방법과 절차에 따라 요구하여야 한다.

1. 개인정보의 항목 및 내용
2. 개인정보의 수집·이용의 목적
3. 개인정보 보유 및 이용 기간
4. 개인정보의 제3자 제공 현황
5. 개인정보 처리에 동의한 사실 및 내용

② 개인정보처리자는 제1항에 따른 열람 요구 방법과 절차를 마련하는 경우 해당 개인정보의 수집 방법과 절차에 비하여 어렵지 아니하도록 다음 각 호의 사항을 준수하여야 한다.

1. 서면, 전화, 전자우편, 인터넷 등 정보주체가 쉽게 활용할 수 있는 방법으로 제공할 것
2. 개인정보를 수집한 창구의 지속적 운영이 곤란한 경우 등 정당한 사유가 있는 경우를 제외하고는 최소한 개인정보를 수집한 창구 또는 방법과 동일하게 개인정보의 열람을 요구할 수 있도록 할 것
3. 인터넷 홈페이지를 운영하는 개인정보처리자는 홈페이지에 열람 요구 방법과 절차를 공개할 것

③ 정보주체가 법 제35조제2항에 따라 보호위원회를 통하여 자신의 개인정보에 대한 열람을 요구하려는 경우에는 보호위원회가 정하여 고시하는 바에 따라 제1항 각 호의 사항 중 열람하려는 사항을 표시한 개인정보 열람요구서를 보호위원회에 제출해야 한다. 이 경우 보호위원회는 지체 없이 그 개인정보 열람요구서를 해당 공공기관에 이송해야 한다.

④ 법 제35조제3항 전단에서 “대통령령으로 정하는 기간” 이란 10일을 말한다.

⑤ 개인정보처리자는 제1항 및 제3항에 따른 개인정보 열람 요구를 받은 날부터 10일 이내에 정보주체에게 해당 개인정보를 열람할 수 있도록 하는 경우와 제42조제1항에 따라 열람 요구 사항 중 일부를 열람하게 하는 경우에는 열람할 개인정보와 열람이 가능한 날짜·시간 및 장소 등(제42조제1항에 따라 열람 요구 사항 중 일부만을 열람하게 하는 경우에는 그 사유와 이의제기 방법을 포함한다)을 보호위원회가 정하여 고시하는 열람통지서로 해당 정보주체에게 알려야 한다. 다만, 즉시 열람하게 하는 경우에는 열람통지서 발급을 생략할 수 있다.

제42조(개인정보 열람의 제한·연기 및 거절) ① 개인정보처리자는 제41조제1항에 따른 열람 요구 사항 중 일부가 법 제35조제4항 각 호의 어느 하나에 해당하는 경우에는 그 일부에 대하여 열람을 제한할 수 있으며, 열람이 제한되는 사항을 제외한 부분은 열람할 수 있도록 하여야 한다.

② 개인정보처리자가 법 제35조제3항 후단에 따라 정보주체의 열람을 연기하거나 같은 조 제4항에 따라 열람을 거절하려는 경우에는 열람 요구를 받은 날부터 10일 이내에 연기 또는 거절의 사유 및 이의제기방법을 보호위원회가 정하여 고시하는 열람의 연기·거절 통지서로 해당 정보주체에게 알려야 한다.

개인정보 처리 방법에 관한 고시(보호위원회 고시 제2020-7호)

제3조(개인정보보호 업무 관련 장부 및 문서 서식) ⑥ 법 제35조제2항과 영 제41조제3항에 따른 개인정보 열람의 요구는 별지 제8호서식의 개인정보 열람요구서에 따른다.

⑦ 법 제35조제5항과 영 제41조제4항에 따른 개인정보 열람 및 일부열람의 통지, 법 제35조제3항 후단과 영 제42조제2항에 따른 개인정보 열람연기의 통지, 법 제35조제4항과 영 제42조제2항에 따른 열람거절의 통지는 별지 제9호서식의 개인정보 열람, 일부열람, 열람연기, 열람거절 통지서에 따른다.

제31조(개인정보 열람 연기 사유의 소멸) ① 개인정보처리자가 법 제35조제3항 후문에 따라 개인정보의 열람을 연기한 후 그 사유가 소멸한 경우에는 정당한 사유가 없는 한 사유가 소멸한 날로부터 10일 이내에 열람하도록 하여야 한다.

② 정보주체로부터 영 제41조제1항제4호의 규정에 따른 개인정보의 제3자 제공 현황의 열람청구를 받은 개인정보처리자는 국가안보에 긴요한 사안으로 법 제35조제4항제3호마목의 규정에 따른 업무를 수행하는데 중대한 지장을 초래하는 경우, 제3자에게 열람청구의 허용 또는 제한, 거부와 관련한 의견을 조회하여 결정할 수 있다.

제32조(개인정보의 정정·삭제) ① 개인정보처리자가 법 제36조제1항에 따른 개인정보의 정정·삭제 요구를 받았을 때는 정당한 사유가 없는 한 요구를 받은 날로부터 10일 이내에 그 개인정보를 조사하여 정보주체의 요구에 따라 정정·삭제 등 필요한 조치를 한 후 그 결과를 정보주체에게 알려야 한다.

② 정보주체의 정정·삭제 요구가 법 제36조제1항 단서에 해당하는 경우에는 정당한 사유가 없는 한 요구를 받은 날로부터 10일 이내에 삭제를 요구할 수 없는 근거법령의 내용을 정보주체에게 알려야 한다.

제33조(개인정보의 처리정지) ① 개인정보처리자가 정보주체로부터 법 제37조제1항에 따라 개인정보처리를 정지하도록 요구받은 때에는 정당한 사유가 없는 한 요구를 받은 날로부터 10일 이내에 개인정보 처리의 일부 또는 전부를 정지하여야 한다. 다만, 법 제37조제2항 단서에 해당하는 경우에는 정보주체의 처리정지 요구를 거절할 수 있다.

② 개인정보처리자는 정보주체의 요구에 따라 처리가 정지된 개인정보에 대하여 정당한 사유가 없는 한 처리정지의 요구를 받은 날로부터 10일 이내에 해당 개인정보의 파기 등 정보주체의 요구에 상응하는 조치를 취하고 그 결과를 정보주체에게 알려야 한다.

제34조(권리행사의 방법 및 절차) ① 개인정보처리자는 정보주체가 법 제38조제1항에 따른 열람등요구를 하는 경우에는 개인정보를 수집하는 방법과 동일하거나 보다 쉽게 정보주체가 열람요구 등 권리를 행사할 수 있도록 간편한 방법을 제공하여야 하며, 개인정보의 수집시에 요구되지 않았던 증빙서류 등을 요구하거나 추가적인 절차를 요구할 수 없다.

② 제1항의 규정은 영 제46조에 따라 본인 또는 정당한 대리인임을 확인하고 자 하는 경우와 영 제47조에 따른 수수료와 우송료의 정산에도 준용한다.

제44조(정보주체의 열람등 요구) ① 정보주체는 영상정보처리기기운영자가 처리하는 개인영상정보에 대하여 열람 또는 존재확인(이하 “열람등” 이라 한다)을 해당 영상정보처리기기운영자에게 요구할 수 있다. 이 경우 정보주체가 열람등을 요구할 수 있는 개인영상정보는 정보주체 자신이 촬영된 개인영상정보 및 명백히 정보주체의 급박한 생명, 신체, 재산의 이익을 위하여 필요한 개인영상정보에 한한다.

② 영상정보처리기기운영자가 공공기관인 경우에는 해당 기관의 장에게 별지 제2호서식에 따른 개인영상정보 열람·존재확인 청구서(전자문서를 포함한다)로 하여야 한다.

③ 영상정보처리기기운영자는 제1항에 따른 요구를 받았을 때에는 지체 없이 필요한 조치를 취하여야 한다. 이때에 영상정보처리기기운영자는 열람등 요구를 한 자가 본인이거나 정당한 대리인인지를 주민등록증·운전면허증·여권 등의 신분증명서를 제출받아 확인하여야 한다.

④ 제3항의 규정에도 불구하고 다음 각 호에 해당하는 경우에는 영상정보처리기기운영자는 정보주체의 개인영상정보 열람등 요구를 거부할 수 있다. 이 경우 영상정보처리기기운영자는 10일 이내에 서면 등으로 거부 사유를 정보주체에게 통지하여야 한다.

1. 범죄수사·공소유지·재판수행에 중대한 지장을 초래하는 경우(공공기관에 한함)

2. 개인영상정보의 보관기간이 경과하여 파기한 경우

3. 기타 정보주체의 열람등 요구를 거부할 만한 정당한 사유가 존재하는 경우

⑤ 영상정보처리기기운영자는 제3항 및 제4항에 따른 조치를 취하는 경우 다음 각 호의 사항을 기록하고 관리하여야 한다.

1. 개인영상정보 열람등을 요구한 정보주체의 성명 및 연락처

2. 정보주체가 열람등을 요구한 개인영상정보 파일의 명칭 및 내용

3. 개인영상정보 열람등의 목적

4. 개인영상정보 열람등을 거부한 경우 그 거부의 구체적 사유

5. 정보주체에게 개인영상정보 사본을 제공한 경우 해당 영상정보의 내용과 제공한 사유

⑥ 정보주체는 영상정보처리기기운영자에게 정보주체 자신의 개인영상정보에 대한 파기를 요구하는 때에는 제1항에 의하여 보존을 요구하였던 개인영상정보에 대하여만 그 파기를 요구할 수 있다. 영상정보처리기기운영자가 해당 파기조치를 취한 경우에는 그 내용을 기록하고 관리하여야 한다.

제45조(개인영상정보 관리대장) 제42조제1항 및 제2항, 제44조제5항 및 제6항에 따른 기록 및 관리는 별지 제3호서식에 따른 ‘개인영상정보 관리대장’을 활용할 수 있다.

제46조(정보주체 이외의 자의 개인영상정보 보호) 영상정보처리기기운영자는 제44조제2항에 따른 열람등 조치를 취하는 경우, 만일 정보주체 이외의 자를 명백히 알아볼 수 있거나 정보주체 이외의 자의 사생활 침해의 우려가 있는 경우에는 해당되는 정보주체 이외의 자의 개인영상정보를 알아볼 수 없도록 보호조치를 취하여야 한다.

정보주체는 개인정보처리자가 자신에 관하여 어떤 정보를 보유하고 있고, 어떻게 활용하고 있으며, 개인정보처리자가 보유하는 개인정보는 정확한지 여부를 확인할 수 있어야 한다. 이와 같은 정보주체의 권리는 개인정보자기결정권의 핵심을 이룬다.

1. 정보주체의 개인정보 열람 요구권

정보주체는 개인정보처리자가 처리하는 자신의 개인정보에 대한 열람을 해당 개인정보처리자에게 요구할 수 있다. 열람에는 사본의 교부를 포함한다. 정보주체가 직접 제공한 개인정보 이외에 제3자 또는 공개된 정보원으로부터 수집한 개인정보, 개인정보처리자가 생산한 개인정보(신용평가, 인사평가, 거래내역, 진료기록 등), 서비스제공 등의 과정에서 자동적으로 생성된 개인정보(수발신내역, 입출기록, 쿠키, 로그기록 등) 등도 열람요구의 대상이 된다.

2. 정보주체의 개인정보 열람 요구 사항

정보주체는 자신의 개인정보에 대한 다음 각 호 사항의 열람을 요구할 수 있다. 이 경우 정보주체는 열람하려는 사항을 개인정보처리자가 마련한 방법과 절차에 따라 요구하여야 한다.

열람요구 사항(영 제41조제1항)

1. 개인정보의 항목 및 내용
2. 개인정보의 수집·이용의 목적
3. 개인정보 보유 및 이용 기간
4. 개인정보의 제3자 제공 현황
5. 개인정보 처리에 대하여 동의한 사실 및 내용

3. 정보주체의 개인정보 열람 요구 방법 및 절차

개인정보처리자가 개인정보 열람 요구 방법과 절차를 마련하는 경우에는 해당 개인정보의 수집 방법과 절차에 비하여 어렵지 않도록 다음 각 호의 사항을 준수하여야 한다.

여기서 어렵지 않아야 한다는 것은 동일하거나 보다 쉬워야 한다는 것을 말한다. 예를 들어 개인정보처리자가 서면으로 수집한 개인정보에 대하여 서면으로 열람 요구 신청을 받는 경우에는 이에 해당할 수 있지만, 전화 또는 전자우편으로 수집한 개인정보에 대하여 서면으로만 열람 요구 신청을 받는 경우에는 이에 해당하지 않는다.

열람 요구·방법 절차 마련 시 준수사항(영 제41조제2항)

1. 서면, 전화, 전자우편, 인터넷 등 정보주체가 쉽게 활용할 수 있는 방법으로 제공할 것
2. 개인정보를 수집한 창구의 지속적 운영이 곤란한 경우 등 정당한 사유가 있는 경우를 제외하고는 최소한 개인정보를 수집한 창구 또는 방법과 동일하게 개인정보의 열람을 요구할 수 있도록 할 것
3. 인터넷 홈페이지를 운영하는 개인정보처리자는 홈페이지에 열람 요구 방법과 절차를 공개할 것

정보주체가 자신의 개인정보에 대한 열람을 공공기관에 요구하고자 할 때에는 공공기관에 직접 열람을 요구하거나 보호위원회를 통하여 열람을 요구할 수 있다(제2항). 정보주체가 보호위원회를 통하여 자신의 개인정보에 대한 열람을 요구하려는 경우에는 개인정보 열람요구서(고시 제3조제6항 별지 제8호 서식)를 보호위원회에 제출하여야 한다. 이 경우 보호위원회는 지체 없이 그 개인정보 열람요구서를 해당 공공기관에 이송하여야 한다(영 제41조제3항).

4. 열람조치 등

개인정보처리자가 정보주체로부터 개인정보 열람을 요구받았을 때에는 요구받은 날로부터 근무일 기준 10일 이내에 정보주체가 해당 개인정보를 열람할 수 있도록 조치하여야 한다(제3항제1문, 영 제41조제4항). 이 경우 개인정보처리자는 열람할 개인정보와 열람이 가능한 일시 및 장소 등을 열람통지서(고시 제3조제7항 별지 제9호 서식)로 해당 정보주체에게 알려야 한다. 다만, 정보주체에게 즉시 열람하게 하는 경우에는 열람통지서 발급을 생략할 수 있다(영 제41조제5항).

개인정보처리자가 정보주체로부터 개인정보 열람을 요구받았지만 10일 이내에 열람을 하게 할 수 없는 정당한 사유가 있을 때에는 정보주체에게 그 사유를 알리고 열람을 연기할 수 있다(제3항제2문). 개인정보 열람을 연기한 후 그 사유가 소멸하였을 경우 연기사유가 소멸한 날로부터 근무일 기준 ‘10일 이내’에 열람하도록 하여야 한다(표준지침 제31조제1항). 개인정보처리자가 정보주체의 열람을 연기하려는 경우에는 열람 요구를 받은 날부터 근무일 기준 10일 이내에 연기의 사유 및 이의제기 방법을 열람의 연기·거절 통지서(고시 제3조제6항 별지 제9호 서식)로 해당 정보주체에게 알려야 한다(영 제42조제2항).

5. 열람의 제한 및 거절

개인정보처리자는 다음 각 호의 어느 하나에 해당하는 경우에는 정보주체에게 그 사유를 알리고 열람을 제한하거나 거절할 수 있다(제4항). 또한 열람 요구 사항 중 일부가 다음 각 호의 어느 하나에 해당하는 경우에는 그 일부에 대하여 열람을 제한할 수 있으며, 열람이 제한되는 사항을 제외한 부분에 대해서는 열람할 수 있도록 하여야 한다(영 제42조제1항).

개인정보처리자가 정보주체의 열람을 거절하려는 경우에는 열람 요구를 받은 날부터 10일 이내에 거절의 사유 및 이의제기 방법을 연기·거절 통지서(고시 제3조제6항 별지 제9호 서식)로 해당 정보주체에게 알려야 한다. 또한, 열람 요구 사항 중 일부만을 열람하게 하는 경우에는 열람할 개인정보, 열람이 가능한 일시 및 장소, 일부만을 열람하게 하는 사유 및 이의제기 방법 등을 열람통지서(고시 제3조제6항 별지 제9호 서식)로 해당 정보주체에게 알려야 한다(영 제42조제2항).

열람 제한·거절사유(제35조제4항)

1. 법률에 따라 열람이 금지되거나 제한되는 경우
2. 다른 사람의 생명·신체를 해할 우려가 있거나 다른 사람의 재산과 그 밖의 이익을 부당하게 침해할 우려가 있는 경우
3. 공공기관이 다음 각 목의 어느 하나에 해당하는 업무를 수행할 때 중대한 지장을 초래하는 경우
 - 가. 조세의 부과·징수 또는 환급에 관한 업무
 - 나. 「초·중등교육법」 및 「고등교육법」에 따른 각급 학교, 「평생교육법」에 따른 평생교육시설, 그 밖의 다른 법률에 따라 설치된 고등교육기관에서의 성적 평가 또는 입학자 선발에 관한 업무
 - 다. 학력·기능 및 채용에 관한 시험, 자격 심사에 관한 업무
 - 라. 보상금·급부금 산정 등에 대하여 진행 중인 평가 또는 판단에 관한 업무
 - 마. 다른 법률에 따라 진행 중인 감사 및 조사에 관한 업무

결정례 정보주체를 식별할 수 있다는 이유만으로 제35조제4항제2호에 따른 열람 거절이 가능한지 여부

정보주체는 개인정보처리자가 자신에 관하여 어떤 정보를 보유하고 있고 어떻게 활용하고 있으며 개인정보처리자가 보유하는 개인정보가 정확한지 여부를 확인할 수 있는 권리를 가지며 이와 같은 정보주체의 권리는 개인정보자기결정권의 핵심을 이루는 점, 개인영상정보에 포함된 제3자에 대하여 보호조치를 취한 경우 정보주체 외의 자는 제3자를 알아볼 수 있는 가능성이 낮아 제3자의 생활 침해의 우려가 크다고 보기 어려운 점, 정보주체가 개인영상정보를 무분별하게 이용할 경우 제3자는 손해배상 등 다른 구제수단을 취할 수 있는 점 등을 고려할 때 정보주체가 보호 조치된 제3자를 식별할 수 있다는 특수한 주관적 사정을 이유로 개인정보 열람 요구권을 제한하는 것은 헌법상 보장되고 있는 개인정보자기결정권에 대한 지나친 제약이라 판단된다.

이에 정보주체가 개인영상정보 열람 및 존재확인 청구서상 청구 목적이 오로지 제3자의 이익을 해하기 위한 것으로 추정되는 등 당해 열람이 다른 사람의 생명·신체를 해할 우려가 있거나 다른 사람의 재산과 그 밖의 이익을 부당하게 침해할 우려가 있다고 인정할 만한 특별한 사정이 없는 이상 정보주체가 보호조치된 제3자를 알아볼 수 있다는 이유만으로 「개인정보 보호법」 제35조 제4항 제2호를 근거로 개인영상정보 열람을 거절할 수는 없다 할 것이다(보호위원회 결정 제2019-14-223호).

단, 개인정보의 제3자 제공 현황에 대한 열람청구를 받은 개인정보처리자가 임의적으로 열람 허용 여부를 결정할 수 있는데, 만약 국가정보원 등 수사기관이 국가안보에 긴요한 사안에 대한 수사를 진행하고 있는 경우 제3자 제공현황이 수사대상자에게 노출된다면 증거인멸 등 수사활동이 제대로 수행되기 어려울 수도 있으므로, 이 경우에는 제3자에 해당하는 당해 수사기관에게 열람청구의 허용 또는 제한, 거부에 관련한 의견을 조회하여 결정할 수 있다(표준지침 제31조제2항)

6. 다른 법률과의 관계

「신용정보법」도 신용정보의 열람 및 정정청구 등에 관하여 규정하고 있으므로, 신용정보회사등은 「신용정보법」에 따라 신용정보주체의 열람청구 등이 있는 경우 필요한 조치를 취하여야 한다.

신용정보법	<p>제38조(신용정보의 열람 및 정정청구 등) ① 신용정보주체는 신용정보회사등에 본인의 신분을 나타내는 증표를 내보이거나 전화, 인터넷 홈페이지의 이용 등 대통령령으로 정하는 방법으로 본인임을 확인받아 신용정보회사등이 가지고 있는 신용정보주체 본인에 관한 신용정보로서 대통령령으로 정하는 신용정보의 교부 또는 열람을 청구할 수 있다.</p> <p>제39조(무료 열람권) 개인인 신용정보주체는 1년 이내로서 대통령령으로 정하는 일정한 기간마다 개인신용평가회사(대통령령으로 정하는 개인신용평가회사는 제외한다)에 대하여 다음 각 호의 신용정보를 1회 이상 무료로 교부받거나 열람할 수 있다.</p> <ol style="list-style-type: none"> 1. 개인신용평점 2. 개인신용평점의 산출에 이용된 개인신용정보 3. 그 밖에 제1호 및 제2호에서 정한 정보와 유사한 정보로서 대통령령으로 정하는 신용정보
-------	--

7. 가명정보의 적용 제외

가명정보에는 이름, 연락처 등 개인을 알아 볼 수 있는 정보가 포함되어 있지 않으므로 정보주체는 가명정보에 대하여 제35조에 따른 열람 요구권을 행사할 수 없다(제28조의7).

8. 벌칙규정

위반행위	벌칙
정보주체의 열람 요구의 부당한 제한·거절 (제35조제3항 위반)	3천만원 이하의 과태료 (제75조제2항제10호)
정보주체의 열람 요구 거부 시 통지의무 불이행(제35조제3항·제4항 위반)	1천만원 이하의 과태료 (제75조제4항제9호)

9. 질의 응답

- Q** | 고객이 현재까지 부가서비스 가입내역 등의 개인정보 이용내역 전부를 확인해 줄 것을 요구하고 있다. 개인정보 이용내역 분량이 매우 많은데, 이러한 경우에는 어떻게 조치하면 되는가?
- A** | 원칙적으로 정보주체의 자기정보 열람 요구가 있는 경우에는 법 제35조제4항에 따른 열람제한·거절사유에 해당하지 않는 한 10일 이내에 필요한 조치를 해야 한다. 단, 개인정보 이용내역 산출 등의 업무에 소요되는 수수료와 우송료 등을 정보주체에게 청구할 수 있다.
- Q** | 고객에게 서면으로 멤버십 가입 신청서를 받은 뒤 포인트 적립이나 신메뉴 안내 등의 서비스를 제공해 왔다. 그런데 어떤 고객이 자신은 멤버십 가입신청서에 동의한 적이 없다면서 확인을 요구해 왔다. 이런 경우 어떻게 해야 하는가?
- A** | 정보주체로부터 개인정보 수집 동의 여부에 대한 확인요구를 받은 경우에는 10일 이내에 해당 회원의 가입신청서를 제시하여 동의 기재란의 자필서명 여부 등을 열람·확인할 수 있도록 하여야 한다.

제36조 | 개인정보의 정정·삭제

법률

제36조(개인정보의 정정·삭제) ① 제35조에 따라 자신의 개인정보를 열람한 정보주체는 개인정보처리자에게 그 개인정보의 정정 또는 삭제를 요구할 수 있다. 다만, 다른 법령에서 그 개인정보가 수집 대상으로 명시되어 있는 경우에는 그 삭제를 요구할 수 없다.

② 개인정보처리자는 제1항에 따른 정보주체의 요구를 받았을 때에는 개인정보의 정정 또는 삭제에 관하여 다른 법령에 특별한 절차가 규정되어 있는 경우를 제외하고는 지체 없이 그 개인정보를 조사하여 정보주체의 요구에 따라 정정·삭제 등 필요한 조치를 한 후 그 결과를 정보주체에게 알려야 한다.

③ 개인정보처리자가 제2항에 따라 개인정보를 삭제할 때에는 복구 또는 재생되지 아니하도록 조치하여야 한다.

④ 개인정보처리자는 정보주체의 요구가 제1항 단서에 해당될 때에는 지체 없이 그 내용을 정보주체에게 알려야 한다.

⑤ 개인정보처리자는 제2항에 따른 조사를 할 때 필요하면 해당 정보주체에게 정정·삭제 요구사항의 확인에 필요한 증거자료를 제출하게 할 수 있다.

⑥ 제1항·제2항 및 제4항에 따른 정정 또는 삭제 요구, 통지 방법 및 절차 등에 필요한 사항은 대통령령으로 정한다.

시행령

제43조(개인정보의 정정·삭제 등) ① 정보주체는 법 제36조제1항에 따라 개인정보처리자에게 그 개인정보의 정정 또는 삭제를 요구하려면 개인정보처리자가 마련한 방법과 절차에 따라 요구하여야 한다. 이 경우 개인정보처리자가 개인정보의 정정 또는 삭제 요구 방법과 절차를 마련할 때에는 제41조제2항을 준용하되, “열람”은 “정정 또는 삭제”로 본다.

② 다른 개인정보처리자로부터 개인정보를 제공받아 개인정보파일을 처리하는 개인정보처리자는 법 제36조제1항에 따른 개인정보의 정정 또는 삭제 요구를 받으면 그 요구에 따라 해당 개인정보를 정정·삭제하거나 그 개인정보 정정·삭제에 관한 요구 사항을 해당 개인정보를 제공한 기관의 장에게 지체 없이 알리고 그 처리 결과에 따라 필요한 조치를 하여야 한다.

③ 개인정보처리자는 제1항과 제2항에 따른 개인정보 정정·삭제 요구를 받은 날부터 10일 이내에 법 제36조제2항에 따라 해당 개인정보의 정정·삭제 등의 조치를 한 경우에는 그 조치를 한 사실을, 법 제36조제1항 단서에 해당하여 삭제 요구에 따르지 아니한 경우에는 그 사실 및 이유와 이의제기방법을 보호위원회가 정하여 고시하는 개인정보 정정·삭제 결과 통지서로 해당 정보주체에게 알려야 한다.

고시

개인정보 처리 방법에 관한 고시(보호위원회 고시 제2020-7호)

	<p>제3조(개인정보보호 업무 관련 장부 및 문서 서식) ⑧ 법 제36조제6항과 영 제43조제3항에 따른 개인정보 정정·삭제 요구에 대한 결과의 통지, 법 제37조제5항과 영 제44조제2항에 따른 개인정보 처리정지 요구에 대한 결과의 통지는 별지 제10호서식의 개인정보 정정·삭제, 처리정지 요구에 대한 결과 통지서에 따른다.</p>
<p>표준지침</p>	<p>제32조(개인정보의 정정·삭제) ① 개인정보처리자가 법 제36조제1항에 따른 개인정보의 정정·삭제 요구를 받았을 때는 정당한 사유가 없는 한 요구를 받은 날로부터 10일 이내에 그 개인정보를 조사하여 정보주체의 요구에 따라 정정·삭제 등 필요한 조치를 한 후 그 결과를 정보주체에게 알려야 한다.</p> <p>② 정보주체의 정정·삭제 요구가 법 제36조제1항 단서에 해당하는 경우에는 정당한 사유가 없는 한 요구를 받은 날로부터 10일 이내에 삭제를 요구할 수 없는 근거법령의 내용을 정보주체에게 알려야 한다.</p>

개인정보처리자가 객관적 사실에 어긋나는 개인정보를 보유하고 있는 경우 정보주체로서는 부당한 처우나 부적절한 서비스 제공 등을 우려할 수 있고 자신에 대한 정체성의 왜곡을 걱정해야 할 수도 있다. 이는 그 자체로 정보주체의 중요한 권익이 침해되는 상황이라 할 수 있으므로, 정정청구권은 가능한 한 폭넓게 보장되어야 할 것이다. 하지만 정보의 일방적인 정정·삭제는 또 다른 문제를 야기할 수 있으므로 그 행사에는 일정한 제약이 따른다.

1. 정보주체의 정정·삭제 요구권

자신의 개인정보를 열람한 정보주체는 개인정보처리자에게 그 개인정보의 정정 또는 삭제를 요구할 수 있다(제1항). 정보주체가 개인정보처리자에게 그 개인정보의 정정 또는 삭제를 요구하려면 개인정보처리자가 마련한 방법과 절차에 따라 요구하여야 한다. 그 방법과 절차는 제35조제1항에 따른 열람 요구 방법과 절차와 동일하다(영 제43조제1항, 제41조제2항). 즉, 개인정보처리자가 정정 또는 삭제의 방법과 절차를 마련하는 경우에는 개인정보를 수집한 방법과 절차에 비하여 어렵지 아니하도록 영 제41조제2항에 따른 사항을 준수하여야 한다(이와 관련하여 자세한 내용은 제35조 개인정보의 열람 해설 참고).

그런데 개인정보의 정정 또는 삭제는 제35조에 따른 개인정보의 열람을 거친 경우에 요구할 수 있도록 규정하고 있으므로, 개인정보처리자가 제35조제4항에 따라 개인정보의 열람을 제한하거나 거절할 수 있는 경우에는 정보주체의 정정·삭제 요구권이 인정되지 않는다.

2. 정정·삭제 등의 조치

가 증거자료의 조사 등

개인정보처리자가 정보주체로부터 정정·삭제의 요구를 받았을 때에는 다른 법령에 특별한 절차가 규정되어 있는 경우를 제외하고는 지체 없이 그 개인정보를 조사하여야 한다. 이 경우 개인정보처리자는 해당 정보주체에게 정정·삭제 요구사항의 확인에 필요한 증거자료를 제출하게 할 수 있다.

나 정정·삭제 등 조치 및 통지

개인정보처리자는 조사결과 정보주체의 요구가 정당하다고 판단되면 개인정보 정정·삭제 요구를 받은 날부터 10일 이내에 그 개인정보를 조사하여 정보주체의 요구에 따라 해당 개인정보의 정정·삭제 등의 조치를 한 후 그 결과를 개인정보 정정·삭제 결과통지서(고시 제3조제8항 별지 제10호 서식)로 해당 정보주체에게 알려야 한다(제2항, 영 제43조제3항 전단).

개인정보처리자가 개인정보를 삭제할 때에는 복구 또는 재생되지 아니하도록 조치하여야 한다(제3항). 복구 또는 재생불가능한 삭제 방법과 관련하여 자세한 내용은 제21조(개인정보의 파기) 해설 부분을 참고하도록 한다.

다 정정·삭제 요구사항의 통지 등

다른 개인정보처리자로부터 개인정보를 제공받아 개인정보파일을 처리하는 개인정보처리자는 정보주체로부터 개인정보의 정정 또는 삭제 요구를 받은 때에는 그 요구에 따라 해당 개인정보를 정정·삭제하거나 그 개인정보 정정·삭제 요구 사항을 해당 개인정보를 제공한 기관의 장에게 지체 없이 알리고 그 처리 결과에 따라 필요한 조치를 하여야 한다(영 제43조제2항). 이 경우 필요한 조치의 방법과 절차는 ‘나. 정정·삭제 등 조치 및 통지의 내용’이 적용된다.

3. 삭제 거부의 통지

다른 법령에서 그 개인정보가 수집 대상으로 명시되어 있는 경우에는 그 삭제를 요구할 수 없다(제1항 단서). 이 경우 개인정보처리자는 개인정보 정정·삭제 요구서를 받은 날부터 10일 이내에 삭제의 요구에 따르지 않기로 한 사실, 그 이유와 이의제기 방법을 개인정보 정

정·삭제 결과통지서(고시 제3조제8항 별지 제10호 서식)로 해당 정보주체에게 알려야 한다(제4항, 영 제43조제3항 후단).

사례 법령에 의한 개인정보 보존의무

「통신비밀보호법 시행령」 제41조(전기통신사업자의 협조의무 등) ② 법 제15조의2제2항에 따른 전기통신사업자의 통신사실확인자료 보관기간은 다음 각 호의 구분에 따른 기간 이상으로 한다.

1. 법 제2조제11호가목부터 라목까지 및 바목에 따른 통신사실확인자료 : 12개월 다만, 시외·시내전화역무와 관련된 자료인 경우에는 6개월로 한다.
2. 법 제2조제11호마목 및 사목에 따른 통신사실확인자료 : 3개월

「전자상거래 등에서의 소비자보호에 관한 법률 시행령」 제6조(사업자가 보존하는 거래기록의 대상 등) ① 법 제6조제3항에 따라 사업자가 보존하여야 할 거래기록의 대상·범위 및 기간은 다음 각 호와 같다. 다만, 법 제20조제1항에 따른 통신판매중개자(이하 “통신판매중개자”라 한다)는 자신의 정보처리시스템을 통하여 처리한 기록의 범위에서 다음 각 호의 거래기록을 보존하여야 한다.

1. 표시·광고에 관한 기록: 6개월
2. 계약 또는 청약철회 등에 관한 기록: 5년
3. 대금결제 및 재화등의 공급에 관한 기록: 5년
4. 소비자의 불만 또는 분쟁처리에 관한 기록: 3년

② 법 제6조제3항에 따라 사업자가 소비자에게 제공하여야 할 거래기록의 열람·보존의 방법은 다음 각 호와 같다.

1. 거래가 이루어진 해당 사이버물(제2조제4호의 사이버물을 말한다. 이하 같다)에서 거래당사자인 소비자가 거래기록을 열람·확인할 수 있도록 하고, 전자문서의 형태로 정보처리시스템 등에 저장할 수 있도록 할 것
2. 거래당사자인 소비자와의 거래기록을 그 소비자의 희망에 따라 방문, 전화, 팩스 또는 전자우편 등의 방법으로 열람하거나 복사할 수 있도록 할 것. 다만, 거래기록 중에 「저작권법」 제4조부터 제6조까지의 규정에 따른 저작물(「저작권법」에 따라 복사할 수 있는 저작물은 제외한다)이 있는 경우에는 그에 대한 복사는 거부할 수 있다.
3. 사업자가 법 제6조제2항에 따라 개인정보의 이용에 관한 동의를 철회한 소비자의 거래기록 및 개인정보를 보존하는 경우에는 개인정보의 이용에 관한 동의를 철회하지 아니한 소비자의 거래기록 및 개인정보와 별도로 보존할 것

4. 다른 법률과의 관계

「신용정보법」은 신용정보주체가 신용정보의 정정청구 및 삭제요구를 할 수 있도록 규정하고 있으므로, 신용정보주체는 「신용정보법」에 따라 신용정보 정정청구권 및 삭제요구권을 행사할 수 있다.

신용정보법	<p>제38조(신용정보의 열람 및 정정청구 등) ② 제1항에 따라 자신의 신용정보를 열람한 신용정보주체는 본인 신용정보가 사실과 다른 경우에는 금융위원회가 정하여 고시하는 바에 따라 정정을 청구할 수 있다. <신설 2020. 2. 4.></p> <p>③ 제2항에 따라 정정청구를 받은 신용정보회사등은 정정청구에 정당한 사유가 있다고 인정하면 지체 없이 해당 신용정보의 제공·이용을 중단한 후 사실인지를 조사하여 사실과 다르거나 확인할 수 없는 신용정보는 삭제하거나 정정하여야 한다.</p> <p>④ 제3항에 따라 신용정보를 삭제하거나 정정한 신용정보회사등은 해당 신용정보를 최근 6개월 이내에 제공받은 자와 해당 신용정보주체가 요구하는 자에게 해당 신용정보에서 삭제하거나 정정한 내용을 알려야 한다.</p> <p>⑤ 신용정보회사등은 제3항 및 제4항에 따른 처리결과를 7일 이내에 해당 신용정보주체에게 알려야 하며, 해당 신용정보주체는 처리결과에 이의가 있으면 대통령령으로 정하는 바에 따라 금융위원회에 그 시정을 요청할 수 있다. 다만, 개인 신용정보에 대한 제45조의3제1항에 따른 상거래기업 및 법인의 처리에 대하여 이의가 있으면 대통령령으로 정하는 바에 따라 「개인정보 보호법」에 따른 개인정보 보호위원회(이하 “보호위원회”라 한다)에 그 시정을 요청할 수 있다.</p> <p>⑥ 금융위원회 또는 보호위원회는 제5항에 따른 시정을 요청받으면 「금융위원회의 설치 등에 관한 법률」 제24조에 따라 설립된 금융감독원의 원장(이하 “금융감독원장”이라 한다) 또는 보호위원회가 지정한 자로 하여금 그 사실 여부를 조사하게 하고, 조사결과에 따라 신용정보회사등에 대하여 시정을 명하거나 그 밖에 필요한 조치를 할 수 있다. 다만, 필요한 경우 보호위원회는 해당 업무를 직접 수행할 수 있다.</p> <p>⑦ 제6항에 따라 조사를 하는 자는 그 권한을 표시하는 증표를 지니고 이를 관계인에게 내보여야 한다.</p> <p>⑧ 신용정보회사등이 제6항에 따른 금융위원회 또는 보호위원회의 시정명령에 따라 시정조치를 한 경우에는 그 결과를 금융위원회 또는 보호위원회에 보고하여야 한다.</p> <p>제38조의3(개인신용정보의 삭제 요구) ① 신용정보주체는 금융거래 등 상거래관계가 종료되고 대통령령으로 정하는 기간이 경과한 경우 신용정보제공·이용자에게 본인의 개인신용정보의 삭제를 요구할 수 있다. 다만, 제20조의2제2항 각 호의 어느 하나에 해당하는 경우에는 그러하지 아니하다.</p> <p>② 신용정보제공·이용자가 제1항의 요구를 받았을 때에는 지체 없이 해당 개인 신용정보를 삭제하고 그 결과를 신용정보주체에게 통지하여야 한다.</p> <p>③ 신용정보제공·이용자는 신용정보주체의 요구가 제1항 단서에 해당될 때에는 다른 개인신용정보와 분리하는 등 대통령령으로 정하는 바에 따라 관리하여야 하며, 그 결과를 신용정보주체에게 통지하여야 한다.</p> <p>④ 제2항 및 제3항에 따른 통지의 방법은 금융위원회가 정하여 고시한다.</p>
-------	--

5. 가명정보의 적용 제외

정보주체는 가명정보에 대하여 제36조에 따른 정정·삭제 요구권을 행사할 수 없다(제28조의7).

6. 벌칙규정

위반행위	벌칙
개인정보의 정정·삭제요청에 대한 필요한 조치를 취하지 않고, 개인정보를 계속 이용하거나 제3자에게 제공한 정보통신서비스 제공자등 (제36조제2항 위반)	5년 이하의 징역 또는 5천만원 이하의 벌금 (제71조제4의4호)
개인정보의 정정·삭제요청에 대한 필요한 조치를 취하지 않고, 개인정보를 계속 이용하거나 제3자에게 제공한 자(제36조제2항 위반)	2년 이하 징역 또는 2천만원 이하의 벌금 (제73조제2호)
정보주체의 정정·삭제요구에 따라 필요조치를 취하지 아니한 자 (제36조제2항 위반)	3천만원 이하의 과태료 (제75조제2항제11호)
정보주체의 정정·삭제 요구 거부 시 통지의무 불이행 (제36조제2항·제4항 위반)	1천만원 이하의 과태료 (제75조제4항제9호)

제37조 | 개인정보의 처리정지 등

법률	<p>제37조(개인정보의 처리정지 등) ① 정보주체는 개인정보처리자에 대하여 자신의 개인정보 처리의 정지를 요구할 수 있다. 이 경우 공공기관에 대하여는 제32조에 따라 등록 대상이 되는 개인정보파일 중 자신의 개인정보에 대한 처리의 정지를 요구할 수 있다.</p> <p>② 개인정보처리자는 제1항에 따른 요구를 받았을 때에는 지체 없이 정보주체의 요구에 따라 개인정보 처리의 전부를 정지하거나 일부를 정지하여야 한다. 다만, 다음 각 호의 어느 하나에 해당하는 경우에는 정보주체의 처리정지 요구를 거절할 수 있다.</p> <ol style="list-style-type: none"> 1. 법률에 특별한 규정이 있거나 법령상 의무를 준수하기 위하여 불가피한 경우 2. 다른 사람의 생명·신체를 해할 우려가 있거나 다른 사람의 재산과 그 밖의 이익을 부당하게 침해할 우려가 있는 경우 3. 공공기관이 개인정보를 처리하지 아니하면 다른 법률에서 정하는 소관 업무를 수행할 수 없는 경우 4. 개인정보를 처리하지 아니하면 정보주체와 약정한 서비스를 제공하지 못하는 등 계약의 이행이 곤란한 경우로서 정보주체가 그 계약의 해지 의사를 명확하게 밝히지 아니한 경우 <p>③ 개인정보처리자는 제2항 단서에 따라 처리정지 요구를 거절하였을 때에는 정보주체에게 지체 없이 그 사유를 알려야 한다.</p> <p>④ 개인정보처리자는 정보주체의 요구에 따라 처리가 정지된 개인정보에 대하여 지체 없이 해당 개인정보의 파기 등 필요한 조치를 하여야 한다.</p> <p>⑤ 제1항부터 제3항까지의 규정에 따른 처리정지의 요구, 처리정지의 거절, 통지 등의 방법 및 절차에 필요한 사항은 대통령령으로 정한다.</p>
시행령	<p>제44조(개인정보의 처리정지 등) ① 정보주체는 법 제37조제1항에 따라 개인정보처리자에게 자신의 개인정보 처리의 정지를 요구하려면 개인정보처리자가 마련한 방법과 절차에 따라 요구하여야 한다. 이 경우 개인정보처리자가 개인정보의 처리 정지 요구 방법과 절차를 마련할 때에는 제41조제2항을 준용하되, “열람”은 “처리 정지”로 본다.</p> <p>② 개인정보처리자는 제1항에 따른 개인정보 처리정지 요구를 받은 날부터 10일 이내에 법 제37조제2항 본문에 따라 해당 개인정보의 처리정지 조치를 한 경우에는 그 조치를 한 사실을, 같은 항 단서에 해당하여 처리정지 요구에 따르지 않은 경우에는 그 사실 및 이유와 이의제기방법을 보호위원회가 정하여 고시하는 개인정보 처리정지 요구에 대한 결과 통지서로 해당 정보주체에게 알려야 한다.</p>
고시	<p style="text-align: center;">개인정보 처리 방법에 관한 고시(보호위원회 고시 제2020-7호)</p> <p>제3조(개인정보보호 업무 관련 장부 및 문서 서식) ⑧ 법 제36조제6항과 영 제</p>

	<p>43조제3항에 따른 개인정보 정정·삭제 요구에 대한 결과의 통지, 법 제37조 제5항과 영 제44조제2항에 따른 개인정보 처리정지 요구에 대한 결과의 통지는 별지 제10호서식의 개인정보 정정·삭제, 처리정지 요구에 대한 결과 통지서에 따른다.</p>
<p>표준지침</p>	<p>제33조(개인정보의 처리정지) ① 개인정보처리자가 정보주체로부터 법 제37조 제1항에 따라 개인정보처리를 정지하도록 요구받은 때에는 정당한 사유가 없는 한 요구를 받은 날로부터 10일 이내에 개인정보 처리의 일부 또는 전부를 정지하여야 한다. 다만, 법 제37조제2항 단서에 해당하는 경우에는 정보주체의 처리정지 요구를 거절할 수 있다.</p> <p>② 개인정보처리자는 정보주체의 요구에 따라 처리가 정지된 개인정보에 대하여 정당한 사유가 없는 한 처리정지의 요구를 받은 날로부터 10일 이내에 해당 개인정보의 파기 등 정보주체의 요구에 상응하는 조치를 취하고 그 결과를 정보주체에게 알려야 한다.</p>

1. 정보주체의 처리정지 요구권

정보주체는 개인정보처리자에 대하여 자신의 개인정보 처리의 정지를 요구할 수 있다(제1항제1문). 처리정지 요구권은 개인정보처리 활동에 대한 정지를 요구하는 것으로 동의 철회권보다 적용 범위가 더 넓다. 동의 철회권은 정보주체 자신이 동의한 것에 대해서만 동의를 철회할 수 있으나, 처리정지 요구권은 정보주체 자신이 처리에 동의하지 않았더라도 개인정보처리자가 처리하고 있는 정보주체에 관한 모든 개인정보의 처리 정지를 요구할 수 있다. 정보주체는 처리정지 요구의 이유를 소명할 필요가 없으며 언제든지 요구가 가능하다.

한편, 정보주체가 공공기관에 대하여 개인정보 처리정지를 요구하는 경우에는 제32조에 따라 보호위원회에 등록 대상이 되는 개인정보파일 중에 포함된 자신의 개인정보에 대해서만 처리정지를 요구할 수 있다(제1항제2문). 따라서 다음 각 호의 파일에 포함되어 있는 개인정보에 대해서는 처리정지 요구권을 행사하지 못한다.

처리정지 요구의 예외인 개인정보파일(제32조제2항)

1. 국가 안전, 외교상 비밀, 그 밖에 국가의 중대한 이익에 관한 사항을 기록한 개인정보파일
2. 범죄의 수사, 공소의 제기 및 유지, 형 및 감호의 집행, 교정처분, 보호처분, 보안관찰처분과 출입국관리에 관한 사항을 기록한 개인정보파일
3. 「조세범처벌법」에 따른 범칙행위 조사 및 「관세법」에 따른 범칙행위 조사에 관한 사항을 기록한 개인정보파일
4. 공공기관의 내부적 업무처리만을 위하여 사용 되는 개인정보파일
5. 다른 법령에 따라 비밀로 분류된 개인정보파일

정보주체는 개인정보처리자에게 자신의 개인정보 처리의 정지를 요구하려는 경우 개인정보처리자가 마련한 방법과 절차에 따라 요구하여야 한다. 그 방법과 절차는 제35조제1항에 따른 열람 요구 방법과 절차와 동일하다(영 제44조제1항, 제41조제2항). 즉, 개인정보처리자가 처리정지의 방법과 절차를 마련하는 경우에는 개인정보를 수집한 방법과 절차에 비하여 어렵지 아니하도록 영 제41조제2항에 따른 사항을 준수하여야 한다(이와 관련하여 자세한 내용은 제35조(개인정보의 열람) 해설 참고).

2. 개인정보의 처리정지

개인정보처리자는 개인정보 처리정지 요구를 받았을 때에는 지체 없이 정보주체의 요구에 따라 개인정보 처리의 전부를 정지하거나 일부를 정지하여야 한다. 개인정보처리자는 처리정지 요구에 대한 예외 혹은 거부 사유가 없는 한 처리정지를 하여야 하는데, 처리정지를 요구받은 대상 처리 유형만을 정지하는 것으로 충분하지만 특정 처리 유형의 정지만으로는 그 처리정지 요구를 이행할 수 없는 경우에는 처리의 전부를 정지하여야 한다. 이 경우 개인정보처리자는 개인정보 처리정지 요구를 받은 날부터 근무일 기준 10일 이내에 처리정지 조치를 한 사실을 적은 개인정보 처리정지 요구에 대한 결과 통지서(고시 제3조제8항 별제 제10호 서식)로 해당 정보주체에게 알려야 한다(제4항). 개인정보처리자는 정보주체의 요구가 있으면 처리가 정지된 개인정보에 대하여 지체 없이 해당 개인정보의 파기 등 필요한 조치를 하여야 한다. 개인정보의 파기 이외의 필요한 조치로는 해당 개인정보를 이용 또는 제공하지 않도록 해당 개인정보를 분리하여 별도의 개인정보파일(예를 들면, 처리정지 개인정보파일)에 분리·보관하는 것이나 해당 개인정보가 처리 정지된 목적을 달성하는데 해가 되지 않는 범위 내에서 이용 또는 제공할 수 있도록 제한 설정 등이 있으며, 개별적인 사안에서 정보주체가 요구한 처리정지의 목적을 달성하기에 적합한 최적의 조치를 취하여야 한다.

3. 처리정지 요구의 거부

개인정보처리자가 정보주체로부터 개인정보 처리정지 요구를 받았을 때 다음 각 호의 어느 하나에 해당하는 경우에는 정보주체의 처리정지 요구를 거절할 수 있다(제2항 각 호). 이 경우 개인정보처리자는 정보주체로부터 개인정보 처리정지 요구를 받은 날부터 근무일 기준 10일 이내에 처리정지 요구를 거절하기로 한 사실 및 그 이유와 이의제기 방법을 적은 개인정보 처리정지 요구에 대한 결과 통지서(고시 제3조제8항 별지 제10호 서식)를 해당 정보주체에게 알려야 한다(제3항, 영 제44조제2항).

처리정지요구 거부사유(제37조제2항)

1. 법률에 특별한 규정이 있거나 법령상 의무를 준수하기 위하여 불가피한 경우
2. 다른 사람의 생명·신체를 해할 우려가 있거나 다른 사람의 재산과 그 밖의 이익을 부당하게 침해할 우려가 있는 경우
3. 공공기관이 개인정보를 처리하지 아니하면 다른 법률에서 정하는 소관 업무를 수행할 수 없는 경우
4. 개인정보를 처리하지 아니하면 정보주체와 약정한 서비스를 제공하지 못하는 등 계약의 이행이 곤란한 경우로서 정보주체가 그 계약의 해지 의사를 명확하게 밝히지 아니한 경우

4. 다른 법률과의 관계

「신용정보법」에서는 개인정보 처리정지에 대하여 별도의 규정을 마련하고 있지 않으므로, 일반법인 「개인정보 보호법」이 적용된다.

5. 가명정보의 적용 제외

가명정보에는 이름, 연락처 등 개인을 알아 볼 수 있는 정보가 포함되어 있지 않으므로 정보주체는 가명정보에 대하여 제37조에 따른 처리정지 요구권을 행사할 수 없다(제28조의7). 다만, 정보주체는 자신의 정보가 가명정보로 처리되기 이전에는 자신의 개인정보에 대한 가명처리 정지를 요구할 수 있다.

6. 벌칙규정

위반행위	벌칙
개인정보의 처리정지 요구에 따라 처리를 중단하지 않고 계속 이용하거나 제3자에게 제공한 자(제37조제2항 위반)	2년 이하의 징역 또는 2천만원 이하의 벌금 (제73조제3호)
처리 정지된 개인정보에 대해 파기 등의 조치를 하지 않은 자(제37조제4항 위반)	3천만원 이하의 과태료 (제75조제2항제12호)
정보주체의 처리정지 요구 거부 시 통지의무 불이행 (제37조제3항 위반)	1천만원 이하의 과태료 (제75조제4항제9호)

7. 질의 응답

Q | 잠재고객들에 대하여 우리 회사 서비스의 광고 메일 및 전화(TM) 홍보를 실시하고 있는데, 어떤 고객이 수신거부를 요청하였다. 이 경우 취해야 할 조치는 무엇인가?

A | 정보주체가 광고메일 및 전화 TM에 대한 수신거부를 요청한 경우에 사업자는 10일 이내(영 제43조)에 발송 중지 및 리스트 삭제 등 필요한 조치를 취하여야 한다.

제38조 | 권리행사의 방법 및 절차

법률

제38조(권리행사의 방법 및 절차) ① 정보주체는 제35조에 따른 열람, 제36조에 따른 정정·삭제, 제37조에 따른 처리정지, 제39조의7에 따른 동의 철회 등의 요구(이하 “열람등요구”라 한다)를 문서 등 대통령령으로 정하는 방법·절차에 따라 대리인에게 하게 할 수 있다.

② 만 14세 미만 아동의 법정대리인은 개인정보처리자에게 그 아동의 개인정보 열람등요구를 할 수 있다.

③ 개인정보처리자는 열람등요구를 하는 자에게 대통령령으로 정하는 바에 따라 수수료와 우송료(사본의 우송을 청구하는 경우에 한한다)를 청구할 수 있다.

④ 개인정보처리자는 정보주체가 열람등요구를 할 수 있는 구체적인 방법과 절차를 마련하고, 이를 정보주체가 알 수 있도록 공개하여야 한다.

⑤ 개인정보처리자는 정보주체가 열람등요구에 대한 거절 등 조치에 대하여 불복이 있는 경우 이의를 제기할 수 있도록 필요한 절차를 마련하고 안내하여야 한다.

시행령

제45조(대리인의 범위 등) ① 법 제38조에 따라 정보주체를 대리할 수 있는 자는 다음 각 호와 같다.

1. 정보주체의 법정대리인
2. 정보주체로부터 위임을 받은 자

② 제1항에 따른 대리인이 법 제38조에 따라 정보주체를 대리할 때에는 개인정보처리자에게 보호위원회가 정하여 고시하는 정보주체의 위임장을 제출하여야 한다.

제46조(정보주체 또는 대리인의 확인) ① 개인정보처리자는 제41조제1항에 따른 열람, 제43조제1항에 따른 정정·삭제, 제44조제1항에 따른 처리정지 또는 법 제39조의7제1항에 따른 동의 철회 등의 요구(이하 이 조, 제47조 및 제48조에서 “열람등요구”라 한다)를 받았을 때에는 열람등요구를 한 사람이 본인이거나 정당한 대리인인지를 확인하여야 한다.

② 공공기관인 개인정보처리자가 「전자정부법」 제36조제1항에 따른 행정정보의 공동이용을 통하여 제1항에 따른 확인을 할 수 있는 경우에는 행정정보의 공동이용을 통하여 확인하여야 한다. 다만, 해당 공공기관이 행정정보의 공동이용을 할 수 없거나 정보주체가 확인에 동의하지 아니하는 경우에는 그러하지 아니하다.

제47조(수수료 등의 금액 등) ① 법 제38조제3항에 따른 수수료와 우송료의 금액은 열람등요구에 필요한 실비의 범위에서 해당 개인정보처리자가 정하는 바에 따른다. 다만, 개인정보처리자가 지방자치단체인 경우에는 그 지방자치단체의 조례로 정하는 바에 따른다.

	<p>② 개인정보처리자는 열람등요구를 하게 된 사유가 그 개인정보처리자에게 있는 경우에는 수수료와 우송료를 청구해서는 아니 된다.</p> <p>③ 법 제38조제3항에 따른 수수료 또는 우송료는 다음 각 호의 구분에 따른 방법으로 낸다. 다만, 국회, 법원, 헌법재판소, 중앙선거관리위원회, 중앙행정기관 및 그 소속 기관(이하 이 조에서 “국가기관”이라 한다) 또는 지방자치단체인 개인정보처리자는 「전자금융거래법」 제2조제11호에 따른 전자지급수단 또는 「정보통신망 이용촉진 및 정보보호 등에 관한 법률」 제2조제10호에 따른 통신과금서비스를 이용하여 수수료 또는 우송료를 내게 할 수 있다.</p> <ol style="list-style-type: none"> 1. 국가기관인 개인정보처리자에게 내는 경우: 수입인지 2. 지방자치단체인 개인정보처리자에게 내는 경우: 수입증지 3. 국가기관 및 지방자치단체 외의 개인정보처리자에게 내는 경우: 해당 개인정보처리자가 정하는 방법 <p>제48조(열람 요구 지원시스템의 구축 등) ① 개인정보처리자는 열람등요구 및 그에 대한 통지를 갈음하여 해당 업무를 전자적으로 처리할 수 있도록 시스템을 구축·운영하거나 그 밖의 절차를 정하여 해당 업무를 처리할 수 있다.</p> <p>② 보호위원회는 개인정보처리자 중 공공기관이 보유하고 있는 개인정보에 관한 열람등요구 및 그에 대한 통지에 관한 공공기관의 업무 수행을 효율적으로 지원하기 위하여 시스템을 구축·운영할 수 있다.</p>
<p>고시</p>	<p>개인정보 처리 방법에 관한 고시(보호위원회 고시 제2020-7호)</p> <p>제3조(개인정보보호 업무 관련 장부 및 문서 서식) ⑨ 영 제45조제2항에 따른 정보주체의 위임장은 별지 제11호서식과 같다.</p>
<p>표준지침</p>	<p>제34조(권리행사의 방법 및 절차) ① 개인정보처리자는 정보주체가 법 제38조제1항에 따른 열람등요구를 하는 경우에는 개인정보를 수집하는 방법과 동일하거나 보다 쉽게 정보주체가 열람요구 등 권리를 행사할 수 있도록 간편한 방법을 제공하여야 하며, 개인정보의 수집시에 요구되지 않았던 증빙서류 등을 요구하거나 추가적인 절차를 요구할 수 없다.</p> <p>② 제1항의 규정은 영 제46조에 따라 본인 또는 정당한 대리인임을 확인하고자 하는 경우와 영 제47조에 따른 수수료와 우송료의 정산에도 준용한다.</p>

개인정보처리자는 정보주체의 권리행사 방법과 절차를 어렵게 하거나 정보주체에게 과도한 비용을 청구하여서는 안 된다. 그러나 정보주체 이외의 자가 권한 없이 또는 권한을 넘어 정보주체의 권리를 대신하여 행사하지 못하도록 적절한 수준의 본인확인 절차를 강구하여야 한다.

1. 대리인에 의한 권리행사

정보주체는 열람의 요구, 정정·삭제의 요구, 처리정지의 요구, 동의 철회의 요구 등(이하 “열람등 요구”라 한다)의 권리행사를 대리인을 통하여 할 수 있다(제1항). 대리인의 범위에는 정보주체의 법정대리인 이외에 정보주체로부터 위임계약 등에 기하여 대리권을 수여받은 임의대리인도 포함된다(영 제45조). 만 14세 이상의 미성년자인 정보주체의 개인정보에 관하여는 미성년자 본인이 위의 권리를 행사할 수도 있고, 만 14세 이상의 미성년자의 법정대리인을 통하여 위의 권리를 행사할 수도 있다. 이처럼 정보주체의 개인정보와 관련한 요구권을 대리인을 통해 하도록 하는 것으로 개인정보자기결정권을 행사하는데 필요한 부수적인 절차적 행위를 대리할 수 있다. 따라서 개인정보자기결정권의 본질인 정보주체의 개인정보 정정·삭제, 처리정지 여부의 결정은 정보주체만이 할 수 있다.

2. 법정대리인의 권리행사

만 14세 미만 아동의 법정대리인은 개인정보처리자에게 그 아동에 관한 개인정보의 열람등요구를 할 수 있다(제2항). 만 14세 미만 아동에 관한 개인정보의 열람등요구는 법정대리인이 직접 해야 하며 아동이 법정대리인의 동의를 받아서 하는 것은 허용되지 않는다. 법 제22조제5항에서 만 14세 미만 아동의 개인정보를 처리하기 위하여 이 법에 따른 동의를 받아야 하는 때에는 그 법정대리인의 동의를 받도록 한 것과 같은 맥락이다.

3. 신원확인 의무와 방법

가 신원확인 의무

개인정보처리자는 개인정보 열람등요구를 받은 때에는 요구를 한 자가 본인이거나 정당한 대리인인지를 확인하여야 한다. 대리인의 경우에는 대리인 자신에 관한 신원확인뿐만 아니라 정보주체와 대리인 사이의 대리관계를 증명할 수 있는 위임장 및 인감 또는 법정대리인의 경우에는 법정대리인임을 확인할 수 있는 서면(주민등록등본, 가족관계증명서 등)을 추가로 확인하여야 한다.

나 신원확인 방법

신원확인의 방법은 별도로 특정되어 있지 않다. 따라서 인터넷의 경우에는 전자서명, 아

이핀, 이동전화번호와 생년월일 등의 방법에 의해서 확인하면 되고, 오프라인의 경우에는 주민등록증, 운전면허증, 여권, 공무원증 등에 의하면 된다. 즉 합리적인 수단이라고 객관적으로 인정되는 방식이면 된다.

다 공공기관의 특례

개인정보처리자가 공공기관인 경우에는 「전자정부법」 제36조제1항에 따른 행정정보의 공동이용을 통하여 신분확인이 가능하면 행정정보의 공동이용을 통하여 확인하여야 한다. 다만, 해당 공공기관이 행정정보의 공동이용을 할 수 없거나 정보주체가 확인에 동의하지 아니하는 경우에는 그러하지 아니하다.

4. 열람수수료 등의 청구

가 부과기준

개인정보처리자는 열람등 요구를 한 자에게 수수료와 우송료(사본의 우송을 청구하는 경우에 한한다)를 청구할 수 있다. 다만, 수수료와 우송료의 금액은 개인정보의 열람등요구에 필요한 실비의 범위에서 청구해야 한다. 개인정보처리자가 지방자치단체인 경우에는 해당 지방자치단체의 조례로 정하는 바에 따른다.

나 납부방법

① 국가기관 및 지방자치단체

국회, 법원, 헌법재판소, 중앙선거관리위원회, 중앙행정기관 및 그 소속기관(이하 이 조에서 “국가기관”이라 한다)인 개인정보처리자에게 수수료 또는 우송료를 납부하는 경우에는 수입인지로, 지방자치단체인 개인정보처리자에게 납부하는 경우에는 수입증지로 각각 납부한다.

다만, 국가기관 또는 지방자치단체인 개인정보처리자는 「전자금융거래법」 제2조제11호에 따른 전자지급수단 또는 「정보통신망 이용촉진 및 정보보호 등에 관한 법률」 제2조제10호에 따른 통신과금서비스를 이용하여 수수료 또는 우송료를 납부하게 할 수 있다.

② 그밖에 개인정보처리자

국가기관 및 지방자치단체 외의 개인정보처리자에게 수수료 또는 우송료를 납부하는 경우의 수수료 납부 방법은 해당 개인정보처리자가 정한다.

다 징수권 상실

개인정보 열람등요구를 하게 된 사유가 해당 개인정보처리자에 있는 경우에는 수수료와 우송료를 청구할 수 없다. 여기서 열람등요구를 하게 된 사유가 해당 개인정보처리자에 있다고 하는 것은 개인정보처리자에게 ‘잘못(고의·과실)이 있는 경우’라는 의미로 해석해서는 안 되고 해당 개인정보의 처리가 개인정보처리자의 이익을 위해서 또는 개인정보처리자의 책임영역에서 발생했다는 의미로 새겨야 할 것이다. 따라서 개인정보처리자가 자신을 위하여 개인정보를 처리하였거나 자신에게 그 처리의 이익이 있는 등의 경우에는 정보주체가 특별한 사유 없이 단지 ‘궁금하다’ 또는 ‘확인해 보고 싶다’라고 해서 열람등요구를 하는 경우를 제외하고는 수수료나 우송료를 청구해서는 안 될 것이다.

5. 권리행사의 방법과 절차

가 권리행사 방법 및 절차

개인정보처리자는 정보주체가 열람등요구를 할 수 있는 구체적인 방법과 절차를 마련하고, 이를 정보주체가 알 수 있도록 공개하여야 한다(제4항). 다수의 정보주체들이 자신의 권리를 알지 못하고, 알고 있는 경우에도 절차가 까다롭고 복잡해 포기하는 경우가 많다. 따라서 정보주체의 권리행사 방법 및 절차는 개인정보를 수집하는 방법과 동일하거나 보다 쉽게 권리를 행사할 수 있도록 간편한 방법을 제공하여야 하며, 개인정보 수집시에 요구되지 않았던 증빙서류 등을 요구하거나 추가적인 절차를 요구해서는 안 된다(표준지침 제34조제1항). 또한, 정보주체가 편리하게 선택할 수 있도록 가급적 다양한 권리행사 방법을 마련하여 제공해야 한다. 예컨대 방문, 서면, 전화, 전자우편, 인터넷 웹사이트 등 다양한 방법으로 정보주체가 열람등요구를 할 수 있도록 해야 한다.

나 이의제기 절차

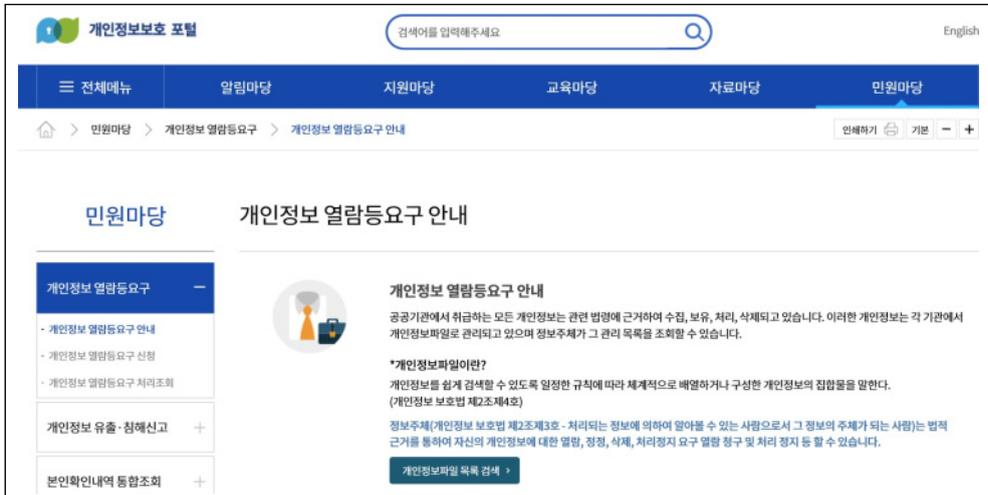
열람등요구에 대한 거절 등 조치에 대하여 불복이 있는 경우 정보주체가 이의를 제기할 수 있도록 개인정보처리자는 필요한 절차를 마련하고 안내하여야 한다(제5항). 이 경우 이의제기 절차는 공정하게 운영될 수 있도록 외부전문가를 참여시키거나 내부의 견제장치가 마련되어 있어야 한다.

다 열람등 지원시스템 구축

개인정보처리자는 열람등요구 및 그에 대한 통지에 갈음하여 해당 업무를 전자적으로 처리할 수 있도록 시스템을 구축·운영하거나 그 밖의 업무처리 절차를 정할 수 있다.

보호위원회는 개인정보처리자 중 공공기관이 보유하고 있는 개인정보에 관한 열람등요구 및 그에 대한 통지에 관한 공공기관의 업무 수행을 효율적으로 지원하기 위하여 개인정보보호 종합포털을 구축하여 운영하고 있다.

< 개인정보보호 종합포털(www.privacy.go.kr)>



6. 다른 법률과의 관계

「신용정보법」에는 신용정보주체의 권리행사 방법 및 절차를 별도로 규정하고 있으므로, 신용정보주체는 「신용정보법」에 따라 열람등요구를 할 수 있다.

신용정보법	<p>제39조의3(신용정보주체의 권리행사 방법 및 절차) ① 신용정보주체는 다음 각 호의 권리행사(이하 “열람등요구”라 한다)를 서면 등 대통령령으로 정하는 방법·절차에 따라 대리인에게 하게 할 수 있다.</p> <ol style="list-style-type: none"> 1. 제33조의2제1항에 따른 전송요구 2. 제36조제1항에 따른 고지요구 3. 제36조의2제1항에 따른 설명 요구 및 제2항 각 호의 어느 하나에 해당하는 행위 4. 제37조제1항에 따른 동의 철회 및 제2항에 따른 연락중지 청구 5. 제38조제1항 및 제2항에 따른 열람 및 정정청구 6. 제38조의2제1항에 따른 통지 요청 7. 제39조에 따른 무료열람
-------	--

8. 제39조의2제2항에 따른 교부 또는 열람

② 만 14세 미만 아동의 법정대리인은 신용정보회사등에 그 아동의 개인신용정보에 대하여 열람등요구를 할 수 있다.

7. 질의응답

Q | 민간사업자의 수수료 청구 기준은?

A | 개인정보처리자는 열람등을 요구하는 자에게 수수료와 우송료를 청구할 수 있다. 다만 열람등에 따른 조치시 필요한 인쇄비, 공공요금, 인건비 등을 계산하여 최소한의 실비만을 청구하여야 한다.

제39조 | 손해배상책임

법률

제39조(손해배상책임) ① 정보주체는 개인정보처리자가 이 법을 위반한 행위로 손해를 입으면 개인정보처리자에게 손해배상을 청구할 수 있다. 이 경우 그 개인정보처리자는 고의 또는 과실이 없음을 입증하지 아니하면 책임을 면할 수 없다.

② 삭제

③ 개인정보처리자의 고의 또는 중대한 과실로 인하여 개인정보가 분실·도난·유출·위조·변조 또는 훼손된 경우로서 정보주체에게 손해가 발생한 때에는 법원은 그 손해액의 3배를 넘지 아니하는 범위에서 손해배상액을 정할 수 있다. 다만, 개인정보처리자가 고의 또는 중대한 과실이 없음을 증명한 경우에는 그러하지 아니하다.

④ 법원은 제3항의 배상액을 정할 때에는 다음 각 호의 사항을 고려하여야 한다.

1. 고의 또는 손해 발생의 우려를 인식한 정도
2. 위반행위로 인하여 입은 피해 규모
3. 위법행위로 인하여 개인정보처리자가 취득한 경제적 이익
4. 위반행위에 따른 벌금 및 과징금
5. 위반행위의 기간·횟수 등
6. 개인정보처리자의 재산상태
7. 개인정보처리자가 정보주체의 개인정보 분실·도난·유출 후 해당 개인정보를 회수하기 위하여 노력한 정도
8. 개인정보처리자가 정보주체의 피해구제를 위하여 노력한 정도

‘개인정보’ 유출이나 오·남용 사건의 경우, 일반적인 ‘정보’ 유출 사건 또는 오·남용 사건과 같이 언제, 어느 단계에서, 누구의 잘못으로 인해 사건이 발생했는지 정확히 파악하기 어려운 경우가 대부분이다. 따라서 제39조는 개인정보 유출사고나 오남용 피해가 발생한 경우에는 해당 개인정보를 처리해서 이익을 얻고 있는 개인정보처리자가 스스로 고의 또는 과실이 없음을 증명하게 하여 개인정보처리자의 권리 중 하나인 신속·공정한 피해구제를 받을 권리를 실질적으로 보장하고자 하는 것이다.

이 법은 일반적인 손해배상청구권뿐만 아니라 개인정보처리자에게 고의 또는 중대한 과실로 인한 위법행위가 있는 경우에는 사회에 미치는 악영향, 위법행위에 대한 강력한 억제 효과, 악성 위법행위로 인한 피해자에 대한 피해구제의 강화 등을 고려하여 실손해액의 3배의 범위 내에서 손해배상청구를 할 수 있는 징벌적 손해배상청구권을 도입하였다.

참고 손해배상책임의 성립요건

- 침해행위가 존재하고 위법할 것
- 손해가 발생하였을 것
- 침해행위와 손해 사이에 인과관계가 있을 것
- 고의 또는 과실 및 책임능력이 있을 것

1. 손해배상청구권의 성립요건

가 이 법 위반행위가 있을 것

이 조에 따른 손해배상청구권이 발생하기 위해서는 개인정보처리자에게 이 법을 위반한 사실(침해행위)이 있어야 한다. 그러나 이 법을 위반했다는 것만으로 곧장 손해배상책임이 발생하는 것은 아니다. 그 위반행위가 법질서 전체의 입장과 객관적으로 모순·충돌하는 경우 즉 위법성(違法性)이 인정되는 경우에 한해서 책임을 진다.

통상적으로 이 법을 위반한 경우에는 일단 위법한 것으로 판단되지만, 그 위반행위가 특정한 사정에 의하여 실질적으로 또는 사회적으로 허용될만한 것이라고 인정되는 경우, 다시 말해 공서양속(公序良俗), 조리(條理), 사회통념 등 사회상규에 반하지 않다고 인정되는 경우에는 위법성이 조각된다. 개인정보는 다른 사람의 생명·신체·재산을 보호하기 위하여 이용되는 경우가 많으므로 손해배상책임을 결정함에 있어서는 특별히 위법성 조각사유에 해당하는지 여부를 면밀히 검토하여야 한다.

이 법 위반행위에 대해서만 이 조에 의한 손해배상을 청구할 수 있고, 「위치정보법」, 「신용정보법」 등의 위반행위에 대해서는 이 조에 의한 손해배상을 청구하지 못한다. 그 경우에는 해당 법률에 의하거나 민법에 의한 손해배상청구를 할 수 있다. 법 위반행위가 있다는 사실은 손해배상을 청구하는 원고인 정보주체가 입증하여야 한다.

나 위반행위로 인해 손해가 발생했을 것

이 법 위반행위로 인해 정보주체에게 손해가 발생해야 한다. 손해는 재산적 손해 또는 경제적 손해에 한정하지 않고 비재산적 손해 즉 정신적 손해도 포함한다. 예컨대 재산적 손해라 함은 신용카드번호·주민등록번호 등의 유출에 따른 신용카드 부정사용, 불법대출 등으로 재산적 손실이 발생한 경우를 말하고, 정신적 손해라고 하면 이메일 주소, 전화번호 등의 유출에 따라 정보주체의 의사에 반하여 스팸메일, 마케팅광고 등이 수신됨으로써

발생하는 비재산적 피해가 발생한 경우를 의미한다. 손해가 발생했다는 사실과 손해액에 대해서는 원고인 정보주체가 증명책임을 진다.

다 손해와 법 위반행위 사이의 인과관계가 있을 것

이 법 위반행위와 손해 사이에 상당한 인과관계가 있어야 한다. 상당인과관계 이론에 따라 손해배상의 범위는 ‘통상의 손해’를 그 한도로 한다. 즉 행위(원인)와 손해(결과) 사이에 인과관계가 존재하는 한 모든 손해를 배상케 하는 것이 아니라 그 중 ‘통상의 손해’를 한도로 하여 배상하면 된다. 위반 행위와 손해 사이에 상당인과관계가 존재한다는 사실은 원고인 정보주체가 증명하여야 한다.

따라서 ‘특별한 사정으로 인한 손해’에 대해서는 원칙적으로는 배상할 책임이 없으나 개인정보처리자가 그와 같은 특별한 사정을 알았거나 알 수 있었을 때에는 배상할 책임이 있다(「민법」 제393조, 제763조). 개인정보처리자가 그 사정을 알았거나 알 수 있었을 것이라는 사실에 대해서는 원고인 정보주체에게 증명책임을 있다.

참고 상당인과관계(相當因果關係)

어떤 원인(행위)이 있으면 경험칙상 통상적으로 그러한 결과(손해)가 발생하리라고 인정되는 관계를 법률상 ‘상당인과관계’에 있다고 한다. 상당인과관계는 그 판단의 기준을 누구로 할 것이냐에 따라 범위가 달라질 수 있다. 행위자를 표준으로 하여 결정할 것인가 또는 일반인(보통인·평균인)을 표준으로 하여 결정할 것인가에 따라 주관적 상당인과관계설과 객관적 상당인과관계설 그리고 절충적 상당인과관계설로 나누어져 있다. 인과관계는 원래 자연현상에 속하는 것이므로 객관적으로 판단되어야 할 것이지만, 인간의 행위에 관하여는 행위자의 주관적인 사정을 전혀 무시하고 판단하는 것은 타당하지 못하므로 인과관계는 객관적인 기준으로 판단하는 것을 원칙으로 하되 행위자의 주관적인 사정도 참작하는 절충적 상당인과관계설이 현재 통설적 지위에 있다.

민법 제393조 및 제763조

제393조(손해배상의 범위) ①채무불이행으로 인한 손해배상은 통상의 손해를 그 한도로 한다.
②특별한 사정으로 인한 손해는 채무자가 그 사정을 알았거나 알 수 있었을 때에 한하여 배상의 책임이 있다.
제763조(준용규정) 제393조, 제394조, 제396조, 제399조의 규정은 불법행위로 인한 손해배상에 준용한다.

라 고의·과실 및 책임능력이 존재할 것

개인정보처리자에게 손해배상책임을 묻기 위해서는 그에게 고의 또는 과실과 책임능력이 있어야 한다.

고의란 개인정보처리자가 이 법 위반을 알면서도 감히 그 행위를 하는 것이다. 일정한 행

위를 하면 일정한 결과가 발생할지도 모른다는 의구심을 가지면서 감히 그 행위를 하는 소위 미필적 고의도 역시 고의에 포함된다.

과실이란 개인정보처리자의 경력·경험·직업 등 사회적 지위에 비추어 신의칙상 요구되는 정도의 주의를 결여하였기 때문에 이 법에 위반함을 인식하지 못한 것을 말한다. 즉 개인정보처리자가 선량한 관리자로서의 주의의무를 다하지 아니한 것을 말한다.

계약책임의 경우에는 신의칙상 개인정보처리자의 고의·과실과 동일시 할 것으로 기대되는 자 예컨대 근로자, 종업원, 임시직, 위촉직, 아르바이트생 등과 같이 개인정보처리자의 선임·지휘·감독을 받는 이행보조자의 고의·과실은 개인정보처리자 자신의 고의·과실로 본다(「민법」 제391조). 나아가 수탁자가 위탁받은 업무와 관련하여 개인정보를 처리하는 과정에서 이 법을 위반하여 발생한 계약상 손해배상책임에 대하여는 수탁자의 고의·과실도 개인정보처리자 자신의 소속 직원의 고의·과실로 본다(제26조제6항).

불법행위 책임의 경우에는 자기책임의 원칙 상 개인정보처리자 자신의 고의 또는 과실에 대하여 책임을 진다. 개인정보처리자가 법인인 경우에는 그 이사, 기타 대표자의 가해행위는 법인 자신의 가해행위로서 법인 자신의 책임이다. 불법행위책임의 경우에도 법에 따라 수탁자는 개인정보처리자 자신의 소속 직원으로 본다(제26조제6항). 한편, 법인의 대표자가 아닌 임직원이 개인정보와 관련하여 「민법」 제750조의 불법행위를 저질러 손해배상책임을 지게 될 경우, 개인정보처리자인 법인은 사용자로서 임직원과 함께 그 사무집행에 관하여 생긴 손해를 배상할 책임을 질 수도 있다. 다만 감독의무를 게을리하지 아니한 경우에는 그러하지 아니하다(「민법」 제756조 참조).

2. 고의·과실에 대한 입증책임의 전환

손해배상의 법리 상 채무불이행(계약불이행)에 의한 손해배상청구의 경우에는 고의 또는 과실의 부존재에 관한 입증책임을 피고(채무자)인 개인정보처리자가 부담하는 것이 원칙이고, 불법행위에 기한 손해배상청구의 경우에는 원고(피해자)인 정보주체가 고의 또는 과실의 존재에 관한 입증책임을 지는 것이 원칙이다.

그러나 이 법 위반에 따른 손해배상청구에 대해서는 고의 또는 과실에 관한 증명책임은 피고인 개인정보처리자 자신이 부담한다. 즉 개인정보처리자 자신에게 고의 또는 과실이 없음을 스스로 증명하여야 한다. 입증에 필요한 정보 소재의 불균형 등으로 일개 개인에 불과한 정보주체가 주로 기업이나 단체 또는 공공기관인 경우가 많은 개인정보처리자의 고의·과실을 증명하는 것은 현실적으로 어렵고, 따라서 정보주체로 하여금 고의·과실을 증명하게 하면 사실상 정보주체가 피해구제를 받는 것을 매우 어렵게 하는 길을 차단하는 결과를 초래하기 때문이다. 따라서 이 법의 규정을 위반한 행위로 인하여 정보주체가 손

해를 입은 경우 개인정보처리자에게 스스로 고의·과실이 없음을 증명할 책임을 부과함으로써 정보주체의 권리 중 하나인 신속·공정한 피해구제를 받을 권리를 실질적으로 보장하고 동시에 개인정보처리자의 준법률도 제고할 수 있는 기제로 작용할 것이다.

3. 징벌적 손해배상

제3항은 가벌성이 더 큰 악성 위법행위로 인하여 손해가 발생한 경우에는 그러한 악성 위법행위의 억지와 예방, 개인정보처리자에 대한 제재, 정보주체의 피해구제의 강화를 위하여 실손해의 3배를 넘지 않는 범위 내에서 징벌적 손해배상을 허용하고 있다. 다만, 징벌적 손해배상이 허용되는 위법행위는 「개인정보 보호법」을 위반하는 모든 행위가 아니라 침해행위의 가벌성이 더 심각한 유형으로서 ‘개인정보처리자의 고의 또는 중대한 과실로 인하여 개인정보가 분실·도난·유출·위조·변조 또는 훼손된 경우’에 한한다. 이러한 악성 위법행위로 인하여 정보주체에게 손해가 발생한 때에는 법원은 그 손해액의 3배를 넘지 아니하는 범위에서 손해배상액을 정할 수 있다. 통상 원고인 정보주체는 일반적 손해배상청구권과 마찬가지로 개인정보처리자의 고의 또는 중대한 과실, 악성 위법행위의 존재, 손해의 발생, 그 위법행위와 손해 발생 사이의 인과관계, 실손해액을 증명하여야 한다. 다만, 손해배상에 관한 일반원칙인 과실책임의 원칙에 대한 불합리한 훼손을 막고, 책임이 가중된 징벌적 손해배상으로 인하여 개인정보처리자가 불합리하게 징벌적 손해배상책임을 지지 않도록 하기 위하여 개인정보처리자가 스스로 적극적인 방어, 즉 개인정보처리자가 자신에게 고의 또는 중대한 과실이 없음을 증명한 경우에는 징벌적 손해배상책임으로부터 벗어날 수 있도록 허용하였다.

징벌적 손해배상액을 정할 때에는 실손해의 3배까지 증액하여 손해배상을 허용하기 때문에 징벌적 목적에 맞는 적정한 징벌적 손해배상액을 산정함으로써 불합리하게 과도한 배상이 되지 않도록 법원이 의무적으로 다음과 같은 다양한 요소를 종합적으로 고려하여 판단하도록 하였다.

징벌적 손해배상액 산정시 의무적 고려사항(제39조제4항)

1. 고의 또는 손해 발생의 우려를 인식한 정도
2. 위반행위로 인하여 입은 피해 규모
3. 위반행위로 인하여 개인정보처리자가 취득한 경제적 이익
4. 위반행위에 따른 벌금 및 과징금
5. 위반행위의 기간·횟수 등
6. 개인정보처리자의 재산상태
7. 개인정보처리자가 정보주체의 개인정보 분실·도난·유출 후 해당 개인정보를 회수하기 위하여 노력한 정도
8. 개인정보처리자가 정보주체의 피해구제를 위하여 노력한 정도

4. 손해배상청구권의 소멸

이 법은 손해배상청구권의 행사기한을 따로 정하고 있지 않기 때문에 「민법」상의 일반규정이 적용되어 일반적 손해배상책임(제1항)이든 징벌적 손해배상책임(제3항)이든 정보주체(피해자)나 그 법정대리인이 이 법 위반행위로 인하여 손해가 발생한 사실과 가해자(개인정보처리자)를 안 날로부터 3년 또는 불법행위를 한 날로부터 10년이 지나면 손해배상청구권은 소멸한다(「민법」 제766조). 이 중에서 3년의 기간은 시효기간이고 10년은 제척기간이다. 여기서 손해를 안다는 것은 손해 발생 사실 뿐만 아니라 그 가해행위가 불법행위로서 이를 근거로 손해배상청구를 할 수 있다는 것을 의미한다.

5. 다른 법률과의 관계

「신용정보법」은 손해배상책임(일반적 손해배상과 징벌적 손해배상)에 관하여 별도의 규정을 두고 있다. 따라서 신용정보회사등과 그 밖의 신용정보 이용자 등은 「신용정보법」에 따라 손해배상책임을 부담한다.

신용정보법	<p>제43조(손해배상의 책임) ① 신용정보회사등과 그 밖의 신용정보 이용자가 이 법을 위반하여 신용정보주체에게 피해를 입힌 경우에는 해당 신용정보주체에 대하여 손해배상의 책임을 진다. 다만, 신용정보회사등과 그 밖의 신용정보 이용자가 고의 또는 과실이 없음을 증명한 경우에는 그러하지 아니하다.</p> <p>② 신용정보회사등이나 그 밖의 신용정보 이용자(수탁자를 포함한다. 이하 이 조에서 같다)가 고의 또는 중대한 과실로 이 법을 위반하여 개인신용정보가 누설되거나 분실·도난·누출·변조 또는 훼손되어 신용정보주체에게 피해를 입힌 경우에는 해당 신용정보주체에 대하여 그 손해의 3배를 넘지 아니하는 범위에서 배상할 책임이 있다. 다만, 신용정보회사등이나 그 밖의 신용정보 이용자가 고의 또는 중대한 과실이 없음을 증명한 경우에는 그러하지 아니하다.</p> <p>③ 법원은 제2항의 배상액을 정할 때에는 다음 각 호의 사항을 고려하여야 한다.</p> <ol style="list-style-type: none"> 1. 고의 또는 손해 발생의 우려를 인식한 정도 2. 위반행위로 인하여 입은 피해 규모 3. 위반행위로 인하여 신용정보회사등이나 그 밖의 신용정보 이용자가 취득한 경제적 이익 4. 위반행위에 따른 벌금 및 과징금 5. 위반행위의 기간·횟수 등 6. 신용정보회사등이나 그 밖의 신용정보 이용자의 재산상태 7. 신용정보회사등이나 그 밖의 신용정보 이용자의 개인신용정보 분실·도난·누출 후 해당 개인신용정보 회수 노력의 정도 8. 신용정보회사등이나 그 밖의 신용정보 이용자의 피해구제 노력의 정도 <p>④ 채권추심회사 또는 위임직채권추심인이 이 법을 위반하여 채무자 및 그 관</p>
-------	---

계인에게 손해를 입힌 경우에는 그 손해를 배상하여야 한다. 다만, 채권추심회사 또는 위임직채권추심인이 자신에게 고의 또는 과실이 없음을 증명한 경우에는 그러하지 아니하다.

⑤ 제4조제1항의 업무를 의뢰받은 신용정보회사가 자신에게 책임 있는 사유로 의뢰인에게 손해를 입힌 경우에는 그 손해를 배상하여야 한다.

⑥ 제17조제2항에 따라 신용정보의 처리를 위탁받은 자가 이 법을 위반하여 신용정보주체에게 피해를 입힌 경우에는 위탁자는 수탁자와 연대하여 손해배상책임을 진다.

⑦ 위임직채권추심인이 이 법 또는 「채권의 공정한 추심에 관한 법률」을 위반하여 채무자나 채무자의 관계인에게 손해를 입힌 경우 채권추심회사는 위임직채권추심인과 연대하여 손해배상책임을 진다. 다만, 채권추심회사가 자신에게 고의 또는 과실이 없음을 증명한 경우에는 그러하지 아니하다.

제39조의2 | 법정손해배상의 청구

법률

- 제39조의2(법정손해배상의 청구)** ① 제39조제1항에도 불구하고 정보주체는 개인 정보처리자의 고의 또는 과실로 인하여 개인정보가 분실·도난·유출·위조·변조 또는 훼손된 경우에는 300만원 이하의 범위에서 상당한 금액을 손해액으로 하여 배상을 청구할 수 있다. 이 경우 해당 개인정보처리자는 고의 또는 과실이 없음을 입증하지 아니하면 책임을 면할 수 없다.
- ② 법원은 제1항에 따른 청구가 있는 경우에 변론 전체의 취지와 증거조사의 결과를 고려하여 제1항의 범위에서 상당한 손해액을 인정할 수 있다.
- ③ 제39조에 따라 손해배상을 청구한 정보주체는 사실심(事實審)의 변론이 종결되기 전까지 그 청구를 제1항에 따른 청구로 변경할 수 있다.

대량의 개인정보 유출 사고에도 불구하고 실제 개인정보 유출 혹은 오·남용으로 인한 정보주체의 손해가 이 법에 의한 손해배상에 의해 실질적으로 구제된 경우는 많지 않다. 가장 큰 이유는 피해자인 정보주체가 자신이 입은 피해의 규모를 명확하게 증명하는 것이 어렵기 때문이다. 개인정보 유출 혹은 오·남용으로 발생하는 피해는 재산적 피해와 정신적 피해로 구분할 수 있지만, 재산적 피해는 개인정보를 위법하게 이용하여 불법대출을 받거나 불법적인 거래로 정보주체의 재산의 손실이 발생하지 않는 한 개인정보 유출만으로 재산상 손해를 인정하는 것은 쉽지 않다. 정신적 손해의 경우에도 유출된 개인정보의 종류와 성격이 무엇인 지, 개인정보 유출로 정보주체를 식별할 가능성이 발생하였는지, 제3자가 유출된 개인정보를 열람하였는지 또는 제3자의 열람 여부가 밝혀지지 않았다면 제3자의 열람 가능성이 있었거나 앞으로 열람 가능성이 있는지, 유출된 개인정보가 어느 범위까지 확산되었는지, 개인정보 유출로 추가적인 법익침해 가능성이 발생하였는지, 개인정보를 처리하는 자가 개인정보를 관리해 온 실태와 개인정보가 유출된 구체적인 경위는 어떠한지, 개인정보 유출로 인한 피해 발생 및 확산을 방지하기 위하여 어떠한 조치가 취하여졌는지 등 여러 사정을 종합적으로 고려하여 구체적 사건에 따라 정신적 손해의 인정여부를 개별적으로 판단하기 때문에, 피해자인 정보주체가 개인정보 유출 등으로 인하여 정신적 손해가 발생했다는 사실과 구체적으로 입은 손해 규모를 증명하는 것은 어렵다. 이러한 배경에서 정보주체가 개인정보 유출로 인해 입은 손해를 쉽게 구제받을 수 있게 함으로써 개인정보처리자에게 개인정보 보호 책임을 실질적으로 부담하게 하기 위해 법정손해배상이라는 제도를 도입한 것이다.

1. 손해배상청구권의 청구요건

참고 법정손해배상책임의 청구요건

- 개인정보처리자의 고의 또는 과실로 인한 개인정보의 분실·도난·유출·위조·변조 또는 훼손이 있을 것
- 300만 원 이하의 범위에서 상당한 금액을 손해액으로 청구할 것
- 고의 또는 과실 및 책임능력이 있을 것

가 개인정보처리자의 고의 또는 과실로 인한 개인정보의 분실·도난·유출·위조·변조 또는 훼손이 있을 것

이 조에 따른 법정손해배상청구권이 발생하기 위해서는 개인정보처리자에게 고의 또는 과실과 함께 이로 인하여 개인정보의 분실·도난·유출·위조·변조 또는 훼손이라고 하는 특정한 침해행위가 존재하여야 한다. 개인정보의 분실이란 자신도 모르는 사이에 개인정보를 잃어버리는 것을 의미하고, 도난이란 자신의 개인정보를 누군가에게 도둑맞은 것을 의미하며, 유출(누출)이란 개인정보가 해당 개인정보처리자의 관리·통제권을 벗어나 당해 개인정보를 모르는 제3자가 그 내용을 알 수 있는 상태에 이르게 하는 것을 의미한다. 위조는 권한 없는 자가 개인정보를 새롭게 생성하는 것을 말하며, 변조는 권한 없이 기존 개인정보에 변경을 가하는 일을 의미하고, 훼손이란 개인정보를 못 쓰게 만드는 것, 즉 효용을 해하는 것을 의미한다. 그리고 이러한 행위가 개인정보처리자의 고의 또는 과실로 인하여 발생하여야 한다.

나 300만원 이하의 범위에서 상당한 금액을 손해액으로 청구할 것

일반적인 손해배상책임의 경우에 손해액의 증명이 어렵다는 점을 고려하여 법정손해배상은 피해자인 정보주체에게 손해액 증명의 어려움을 완화시켜주기 위한 제도인 바, 원고인 정보주체는 구체적인 손해액을 증명할 필요는 없다. 법정손해배상 청구가 있는 경우에 법원은 변론 전체의 취지와 증거조사의 결과를 고려하여 300만 원의 범위에서 상당한 손해액을 인정할 수 있는데, 달리 하한이 정해져 있지 않기 때문에 적절치 않을 경우 손해액을 인정하지 아니할 수도 있다. 다만, 정보주체는 개인정보처리자의 고의 또는 과실로 인한 개인정보의 분실·도난·유출·위조·변조 또는 훼손으로 인하여 손해(구체적인 손해액이 아님)가 발생하였다는 점을 주장하여야 한다. 그러나 정보주체는 구체적인 손해액을 증명할 필요는 없다. 정보주체가 300만 원의 범위 내에서 최대한의 피해 배상을 받아내고자 한다면 법원에 손해 발생의 개연성을 비롯하여 손해액의 산정에 도움이 될 수 있는 사항에 대하여 증명하고자 하는 노력을 기울이는 것이 필요할 것이다.

다 위법한 개인정보의 분실·도난·유출·위조·변조 또는 훼손과 손해 사이의 인과관계가 있을 것

법정손해배상은 제39조의 일반 손해배상을 대체하는 손해배상청구권으로서 일반 손해배상과 같이 배상의 범위는 실제로 입은 손해의 범위로 한정된다. 즉, 법원이 법정손해배상으로서 상당한 손해액을 산정함에 있어서도 이 조에서 열거된 위법행위와 손해 사이의 상당한 인과관계의 범위 내로 한정된다. 따라서 ‘통상의 손해’를 한도로 하여 법원이 증거조사 결과에 따라 상당한 손해액을 인정하면 된다. 정보주체는 위법 행위와 손해 사이에 상당한 인과관계가 존재한다는 사실을 증명하여야 한다. 다만, ‘특별한 사정으로 인한 손해’에 대해서는 개인정보처리자가 그 사정을 알았거나 알 수 있었을 때에는 배상할 책임이 있으며(「민법」 제393조, 제763조), 개인정보처리자가 그 사정을 알았거나 알 수 있었을 것이라는 사실에 대해서는 원고인 정보주체에게 입증책임이 있다.

민법 제393조 및 제763조

제393조(손해배상의 범위) ① 채무불이행으로 인한 손해배상은 통상의 손해를 그 한도로 한다.

② 특별한 사정으로 인한 손해는 채무자가 그 사정을 알았거나 알 수 있었을 때에 한하여 배상의 책임이 있다.

제763조(준용규정) 제393조, 제394조, 제396조, 제399조의 규정은 불법행위로 인한 손해배상에 준용한다.

라 고의 또는 과실 및 책임능력이 존재할 것

개인정보처리자에게 법정손해배상책임을 묻기 위해서는 그에게 고의 또는 과실과 책임능력이 있어야 한다.

고의란 개인정보처리자가 이 법 위반을 알면서도 감히 그 행위를 하는 것이다. 일정한 행위를 하면 일정한 결과가 발생할지도 모른다는 의구심을 가지면서 감히 그 행위를 하는 소위 미필적 고의도 역시 고의에 포함된다.

과실이란 개인정보처리자의 경력·경험·직업 등 사회적 지위에 비추어 신의칙상 요구되는 정도의 주의를 결여하였기 때문에 이 법에 위반함을 인식하지 못한 것을 말한다. 즉 개인정보처리자가 선량한 관리자로서의 주의의무를 다하지 아니한 것을 말한다.

수탁자의 고의·과실도 개인정보처리자 자신의 소속 직원의 고의·과실로 본다(제26조제6항).

2. 고의 또는 과실에 대한 증명책임의 전환

채무불이행(계약불이행)에 의한 손해배상청구의 경우에는 고의 또는 과실의 부존재에 관한 입증책임을 피고(채무자)인 개인정보처리자가 부담하는 것이 원칙이고, 불법행위에 기한 손해배상청구의 경우에는 원고(피해자)인 정보주체가 고의 또는 과실의 존재에 관한 입증책임을 지는 것이 원칙이다.

그러나 법정손해배상청구에서는 계약불이행에 의한 것이든 불법행위에 의한 것이든 고의 또는 과실의 부존재에 관한 입증책임을 피고인 개인정보처리자가 부담한다.

3. 법정손해배상청구의 행사 시기

제39조의 일반 손해배상책임과 본조의 법정손해배상책임은 서로 별개의 법적 근거에 의하여 인정되며 그 요건 및 효과 또한 상이하므로 소송 과정에서 어느 조항의 손해배상책임을 주장하는지는 원고인 정보주체가 선택하여야 한다.

한편, 원고인 정보주체가 제39조에 따라 손해배상을 청구했다라도 사실심(事實審)의 변론이 종결되기 전까지는 언제든지 그 청구를 법정손해배상 청구로 변경할 수 있다. 이는 권리구제의 실효성을 강화하고자 하는 취지를 명확히 하기 위함이다. 반대로 명문의 규정은 없지만 같은 취지에 근거하여 법정손해배상을 청구한 정보주체는 사실심 변론 종결 전까지 실손해를 증명함으로써 제39조에 따른 손해배상 청구로 변경하는 것도 가능하다.

4. 손해배상청구권의 소멸

이 법은 법정손해배상의 청구기간에 대하여 아무런 규정을 두지 않아서 일반법인 민법상의 채권 소멸시효 기간에 따라 손해배상청구권의 행사기한이 정해진다. 즉, 법정손해배상의 청구권은 피해자나 그 법정대리인이 그 손해 및 가해자를 안 날로부터 3년간 이를 행사하지 않으면 그 법정손해배상청구권은 소멸한다(「민법」 제766조제1항). 법정손해배상청구의 근거가 되는 불법행위가 있는 날로부터 10년을 경과한 때에도 마찬가지이다(「민법」 제766조제2항).

5. 다른 법률과의 관계

「신용정보법」은 법정손해배상책임에 관하여 별도의 규정을 두고 있다. 따라서 신용정보회사등은 「신용정보법」에 따라 법정손해배상책임을 부담한다.

신용정보법	<p>제43조의2(법정손해배상의 청구) ① 신용정보주체는 신용정보회사등이나 그로부터 신용정보를 제공받은 자가 이 법의 규정을 위반한 경우에는 신용정보회사등이나 그로부터 신용정보를 제공받은 자에게 제43조에 따른 손해배상을 청구하는 대신 300만원 이하의 범위에서 상당한 금액을 손해액으로 하여 배상을 청구할 수 있다. 이 경우 해당 신용정보회사등이나 그로부터 신용정보를 제공받은 자는 고의 또는 과실이 없음을 입증하지 아니하면 책임을 면할 수 없다. <개정 2020. 2. 4.></p> <p>1. 삭제 <2020. 2. 4.></p> <p>2. 삭제 <2020. 2. 4.></p> <p>② 제1항에 따른 손해배상 청구의 변경 및 법원의 손해액 인정에 관하여는 「개인정보 보호법」 제39조의2제2항 및 제3항을 준용한다. <개정 2020. 2. 4.></p> <p>③ 삭제 <2020. 2. 4.></p>
-------	--

제6장

정보통신서비스 제공자등의 개인정보 처리 등 특례

- 제39조의3 개인정보의 수집·이용 동의 등에 대한 특례
- 제39조의4 개인정보 유출등의 통지·신고에 대한 특례
- 제29조, 제39조의5 개인정보의 보호조치에 대한 특례
- 제39조의6 개인정보의 파기에 대한 특례
- 제39조의7 이용자의 권리 등에 대한 특례
- 제39조의8 개인정보 이용내역의 통지
- 제39조의9 손해배상의 보장
- 제39조의10 노출된 개인정보의 삭제·차단
- 제39조의11 국내대리인의 지정
- 제39조의12 국외 이전 개인정보의 보호
- 제39조의13 상호주의
- 제39조의14 방송사업자등에 대한 특례
- 제39조의15 과징금의 부과 등에 대한 특례



1. 특례 신설 배경

4차 산업혁명 시대를 맞아 인공지능(AI), 클라우드, 사물인터넷(IoT) 등 신기술과 연계된 서비스 분야에서 핵심 자원인 데이터를 안전하게 활용할 수 있도록 하고, 동시에 정보주체의 개인정보 보호 수준을 높이기 위한 사회적 규범 정립이 필요해지고 있다.

그러나, 종전 개인정보 보호 관련 법령은 일반법인 「개인정보 보호법」과 정보통신서비스 제공자등에 대한 개인정보 보호를 규율하는 「정보통신망법」으로 분산되어 있어 두 법률의 체계적인 통합 정비가 필요한 상황이 유지되어 왔다.

이에 따라 「정보통신망법」의 개인정보 보호 규정을 「개인정보 보호법」에 편입하여 통합하고, 소관부처도 보호위원회로 일원화하는 내용으로 「개인정보 보호법」과 「정보통신망법」을 정비하였다(2020. 2. 4. 공포, 2020. 8. 5. 시행).

개정된 「개인정보 보호법」에서는 ① 종전 「정보통신망법」의 규정 중 정보통신서비스의 특성을 반영하여 유지할 필요가 있는 경우 「개인정보 보호법」 제6장 ‘정보통신서비스 제공자 등의 개인정보 처리 등 특례’에 반영하였고 ② 제재규정(과태료, 벌칙 등) 등 「개인정보 보호법」의 기존 규정에 추가하여 포함할 수 있는 내용은 「개인정보 보호법」 체계에 맞추어 수정 반영하였다.

이 장에서는 종전 「정보통신망법」 규정이 반영되어 정보통신서비스 제공자등에게 적용되는 「개인정보 보호법」 규정을 ‘특례규정’, 그 외 「개인정보 보호법」 규정을 ‘일반규정’으로 지칭한다.

2. 적용 대상

가 정보통신서비스 제공자등

1) 정보통신서비스 제공자

정보통신서비스 제공자란 전기통신사업법 규정에 의한 ① 전기통신사업자와 ② 영리를 목적으로 전기통신사업자의 전기통신역무를 이용하여 정보를 제공하거나 정보의 제공을 매개하는 자를 말한다(「정보통신망법」 제2조제1항제3호).

① 전기통신사업자

전기통신사업자는 「전기통신사업법」에 따라 등록 또는 신고(신고가 면제된 경우를 포함한다)를 하고 전기통신역무¹¹⁾를 제공하는 자(기간통신사업자와 부가통신사업자)를 말한다(「전기통신사업법」 제2조제8호, 제5조).

기간통신사업자는 전기통신회선설비를 설치하거나 이용하여 기간통신역무를 제공하는 사업을 경영하려는 자로서 「전기통신사업법」 제6조제1항에 따라 과학기술정보통신부장관에게 등록을 하거나 같은 항 단서에 따라 신고한 자를 의미한다(「전기통신사업법」 제5조제2항, 제6조). 예를 들어, 초고속인터넷·이동통신·알뜰폰(MVNO)·국제전화·인터넷전화 등 유무선 통신사업자, 가전·자동차 등 상품을 제공하면서 사물인터넷(IoT)과 같은 기간통신역무를 부수적으로 이용하고 그 요금을 청구하는 제조사 등이 이에 해당한다.

부가통신사업자는 기간통신역무 이외의 전기통신역무를 제공하는 사업자를 말하며, ① 「전기통신사업법」 제22조제1항에 따라 과학기술정보통신부장관에게 부가통신사업을 신고한 자 ② 같은 조 제2항에 따라 부가통신사업을 등록한 자(특수한 유형의 부가통신사업자) 또는 ③ 같은 조 제4항에 따라 부가통신사업을 신고한 것으로 보는 자(인터넷을 이용하여 부가통신역무를 제공하는 자본금 1억원 이하인 소규모 사업자와 부가통신사업을 경영하려는 기간통신사업자)를 모두 포함한다(「전기통신사업법」 제5조제3항, 제22조, 제24조) 예를 들어, 인터넷 포털, 온라인 쇼핑몰, 온라인 게임, SNS(Social Network Service) 등과 같이 인터넷·모바일 상에서 웹사이트·앱 등을 운영하는 사업자가 이에 해당한다.

이 중 특수한 유형의 부가통신사업자는 「저작권법」 제104조에 따른 특수한 유형의 온라인서비스제공자(다른 사람들 상호 간에 컴퓨터를 이용하여 저작물등을 전송하도록 하는 것을 주된 목적으로 하는 온라인서비스제공자)의 부가통신역무를 제공하는 사업자 또는 문자메시지 발송시스템을 전기통신사업자의 전기통신설비에 직접 또는 간접적으로 연결하여 문자메시지를 발송하는 부가통신역무를 제공하는 사업자를 의미한다. 예를 들어, 웹하드나 P2P 사이트 운영 사업자, 인터넷발송문자서비스 사업자 등이 이에 해당된다.

② 영리 목적으로 전기통신역무를 이용하는 정보 제공자 또는 제공 매개자

전기통신사업자가 아니더라도 ‘영리를 목적으로 전기통신사업자의 전기통신역무를 이용하여 정보를 제공 또는 정보의 제공을 매개하는 자’는 정보통신서비스 제공자에 해당한다.

‘영리를 목적으로’의 의미는 널리 경제적 이익을 취할 목적을 의미하며, 법인의 종류가 영리법인 또는 비영리법인인지 실제 수익이 발생했는지 여부와는 직접적인 관계가 없

11) ‘전기통신역무’란 전기통신설비를 이용하여 타인의 통신을 매개하거나 전기통신설비를 타인의 통신용으로 제공하는 것을 말함(「전기통신사업법」 제2조제6호)

다. 예를 들어, 학술·종교·자선단체 등 비영리단체가 순수하게 해당 단체의 설립목적을 실현하기 위해 웹사이트를 개설하여 운영하는 경우에는 정보통신서비스 제공자에 해당하지 않으나, 이들 비영리단체가 전기통신역무를 이용하여 이용자와 정보통신서비스 이용관계를 맺고 있고 그 서비스가 영리를 목적으로 한다면 정보통신서비스 제공자에 해당할 수 있다.

‘전기통신역무’란 전기통신설비를 이용하여 타인의 통신을 매개하거나 전기통신설비를 타인의 통신용으로 제공하는 것을 말한다(「전기통신사업법」 제2조제6호). 정보통신서비스 제공자에 해당하려면 전기통신사업자의 전기통신역무를 이용하여야 하므로 법인 또는 개인이 자체적으로 전기통신설비를 갖추어 자신의 전기통신에 이용하는 경우는 제외된다.

‘정보의 제공’이란 각종 정보를 게시·전송·대여·공유하는 등 일련의 정보 제공 행위를 말하며, ‘정보의 제공을 매개’란 정보를 제공하려는 자와 제공받으려는 자를 연결시켜 서비스 제공이 가능하도록 하는 것을 말한다. 이때의 정보 제공 또는 정보 제공의 매개는 전기통신사업자의 전기통신역무를 이용한 것이므로(이를 전기통신역무와 함께 정보통신서비스라 한다, 「정보통신망법」 제2조제1항제2호 참고), 오프라인으로만 서비스를 제공하는 자는 정보통신서비스 제공자에 해당하지 않는다. 한편, 오프라인으로 물품을 판매하고 유통하는 서비스를 제공함과 동시에 자사 웹사이트를 통해 서비스를 제공하는 과정에서 각종 정보를 게시·전송·공유하는 경우에는 정보통신망(온라인)을 통해 영리 목적으로 정보를 제공 또는 매개한다고 볼 수 있으므로 업종과 상관없이 정보통신서비스 제공자에 해당한다고 볼 수 있다.

< 사례별 정보통신서비스 제공자 해당 여부 >

구분		정보통신서비스 제공자 해당 여부
전기통신사업자		· 정보통신서비스 제공자에 해당
영리 목적으로 전기통신 역무를 이용하는 정보 제공자 또는 제공 매개자	상법상의 상인 및 회사	· 상법 상의 상인 및 회사는 영리를 목적으로 사업을 영위하므로 구체적인 영리행위가 없어도 기본적으로 정보통신서비스 제공자에 해당
	비영리 법인	· 학술·종교·자선·기예·사교 등 영리 아닌 사업을 목적으로 설립된 비영리법인이 순수하게 해당 법인의 설립 목적을 실현하기 위해 정보통신서비스를 제공하는 경우 정보통신서비스 제공자에 해당하지 않음 · 다만, 비영리법인이 수익사업을 위해 정보통신서비스를 제공하는 경우 정보통신서비스 제공자에 해당
	특수법인	· 특수법인이 법률 상 목적 중 비영리사업을 위해 정보통신서비스를 제공하는 경우 정보통신서비스 제공자에 해당하지 않음 · 다만, 특수법인이 목적사업으로 수행하는 영리사업을 위해 정보통신서비스를 제공하는 경우 정보통신서비스 제공자에 해당
	공기업	· 기본적으로 영리를 목적으로 사업을 영위하므로 해당 사업을 목적으로 서비스를 제공하는 경우 정보통신서비스 제공자에 해당

준정부 기관	· 정부 업무의 수탁 수행 또는 기금관리 업무를 수행하는 점에서 기본적으로 정보통신서비스 제공자에 해당하지 않음
기타 공공기관	· 개별적으로 영리 목적의 정보통신서비스 제공 여부를 판단 · 연구개발목적기관으로 분류된 경우 원칙적으로 정보통신서비스 제공자에 해당하지 않는 것으로 판단
의료 기관	· 의료기관이 웹사이트 등 정보통신서비스를 제공하면서 경제적 이익을 취할 목적으로 영리행위를 하는 경우에는 정보통신서비스 제공자에 해당 · 다만, 의료기관이 내원 환자를 대상으로 오프라인 진료만을 수행하는 경우 (진료 사전예약을 위한 웹사이트, 전화예약서비스 등을 운영하는 경우 포함)에는 정보통신서비스 제공자에 해당하지 않음
학교	· 관련 법률에 따라 설립되어 교육을 수행하는 학교는 그 범위 안에서는 비영리 목적에 해당하므로 원칙적으로 정보통신서비스 제공자에 해당하지 않음 · 다만, 사립학교 등이 상행위 등 영리 목적으로 정보통신서비스를 제공하는 경우에는 정보통신서비스 제공자에 해당
금융회사	· 금융회사는 영리를 목적으로 금융업을 영위하는 자이므로 기본적으로 정보통신서비스 제공자 해당

2) 정보통신서비스 제공자로부터 개인정보를 제공받은 자

정보통신서비스 제공자로부터 이용자의 개인정보를 제공받은 자는 정보통신서비스 제공자의 관리를 받지 않고 자기 책임하에 제공받은 목적 범위 내에서 개인정보를 이용하는 자이므로 정보통신서비스 제공자와 유사한 정도의 의무를 부담한다. 이에 따라 법 제39조의4제1항에서는 ‘정보통신서비스 제공자등’을 ‘정보통신서비스 제공자’와 그로부터 제17조제1항에 따라 ‘이용자의 개인정보를 제공받은 자’로 정의하고 있으며, 다음과 같은 특례 규정에서 의무주체로 규율하고 있다.

‘정보통신서비스 제공자등’을 의무주체로 하고 있는 규정	
법 제39조의4(개인정보 유출등의 통지·신고에 대한 특례)	법 제39조의10(노출된 개인정보의 삭제·차단)
법 제39조의5(개인정보의 보호조치에 대한 특례) 영 제48조의2(개인정보의 안전성 확보 조치)	법 제39조의11(국내대리인의 지정)
법 제39조의6(개인정보의 파기에 대한 특례)	법 제39조의12(국외 이전 개인정보의 보호)
법 제39조의7(이용자의 권리 등에 대한 특례)	법 제39조의13(상호주의)
법 제39조의8(개인정보 이용내역의 통지)	법 제39조의15(과징금의 부과 등에 대한 특례)
법 제39조의9(손해배상의 보장)	-

나 방송사업자등

이 법은 방송사업자등이 시청자의 개인정보를 처리하는 경우에는 정보통신서비스 제공자에게 적용되는 관련 규정을 모두 준용하도록 규정하고 있다(제39조의14).

이에 따라 준용되는 방송사업자등(「방송법」 제2조제3호 가목부터 마목까지와 같은 조 제6호·제9호·제10호 및 제14호에 해당하는 자)의 구체적인 범위는 다음과 같다.

< 방송사업자등의 범위 >

분류		내용
방송사업자	지상파방송사업자	· 지상파방송사업을 하기 위하여 방송법 제9조제1항에 따라 허가를 받은 자
	종합유선방송사업자	· 종합유선방송사업을 하기 위하여 방송법 제9조제2항에 따라 허가를 받은 자
	위성방송사업자	· 위성방송사업을 하기 위하여 방송법 제9조제2항에 따라 허가를 받은 자
	방송채널사용사업자	· 방송채널사용사업을 하기 위하여 방송법 제9조제5항에 따라 등록을 하거나 승인을 얻은 자
	공동체라디오 방송사업자	· 안테나공급전력 10와트 이하로 공익목적으로 라디오방송을 하기 위하여 방송법 제9조제11항에 따라 허가를 받은 자
'등'	중계유선방송사업자	· 중계유선방송사업을 하기 위하여 방송법 제9조제2항에 따라 허가를 받은 자
	음악유선방송사업자	· 음악유선방송사업을 하기 위하여 방송법 제9조제5항에 따라 등록을 한 자
	전광판방송사업자	· 전광판방송사업을 하기 위하여 방송법 제9조제5항에 따라 등록을 한 자
	전송망사업자	· 전송망사업을 하기 위하여 방송법 제9조제10항에 따라 등록을 한 자

참고 수탁자에 대한 법 적용 변경사항

- 2020. 2. 4. 개정 전 「정보통신망법」은 정보통신서비스 제공자등으로부터 이용자의 개인정보의 처리 업무를 위탁받은 수탁자에 대하여 「정보통신망법」 규정을 준용하도록 규정하였으나(동법 제67조제2항), 개정 후 「개인정보 보호법」 특례규정에서는 위의 수탁자 준용 규정이 일반규정의 수탁자 규정과 중복되는 부분이 있어 삭제되었다. 이에 따라, 수탁자는 원칙적으로 「개인정보 보호법」 제26조(업무위탁에 따른 개인정보의 처리 제한)의 일반규정이 적용되지만, 정보통신서비스 제공자등으로부터 개인정보 처리 업무를 위탁받은 범위 안에서는 특례규정을 준수하여야 한다.
- 한편, 수탁자가 수탁자로서의 지위와는 별도로 고유의 정보통신서비스를 제공하는 경우에는 정보통신서비스 제공자로서 특례 적용 대상에 해당된다는 점을 유의해야 한다.

3. 보호 범위

특례규정은 정보통신서비스 제공자등이 처리하는 이용자의 개인정보를 보호하는 것을 목적으로 한다. 따라서 정보통신서비스 제공자가 이용자와 정보통신서비스 이용관계를 맺고 있는 경우에 적용된다.

여기서 이용자는 일반 불특정 다수가 아닌 정보통신서비스 제공자가 제공하는 정보통신서비스를 이용하는 자를 의미한다(「개인정보 보호법」 제18조제2항, 「정보통신망법」 제2조제1항제4호). 따라서 정보통신서비스 제공자와 정보통신서비스 이용관계를 맺고 있는 자이면 회원/비회원 여부, 유료/무료 서비스 이용 여부, 이벤트 등 일시적 서비스 이용 여부 등과 관계없이 이용자에 해당할 수 있다. 반면 정보통신서비스 제공자의 임직원은 정보통신서비스 제공자와 정보통신서비스 이용관계가 없으므로 이용자에 해당하지 않는다.

또한, 시청자의 개인정보를 처리하는 방송사업자등의 경우 정보통신서비스 제공자에게 적용되는 규정이 준용되므로(제39조의14), 시청자 역시 특례규정에 따른 이용자의 권리를 동일하게 보장받는다.

4. 「개인정보 보호법」의 일반규정과 특례규정 간의 관계

가 일반원칙

보호위원회는 2020. 2. 4. 개정 이전 「개인정보 보호법」과 「정보통신망법」의 개인정보 보호 규정의 관계에 대하여 ① 상호 모순·저촉되는 규정의 존재 여부 ② 「개인정보 보호법」 관련 조항을 배제하고자 하는 내용의 포함 여부를 기준으로 「개인정보 보호법」 제6조의 ‘특별한 규정’에 해당하는지를 판단할 수 있다고 하여 일반법과 특별법 관계에 있는 것으로 보았다(보호위원회 결정 2018-02-006호 참고).

2020. 2. 4. 개정 「개인정보 보호법」은 「정보통신망법」의 개인정보 보호 규정을 「개인정보 보호법」으로 일원화하면서 「개인정보 보호법」과 상이하거나 「정보통신망법」에만 있는 규정 등을 특례규정으로 반영함으로써 종전 「개인정보 보호법」과 「정보통신망법」의 일반법과 특별법 관계를 일반규정과 특례규정 관계로 유지하였다. 즉, 일반규정은 공공·민간부문에 포괄적으로 적용되는 일반법적인 성격을 가지고, 특례규정은 정보통신서비스 제공자등에 적용되는 특별법적 성격을 가지게 되었다고 할 수 있다. 따라서 구체적 사안에서 적용할 수 있는 일반규정과 특례규정이 모두 존재하고 양자가 상호 모순·저촉되거나 특례규정에 일반규정의 적용을 배제하는 내용이 포함되어 있는 경우에는 특례규정이 우선 적용된다. 한편, 일반규정이 특례규정에 존재하지 않는 사항을 담고 있는 경우에는 해당 일반규정이 적용된다.

나 법 개정에 따른 적용규정의 변화

종전 「정보통신망법」의 개인정보 관련 규정 중 「개인정보 보호법」과 상이하거나 「정보통신망법」에만 있는 규정은 「개인정보 보호법」의 특례규정에 반영되었으며, 「개인정보 보호법」과 유사·중복되는 규정은 일반규정으로 통합되었다. 이에 따라 제1장(총칙)·제2장(개인정보 보호정책의 수립 등)·제7장(개인정보 분쟁조정위원회)·제8장(개인정보 단체소송)·제9장(보칙)·제10장(벌칙)·부칙과 같은 일반규정은 정보통신서비스 제공자등에 해당하는 사항이 있는 경우 일반적으로 적용되고, 제3장(개인정보의 처리)·제4장(개인정보의 안전한 관리)·제5장(정보주체의 권리 보장)·제6장(정보통신서비스 제공자 등의 개인정보 처리 등 특례)까지의 규정은 일반규정과 특례규정 간의 법 적용 일반원칙에 따라 구체적 적용여부를 판단해야 한다. 이와 함께, 방송사업자등의 경우 시청자의 개인정보를 처리하는 경우에는 정보통신서비스 제공자에게 적용되는 규정을 준용한다. 이에 따라 적용되는 규정의 주요내용은 다음과 같다.

< 정보통신서비스 제공자에게 적용되는 규정 주요내용 >

구분	정보통신서비스 제공자에게 적용되는 규정		
	적용되는 일반규정	적용되는 특례규정	변화된 주요내용
제15조 (개인정보의 수집·이용)	제15조 제3항 (개인정보의 추가적인 이용) ※ 제1항, 제2항은 특례 우선 적용	제39조의3(개인정보의 수집·이용 동의 등에 대한 특례) 제1항, 제2항	· 개인정보의 추가적인 이용 적용(제15조제3항)
제16조 (개인정보의 수집 제한)	제16조	제39조의3 (개인정보의 수집·이용 동의 등에 대한 특례) 제3항	· 일반규정(제16조 제1항, 제2항)이 적용되나, 필요한 최소한의 정보 범위는 특례 규정(제39조의3제3항) 적용
제17조 (개인정보의 제공)	제17조 제1항, 제2항, 제4항 ※ 제3항(국외제공)은 특례 우선 적용	제39조의12 (국외 이전 개인정보의 보호)	· 제공에 대하여는 일반규정이 적용되나, 국외제공에 대하여는 특례규정이 우선 적용
제18조 (개인정보의 목적 외 이용제공 제한)	제18조	-	· 일반규정 적용
제19조 (개인정보를 제공받은 자의 이용·제공 제한)	제19조	-	· 일반규정 적용
제20조 (정보주체 이외로부터)	제20조	-	· 일반규정 적용 ※ 종전에는 「정보통신망법」에

수집한 개인정보의 수집 출처 등 고지)			따라 제공받은 경우는 제외하고 있었으므로 법 시행일(2020.8.5.) 이후 제공받은 경우에 한정
제21조 (개인정보의 파기)	제21조	제39조의6 (개인정보의 파기에 대한 특례) ※ 1년 미이용자 파기등 특례	· 일반규정이 적용되고, 특례규정의 1년 미이용자 파기등 의무 추가 적용
제22조 (동의를 받는 방법)	제22조	제39조의3 (개인정보의 수집·이용 동의 등에 대한 특례) 제4항, 제5항 ※ 만14세 미만 아동 동의 시 법정대리인 동의 및 확인 특례	· 일반규정이 모두 적용되고, 만14세 미만 아동 동의 시 법정대리인 동의 및 확인의무는 특례규정 추가 적용
제23조 (민감정보의 처리 제한)	제23조	-	· 일반규정 적용 ※ 법 제29조에 따른 안전성 확보 조치는 영 제48조의2 특례규정 적용
제24조 (고유식별정보 의 처리 제한)	제24조	-	· 일반규정 적용 ※ 법 제29조와 영 제21조에 따라 안전성 확보 조치는 영 제48조의2 특례규정 적용
제24조의2 (주민등록번호 처리의 제한)	제24조의2	-	· 일반규정 적용
제25조(영상정 보처리기기의 설치·운영 제한)	제25조 (적용대상 : '누구든지')	-	· 일반규정 적용
제26조(업무위 탁에 따른 개인정보의 처리 제한)	제26조	-	· 일반규정 적용
제27조 (영업양도 등에 따른 개인정보의 이전 제한)	제27조	-	· 일반규정 적용
제28조 (개인정보취급 자에 대한 감독)	제28조	-	· 일반규정 적용
제3장 제3절 (가명정보의 처리에 관한 특례)	제3장 제3절	-	· 가명정보 처리에 관한 특례 규정 적용
제29조 (안전조치의무)	제29조	영 제48조의2 (개인정보의 안전성 확보 조치에 대한 특례) 제39조의5 (개인정보의 보호조치에 대한 특례)	· 안전성 확보 조치는 제29조의 위임에 따른 시행령 제48조의2와 법 제39조의5 특례규정이 적용

제30조 (개인정보 처리방침의 수립 및 공개)	제30조	-	· 일반규정 적용
제31조 (개인정보 보호 책임자의 지정)	제31조	-	· 일반규정 적용
제32조의2 (개인정보 보호 인증)	제32조의2	-	· 일반규정 적용
제33조 (개인정보 영향평가)	제33조 제8항	-	· 일반규정 적용
제34조 (개인정보 유출 통지 등)	-	제39조의4 (개인정보 유출등의 통지·신고에 대한 특례)	· 특례규정 적용
제34조의2 (과징금의 부과 등)	제34조의2	-	· 일반규정 적용
제35조 (개인정보의 열람)	제35조 제1항, 제3항, 제4항, 제5항	-	· 일반규정이 적용되고, 동의철회 등 제37조의7의 특례규정은 추가 적용
제36조 (개인정보의 정정·삭제)	제36조	-	
제37조 (개인정보의 처리금지 등)	제37조	-	
제38조 (권리행사의 방법 및 절차)	제38조	-	
<특례>	-	제39조의7 (이용자의 권리 등에 대한 특례)	
제39조 (손해배상책임)	제39조	-	· 일반규정 적용
제39조의2 (법정손해배상 의 청구)	제39조의2	-	
<특례>	-	제39조의8 (개인정보 이용내역의 통지)	· 특례규정 적용
	-	제39조의9(손해배상의 보장)	· 특례규정 적용
	-	제39조의10 (노출된 개인정보의 삭제·차단)	· 특례규정 적용
	-	제39조의11(국내대리인의 지정)	· 특례규정 적용
	-	제39조의13(상호주의)	· 특례규정 적용
	-	제39조의14 (방송사업자등에 대한 특례)	· 특례규정 적용
	-	제39조의15 (과징금의 부과 등에 대한 특례)	· 특례규정 적용

제39조의3 | 개인정보의 수집·이용 동의 등에 대한 특례

법률

제39조의3(개인정보의 수집·이용 동의 등에 대한 특례) ① 정보통신서비스 제공자는 제15조제1항에도 불구하고 이용자의 개인정보를 이용하려고 수집하는 경우에는 다음 각 호의 모든 사항을 이용자에게 알리고 동의를 받아야 한다. 다음 각 호의 어느 하나의 사항을 변경하려는 경우에도 또한 같다.

1. 개인정보의 수집·이용 목적
2. 수집하는 개인정보의 항목
3. 개인정보의 보유·이용 기간

② 정보통신서비스 제공자는 다음 각 호의 어느 하나에 해당하는 경우에는 제1항에 따른 동의 없이 이용자의 개인정보를 수집·이용할 수 있다.

1. 정보통신서비스(「정보통신망 이용촉진 및 정보보호 등에 관한 법률」 제2조제1항제2호에 따른 정보통신서비스를 말한다. 이하 같다)의 제공에 관한 계약을 이행하기 위하여 필요한 개인정보로서 경제적·기술적인 사유로 통상적인 동의를 받는 것이 뚜렷하게 곤란한 경우
2. 정보통신서비스의 제공에 따른 요금정산을 위하여 필요한 경우
3. 다른 법률에 특별한 규정이 있는 경우

③ 정보통신서비스 제공자는 이용자가 필요한 최소한의 개인정보 이외의 개인정보를 제공하지 아니한다는 이유로 그 서비스의 제공을 거부해서는 아니 된다. 이 경우 필요한 최소한의 개인정보는 해당 서비스의 본질적 기능을 수행하기 위하여 반드시 필요한 정보를 말한다.

④ 정보통신서비스 제공자는 만 14세 미만의 아동으로부터 개인정보 수집·이용·제공 등의 동의를 받으려면 그 법정대리인의 동의를 받아야 하고, 대통령령으로 정하는 바에 따라 법정대리인이 동의하였는지를 확인하여야 한다.

⑤ 정보통신서비스 제공자는 만 14세 미만의 아동에게 개인정보 처리와 관련한 사항의 고지 등을 하는 때에는 이해하기 쉬운 양식과 명확하고 알기 쉬운 언어를 사용하여야 한다.

⑥ 보호위원회는 개인정보 처리에 따른 위험성 및 결과, 이용자의 권리 등을 명확하게 인지하지 못할 수 있는 만 14세 미만의 아동의 개인정보 보호 시책을 마련하여야 한다.

시행령

제48조의3(법정대리인 동의를 확인방법) ① 정보통신서비스 제공자는 법 제39조의3제4항에 따라 다음 각 호의 어느 하나에 해당하는 방법으로 법정대리인이 동의했는지를 확인해야 한다.

1. 동의 내용을 게재한 인터넷 사이트에 법정대리인이 동의 여부를 표시하도록 하고 정보통신서비스 제공자가 그 동의 표시를 확인했음을 법정대리인의 휴대전화 문자메시지로 알리는 방법

2. 동의 내용을 게재한 인터넷 사이트에 법정대리인이 동의 여부를 표시하도록 하고 법정대리인의 신용카드·직불카드 등의 카드정보를 제공받는 방법
 3. 동의 내용을 게재한 인터넷사이트에 법정대리인이 동의 여부를 표시하도록 하고 법정대리인의 휴대전화 본인인증 등을 통하여 본인 여부를 확인하는 방법
 4. 동의 내용이 적힌 서면을 법정대리인에게 직접 발급하거나, 우편 또는 팩스를 통하여 전달하고 법정대리인이 동의 내용에 대하여 서명날인 후 제출하도록 하는 방법
 5. 동의 내용이 적힌 전자우편을 발송하고 법정대리인으로부터 동의의 의사표시가 적힌 전자우편을 전송받는 방법
 6. 전화를 통하여 동의 내용을 법정대리인에게 알리고 동의를 받거나 인터넷주소 등 동의 내용을 확인할 수 있는 방법을 안내하고 재차 전화 통화를 통하여 동의를 받는 방법
 7. 그 밖에 제1호부터 제6호까지의 규정에 따른 방법에 준하는 방법으로 법정대리인에게 동의 내용을 알리고 동의의 의사표시를 확인하는 방법
- ② 정보통신서비스 제공자는 개인정보 수집 매체의 특성상 동의 내용을 전부 표시하기 어려운 경우 법정대리인에게 동의 내용을 확인할 수 있는 방법(인터넷주소·사업장 전화번호 등)을 안내할 수 있다.

1. 일반규정과의 관계

개인정보처리자는 일반규정인 제15조에 따라 정보주체의 개인정보를 수집·이용하여야 하며, 제16조에 따라 필요한 최소한의 정보를 수집하여야 한다. 또한, 만 14세 미만 아동의 개인정보를 처리하기 위하여 그 아동의 동의를 받아야 하는 경우에는 일반규정인 제22조제6항에 따라 법정대리인의 동의를 받아야 한다.

위의 일반규정은 정보통신서비스 제공자가 이용자의 개인정보를 수집·이용하거나 아동의 개인정보를 처리하는 경우에도 적용된다고 할 것이나 특례규정인 제39조의3은 개인정보 수집·이용 동의, 필요한 최소한 정보의 범위, 법정대리인의 동의 확인 방법 등을 별도로 규정하고 있으므로 이에 해당하는 경우에는 특례규정이 적용된다.

이는 정보처리 기술의 발전으로 정보통신망을 통한 개인정보 수집 규모는 나날이 증가하고 있는 반면, 정보통신망에 기반한 서비스의 경우 주로 비대면으로 이루어지고 있어, 그 서비스 이용자는 자신의 개인정보가 얼마나 수집되며 어떻게 이용될 것인지 제대로 알지 못한 채 개인정보의 수집에 동의할 위험성이 있는 등 정보통신망을 통한 개인정보 수집·이용 시 이용자 보호의 필요성이 보다 큰 점을 고려한 것이라고 할 수 있다.

2. 개인정보 수집·이용 동의에 대한 특례

가 이용자의 동의를 받는 경우

정보통신서비스 제공자가 이용자의 개인정보를 이용하려고 수집하는 경우 ① 개인정보의 수집·이용 목적 ② 수집하는 개인정보의 항목 ③ 개인정보의 보유·이용 기간을 이용자에게 알리고 동의를 받아야 한다(제1항). 이 경우 정보통신서비스 제공자는 수집 시점(회원 가입, 서비스 가입 등) 이전에 위의 세 가지 고지 사항 모두를 명확하게 인지할 수 있도록 알리고 동의를 받아야 한다.

제1항은 정보통신서비스 제공자가 개인정보를 이용하려고 수집하는 경우에 이용자의 동의를 받는 것을 전제로 이용자에게 알려야 할 항목을 규정하고 있으므로, 마찬가지로 정보주체에게 알려야 할 항목을 규정하고 있는 제15조제2항은 적용되지 않는 것으로 해석된다. 따라서 정보통신서비스 제공자는 특례에 따른 항목만을 고지하고 동의를 받는 것도 가능하다. 다만, 이용자 보호를 위하여 정보통신서비스 제공자는 특례에 따른 고지 사항 이외에도 제15조제2항에 따른 동의 거부권에 대한 사실 및 동의 거부 시 불이익 내용에 대해서도 알리고 동의를 받는 것이 바람직하다.

< 제15조제2항 및 제39조의3제1항에 따른 고지 사항 비교 >

제15조제2항에 따른 고지 사항	제39조의3제1항에 따른 고지사항
개인정보의 수집·이용 목적	개인정보의 수집·이용 목적
수집하는 개인정보의 항목	수집하는 개인정보의 항목
개인정보의 보유·이용 기간	개인정보의 보유·이용 기간
동의 거부권에 대한 사실 및 동의 거부 시 불이익 내용	-

나 이용자의 동의를 받지 않아도 되는 경우

1) 정보통신서비스의 제공에 관한 계약의 이행을 위하여 필요한 개인정보로서 경제적·기술적인 사유로 통상의 동의를 받는 것이 현저히 곤란한 경우

이용자가 요구하는 정보통신서비스를 제공하는 과정에서는 과금 정보, 통화 사실 기록(도수), 접속 로그(log), 결제 기록, 이용 정지기록 등과 같은 정보가 불가피하게 생성되게 된다. 이러한 정보는 계약 이행 과정에서 실시간으로 생성되어 수집되지만 이용자에게 매번 고지하고 동의를 얻는 것이 경제적으로 큰 비용이 들거나 기술적으로 통상의 동의를 받는 것이 현저히 어려운 경우가 많으므로 이용자의 동의 없이도 개인정보를 수집할 수 있도록 한 것이다.

위의 정보를 마케팅 등의 목적으로 활용하려면 수집 및 이용 목적을 통해 개인정보의 이용 목적을 명시하고 이용자에게 동의를 얻어야 한다. 만약 동의를 얻지 않고 임의로 이용하면 목적 외 이용에 해당되어 과징금 및 형사 처벌의 대상이 될 수 있다.

이와 유사하게 일반규정인 제15조제1항 또한 개인정보를 수집·이용할 수 있는 경우로서 계약의 체결 및 이행을 위하여 불가피하게 필요한 경우를 규정하고 있으나(동항 제4호), 특례의 경우 계약의 이행을 위하여 필요할 것뿐만 아니라 경제적·기술적인 사유로 통상의 동의를 받는 것이 현저히 곤란할 것을 요건으로 하는 점에서 차이가 있다. 즉, 정보통신서비스 제공자는 계약의 이행을 위하여 불가피하게 필요한 개인정보라 하더라도 경제적·기술적인 사유로 통상의 동의를 받는 것이 현저히 곤란한 경우가 아니라면 이용자의 동의를 받아야 한다.

2) 정보통신서비스의 제공에 따른 요금정산을 위해 필요한 경우

이용자의 서비스 이용에 따른 서비스별 요금액, 납부 또는 미납한 사실, 미납액 등에 관한 정보가 해당할 수 있으며, 정보통신서비스 제공자는 요금정산이 완료될 때까지 이들 정보를 이용자의 동의 여부와 관계없이 수집·이용할 수 있다.

3) 다른 법률에 특별한 규정이 있는 경우

다른 법률에서 개인정보의 수집·이용을 구체적으로 요구하거나 허용하고 있는 조항이 있으면 이용자의 동의 없이 개인정보를 수집·이용할 수 있다(다른 법률에 특별한 규정이 있는 경우의 예시는 제15조(개인정보의 수집·이용) 해설 참고).

3. 필요한 최소한의 개인정보 수집에 대한 특례

정보통신서비스 제공자는 이용자의 개인정보를 수집하는 경우 일반규정인 제16조에 따른 필요한 최소한의 개인정보 수집, 필요한 최소한의 정보 외의 개인정보 수집에 동의하지 않을 수 있다는 사실의 고지 및 정보주체가 이에 동의하지 않는 것을 이유로 한 재화 또는 서비스의 제공 금지 등을 준수하여야 한다(이와 관련하여 자세한 내용은 제16조(개인정보의 수집 제한) 해설 참고).

다만, 특례규정인 제39조의3제3항은 제16조제3항의 내용에 추가하여 ‘필요한 최소한의 개인정보’의 개념을 정의하고 있으므로 일반규정에 우선하여 적용된다. 따라서, 정보통신서비스 제공자의 개인정보 수집이 필요한 최소한의 정보에 해당하는지에 대한 판단은 특례규정에 따라 이루어져야 한다.

제3항에 따르면 ‘필요한 최소한의 개인정보’란 ‘해당 서비스’의 본질적 기능을 수행하기 위하여 반드시 필요한 정보를 말한다. 여기서 ‘해당 서비스’란 사업자가 정보통신망을 통해 이용약관, 개인정보 처리방침, 서비스 안내·설명자료 등에 따라 이용자에게 제공하는 개별 서비스를 말하며, 이와 같은 개별 서비스는 통상적인 이용자가 합리적으로 예상할 수 있어야 한다. 또한, ‘본질적 기능’이란 사업자가 해당 서비스를 제공하기 위해 반드시 필요한 기능을 의미한다.

정보통신서비스 제공자가 해당 서비스 제공에 반드시 필요한 개인정보에 대해서는 이용자로부터 수집 동의를 받아야 하고(필수동의 항목), 해당 서비스의 추가적 기능 또는 사업자의 필요에 의해 이용자에게 개인정보 수집 동의를 요청할 수 있다(선택동의 항목). 정보통신서비스 제공자는 이용자의 개인정보 수집 시 필수동의 항목과 선택동의 항목으로 구분하여 각각 동의를 받아야 한다.

4. 아동의 개인정보 수집·이용·제공 동의 등에 대한 특례

정보통신서비스 제공자가 만 14세 미만 아동으로부터 개인정보의 수집·이용·제공 등의 동의를 받아야 하는 경우에는 일반규정인 제22조제6항에 따라 법정대리인의 동의를 받아야 한다. 다만, 최근 인공지능 등 신기술이 적용된 정보통신서비스를 통하여 법정대리인의 동의 없이 아동의 개인정보가 수집되거나 아동에게 부적절한 내용의 정보가 제공되는 사건이 발생하여 문제가 되고 있어 특례규정인 제39조의3제4항, 제5항 및 제6항은 정보통신망에서의 아동의 개인정보 보호를 강화하기 위한 조치를 규정하였다.

가 법정대리인 동의의 확인 방법

정보통신서비스 제공자가 만 14세 미만의 아동으로부터 개인정보 수집·이용·제공 등의 동의를 받기 위하여 그 법정대리인의 동의를 받는 경우 다음 중 하나의 방법으로 법정대리인이 동의하였는지 확인해야 한다(제4항, 영 제48조의3제1항).

이는 정보통신서비스 제공자가 법정대리인의 동의를 받는 경우 동의가 형식적으로 이루어지거나 동의를 받지 않는 사례가 다수 있는 점을 고려하여 법정대리인이 실제로 동의하였는지 확인하도록 한 것이다.

법정대리인 동의의 확인 방법(영 제48조의3)

1. 동의 내용을 게재한 인터넷 사이트에 법정대리인이 동의 여부를 표시하도록 하고 정보통신 서비스 제공자들이 그 동의 표시를 확인했음을 법정대리인의 휴대전화 문자메시지로 알리는 방법
2. 동의 내용을 게재한 인터넷 사이트에 법정대리인이 동의 여부를 표시하도록 하고 법정대리인의 신용카드·직불카드 등의 카드정보를 제공받는 방법
3. 동의 내용을 게재한 인터넷 사이트에 법정대리인이 동의 여부를 표시하도록 하고 법정대리인의 휴대전화 본인인증 등을 통해 본인 여부를 확인하는 방법
4. 동의 내용이 적힌 서면을 법정대리인에게 직접 발급하거나, 우편 또는 팩스를 통하여 전달하고 법정대리인이 동의 내용에 대하여 서명날인 후 제출하도록 하는 방법
5. 동의 내용이 적힌 전자우편을 발송하여 법정대리인으로부터 동의의 의사표시가 적힌 전자우편을 전송받는 방법
6. 전화를 통하여 동의 내용을 법정대리인에게 알리고 동의를 얻거나 인터넷주소 등 동의 내용을 확인할 수 있는 방법을 안내하고 재차 전화 통화를 통하여 동의를 얻는 방법
7. 그 밖에 제1호부터 제6호까지의 규정에 따른 방법에 준하는 방법으로 법정대리인에게 동의 내용을 알리고 동의의 의사표시를 확인하는 방법
8. 개인정보 수집 매체의 특성상 동의 내용을 전부 표시하기 어려운 경우 법정대리인에게 동의 내용을 확인할 수 있는 방법(인터넷주소·사업장 전화번호 등)을 안내

나 만 14세 미만 아동에 대한 개인정보 처리 관련 사항의 고지 방법

정보통신서비스 제공자가 만 14세 미만의 아동에게 개인정보 처리와 관련한 사항의 고지 등을 할 때에는 이해하기 쉬운 양식과 명확하고 알기 쉬운 언어를 사용하여야 한다(제5항). 아동은 인지능력 등이 부족할 수 있어 개인정보 처리에 관한 사항을 아동에게 알리는 경우 그 구체적인 내용을 제대로 이해하지 못하는 경우가 많다는 점을 고려한 것이다.

다 만 14세 미만 아동의 개인정보 보호시책 마련

보호위원회는 만14세 미만의 아동이 개인정보 처리에 따른 위험성 및 결과, 이용자의 권리 등을 명확하게 인지하지 못할 수 있다는 점을 고려하여 개인정보 보호 시책을 마련하여야 한다(제6항).

5. 가명정보의 적용 제외

제39조의3 특례규정은 가명정보의 수집·이용 등에는 적용되지 않는다(제28조의7).

6. 벌칙규정

위반행위	벌칙
이용자의 동의를 받지 아니하고 개인정보를 수집한 경우 (제39조의14에 따라 준용되는 경우 포함) (제39조의3제1항 위반)	위반행위와 관련한 매출액의 100분의 3 이하 과징금 (제39조의15제1항제6호)
이용자의 동의를 받지 아니하고 개인정보를 수집한 자 (제39조의14에 따라 준용되는 경우 포함) (제39조의3제1항 위반)	5년 이하의 징역 또는 5천만원 이하의 벌금 (제71조제4호의5)
필요한 최소한의 정보 이외의 정보 수집에 동의하지 않는다는 이유로 서비스의 제공을 거부한 자 (제39조의14에 따라 준용되는 경우를 포함) (제39조의3제3항 위반)	3천만원 이하의 과태료 (제75조제2항제12호의2)
법정대리인의 동의를 받지 아니한 자 또는 법정대리인이 동의하였는지를 확인하지 아니하고 만 14세 미만인 아동의 개인정보를 수집한 자 (제39조의14에 따라 준용되는 경우 포함) (제39조의3제4항 위반)	5년 이하의 징역 또는 5천만원 이하의 벌금 (제71조제4호의6)

제39조의4 | 개인정보 유출등의 통지·신고에 대한 특례

법률

제39조의4(개인정보 유출등의 통지·신고에 대한 특례) ① 제34조제1항 및 제3항에도 불구하고 정보통신서비스 제공자와 그로부터 제17조제1항에 따라 이용자의 개인정보를 제공받은 자(이하 “정보통신서비스 제공자등”이라 한다)는 개인정보의 분실·도난·유출(이하 “유출등”이라 한다) 사실을 안 때에는 지체 없이 다음 각 호의 사항을 해당 이용자에게 알리고 보호위원회 또는 대통령령으로 정하는 전문기관에 신고하여야 하며, 정당한 사유 없이 그 사실을 안 때부터 24시간을 경과하여 통지·신고해서는 아니 된다. 다만, 이용자의 연락처를 알 수 없는 등 정당한 사유가 있는 경우에는 대통령령으로 정하는 바에 따라 통지를 갈음하는 조치를 취할 수 있다.

1. 유출등이 된 개인정보 항목
2. 유출등이 발생한 시점
3. 이용자가 취할 수 있는 조치
4. 정보통신서비스 제공자등의 대응 조치
5. 이용자가 상담 등을 접수할 수 있는 부서 및 연락처

② 제1항의 신고를 받은 대통령령으로 정하는 전문기관은 지체 없이 그 사실을 보호위원회에 알려야 한다.

③ 정보통신서비스 제공자등은 제1항에 따른 정당한 사유를 보호위원회에 소명하여야 한다.

④ 제1항에 따른 통지 및 신고의 방법·절차 등에 필요한 사항은 대통령령으로 정한다.

시행령

제48조의4(개인정보 유출 등의 통지·신고에 관한 특례) ① 법 제39조의4제1항 각 호 외의 부분 본문 및 제2항에서 “대통령령으로 정하는 전문기관”이란 한국인터넷진흥원을 말한다.

② 정보통신서비스 제공자등은 개인정보의 분실·도난·유출의 사실을 안 때에는 지체 없이 법 제39조의4제1항 각 호의 모든 사항을 서면등의 방법으로 이용자에게 알리고 보호위원회 또는 한국인터넷진흥원에 신고해야 한다.

③ 정보통신서비스 제공자등은 제2항에 따른 통지·신고를 하려는 경우에는 법 제39조의4제1항제1호 또는 제2호의 사항에 관한 구체적인 내용이 확인되지 않았으면 그때까지 확인된 내용과 같은 항 제3호부터 제5호까지의 사항을 우선 통지·신고한 후 추가로 확인되는 내용에 대해서는 확인되는 즉시 통지·신고해야 한다.

④ 정보통신서비스 제공자등은 법 제39조의4제1항 각 호 외의 부분 단서에 따른 정당한 사유가 있는 경우에는 법 제39조의4제1항 각 호의 사항을 자신의 인터넷 홈페이지에 30일 이상 게시하는 것으로 제2항의 통지를 갈음할 수 있다.

⑤ 천재지변이나 그 밖의 부득이한 사유로 제4항에 따른 홈페이지 게시가 곤란한 경우에는 「신문 등의 진흥에 관한 법률」에 따른 전국을 보급지역으로 하는 둘 이상의 일반일간신문에 1회 이상 광고하는 것으로 제4항에 따른 홈페이지 게시를 갈음할 수 있다.

⑥ 정보통신서비스 제공자들은 법 제39조의4제1항 각 호 외의 부분 본문 및 단서에 따른 정당한 사유를 지체 없이 서면으로 보호위원회에 소명해야 한다.

1. 일반규정과의 관계

개인정보처리자는 개인정보가 유출되었음을 알게 된 때에는 일반규정인 제34조에 따라 지체 없이 정보주체에게 유출 통지 등의 조치를 하여야 한다.

한편, 특례규정인 제39조의4는 정보통신서비스 제공자들이 개인정보 유출등의 사실을 안 때에는 24시간 내 이용자에게 통지하고 보호위원회 또는 한국인터넷진흥원에 신고하도록 규정하고 있으므로, 정보통신서비스 제공자들에 대해서는 위의 일반규정이 아닌 특례규정이 적용된다.

이처럼 유출등 통지·신고에 대한 특례를 규정한 것은 정보통신망에서의 개인정보 유출은 파급력과 전파력이 오프라인과 비교할 수 없이 크다는 점을 고려한 것으로, 정보통신망에서 보다 신속하고 효과적인 보호조치를 도입하여 인터넷 명의도용, 전화사기(보이스피싱), 스팸 등 2차 피해 확산을 최소화할 필요가 있기 때문이다.

2. 개인정보 유출등의 통지 및 신고 의무

가 통지 및 신고 의무의 발생

개인정보의 유출등이란 개인정보가 해당 정보통신서비스 제공자의 관리·통제권을 벗어나 제3자가 그 내용을 알 수 있는 상태에 이르게 된 것을 의미하며(대법원 2014. 5. 16. 선고 2011다24555판결 참고), 정보통신서비스 제공자들이 개인정보의 분실·도난·유출(이하 “유출등”이라 한다) 사실을 안 때에 이용자에게 통지 및 보호위원회 또는 한국인터넷진흥원에 신고해야 하는 의무가 발생한다.

정보통신서비스 제공자들의 통지 및 신고 의무는 유출등의 규모와 관계 없이 발생한다. 이는 정보통신망의 파급력 및 전파력을 고려한 것으로서, 일반규정이 적용되는 개인정보처리자의 유출등 신고의 경우 1천 명 이상의 개인정보가 유출된 경우로 제한하고 있는 것과 구분된다.

1) 통지 및 신고의 시기

특례규정인 제39조의4제1항은 지체 없이 통지 및 신고하도록 하면서 정당한 사유 없이 그 사실을 안 때로부터 24시간을 경과할 수 없도록 규정하고 있으므로 유출등 통지 및 신고는 정당한 사유가 없는 한 유출등이 된 사실을 안 때로부터 24시간 이내에 이루어져야 한다.

이는 정보통신망에서 개인정보 유출등 발생 시 파급력과 전파력을 고려하여 일반규정인 제34조에 따른 유출 통지 시기인 5일 이내(표준지침 제26조제1항)보다 단기의 기간(24시간 이내)을 법률 차원에서 명확하게 규정한 것이다.

다만, 24시간 이내에 통지 및 신고를 완료하였다더라도 그 내용이 허위로 작성되었거나 고의로 법정 사항을 누락한 경우에는 적법한 통지 및 신고로 볼 수 없다.

한편, 정당한 사유가 있는 경우에는 24시간을 경과하여 통지 및 신고할 수 있다. 통지와 관련한 정당한 사유로는 수사 상의 이유(예: 경찰이 이용자 통지에 대해 보류를 요청한 경우), 물리적·기술적·관리적인 사유로 통지가 불가능한 경우, 그 밖에 단전, 홍수, 폭설 등의 천재지변으로 인해 24시간 내에 통지가 불가능한 경우 등이 해당할 수 있다. 또한, 신고와 관련한 정당한 사유로는 단전, 홍수, 폭설 등의 천재지변으로 인해 24시간 내에 신고가 불가능한 경우 등이 해당할 수 있다. 이 경우 정보통신서비스 제공자들은 정당한 사유를 지체 없이 서면(전자문서를 포함한다)으로 보호위원회에 소명하여야 한다(제39조의4 제3항, 영 제48조의4제6항).

2) 통지 및 신고의 내용

정보통신서비스 제공자들은 다음 사항 모두를 통지 및 신고하여야 한다. 개인정보 유출등 통지 및 신고 제도는 개인정보 유출등으로 인한 2차 피해 확산 방지가 목적이므로 제39조의4제1항은 통지 사항과 신고 사항을 동일하게 규정하고 있다. 이는 개인정보처리자의 경우 유출 통지 및 신고 사항이 다른 것과 구분된다(제34조 참고).

유출등 통지 및 신고 사항(제39조의4제1항)

1. 유출등이 된 개인정보 항목
2. 유출등이 발생한 시점
3. 이용자가 취할 수 있는 조치
4. 정보통신서비스 제공자들의 대응 조치
5. 이용자가 상담 등을 접수할 수 있는 부서 및 연락처

다 확인사실의 우선 통지 및 신고

정보통신서비스 제공자등이 개인정보 유출등의 사실을 안 때에도 유출등이 된 개인정보의 항목 또는 유출등이 발생한 시점에 관한 구체적인 내용이 확인되지 않은 경우에는 그때까지 확인된 내용과 이용자가 취할 수 있는 조치, 정보통신서비스 제공자등의 대응 조치, 이용자가 상담 등을 접수할 수 있는 부서 및 연락처를 우선 통지 및 신고한 후 추가로 확인되는 내용은 확인되는 즉시 통지 및 신고하여야 한다(영 제48조의4제3항).

따라서 24시간 이내에 진행된 통지 및 신고 내용 중 유출등이 된 개인정보 항목 및 유출등이 발생한 시점에 관한 내용이 미흡하다는 사실만으로는 해당 통지 및 신고가 위법하다 할 수 없으나 이에 대하여는 추후에 해당 내용을 보충하여 빠른 시일 내에 통지가 이루어져야 한다. 한편, 이용자가 취할 수 있는 조치, 정보통신서비스 제공자등의 대응 조치, 이용자가 상담 등을 접수할 수 있는 부서 및 연락처는 정당한 사유가 없는 한 24시간 이내에 충실하게 통지 및 신고하여야 하며 이를 부실하게 한 경우에는 해당 통지 및 신고는 위법한 것으로 볼 수 있다.

라 통지 및 신고의 방법

통지 및 신고는 서면, 전자우편, 팩스, 전화, 문자전송 또는 이에 상당하는 방법(서면등)으로 하여야 한다(영 제48조의4제2항). 특례규정은 유출등 사고 발생이라는 긴박한 상황에서 정보통신서비스 제공자등이 보다 신속하고 효율적으로 대응할 수 있도록 통지와 신고의 방법을 동일하게 규정하였다.

한편, 정보통신서비스 제공자등은 이용자의 연락처를 알 수 없는 등 정당한 사유가 있는 경우에는 통지 항목을 자신의 인터넷 홈페이지에 30일 이상 게시하는 것으로 통지를 갈음할 수 있다(영 제48조의4제4항). 이 경우 정보통신서비스 제공자등은 정당한 사유를 지체 없이 서면(전자문서를 포함한다)으로 보호위원회에 소명하여야 한다(제39조의4제3항, 영 제48조의4제6항). 또한, 천재지변이나 그 밖에 부득이한 사유로 위의 홈페이지 게시가 곤란한 경우에는 전국을 보급지역으로 하는 둘 이상의 일반일간신문에 1회 이상 공고하는 것으로 홈페이지 게시를 갈음할 수 있다(영 제48조의4제5항).

3. 가명정보의 적용 제외

제39조의4 특례규정은 가명정보가 유출등이 된 경우에는 적용되지 않는다(제28조의7).

4. 제34조에 따른 유출 통지 제도와 비교

일반규정인 제34조에 따른 유출 통지 제도와 특례규정인 제39조의4에 따른 유출등 통지·신고 제도는 통지 및 신고 시기, 신고 기준(범위) 제한 유무, 신고의 내용 등에서 차이가 있으며, 그 구체적인 내용은 다음과 같다.

구분		제34조에 따른 유출 통지 등	제39조의4에 따른 유출등 통지·신고
통지 및 신고 대상		개인정보의 유출	개인정보의 분실·도난·유출(유출등)
과태료		3천만원 이하	3천만원 이하
통지	시기	유출 사실 인지 시 5일 이내 통지	유출등 사실 인지 시 24시간 이내 통지
	내용	<ol style="list-style-type: none"> 1. 유출된 개인정보의 항목 2. 유출된 시점과 그 경위 3. 유출로 인하여 발생할 수 있는 피해를 최소화하기 위하여 정보주체가 할 수 있는 방법 등에 관한 정보 4. 개인정보처리자의 대응조치 및 피해 구제절차 5. 정보주체에게 피해가 발생한 경우 신고 등을 접수할 수 있는 담당부서 및 연락처 	<ol style="list-style-type: none"> 1. 유출등이 된 개인정보 항목 2. 유출등이 발생한 시점 3. 이용자가 취할 수 있는 조치 4. 정보통신서비스 제공자등의 대응 조치 5. 이용자가 상담 등을 접수할 수 있는 부서 및 연락처
	방법	서면등 단, 1천명 이상 정보주체의 개인정보 유출 시 7일 이상 홈페이지 게재도 병행 (홈페이지 미운영 시 사업장등에 게시 가능)	서면등 이용자 연락처를 알 수 없는 등 정당한 사유가 있는 경우 홈페이지 게시(30일 이상) (홈페이지 게시 곤란 시 일간신문 공고로 같음 가능)
신고	범위	1천명 이상 정보주체의 개인정보 유출 시	제한 없음
	시점	통지 및 조치 결과를 5일 이내 신고	유출등 사실 인지 시 24시간 이내 통지 (통지 시기와 동일)
	접수 기관	보호위원회, 한국인터넷진흥원	보호위원회, 한국인터넷진흥원
	내용	정보주체에 대한 통지 및 조치 결과	통지 내용과 동일
	방법	전자우편, 팩스, 인터넷사이트를 통해 유출사고 신고 및 신고서 제출, 특별한 사정이 있는 경우 전화 신고 후 유출 신고서 제출 가능	통지 방법과 동일

5. 벌칙규정

위반행위	벌칙
<p>개인정보 유출등 통지 또는 신고를 하지 않는 자 또는 정당한 사유 없이 24시간을 경과하여 통지 또는 신고한 자 (제39조의14에 따라 준용되는 경우 포함) (제39조의4제1항 위반)</p>	<p>3천만원 이하 과태료 (제75조제2항제12호의3)</p>
<p>정당한 사유에 관한 소명을 하지 않은 자 또는 허위로 한 자 (제39조의14에 따라 준용되는 경우 포함) (제39조의4제3항 위반)</p>	<p>3천만원 이하 과태료 (제75조제2항제12호의4)</p>

제29조, 제39조의5 | 개인정보 보호조치에 대한 특례

<p style="text-align: center;">법률</p>	<p>제29조(안전조치의무) 개인정보처리자는 개인정보가 분실·도난·유출·위조·변조 또는 훼손되지 아니하도록 내부 관리계획 수립, 접속기록 보관 등 대통령령으로 정하는 바에 따라 안전성 확보에 필요한 기술적·관리적 및 물리적 조치를 하여야 한다.</p> <p>제39조의5(개인정보의 보호조치에 대한 특례) 정보통신서비스 제공자등은 이용자의 개인정보를 처리하는 자를 최소한으로 제한하여야 한다.</p>
<p style="text-align: center;">시행령</p>	<p>제48조의2(개인정보의 안전성 확보 조치에 관한 특례) ① 정보통신서비스 제공자(「정보통신망 이용촉진 및 정보보호 등에 관한 법률」 제2조제1항제3호에 해당하는 자를 말한다. 이하 같다)와 그로부터 이용자(같은 법 제2조제1항제4호에 해당하는 자를 말한다. 이하 같다)의 개인정보를 법 제17조제1항제1호에 따라 제공받은 자(이하 “정보통신서비스 제공자등”이라 한다)는 이용자의 개인정보를 처리하는 경우에는 제30조에도 불구하고 법 제29조에 따라 다음 각 호의 안전성 확보 조치를 해야 한다.</p> <ol style="list-style-type: none"> 1. 개인정보의 안전한 처리를 위한 다음 각 목의 내용을 포함하는 내부관리계획의 수립·시행 <ul style="list-style-type: none"> 가. 개인정보 보호책임자의 지정 등 개인정보 보호 조직의 구성·운영에 관한 사항 나. 정보통신서비스 제공자등의 지휘·감독을 받아 이용자의 개인정보를 처리하는 자(이하 이 조에서 “개인정보취급자”라 한다)의 교육에 관한 사항 다. 제2호부터 제6호까지의 규정에 따른 조치를 이행하기 위하여 필요한 세부 사항 2. 개인정보에 대한 불법적인 접근을 차단하기 위한 다음 각 목의 조치 <ul style="list-style-type: none"> 가. 개인정보를 처리할 수 있도록 체계적으로 구성된 데이터베이스시스템(이하 이 조에서 “개인정보처리시스템”이라 한다)에 대한 접근 권한의 부여·변경·말소 등에 관한 기준의 수립·시행 나. 개인정보처리시스템에 대한 침입차단시스템 및 침입탐지시스템의 설치·운영 다. 개인정보처리시스템에 접속하는 개인정보취급자의 컴퓨터 등에 대한 외부 인터넷망 차단[전년도 말 기준 직전 3개월간 그 개인정보가 저장·관리되고 있는 이용자 수가 일일평균 100만명 이상이거나 정보통신서비스(「정보통신망 이용촉진 및 정보보호 등에 관한 법률」 제2조제1항제2호에 따른 정보통신서비스를 말한다. 이하 같다) 부문 전년도(법인인 경우에는 전 사업연도를 말한다) 매출액이 100억원 이상인 정보통신서비스 제공자등만 해당한다]

- 라. 비밀번호의 생성 방법 및 변경 주기 등의 기준 설정 및 운영
- 마. 그 밖에 개인정보에 대한 접근 통제를 위하여 필요한 조치
3. 접속기록의 위조·변조 방지를 위한 다음 각 목의 조치
- 가. 개인정보취급자가 개인정보처리시스템에 접속하여 개인정보를 처리한 경우 접속일시, 처리내역 등의 저장 및 이의 확인·감독
- 나. 개인정보처리시스템에 대한 접속기록을 별도의 저장장치에 백업 보관
4. 개인정보가 안전하게 저장·전송될 수 있도록 하기 위한 다음 각 목의 조치
- 가. 비밀번호의 일방향 암호화 저장
- 나. 주민등록번호, 계좌정보 및 제18조제3호에 따른 정보 등 보호위원회가 정하여 고시하는 정보의 암호화 저장
- 다. 정보통신망을 통하여 이용자의 개인정보 및 인증정보를 송신·수신하는 경우 보안서버 구축 등의 조치
- 라. 그 밖에 암호화 기술을 이용한 보안조치
5. 개인정보처리시스템 및 개인정보취급자가 개인정보 처리에 이용하는 정보 기기에 컴퓨터바이러스, 스파이웨어 등 악성프로그램의 침투 여부를 항시 점검·치료할 수 있도록 하기 위한 백신소프트웨어 설치 및 주기적 갱신·점검 조치
6. 그 밖에 개인정보의 안전성 확보를 위하여 필요한 조치
- ② 보호위원회는 정보통신서비스 제공자등이 제1항에 따른 안전성 확보 조치를 하도록 시스템을 구축하는 등 필요한 지원을 할 수 있다.
- ③ 제1항에 따른 안전성 확보 조치에 관한 세부 기준은 보호위원회가 정하여 고시한다.

개인정보의 기술적·관리적 보호조치 기준(보호위원회 고시 제2020-5호)

제1조(목적) ① 이 기준은 「개인정보 보호법」(이하 “법”이라 한다) 제29조 및 같은 법 시행령 제48조의2제3항에 따라 정보통신서비스 제공자등(제39조의14에 따라 준용되는 자를 포함한다. 이하 같다)이 이용자의 개인정보를 처리함에 있어서 개인정보의 분실·도난·유출·위조·변조 또는 훼손을 방지하고 개인정보의 안전성 확보를 위하여 필요한 기술적·관리적 보호조치의 최소한의 기준을 정하는 것을 목적으로 한다.

② 정보통신서비스 제공자등은 사업규모, 개인정보 보유 수 등을 고려하여 스스로의 환경에 맞는 개인정보 보호조치 기준을 수립하여 시행하여야 한다.

제2조(정의) 이 기준에서 사용하는 용어의 뜻은 다음과 같다.

1. “개인정보 보호책임자”란 이용자의 개인정보보호 업무를 총괄하거나 업무처리를 최종 결정하는 임직원을 말한다.
2. “개인정보취급자”란 이용자의 개인정보를 수집, 보관, 처리, 이용, 제공, 관리 또는 파기 등의 업무를 하는 자를 말한다.

3. “내부관리계획” 이라 함은 정보통신서비스 제공자들이 개인정보의 안전한 처리를 위하여 개인정보보호 조직의 구성, 개인정보취급자의 교육, 개인정보 보호조치 등을 규정한 계획을 말한다.
4. “개인정보처리시스템” 이라 함은 개인정보를 처리할 수 있도록 체계적으로 구성된 데이터베이스시스템을 말한다.
5. “망분리” 라 함은 외부 인터넷망을 통한 불법적인 접근과 내부정보 유출을 차단하기 위해 업무망과 외부 인터넷망을 분리하는 망 차단조치를 말한다.
6. “비밀번호” 라 함은 이용자 및 개인정보취급자 등이 시스템 또는 정보통신망에 접속할 때 식별자와 함께 입력하여 정당한 접속 권한을 가진 자라는 것을 식별할 수 있도록 시스템에 전달해야 하는 고유의 문자열로서 타인에게 공개되지 않는 정보를 말한다.
7. “접속기록” 이라 함은 이용자 또는 개인정보취급자 등이 개인정보처리시스템에 접속하여 수행한 업무 내역에 대하여 식별자, 접속일시, 접속지를 알 수 있는 정보, 수행업무 등 접속한 사실을 전자적으로 기록한 것을 말한다.
8. “바이오정보” 라 함은 지문, 얼굴, 홍채, 정맥, 음성, 필적 등 개인을 식별할 수 있는 신체적 또는 행동적 특징에 관한 정보로서 그로부터 가공되거나 생성된 정보를 포함한다.
9. “P2P(Peer to Peer)” 라 함은 정보통신망을 통해 서버의 도움 없이 개인과 개인이 직접 연결되어 파일을 공유하는 것을 말한다.
10. “공유설정” 이라 함은 컴퓨터 소유자의 파일을 타인이 조회·변경·복사 등을 할 수 있도록 설정하는 것을 말한다.
11. “보안서버” 라 함은 정보통신망에서 송·수신하는 정보를 암호화하여 전송하는 웹서버를 말한다.
12. “인증정보” 라 함은 개인정보처리시스템 또는 정보통신망을 관리하는 시스템 등이 요구한 식별자의 신원을 검증하는데 사용되는 정보를 말한다.
13. “모바일 기기” 란 스마트폰, 태블릿PC 등 무선망을 이용할 수 있는 휴대용 기기를 말한다.
14. “보조저장매체” 란 이동형 하드디스크(HDD), USB메모리, CD(Compact Disk) 등 자료를 저장할 수 있는 매체로서 개인정보처리시스템 또는 개인용 컴퓨터 등과 쉽게 분리·접속할 수 있는 저장매체를 말한다.

제3조(내부관리계획의 수립·시행) ① 정보통신서비스 제공자들은 다음 각 호의 사항을 정하여 개인정보보호 조직을 구성·운영하여야 한다.

1. 개인정보 보호책임자의 자격요건 및 지정에 관한 사항
2. 개인정보 보호책임자와 개인정보취급자의 역할 및 책임에 관한 사항
3. 개인정보 내부관리계획의 수립 및 승인에 관한 사항
4. 개인정보의 기술적·관리적 보호조치 이행 여부의 내부 점검에 관한 사항

- 5. 개인정보 처리업무를 위탁하는 경우 수탁자에 대한 관리 및 감독에 관한 사항
- 6. 개인정보의 분실·도난·유출·위조·변조·훼손 등이 발생한 경우의 대응 절차 및 방법에 관한 사항

7. 그 밖에 개인정보보호를 위해 필요한 사항

② 정보통신서비스 제공자등은 다음 각 호의 사항을 정하여 개인정보 보호책임자 및 개인정보취급자를 대상으로 사업규모, 개인정보 보유 수 등을 고려하여 필요한 교육을 정기적으로 실시하여야 한다.

1. 교육목적 및 대상
2. 교육 내용
3. 교육 일정 및 방법

③ 정보통신서비스 제공자등은 제1항 및 제2항에 대한 세부 계획, 제4조부터 제8조까지의 보호조치 이행을 위한 세부적인 추진방안을 포함한 내부관리계획을 수립·시행하여야 한다.

제4조(접근통제) ① 정보통신서비스 제공자등은 개인정보처리시스템에 대한 접근권한을 서비스 제공을 위하여 필요한 개인정보 보호책임자 또는 개인정보취급자에게만 부여한다.

② 정보통신서비스 제공자등은 전보 또는 퇴직 등 인사이동이 발생하여 개인정보취급자가 변경되었을 경우 지체 없이 개인정보처리시스템의 접근권한을 변경 또는 말소한다.

③ 정보통신서비스 제공자등은 제1항 및 제2항에 의한 권한 부여, 변경 또는 말소에 대한 내역을 기록하고, 그 기록을 최소 5년간 보관한다.

④ 정보통신서비스 제공자등은 개인정보취급자가 정보통신망을 통해 외부에서 개인정보처리시스템에 접속이 필요한 경우에는 안전한 인증 수단을 적용하여야 한다.

⑤ 정보통신서비스 제공자등은 정보통신망을 통한 불법적인 접근 및 침해사고 방지를 위해 다음 각 호의 기능을 포함한 시스템을 설치·운영하여야 한다.

1. 개인정보처리시스템에 대한 접속 권한을 IP주소 등으로 제한하여 인가받지 않은 접근을 제한
2. 개인정보처리시스템에 접속한 IP주소 등을 재분석하여 불법적인 개인정보 유출 시도를 탐지

⑥ 전년도 말 기준 직전 3개월간 그 개인정보가 저장·관리되고 있는 이용자 수가 일일평균 100만명 이상이거나 정보통신서비스 부문 전년도(법인인 경우에는 전 사업연도를 말한다) 매출액이 100억원 이상인 정보통신서비스 제공자등은 개인정보처리시스템에서 개인정보를 다운로드 또는 파기할 수 있거나 개인정보처리시스템에 대한 접근권한을 설정할 수 있는 개인정보취급자의 컴퓨터 등을 물리적 또는 논리적으로 망분리 하여야 한다.

⑦ 정보통신서비스 제공자등은 이용자가 안전한 비밀번호를 이용할 수 있도록 비밀번호 작성규칙을 수립하고, 이행한다.

⑧ 정보통신서비스 제공자등은 개인정보취급자를 대상으로 다음 각 호의 사항을 포함하는 비밀번호 작성규칙을 수립하고, 이를 적용·운영하여야 한다.

1. 영문, 숫자, 특수문자 중 2종류 이상을 조합하여 최소 10자리 이상 또는 3종류 이상을 조합하여 최소 8자리 이상의 길이로 구성
2. 연속적인 숫자나 생일, 전화번호 등 추측하기 쉬운 개인정보 및 아이디와 비슷한 비밀번호는 사용하지 않는 것을 권고
3. 비밀번호에 유효기간을 설정하여 반기별 1회 이상 변경

⑨ 정보통신서비스 제공자등은 처리중인 개인정보가 인터넷 홈페이지, P2P, 공유설정 등을 통하여 열람권한이 없는 자에게 공개되거나 외부에 유출되지 않도록 개인정보처리시스템 및 개인정보취급자의 컴퓨터와 모바일 기기에 조치를 취하여야 한다.

⑩ 정보통신서비스 제공자등은 개인정보처리시스템에 대한 개인정보취급자의 접속이 필요한 시간 동안만 최대 접속시간 제한 등의 조치를 취하여야 한다.

제5조(접속기록의 위·변조방지) ① 정보통신서비스 제공자등은 개인정보취급자가 개인정보처리시스템에 접속한 기록을 월 1회 이상 정기적으로 확인·감독하여야 하며, 시스템 이상 유무의 확인 등을 위해 최소 1년 이상 접속기록을 보존·관리하여야 한다.

② 단, 제1항의 규정에도 불구하고 「전기통신사업법」 제5조의 규정에 따른 기간통신사업자의 경우에는 보존·관리해야할 최소 기간을 2년으로 한다.

③ 정보통신서비스 제공자등은 개인정보취급자의 접속기록이 위·변조되지 않도록 별도의 물리적인 저장 장치에 보관하여야 하며 정기적인 백업을 수행하여야 한다.

제6조(개인정보의 암호화) ① 정보통신서비스 제공자등은 비밀번호는 복호화되지 아니하도록 일방향 암호화하여 저장한다.

② 정보통신서비스 제공자등은 다음 각 호의 정보에 대해서는 안전한 암호알고리즘으로 암호화하여 저장한다.

1. 주민등록번호
2. 여권번호
3. 운전면허번호
4. 외국인등록번호
5. 신용카드번호
6. 계좌번호
7. 바이오정보

③ 정보통신서비스 제공자등은 정보통신망을 통해 이용자의 개인정보 및 인증

정보를 송·수신할 때에는 안전한 보안서버 구축 등의 조치를 통해 이를 암호화해야 한다. 보안서버는 다음 각 호 중 하나의 기능을 갖추어야 한다.

1. 웹서버에 SSL(Secure Socket Layer) 인증서를 설치하여 전송하는 정보를 암호화하여 송·수신하는 기능
 2. 웹서버에 암호화 응용프로그램을 설치하여 전송하는 정보를 암호화하여 송·수신하는 기능
- ④ 정보통신서비스 제공자들은 이용자의 개인정보를 컴퓨터, 모바일 기기 및 보조저장매체 등에 저장할 때에는 이를 암호화해야 한다.

제7조(악성프로그램 방지) 정보통신서비스 제공자들은 악성 프로그램 등을 방지·치료할 수 있는 백신 소프트웨어 등의 보안 프로그램을 설치·운영하여야 하며, 다음 각호의 사항을 준수하여야 한다.

1. 보안 프로그램의 자동 업데이트 기능을 사용하거나, 또는 일 1회 이상 업데이트를 실시하여 최신의 상태로 유지
2. 악성프로그램관련 경보가 발령된 경우 또는 사용 중인 응용 프로그램이나 운영체제 소프트웨어의 제작업체에서 보안 업데이트 공지가 있는 경우, 즉시 이에 따른 업데이트를 실시

제8조(물리적 접근 방지) ① 정보통신서비스 제공자들은 전산실, 자료보관실 등 개인정보를 보관하고 있는 물리적 보관 장소에 대한 출입통제 절차를 수립·운영하여야 한다.

- ② 정보통신서비스 제공자들은 개인정보가 포함된 서류, 보조저장매체 등을 잠금장치가 있는 안전한 장소에 보관하여야 한다.
- ③ 정보통신서비스 제공자들은 개인정보가 포함된 보조저장매체의 반출·입통제를 위한 보안대책을 마련하여야 한다.

제9조(출력·복사시 보호조치) ① 정보통신서비스 제공자들은 개인정보처리시스템에서 개인정보의 출력시(인쇄, 화면표시, 파일생성 등) 용도를 특정하여야 하며, 용도에 따라 출력 항목을 최소화 한다.

- ② 정보통신서비스 제공자들은 개인정보가 포함된 종이 인쇄물, 개인정보가 복사된 외부 저장매체 등 개인정보의 출력·복사물을 안전하게 관리하기 위해 출력·복사 기록 등 필요한 보호조치를 갖추어야 한다.

제10조(개인정보 표시 제한 보호조치) 정보통신서비스 제공자들은 개인정보 업무 처리를 목적으로 개인정보의 조회, 출력 등의 업무를 수행하는 과정에서 개인정보보호를 위하여 개인정보를 마스킹하여 표시제한 조치를 취할 수 있다.

제11조(재검토 기한) 개인정보보호위원회는 「훈령·예규 등의 발령 및 관리에 관한 규정」에 따라 이 고시에 대하여 2020년 8월 11일을 기준으로 매 3년이 되는 시점(매 3년째의 8월 10일까지를 말한다)마다 그 타당성을 검토하여 개선 등의 조치를 하여야 한다.

1. 일반규정과의 관계

영 제48조의2제1항은 정보통신망의 파급력과 전파력, 주로 온라인을 통해서 서비스가 제공되는 특성 등을 고려하여 정보통신서비스 제공자등에 대해서는 외부 인터넷망 분리 등 상세한 조치 기준을 규정하면서, 영 제30조제1항 대신 영 제48조의2제1항을 적용하도록 규정하고 있다. 따라서 정보통신서비스 제공자등이 법 제29조에 따른 조치를 하는 경우에는 영 제30조제1항이 아니라 영 제48조의2제1항과 제3항에 따라 보호위원회가 고시한 세부기준을 준수하여야 하며, 일반규정인 영 제30조제1항은 적용되지 않는다.

2. 정보통신서비스 제공자등의 안전성 확보조치

영 제48조의2제1항 및 「개인정보의 기술적·관리적 보호조치 기준(보호위원회 고시 제2020-5호)」(이하 ‘기술적·관리적 보호조치 기준’이라 한다)에서는 정보통신서비스 제공자등이 개인정보의 안전성 확보에 필요한 조치 기준을 정하고 있다.

위 고시의 내용은 정보통신서비스 제공자등이 개인정보의 안전성 확보를 위하여 반드시 준수하여야 하는 최소한의 기준을 정하고 있으므로 정보통신서비스 제공자등은 사업 규모, 서비스의 유형, 개인정보 보유 수, 처리하는 개인정보의 유형 및 중요도, 개인정보를 처리하는 방법 및 환경, 보안위험요인 등을 고려하여 스스로의 환경에 맞도록 필요 시 추가적인 개인정보 보호조치 기준을 수립하고 시행하여야 한다(고시 제1조 참고).

(영 제48조의2제1항 및 기술적·관리적 보호조치 기준에서 정하고 있는 보호조치 기준의 상세한 내용은 “개인정보보호 종합포털(www.privacy.go.kr)”에 게시되어 있는 ‘개인정보의 기술적·관리적 보호조치 기준 해설서’ 참조)

가 관리적 보호조치

정보통신서비스 제공자등은 개인정보를 안전하게 처리하기 위한 내부관리계획을 수립·시행하여야 한다(영 제48조의2제1항제1호). 여기서 내부관리계획이란 정보통신서비스 제공자등이 개인정보의 안전한 처리를 위하여 개인정보보호 조직의 구성, 개인정보취급자의 교육, 개인정보 보호조치 등을 규정한 계획을 말한다.

정보통신서비스 제공자등은 내부관리계획에 다음의 사항을 포함하여야 한다.

내부관리계획에 포함되어야 하는 사항

1. 개인정보 보호책임자의 지정 등 개인정보보호 조직의 구성·운영에 관한 사항
2. 정보통신서비스 제공자들의 지휘·감독을 받아 이용자의 개인정보를 처리하는 개인정보 취급자의 교육에 관한 사항
3. 영 제48조의2제1항제2호부터 제6호까지의 규정에 따른 보호조치를 이행하기 위하여 필요한 세부 사항

정보통신서비스 제공자들은 개인정보 보호책임자의 지정 등 개인정보보호 조직을 구성·운영하여야 한다. 이 경우 ① 개인정보 보호책임자의 자격요건 및 지정에 관한 사항 ② 개인정보 보호책임자와 개인정보취급자의 역할 및 책임에 관한 사항 ③ 개인정보 내부관리계획의 수립 및 승인에 관한 사항 ④ 개인정보의 기술적·관리적 보호조치 이행 여부의 내부 점검에 관한 사항 ⑤ 개인정보 처리업무를 위탁하는 경우 수탁자에 대한 관리 및 감독에 관한 사항 ⑥ 개인정보의 분실·도난·유출·위조·변조·훼손 등이 발생한 경우의 대응절차 및 방법에 관한 사항 ⑦ 그 밖에 개인정보보호를 위해 필요한 사항을 정하여야 하며, 내부관리계획에는 이에 대한 세부 계획이 포함되어야 한다(「기술적·관리적 보호조치 기준」 제3조제1항, 제3항).

또한, 정보통신서비스 제공자들은 개인정보 보호책임자 및 개인정보취급자를 대상으로 사업규모, 개인정보 보유 수 등을 고려하여 필요한 교육을 정기적으로 실시하여야 한다. 이 경우 교육목적 및 대상, 교육 내용 및 교육 일정 및 방법을 정하여야 하며, 내부관리계획에는 이에 대한 세부 계획이 포함되어야 한다(「기술적·관리적 보호조치 기준」 제3조제2항, 제3항).

더불어, 내부관리계획에는 개인정보에 대한 불법적인 접근을 차단하기 위한 조치(영 제48조의2제1항제2호, 「기술적·관리적 보호조치 기준」 제4조), 접속기록의 위조·변조 방지를 위한 조치(영 제48조의2제1항제3호, 「기술적·관리적 보호조치 기준」 제5조), 개인정보가 안전하게 저장·전송될 수 있도록 하기 위한 보안조치(영 제48조의2제1항제4호, 「기술적·관리적 보호조치 기준」 제6조), 개인정보처리시스템 및 개인정보 취급자가 개인정보 처리에 이용하는 정보기에 컴퓨터 바이러스, 스파이웨어 등 악성프로그램의 침투 여부를 항시 점검·치료할 수 있도록 하기 위한 백신소프트웨어 설치 및 주기적 갱신·점검 조치(영 제48조의2제1항제5호, 「기술적·관리적 보호조치 기준」 제7조), 그 밖에 개인정보의 안전성 확보를 위하여 필요한 보호조치(영 제48조의2제1항제6호, 「기술적·관리적 보호조치 기준」 제8조) 등을 이행하기 위한 세부적인 추진 방안이 포함되어야 한다(영 제48조의2제1항제1호, 「기술적·관리적 보호조치 기준」 제3조제3항).

1) 접근 통제 조치

정보통신서비스 제공자등은 개인정보에 대한 불법적인 접근을 차단하기 위한 다음의 접근 통제 조치를 하여야 한다(영 제48조의2제1항제2호).

접근 통제 조치

1. 개인정보처리시스템에 대한 접근권한의 부여·변경·말소 등에 관한 기준의 수립·시행
2. 개인정보처리시스템에 대한 침입차단시스템 및 침입탐지시스템의 설치·운영
3. 개인정보처리시스템에 접속하는 개인정보취급자 컴퓨터 등에 대한 외부 인터넷망 차단
4. 비밀번호의 생성 방법 및 변경 주기 등의 기준 설정과 운영
5. 그 밖에 개인정보에 대한 접근통제를 위하여 필요한 조치

① 개인정보처리시스템에 대한 접근권한의 부여·변경·말소 등에 관한 기준의 수립·시행

정보통신서비스 제공자등은 개인정보처리시스템에 관한 접근권한을 서비스 제공을 위하여 필요한 개인정보 보호책임자 또는 개인정보취급자에게만 부여하여야 하며, 전보, 퇴직 등 인사이동이 발생하여 개인정보취급자가 변경되었을 경우 지체 없이 접근권한을 변경 또는 말소하여야 한다(「기술적·관리적 보호조치 기준」 제4조제1항, 제2항). 한편, 정보통신서비스 제공자등은 이러한 권한 부여, 변경 또는 말소에 대한 내역을 기록하고 그 기록을 최소 5년간 보관하여야 한다(「기술적·관리적 보호조치 기준」 제4조제3항).

또한, 정보통신서비스 제공자등은 개인정보취급자가 정보통신망을 통해 외부에서 개인정보처리시스템에 접속이 필요한 경우 안전한 인증 수단을 적용하여야 한다(「기술적·관리적 보호조치 기준」 제4조제4항). 여기서 안전한 인증 수단의 적용이란 개인정보처리시스템에 사용자 계정과 비밀번호를 입력하여 정당한 개인정보취급자 여부를 식별·인증하는 절차 이외에 추가적인 인증 수단을 적용하는 것을 말한다.

② 개인정보처리시스템에 대한 침입차단시스템 및 침입탐지시스템의 설치·운영

정보통신서비스 제공자등은 정보통신망을 통한 불법적인 접근 및 침해사고 방지를 위한 시스템을 설치·운영하여야 한다(「기술적·관리적 보호조치 기준」 제4조제5항). 이 경우 해당 시스템은 개인정보처리시스템에 대한 접속 권한을 IP주소 등으로 제한하여 인가받지 않은 접근을 제한하는 기능과 개인정보처리시스템에 접속한 IP주소 등을 재분석하여 불법적인 개인정보 유출 시도를 탐지하는 기능을 포함하여야 한다(「기술적·관리적 보호조치 기준」 제4조제5항).

③ 개인정보처리시스템에 접속하는 개인정보취급자 컴퓨터 등에 대한 외부 인터넷망 차단

일정 규모 이상의 정보통신서비스 제공자 등은 개인정보처리시스템에 접속하는 개인정보취급자의 컴퓨터 등에 대하여 외부 인터넷망을 차단하는 조치(이하 ‘망분리’라 한다)를 하여야 한다(영 제48조의2제1항제2호다목, 「기술적·관리적 보호조치 기준」 제4조).

망분리를 하여야 하는 정보통신서비스 제공자등은 전년도 말 기준 직전 3개월간 그 개인정보가 저장·관리되고 있는 이용자 수가 일일평균 100만명 이상인 자 또는 정보통신서비스 부문 전년도(법인의 경우에는 전 사업연도) 매출액이 100억원 이상인 자이다(영 제48조의2제1항제2호다목)¹²⁾.

또한, 망분리는 모든 직원의 컴퓨터 등이 아니라 개인정보처리시스템에서 개인정보를 다운로드 또는 파기할 수 있거나 개인정보처리시스템에 대한 접근권한을 설정할 수 있는 개인정보취급자의 컴퓨터 등에 적용하여야 한다(「기술적·관리적 보호조치 기준」 제4조제6항).

한편, 정보통신서비스 제공자등은 물리적 또는 논리적으로 망분리를 하여야 하며(「기술적·관리적 보호조치 기준」 제4조제6항), 이 중 스스로의 환경에 맞는 방식을 선택할 수 있다. 여기서 물리적 망분리란 통신망, 장비 등을 물리적으로 이원화하여 인터넷 접속이 불가능한 컴퓨터와 인터넷 접속만 가능한 컴퓨터로 분리하는 방식을 말하며, 논리적 망분리란 물리적으로 하나의 통신망, 장비 등을 사용하지만 가상화 등의 방법으로 인터넷 접속이 불가능한 내부 업무영역과 인터넷 접속영역을 분리하는 방식을 말한다(망분리의 구체적인 방법에 대하여는 ‘개인정보의 기술적·관리적 보호조치 기준 해설서’ 내용 중 ‘부록’ 참고).

④ 비밀번호의 생성 방법 및 변경 주기 등의 기준 설정·운영

정보통신서비스 제공자등은 이용자가 안전한 비밀번호를 이용할 수 있도록 비밀번호 작성규칙을 수립하고 이행하여야 한다(「기술적·관리적 보호조치 기준」 제4조제7항).

개인정보취급자의 비밀번호 작성 규칙에 대하여는 이용자의 비밀번호 작성규칙과는 달리 다음과 같은 최소한의 기준을 제시하고 있으므로 다음의 사항을 포함한 비밀번호 작성 규칙을 수립하고 적용·운영하여야 한다(「기술적·관리적 보호조치 기준」 제4조제8항).

- ① 영문, 숫자, 특수문자 중 2종류 이상을 조합하여 최소 10자리 이상 또는 3종류 이상을 조합하여 최소 8자리 이상의 길이로 구성
- ② 연속적인 숫자나 생일, 전화번호 등 추측하기 쉬운 개인정보 및 아이디와 비슷한 비밀번호는 사용하지 않는 것을 권고
- ③ 비밀번호에 유효기간 설정 및 반기별 1회 이상 변경

12) 이용자수 및 매출액 산정에 대해서는 제39조의8(개인정보 이용내역의 통지) 해설을 참고

⑤ 그 밖에 개인정보에 대한 접근통제를 위하여 필요한 조치

이와 관련하여 정보통신서비스 제공자들은 처리 중인 개인정보가 인터넷 홈페이지, P2P, 공유설정 등을 통하여 열람 권한이 없는 자에게 공개되거나 외부에 유출되지 않도록 개인정보처리시스템 및 개인정보취급자의 컴퓨터와 모바일 기기에 조치를 취하여야 한다(「기술적·관리적 보호조치 기준」 제4조제9항). 또한, 개인정보처리시스템에 대한 개인정보취급자의 접속이 필요한 시간 동안만 최대 접속시간 제한 등의 조치를 취하여야 한다(「기술적·관리적 보호조치 기준」 제4조제10항).

2) 접속기록의 위조·변조 방지

정보통신서비스 제공자들은 접속기록의 위조·변조 방지를 위한 다음의 조치를 하여야 한다(영 제48조의2제1항제3호).

접속기록 위조·변조 방지 조치

1. 개인정보취급자가 개인정보처리시스템에 접속하여 개인정보를 처리한 경우 접속일시, 처리내역 등의 저장 및 이의 확인·감독
2. 개인정보처리시스템에 대한 접속기록을 별도 저장장치에 백업 보관

접속기록이란 이용자 또는 개인정보취급자 등이 개인정보처리시스템에 접속하여 수행한 업무내역에 대하여 식별자, 접속일시, 접속지를 알 수 있는 정보, 수행업무 등 접속한 사실을 전자적으로 기록한 것을 말한다(「기술적·관리적 보호조치 기준」 제2조제7호).

정보통신서비스 제공자들은 개인정보취급자가 개인정보처리시스템에 접속한 기록을 월 1회 이상 정기적으로 확인·감독하여야 하며, 시스템 이상 유무의 확인 등을 위해 최소 1년 이상 접속기록을 보존·관리하여야 한다(「기술적·관리적 보호조치 기준」 제5조제1항). 이 경우 정보통신서비스 제공자들은 개인정보취급자의 접속기록이 위·변조되지 않도록 별도의 물리적인 저장 장치에 보관하여야 하며 정기적인 백업을 수행하여야 한다(「기술적·관리적 보호조치 기준」 제5조제3항).

한편, 기간통신사업자의 경우에는 최소 2년 이상 접속기록을 보존·관리하여야 한다(「기술적·관리적 보호조치 기준」 제5조제2항). 이는 기간통신사업자의 경우 대규모의 이용자 개인정보를 처리하고 개인정보의 유출 등으로 인한 피해 가능성이 매우 높은 특수성을 고려한 것이다.

3) 암호화 기술을 이용한 보안조치

정보통신서비스 제공자들은 개인정보를 안전하게 저장·전송될 수 있도록 암호화 기술을 이용한 다음의 보안조치를 하여야 한다(영 제48조의2제1항제4호).

암호화 기술을 이용한 보안조치

1. 비밀번호의 일방향 암호화 저장
2. 주민등록번호, 계좌정보 및 제18조제3호에 따른 정보 등 보호위원회가 정하여 고시하는 정보의 암호화 저장
3. 정보통신망을 통하여 이용자의 개인정보 및 인증정보를 송신·수신하는 경우 보안서버 구축 등의 조치
4. 그 밖에 암호화 기술을 이용한 보안조치

정보통신서비스 제공자들은 비밀번호를 복호화되지 아니하도록 일방향 암호화하여 저장한다(「기술적·관리적 보호조치 기준」 제6조제1항). 한편, 주민등록번호, 여권번호, 운전면허번호, 외국인등록번호, 신용카드번호, 계좌번호, 영 제18조제3호에 따른 정보(바이오정보)에 대해서는 안전한 암호 알고리즘으로 암호화하여 저장한다(「기술적·관리적 보호조치 기준」 제6조제2항).

또한, 정보통신망을 통하여 이용자의 개인정보 및 인증정보를 송신·수신할 때에는 안전한 보안서버 구축 등의 조치를 통해 이를 암호화하여야 한다. 이 경우 보안서버는 다음 중 하나의 기능을 갖추어야 한다(「기술적·관리적 보호조치 기준」 제6조제3항).

- ① 웹서버에 SSL(Secure Socket Layer) 인증서를 설치하여 전송하는 정보를 암호화하여 송·수신하는 기능
- ② 웹서버에 암호화 응용프로그램을 설치하여 전송하는 정보를 암호화하여 송·수신하는 기능

여기서 SSL(Secure Socket Layer)은 웹 브라우저와 웹 서버간에 데이터를 안전하게 주고받기 위해 암호화 기술이 적용된 보안 프로토콜로서 SSL 인증서를 이용한 보안서버는 별도의 보안 프로그램 설치 없이, 웹서버에 설치된 SSL 인증서를 통해 개인정보를 암호화 전송하는 방식을 말한다.

마지막으로, 정보통신서비스 제공자들은 이용자의 개인정보를 컴퓨터, 모바일 기기 및 보조저장매체 등에 저장할 때에는 이를 암호화하여야 한다(「기술적·관리적 보호조치 기준」 제6조제4항).

< 일반규정과 특례규정의 암호화 대상 개인정보 비교 >

구 분	일반규정(영 제30조제1항)	특례규정(영 제48조의2제1항)
정보통신망을 통한 전송 시	고유식별정보, 비밀번호, 바이오정보	개인정보, 인증정보
보조저장매체로 저장·전달 시	고유식별정보, 비밀번호, 바이오정보	개인정보
개인정보처리 시스템 저장 시	비밀번호, 바이오정보 (단, 비밀번호는 일방향 암호화)	비밀번호, 바이오정보 (단, 비밀번호는 일방향 암호화)
	-	신용카드번호, 계좌번호
	주민등록번호	주민등록번호
	여권번호, 외국인등록번호, 운전면허번호	인터넷구간, DMZ 저장 시 암호화 저장 내부망 저장 시 암호화 저장 또는 위험도 분석 (또는 영향평가)
업무용 컴퓨터/모바일 기기 저장 시	고유식별정보, 비밀번호, 바이오정보	개인정보

4) 백신 소프트웨어 등 보안 프로그램의 설치·운영 조치

정보통신서비스 제공자등은 개인정보처리시스템 및 개인정보취급자가 개인정보 처리에 이용하는 정보기기에 컴퓨터 바이러스, 스파이웨어 등 악성프로그램의 침투 여부를 항상 점검·치료할 수 있도록 백신소프트웨어 등 보안 프로그램을 설치·운영하여야 한다(영 제48조의2제1항제5호, 「기술적·관리적 보호조치 기준」 제7조).

또한, 백신 소프트웨어 등 보안 프로그램이 주기적 갱신·점검이 가능하도록 조치하여야 한다(영 제48조의2제1항제5호, 「기술적·관리적 보호조치 기준」 제7조). 이를 위하여 정보통신서비스 제공자등은 보안 프로그램의 자동 업데이트 기능을 사용하거나 일 1회 이상 업데이트를 실시하여 최신의 상태로 유지하여야 하며, 악성프로그램 관련 정보가 발령된 경우 또는 사용 중인 응용 프로그램이나 운영체제 소프트웨어의 제작업체에서 보안 업데이트 공지가 있는 경우에는 즉시 이에 따른 업데이트를 실시하여야 한다(「기술적·관리적 보호조치 기준」 제7조).

다 그 밖에 개인정보의 안전성 확보를 위하여 필요한 조치

1) 물리적 접근 방지 조치

정보통신서비스 제공자등은 전산실, 자료보관실 등 개인정보를 보관하고 있는 물리적

보관 장소에 대한 출입통제 절차를 수립·운영하여야 한다(「기술적·관리적 보호조치 기준」 제8조제1항).

또한, 정보통신서비스 제공자등은 개인정보가 포함된 서류, 보조저장매체 등을 잠금장치가 있는 안전한 장소에 보관하여야 한다(「기술적·관리적 보호조치 기준」 제8조제2항).

마지막으로, 정보통신서비스 제공자등은 개인정보가 포함된 보조저장매체의 반출·입통제를 위한 보안대책을 마련하여야 한다(「기술적·관리적 보호조치 기준」 제8조제3항).

2) 출력·복사 시 보호조치

정보통신서비스 제공자등은 개인정보처리시스템에서 개인정보를 출력할 때(인쇄, 화면 표시, 파일생성 등) 용도를 특정하여야 하며, 용도에 따라 출력 항목을 최소화하여야 한다(「기술적·관리적 보호조치 기준」 제9조제1항).

또한, 개인정보가 포함된 종이 인쇄물, 개인정보가 복사된 외부 저장매체 등 개인정보의 출력·복사물을 안전하게 관리하기 위해 출력·복사 기록 등 필요한 보호조치를 갖추어야 한다(「기술적·관리적 보호조치 기준」 제9조제2항).

3) 개인정보 표시 제한 보호조치

정보통신서비스 제공자 등은 개인정보 업무처리를 목적으로 개인정보의 조회, 출력 등의 업무를 수행하는 과정에서 개인정보 보호를 위하여 개인정보를 마스킹하여 표시제한 조치를 취할 수 있다(「기술적·관리적 보호조치 기준」 제10조).

3. 정보통신서비스 제공자등의 개인정보 보호조치에 대한 특례

정보통신서비스 제공자등은 이용자의 개인정보를 처리하는 자를 최소한으로 제한하여야 한다(제39조의5). 안전성 확보조치의 접근통제 규정(「기술적·관리적 보호조치 기준」 제4조)은 개인정보처리시스템에 대한 접근권한을 부여하는 자를 서비스 제공을 위하여 필요한 범위로 제한하도록 하고 있으나, 이에 비해 개인정보의 보호조치에 대한 특례는 이용자의 개인정보를 처리하는 자의 범위를 최소화하도록 규정하고 있다.

4. 정보통신서비스 제공자등과 개인정보처리자 간 보호조치 내용 비교

정보통신서비스 제공자등과 일반 개인정보처리자에 적용되는 안전성 확보조치 내용의 주요 차이점은 다음과 같다.

구분	정보통신서비스 제공자등	일반 개인정보처리자
세부 기준	개인정보의 기술적·관리적 보호조치 기준 (보호위원회 고시 제2020-5호)	개인정보의 안전성 확보조치 기준 (보호위원회 고시 제2020-2호)
내부 관리 계획의 수립·시행	사업 규모에 따른 예외 규정 없음	1만명 미만의 정보주체에 관한 개인정보를 보유한 소상공인, 단체, 개인 적용 제외
접근 통제	개인정보처리시스템에 대한 접근권한 부여 등의 내역 기록 보관 의무 : 최소 5년간 보관	개인정보처리시스템에 대한 접근권한 부여 등의 내역 기록 보관 의무 : 최소 3년간 보관
	개인정보취급자의 비밀번호 작성 규칙을 구체적으로 명시 - 10자리 이상 : 영문, 숫자, 특수문자 중 2종류 이상 조합 - 8자리 이상 : 영문, 숫자, 특수문자 중 3종류 이상 조합	비밀번호 설정 관련 세부 기준을 명시하지 않음 (※해설서에서 개인정보취급자 또는 정 보주체의 구체적 작성 규칙을 예시함 - 10자리 이상 : 영문 대문자와 소문자, 특수문자, 숫자 중 1종류 이상 조합 - 8자리 이상 : 영문 대문자와 소문자, 특수문자, 숫자 중 3종류 이상 조합)
	사업자, 개인정보취급자 기준에 해당하는 자의 PC등에 대한 외부 인터넷망 차단 의무화 -	외부 인터넷망 차단 의무화 규정 없음 고유식별정보의 경우 연 1회 이상 취약점 점검
암호화 대상 (개인정보처리 시스템 저장 시)	비밀번호(일방향 암호화), 바이오정보, 주민번호, 여권번호, 운전면허번호, 외국인 등록번호, 신용카드번호, 계좌번호	비밀번호(일방향 암호화), 바이오정보, 고유식별정보(주민번호, 여권번호, 운전면허 번호, 외국인등록번호)
접속 기록	접속기록 범위 : 식별자, 접속일시, 접속지를 알 수 있는 정보, 수행업무 등	접속기록 범위 : 개인정보취급자 등 계정, 접속일시, 접속지 정보, 처리한 정보주체 정보, 수행업무 등
	개인정보 처리시스템 접속기록은 최소 1년 이상 보관 ※ 기간통신사업자는 최소 2년 이상 보관	개인정보 처리시스템 접속기록은 최소 1년 이상 보관 ※ 5만명 이상 정보주체의 개인정보를 처리하거 나 고유식별정보 또는 민감정보 처리 개인정 보처리시스템의 경우 최소 2년 이상 보관

5. 벌칙규정

위반행위	벌칙
안전성 확보에 필요한 조치를 하지 않은 자 (제29조 위반)	3천만원 이하 과태료 (제75조제2항제6호)
안전성 확보에 필요한 조치를 하지 않아서 개인정보를 분실·도난·유출·위조·변조 또는 훼손당한 자 (제29조 위반)	2년 이하의 징역 또는 2천만원 이하 벌금 (제73조제1호)
이용자의 개인정보를 분실·도난·유출·위조·변조·훼손한 경우로서 제29조의 조치(내부 관리계획 수립에 관한 사항 제외)를 하지 않은 자 (제29조 위반)	위반행위와 관련한 매출액의 100분의 3 이하 과징금 (제39조의15제1항제5호)

제39조의6 | 개인정보의 파기에 대한 특례

<p style="text-align: center;">법률</p>	<p>제39조의6(개인정보의 파기에 대한 특례) ① 정보통신서비스 제공자등은 정보통신서비스를 1년의 기간 동안 이용하지 아니하는 이용자의 개인정보를 보호하기 위하여 대통령령으로 정하는 바에 따라 개인정보의 파기 등 필요한 조치를 취하여야 한다. 다만, 그 기간에 대하여 다른 법령 또는 이용자의 요청에 따라 달리 정한 경우에는 그에 따른다.</p> <p>② 정보통신서비스 제공자등은 제1항의 기간 만료 30일 전까지 개인정보가 파기되는 사실, 기간 만료일 및 파기되는 개인정보의 항목 등 대통령령으로 정하는 사항을 전자우편 등 대통령령으로 정하는 방법으로 이용자에게 알려야 한다.</p>
<p style="text-align: center;">시행령</p>	<p>제48조의5(개인정보의 파기 등에 관한 특례) ① 정보통신서비스 제공자등은 이용자가 정보통신서비스를 법 제39조의6제1항의 기간 동안 이용하지 않는 경우에는 이용자의 개인정보를 해당 기간 경과 후 즉시 파기하거나 다른 이용자의 개인정보와 분리하여 별도로 저장·관리해야 한다. 다만, 법 제39조의6제1항 본문에 따른 기간(법 제39조의6제1항 단서에 따라 이용자의 요청에 따라 달리 정한 경우에는 그 기간을 말한다)이 경과한 경우로서 다른 법령에 따라 이용자의 개인정보를 보존해야 하는 경우에는 다른 법령에서 정한 보존기간이 경과할 때까지 다른 이용자의 개인정보와 분리하여 별도로 저장·관리해야 한다.</p> <p>② 정보통신서비스 제공자등은 제1항에 따라 개인정보를 별도로 저장·관리하는 경우에는 법 또는 다른 법률에 특별한 규정이 있는 경우를 제외하고는 해당 개인정보를 이용하거나 제공해서는 안 된다.</p> <p>③ 법 제39조의6제2항에서 “개인정보가 파기되는 사실, 기간 만료일 및 파기되는 개인정보의 항목 등 대통령령으로 정하는 사항” 이란 다음 각 호의 사항을 말한다.</p> <ol style="list-style-type: none"> 1. 개인정보를 파기하는 경우: 개인정보가 파기되는 사실, 기간 만료일 및 파기되는 개인정보의 항목 2. 다른 이용자의 개인정보와 분리하여 개인정보를 저장·관리하는 경우: 개인정보가 분리되어 저장·관리되는 사실, 기간 만료일 및 분리·저장되어 관리되는 개인정보의 항목 <p>④ 법 제39조의6제2항에서 “전자우편 등 대통령령으로 정하는 방법” 이란 서면등의 방법을 말한다.</p>

1. 일반규정과의 관계

개인정보처리자는 일반규정인 제21조에 따라 개인정보를 파기하여야 하며, 동조는 정보통신서비스 제공자등이 이용자의 개인정보를 파기하는 경우에도 적용된다.

한편, 특례규정인 제39조의6은 장기간 정보통신서비스를 이용하지 않는 자의 개인정보의 파기에 대해서 별도로 규정하고 있으므로 이에 해당하는 경우에는 특례규정이 적용된다. 동 특례규정은 ‘개인정보 유효기간 제도’ 또는 ‘장기 미이용자의 개인정보 파기제도’ 라고도 한다. 이는 개인정보 유출등 사고가 발생하는 경우 사고 당시 정보통신서비스를 이용 중인 이용자의 개인정보 뿐만 아니라 사고 당시 장기 미이용자의 개인정보도 상당 부분 포함되어 있다는 점에서 장기간 서비스를 이용하지 않고 방치되고 있는 개인정보로 인한 이용자의 피해를 방지하고 정보통신서비스 제공자등의 불필요한 개인정보 보관을 최소화하기 위한 것이다.

2. 개인정보의 파기 등 필요한 조치를 하여야 하는 서비스 미이용 기간

가 서비스 미이용 기간

정보통신서비스 제공자등은 정보통신서비스를 1년 동안 이용하지 않은 이용자의 개인정보를 보호하기 위하여 이용자의 개인정보를 해당 기간 경과 후 즉시 파기하거나 다른 이용자의 개인정보와 분리하여 별도로 저장·관리하여야 한다(제39조의6제1항 본문, 영 제48조의5제1항 본문).

다만, 다른 법령 또는 이용자의 요청에 따라 기간을 달리 정한 경우에는 그 기간 경과 후 즉시 파기하거나 분리하여 별도 저장·관리하여야 한다(제39조제1항 단서).

다른 법령에 따라 기간을 달리 정한 경우란 「통신비밀보호법」, 「전자상거래 등에서의 소비자보호에 관한 법률」 등과 같이 개별 법령에서 개인정보의 보존기간을 별도로 정하고 있거나 「국세기본법」, 「상법」 등과 같이 법령 상의 책임이나 의무를 준수하기 위해 별도의 기간(소멸시효 등)을 명시한 경우가 해당한다.

< 개인정보 보존의무를 명시한 다른 법령의 예시 >

근거법령	개인정보의 종류	보존기간
통신비밀보호법 시행령 제41조 (통신사실확인자료)	로그기록자료, 접속지의 추적자료	3개월
전자상거래 등에서의 소비자보호에 관한 법률 시행령 제6조(거래기록)	전기통신일시, 전기통신개시·종료시간, 사용도수, 상대방의 가입자번호, 발신기지국의 위치추적자료	1년
전자금융거래법 시행령 제12조 (전자금융 거래기록)	소비자의 불만 또는 분쟁처리에 관한 기록	3년
	계약 또는 청약철회 등에 관한 기록, 대금 결제 및 재화 등의 공급에 관한 기록	5년
신용정보법 제20조 (업무처리기록)	건당 거래금액 1만원 이하 전자금융거래에 관한 기록, 전자지급수단 이용과 관련된 거래승인에 관한 기록	1년
	전자금융거래 종류 및 금액, 상대방에 관한 정보, 지급인의 출금 동의에 관한 사항, 전자금융거래와 관련한 전자적 장치의 접속기록, 전자금융거래 신청 및 조건의 변경에 관한 사항, 건당 거래금액 1만원 초과 전자금융거래에 관한 기록	5년
의료법 시행규칙 제15조 (진료에 관한 기록)	신용정보 업무처리에 관한 기록	3년
	처방전	2년
	진단서 등의 부분	3년
	환자 명부, 검사소견기록, 간호기록부, 방사선 사진 및 그 소견서, 조산기록부	5년
국세기본법제85조의3 (장부 및 증거서류)	진료기록부, 수술기록	10년
	국세 부과 제척기간(조세시효)	10년
상법 제64조, 제464조의2, 제487조, 제662조 (보험금 등 관련 자료)	국세징수권 및 국세환급금 소멸시효	5년
	보험료청구권 소멸시효	2년
	보험료/적립금 반환청구권 소멸시효	3년
	상사채권 소멸시효, 배당금 지급청구권 소멸시효	5년
	사채상환청구권 소멸시효	10년

이용자의 요청에 따라 기간을 달리 정한 경우란 이용자가 유학, 군입대, 입원, 질병 등으로 장기간 해당 정보통신서비스를 이용할 수 없어 정보통신서비스 제공자등에게 1년 이외의 서비스 미이용 기간을 요청하여 정하는 경우가 해당한다. 1년 이외의 기간으로 정하고자 하는 경우 정보통신서비스 제공자등은 이용자가 이를 선택하여 요청할 수 있는 형태로 제시하는 등 이용자의 요청에 따라 서비스 미이용 기간을 정할 수 있도록 하는 것이 바람직하다.

< 서비스 미이용 기간 선택 기능 제공 예시 >

<p>(예시①) 개인정보를 파기 또는 분리 저장·관리하여야 하는 서비스 미이용 기간을 <input type="text"/> 년으로 요청합니다.</p> <p>※ 다만, 별도의 요청이 없을 경우 서비스 미이용 기간은 1년으로 합니다.</p>
<p>(예시②) 개인정보를 파기 또는 분리 저장·관리하여야 하는 서비스 미이용 기간을 2년 <input type="text"/> 3년 <input type="text"/> 회원 탈퇴 시까지 <input type="text"/> 으로 요청합니다.</p> <p>※ 다만, 별도의 요청이 없을 경우 서비스 미이용 기간은 1년으로 합니다.</p>

한편, 1년 또는 이용자의 요청에 따라 달리 정한 기간이 경과한 경우로서 다른 법령에 따라 이용자의 개인정보를 보존하여야 하는 경우에는 다른 법령에서 정한 보존기간이 경과할 때까지 다른 이용자의 개인정보와 분리하여 별도로 저장·관리하여야 한다(제39조의6제1항 단서, 영 제48조의5제1항 단서).

참고 (구) 「정보통신망법」 제29조제2항(현행 「개인정보 보호법」 제39조의6제1항) 해석례

정보통신서비스 이용자가 정보통신서비스 이용계약을 해지하지 않은 상태에서 정보통신서비스를 이용하지 않은 기간이 “1년” 또는 “이용자가 정한 기간”을 지난 경우에는, 「국세기본법」 제85조의3제2항에 따른 5년의 보존의무기간이 아직 지나지 않았더라도, 정보통신서비스 제공자들은 「정보통신망 이용촉진 및 정보보호 등에 관한 법률」 제29조제2항 및 같은 법 시행령 제16조제2항에 따라 이용자의 개인정보를 다른 이용자의 개인정보와 분리하여 별도로 저장·관리하여야 할 의무가 있습니다(법제처 법령해석총괄과-3822, 2015. 9. 30.).

나 정보통신서비스 미이용 판단 기준

정보통신서비스 이용자가 정보통신서비스를 마지막으로 이용한 이후 1년 동안 이용한 기록이 없다면 해당 정보통신서비스 미이용자로 볼 수 있다.

온라인 서비스의 경우에는 업종별 특성을 고려하여 서비스 이용 기록, 접속 로그(log) 등을 기준으로 서비스 이용 여부를 판단할 수 있으며, 이용자의 이해를 돕기 위해 이용약관 등을 통해 그 적용기준에 대해 명확히 알려주는 것이 필요하다.

백화점 등과 같이 오프라인과 온라인 서비스를 함께 연계하여 이용하는 경우에는 온라인 서비스 이용이 없더라도 오프라인 연계 서비스를 이용한 기록이 있으면 미이용에 해당하지 않는다.

정보통신서비스 제공자들이 자신이 제공하는 서비스를 광고하기 위하여 이용자에게 문자나 이메일을 보낸 기록은 이용 기록으로 볼 수 없으며, 이는 이용자가 광고 문자나 이메일을 단순히 확인하였다 하더라도 이용 기록으로 볼 수 없다.

3. 파기 등 필요한 조치 내용

가 개인정보의 파기

정보통신서비스 제공자들은 이용자가 정보통신서비스를 1년(이용자의 요청에 따라 달리 정한 경우에는 그 기간) 동안 이용하지 않은 경우 이용자의 개인정보를 해당 기간 경과 후 즉시 파기하거나 다른 이용자의 개인정보와 분리하여 별도로 저장·관리하여야 한다(영 제48조의5제1항).

개인정보를 파기할 때에는 일반규정인 제21조제1항 및 영 제16조에 따라 복구·재생활 수 없도록 조치하여야 하며, 이에 따른 정보통신서비스 제공자들의 구체적인 파기 방법은 다음과 같이 제시할 수 있다.

참고 정보통신서비스 제공자들의 복구·재생활 수 없는 파기 방법 예시

1. 하드 디스크 등 매체 전체의 데이터를 파기하는 경우
 - 1) 프로그램을 이용한 파기
 - ① 하드디스크, USB 메모리의 경우 '로우레벨포맷(Low level format)' 방법으로 파기
※ 로우레벨포맷 : 하드디스크를 공장에서 나온 초기상태로 만들어주는 포맷
 - ② 0, 1 혹은 랜덤한 값으로 기존 데이터를 여러 번 덮어쓰우는 와이핑(Wiping) 방법으로 파기
 - 2) 물리적인 파기
 - ① 데이터가 저장되는 디스크 플레터에 강력한 힘으로 구멍을 내어 복구가 불가능하도록 하는 천공 방법으로 파기
 - ② CD/DVD의 경우 가위 등으로 작은 입자로 조각 내거나, 전용 CD파쇄기나 CD 파쇄가 가능한 문서파쇄기 등을 이용하여 파기
 - ③ 고온에 불타는 종류의 매체는 소각하는 방법으로 파기
 - ④ 자기장치를 이용해 강한 자기장으로 데이터를 복구 불가능하게 하는 디가우저(Degausser) 파기
2. 고객 서비스에 이용 중인 DB서버에 저장된 일부 데이터를 파기하는 경우
 - ① 서비스 중인 DB의 해당 개인정보 위에 임의의 값(NULL값 등)을 덮어쓰기한 후 삭제(delete)
 - ② DB의 특정부분에 덮어쓰기가 곤란한 경우에는 테이블 데이터에 대한 논리적인 삭제(delete)도 허용되나, 신속하게 다른 데이터로 덮어쓰기(overwriting)될 수 있도록 운영

나 개인정보의 분리 저장·관리

정보통신서비스 제공자들은 장기 미이용자의 개인정보를 보호하기 위해 미이용 기간 경과 후 즉시 파기하거나 파기에 준하는 조치의 일환으로 개인정보를 다른 이용자의 개인정보와 분리하여 별도로 저장·관리할 수 있다(영 제48조의5제1항).

이 경우 장기 미이용자의 개인정보는 일반 이용자의 개인정보 DB와 분리하여 별도로

저장·관리하고 일반 직원들의 접근을 제한하는 등 접근 권한을 최소화하여야 한다. 반면, 별도 저장·관리를 하는 개인정보에 접근통제를 하지 않아 모든 개인정보취급자가 접근할 수 있도록 운영하는 것은 개인정보 유효기간 제도의 입법 취지에 반하며 파기 등 필요한 조치를 취한 것으로 볼 수 없다.

또한, 필요한 조치로서 분리 저장·관리는 파기에 준하는 조치이므로 물리적으로 DB를 분리하여 저장하는 것이 바람직하나 테이블 분리 등 논리적으로 분리하는 것도 가능하다.

한편, 이용자의 잔여 마일리지, 적립 포인트 등이 남아 있어 이용자의 권리를 보호할 필요가 있고 향후 재이용의 가능성이 높다고 판단되는 경우 이용자의 재이용 요청이 있는 경우를 대비하여 온라인 이용자의 편의성을 높이기 위한 목적으로 아이디 등 최소한의 연결값을 서비스 중인 DB에 남겨두는 것은 가능하다.

분리 저장·관리되는 개인정보는 재이용하거나 제3자에게 제공할 수 없으나, ① 이용자가 정보통신서비스의 재이용(계정 활성화)을 요구하는 경우 ② 「개인정보 보호법」(제63조 자료 제출 요구 및 검사) 또는 「형사소송법」(제106조 압수, 제109조 수색, 제139조 검증), 「통신비밀보호법」(제13조 범죄수사를 위한 통신사실확인자료 제공의 절차, 제13조의2 법원에의 통신사실확인자료 제공, 제13조의4 국가안보를 위한 통신사실확인자료 제공의 절차 등) 등과 같이 법률에 특별한 규정이 있는 경우에 예외가 인정된다(영 제48조의5 제2항 참고).

다 파기 등 필요한 조치 대상 개인정보의 범위

최초 회원가입 또는 회원정보 수정 등의 단계에서 수집·관리되는 개인정보뿐만 아니라 접속 로그(log), 쿠키(cookie), 결제 기록 등 서비스를 이용하는 과정에서 생성되는 정보 또한 파기 등 필요한 조치의 대상이 되는 개인정보에 포함된다. 예를 들어 이름, 생년월일, 전자우편, 전화번호, 주소 등 직접 수집하는 인적정보와 서비스 이용 과정에서 생성된 정보로서 다른 정보와 쉽게 결합하여 개인 식별이 가능한 경우 해당 정보도 조치 대상 개인정보에 해당할 수 있다.

한편, 개인정보 유효기간 제도의 취지는 1년 동안 서비스를 이용하지 않는 이용자의 개인정보를 파기하거나 안전하게 분리 보관·관리하도록 하여 유출 위험 등으로부터 개인정보를 안전하게 보호하기 위한 것이므로 이용자가 공개를 목적으로 인터넷 상에 게시한 콘텐츠는 파기 등 조치 대상 개인정보에 포함되지 않는다. 해당 콘텐츠는 콘텐츠 작성자 표시 정보와 함께 서비스에 이용 중인 DB에 보관하여 게시글 등이 최초 이용자가 의도한 대로 표시되도록 운영할 수 있다.

4. 미이용 기간 도래 통지 시기 및 방법

정보통신서비스 제공자들은 서비스 미이용 기간 만료 30일 전까지 서면, 전자우편, 팩스, 전화, 문자전송 또는 이에 상당하는 방법(서면등)으로 해당 이용자에게 본인의 개인정보가 파기 또는 분리 저장·관리되는 사실, 기간 만료일 및 파기 또는 분리 저장·관리되는 개인정보의 항목을 통지하여야 한다(제39조의6제2항, 영 제48조의5제3항 및 제4항).

한편, 정보통신서비스 제공자들이 이용자의 연락처를 보유하고 있지 않거나, 이용자의 연락처가 변경 또는 오류 등으로 통지가 불가능한 경우에는 제39조의6 및 영 제48조의5에 따라 개인정보 파기 또는 분리 저장·관리되는 사실을 이용자에게 통지하였으며, 통지의 오배송에 대한 고의·과실이 없음을 입증할 수 있어야 한다. 다만, 신규 회원 가입시 서비스 이용약관 및 개인정보 처리방침 등에 제도의 주요 내용을 공지하고, 기존 이용자에 대해서는 공지사항, 전자우편 등 이용자가 알아볼 수 있는 방법으로 서비스 미이용 기간 만료 후 개인정보 파기 등의 조치가 취해질 수 있다는 사실 및 정확한 연락처 정보를 제공·수정하도록 적극적으로 알리는 노력을 할 필요가 있다.

5. 가명정보의 적용 제외

제39조의6 특례규정은 가명정보의 파기에 대해서는 적용되지 않는다(제28조의7).

6. 벌칙규정

위반행위	벌칙
개인정보의 파기 등 필요한 조치를 하지 아니한 자 (제39조의14에 따라 준용되는 경우 포함) (제39조의6 위반)	3천만원 이하 과태료 (제75조제2항제4호)

7. 질의 응답

Q | 개인정보 유효기간제 준수를 위해 사업자는 매일 유효기간이 경과한 이용자의 개인정보를 파기해야 하는지, 아니면 주기적으로 해도 되는지?

A | 이용자별로 유효기간 경과시점이 다를 것이므로 매일 확인하여 파기 등 필요한 조치를 하는 것이 원칙이다. 다만, 현실적으로 매일 확인하여 조치를 취하는 것이 어려울 수 있으므로 유효기간이 도래한 시점부터 영업일 기준 5일 이내에 파기 등 필요한 조치를 취한다면 적법한 것으로 판단할 수 있을 것이다.

Q | **이용자로부터 영리목적의 광고성 정보 전송에 대한 수신동의를 받았는데, 유효기간이 경과하여 이용자의 개인정보를 분리 저장·관리하는 경우 「정보통신망법」 제50조에 따른 영리목적의 광고성 정보 전송에 대한 2년 주기의 수신동의 여부를 확인해야 하는가?**

A | 유효기간이 경과한 이용자의 개인정보를 분리 저장·관리하는 경우 해당 이용자의 개인정보는 이용자의 요청이 없는 한 이용할 수 없으므로, 영리목적의 광고성 정보를 전송해서는 안 된다.
영리목적의 광고성 정보 전송에 대한 수신동의 여부를 2년마다 확인하도록 하는 취지는 최초에 수신동의를 했다 하더라도 앞으로도 계속해서 수신할 것인지 선택권을 주고자 함에 있다. 따라서 영리목적의 광고성 정보를 전송해서는 안 되는 이용자에게 수신동의 여부를 확인할 필요는 없을 것으로 판단된다.

Q | **이용자와의 별도 계약(약관 포함)으로 유효기간을 설정하는 것이 법 제39조의6제1항 단서의 이용자의 요청에 따라 기간을 달리 정한 경우에 해당하는지?**

A | 약관으로 사업자가 개인정보 유효기간을 정하여 이용자의 동의를 받은 경우는 법 제39조의6제1항 단서의 이용자의 요청에 따라 기간을 달리 정한 경우에 해당하지 않는다. 이용자의 요청에 따라 기간을 달리 정한 경우에 해당하려면 이용자가 직접 기간을 요청하거나 선택할 수 있어야 한다.

Q | **서비스 미이용 기간이 경과한 경우 해당 이용자의 모든 개인정보에 대해 파기 등 조치를 취해야 하는가?**

A | 최초 회원가입 또는 회원정보 수정 등의 단계에서 수집·관리되는 개인정보뿐만 아니라 접속 로그(log), 쿠키(cookie), 결제 기록 등 서비스를 이용하는 과정에서 생성되는 정보도 파기 등 조치 대상이 되는 개인정보에 포함된다. 또한 해당 개인정보를 파기할 경우 이용자의 권리를 침해하거나 추후 분쟁의 소지가 있을 것으로 판단되는 경우에는 개인정보를 분리 저장·관리하여야 한다.

Q | **1년 동안 이용내역이 없는 이용자의 정보는 별도 보관 등의 조치를 취해야 하는데 별도 보관한 이용자를 대상으로도 법 제39조의8에 따른 이용내역을 통지해야 하는가?**

A | 이용내역 통지제도는 이용자의 개인정보를 이용한 내역을 이용자에게 알려주기 위한 제도인데, 1년 동안 서비스를 이용하지 않은 이용자에게 이용내역을 통지하는 것은 필요하지 않을 것으로 판단된다.

제39조의7 | 이용자의 권리 등에 대한 특례

법률

제39조의7(이용자의 권리 등에 대한 특례) ① 이용자는 정보통신서비스 제공자등에 대하여 언제든지 개인정보 수집·이용·제공 등의 동의를 철회할 수 있다.
② 정보통신서비스 제공자등은 제1항에 따른 동의를 철회, 제35조에 따른 개인정보의 열람, 제36조에 따른 정정을 요구하는 방법을 개인정보의 수집방법보다 쉽게 하여야 한다.
③ 정보통신서비스 제공자등은 제1항에 따라 동의를 철회하면 지체 없이 수집된 개인정보를 복구·재생할 수 없도록 파기하는 등 필요한 조치를 하여야 한다.

1. 일반규정과의 관계

정보주체는 자신의 개인정보를 처리하는 개인정보처리자에 대하여 일반규정인 제35조, 제36조 및 제37조에 따라 열람, 정정·삭제 및 처리정지를 요구할 수 있다.

정보통신서비스 이용자 또한 자신의 개인정보를 처리하는 정보통신서비스 제공자등에 대하여 위의 규정에 따른 권리를 행사할 수 있다. 이 외에도 특례규정인 제39조의7은 이용자가 개인정보 수집·이용·제공 등에 대한 동의를 철회할 수 있도록 하고, 정보통신서비스 제공자등은 이용자 권리 행사 방법을 개인정보 수집 방법보다 쉬운 방법으로 제공하도록 규정하고 있다. 즉, 이용자는 일반규정 및 특례규정에 따른 권리 모두를 행사할 수 있다.

정보통신서비스 제공자등의 경우 서비스 제공 및 개인정보 처리 과정에서 일반 개인정보처리자보다 이용자 동의의 비중이 크고, 서비스 이용이 주로 비대면으로 이루어지는 특징을 고려하여 이용자의 동의 철회권을 추가로 규정하고 있다.

2. 개인정보 수집·이용·제공 등 동의 철회권

이용자는 정보통신서비스 제공자등에 대하여 개인정보의 수집·이용·제공 등에 대한 동의를 철회할 수 있다. 동의 철회권은 처리정지권과는 그 개념 범위가 다르므로(이와 관련한 자세한 내용은 제37조(개인정보의 처리정지 등) 해설 참고) 이용자가 자신이 했던 동의를 철회하는 경우에는 제37조에 따른 처리정지권 규정이 아닌 제1항에 따른 동의 철회권 규정이 적용된다.

이용자는 언제든지 동의를 철회할 수 있으므로 정보통신서비스 제공자등은 이용자가 언제든지 회원탈퇴, 서비스 철회 등의 동의 철회 의사를 표시할 수 있는 방법을 마련할 필

요가 있다. 가령 웹사이트는 통상적으로 회원탈퇴 메뉴를 설정하는 방식으로 동의 철회 의사를 표시하는 절차를 마련할 수 있으며, 이는 이용자가 웹사이트 회원가입을 위해 개인정보를 제공했다면 회원에서 탈퇴하는 행위는 개인정보 이용에 대한 동의를 철회한 것으로 볼 수 있기 때문이다.

3. 수집 방법보다 쉬운 이용자 권리 행사 방법 제공

이용자가 개인정보 수집·이용·제공 등에 대한 동의를 철회하는 방법, 개인정보 열람, 정정 등을 요구하는 방법은 개인정보의 수집 방법보다 쉬워야 한다. 또한, 동의 철회 요구 방법을 포함한 이용자 권리 행사 방법은 이용자가 언제든지 쉽게 확인할 수 있도록 개인정보 처리방침을 통해 안내되어야 한다(제30조 참고).

이는 일부 정보통신서비스 제공자들이 회원가입 절차는 쉽게 하면서도 탈퇴 절차 등 권리 행사 절차는 까다롭게 만들어 이용자의 개인정보를 악용하는 경우를 방지하기 위한 것으로 더 쉬운 방법인지 여부는 구체적인 사안 별로 접근매체의 다양성을 고려하여 개별적으로 판단하여야 한다.

일반적으로 동의 철회 등 권리 행사 방법이 수집 시와 동일한 방법으로 제공되고 이에 더하여 추가적인 조치가 제공되는 경우 더 쉬운 방법으로 인정될 수 있다. 이 경우 추가적인 조치로는 접근매체의 확대(전화, ARS, 이메일 등을 통한 권리 행사도 가능하도록 조치), 권리 행사 메뉴의 다양화(철회 메뉴를 메인화면 외에 개인정보 처리방침, 나의 개인정보, 해당 서비스의 게시판 등에서도 언제든지 쉽게 발견하고 신청할 수 있도록 조치) 등을 고려할 수 있다.

4. 동의 철회권 행사에 대한 파기 등 필요한 조치

정보통신서비스 제공자들은 이용자로부터 개인정보에 대한 동의 철회 요구를 받으면 지체 없이 수집된 개인정보를 복구·재생활 수 없도록 파기하는 등 필요한 조치를 하여야 한다. 여기서 지체 없이란 합리적 이유와 근거가 없는 한 곧바로 조치하는 것을 말한다. 예를 들어, 이용자가 회원 탈퇴(동의 철회) 신청을 하는 경우 수집된 개인정보를 복구·재생활 수 없도록 파기하는데 걸리는 시간을 감안하여 이용자의 회원 탈퇴 신청에 대한 조치를 할 수 있다(개인정보를 복구·재생활 수 없는 파기 방법에 대해서는 제39조의6(개인정보의 파기에 대한 특례) 해설 참고).

5. 가명정보의 적용 제외

이용자는 가명정보에 대하여 제39조의7 특례규정에 따른 권리를 행사할 수 없다(제28조의7).

6. 벌칙규정

위반행위	벌칙
수집 방법보다 쉬운 동의 철회·열람·정정 방법을 제공하지 않는 자 (제39조의14에 따라 준용되는 경우 포함) (제39조의7제2항 위반)	3천만원 이하 과태료 (제75조제2항제12호의5)
이용자가 동의 철회 시 파기 등 필요한 조치를 하지 않은 정보통신서비스 제공자등 (제39조의14에 따라 준용되는 경우와 제27조에 따라 정보통신서비스 제공자등으로부터 개인정보를 이전받은 자를 포함) (제39조의7제3항 위반)	3천만원 이하 과태료 (제75조제2항제12호의6)

제39조의8 | 개인정보 이용내역의 통지

<p>법률</p>	<p>제39조의8(개인정보 이용내역의 통지) ① 정보통신서비스 제공자 등으로서 대통령령으로 정하는 기준에 해당하는 자는 제23조, 제39조의3에 따라 수집한 이용자의 개인정보의 이용내역(제17조에 따른 제공을 포함한다)을 주기적으로 이용자에게 통지하여야 한다. 다만, 연락처 등 이용자에게 통지할 수 있는 개인정보를 수집하지 아니한 경우에는 그러하지 아니한다.</p> <p>② 제1항에 따라 이용자에게 통지하여야 하는 정보의 종류, 통지주기 및 방법, 그 밖에 이용내역 통지에 필요한 사항은 대통령령으로 정한다.</p>
<p>시행령</p>	<p>제48조의6(개인정보 이용내역의 통지) ① 법 제39조의8제1항 본문에서 “대통령령으로 정하는 기준에 해당하는 자”란 다음 각 호의 어느 하나에 해당하는 자를 말한다.</p> <ol style="list-style-type: none"> 1. 정보통신서비스 부문 전년도(법인인 경우에는 전 사업연도를 말한다) 매출액이 100억원 이상인 정보통신서비스 제공자등 2. 전년도 말 기준 직전 3개월간 그 개인정보가 저장·관리되고 있는 이용자 수가 일일평균 100만명 이상인 정보통신서비스 제공자등 <p>② 법 제39조의8제1항에 따라 이용자에게 통지해야 하는 정보의 종류는 다음 각 호와 같다.</p> <ol style="list-style-type: none"> 1. 개인정보의 수집·이용 목적 및 수집한 개인정보의 항목 2. 개인정보를 제공받은 자와 그 제공 목적 및 제공한 개인정보의 항목. 다만, 「통신비밀보호법」 제13조, 제13조의2, 제13조의4 및 「전기통신사업법」 제83조제3항에 따라 제공한 정보는 제외한다. <p>③ 법 제39조의8제1항에 따른 통지는 서면등의 방법으로 연 1회 이상 해야 한다.</p>

1. 입법 취지

이용자는 자신에 관한 정보가 언제, 누구에게 어느 범위까지 알려지고 또 이용되도록 할 것인지를 스스로 결정할 수 있는 권리를 가진다. 이에 따라 특례규정인 제39조의8은 매출액 또는 이용자 수가 일정 기준 이상인 정보통신서비스 제공자등에 대하여 주기적으로 이용자의 개인정보를 이용한 내역을 통지하도록 규정함으로써 이와 같은 이용자의 권리를 보장하고 있다.

한편, 개인정보 이용내역 통지제도는 특례규정인 제39조의8에서만 규정하고 있으므로 정보통신서비스 제공자등에게만 적용된다.

2. 통지 의무 적용대상

정보통신서비스 제공자들은 ① 전년도말 기준 직전 3개월간 그 개인정보가 저장·관리되고 있는 이용자 수가 일일평균 100만명 이상 또는 ② 정보통신서비스 부문 전년도 매출액이 100억원 이상에 해당하는 경우 이용내역 통지 의무 대상이 된다(제39조의8제1항, 영 제48조의6제1항).

이용자 수란 정보통신서비스 제공자들이 그 개인정보를 저장·관리하고 있는 이용자의 수를 말하며 일일 방문자수, 페이지뷰(PV:page view), 순방문자수(UV:unique visitor)와는 무관하다. 또한, 전년도말 기준 직전 3개월간 일일평균 이용자 수는 이용내역을 통지하여야 할 연도의 전년도 10월, 11월, 12월 전체 일일 이용자 수의 총합을 92(일)로 나누어 산정한다.

매출액은 이용내역을 통지하여야 할 연도의 전년도(법인인 경우에는 전 사업연도) 매출액을 말하며, 매출액의 범위는 정보통신서비스 제공자들의 총 매출액이 아니라 정보통신서비스 부문 매출액만을 대상으로 한다. 여기서 정보통신서비스 부문 매출액이란 전기통신설비를 이용하여 타인의 통신을 매개, 전기통신설비를 타인의 통신용으로 제공 또는 전기통신설비를 이용하여 정보를 제공하거나 정보의 제공을 매개하여 발생하는 매출액을 의미한다.

3. 통지 대상 정보

정보통신서비스 제공자들은 개인정보의 수집·이용 목적 및 수집한 개인정보의 항목, 개인정보를 제3자에게 제공한 경우 개인정보를 제공받은 자와 제공 목적 및 제공한 개인정보의 항목을 이용자에게 통지하여야 한다(제39조의8제1항, 영 제48의6제2항).

개인정보의 수집·이용 목적 및 항목만을 통지하면 되므로 개별적인 건별 이용내역은 통지하지 않아도 된다. 통지 대상 정보와 관련된 사항은 개인정보 처리방침에 포함된 사항이므로 개인정보 처리방침의 해당 내용을 기초로 하여 개인정보의 수집·이용 목적 및 항목과 해당 목적 내에서 실제로 제공한 내역(제공받은 자, 제공 목적 및 제공한 항목)을 통지하여야 한다. 만약 제공한 내역이 없다면 개인정보의 수집·이용 목적 및 수집한 개인정보의 항목과 함께 제공한 내역이 없음을 통지하여야 한다.

한편, 개인정보 이용내역 통지로 인하여 수사 중인 사항이 노출될 경우 수사목적 달성에 지장을 초래할 수 있으므로 「통신비밀보호법」 제13조, 제13조의2, 제13조의4 및 「전기통신사업법」 제83조제3항에 따라 제공한 정보는 통지 대상 정보에서 제외된다(영 제48조의6제2항제2호).

4. 통지 주기 및 방법

정보통신서비스 제공자등은 연 1회 이상 개인정보 이용내역을 주기적으로 이용자에게 통지하여야 하며(영 제48조의6제3항), 그 시기는 정보통신서비스 제공자등이 자유롭게 결정할 수 있다.

통지는 서면, 전자우편, 팩스, 전화, 문자전송 또는 이에 상당하는 방법(서면등)으로 하여야 한다(영 제48조의6제3항). 이에 상당하는 방법으로는 인스턴트 메신저를 이용하거나 통지 시 이용내역을 확인할 수 있는 웹사이트 등을 안내하고 이용자가 해당 웹사이트 등에 로그인하여 확인할 수 있도록 조치하는 방법 등이 포함될 수 있다. 다만, 개별적인 통지 없이 웹사이트 게재를 통해서 이용내역을 확인할 수 있는 조치를 하는 것은 통지 방법으로 볼 수 없다.

한편, 정보통신서비스 제공자등이 연락처 등 이용자에게 통지할 수 있는 개인정보를 수집하지 않은 경우에는 통지 자체가 불가능하므로 이용내역을 통지하지 않아도 된다(제39조의8제1항 단서).

5. 가명정보의 적용 제외

정보통신서비스 제공자등이 이용자의 가명정보를 이용한 내역에 대해서는 제39조의7 특례규정에 따른 통지 의무가 적용되지 않는다(제28조의7).

6. 벌칙규정

위반행위	벌칙
개인정보 이용내역을 통지하지 않은 자 (제39조의14에 따라 준용되는 경우 포함) (제39조의8제1항 위반)	3천만원 이하 과태료 (제75조제2항제12호의7)

7. 질의 응답

Q | 이용자의 선택에 따라 이용내역을 통지하지 않을 수 있는가?

A 「개인정보 보호법」에 정보통신서비스 제공자등으로서 대통령령으로 정하는 기준(전년도 말 기준 직전 3개월간 그 개인정보가 저장·관리되고 있는 이용자 수가 일일평균 100만명 이상이거나 정보통신서비스 부문 전년도 매출액이 100억원 이상인 정보통신서비스 제공자등)에 해당하는 자는 주기적으로 이용자에게 이용내역을 통지하여야 한다고 규정되어 있으므로, 이용자의 선택과 무관하게 반드시 이용내역을 통지하여야 한다.

제39조의9 | 손해배상의 보장

법률	<p>제39조의9(손해배상의 보장) ① 정보통신서비스 제공자등은 제39조 및 제39조의2에 따른 손해배상책임의 이행을 위하여 보험 또는 공제에 가입하거나 준비금을 적립하는 등 필요한 조치를 하여야 한다.</p> <p>② 제1항에 따른 가입 대상 개인정보처리자의 범위, 기준 등에 필요한 사항은 대통령령으로 정한다.</p>
시행령	<p>제48조의7(손해배상책임의 이행을 위한 보험 등 가입 대상자의 범위 및 기준 등)</p> <p>① 다음 각 호의 요건을 모두 갖춘 정보통신서비스 제공자등(이하 이 조에서 “가입 대상 개인정보처리자” 라 한다)은 법 제39조의9제1항에 따라 보험 또는 공제에 가입하거나 준비금을 적립해야 한다.</p> <ol style="list-style-type: none"> 1. 전년도(법인의 경우에는 전 사업연도를 말한다)의 매출액이 5천만원 이상일 것 2. 전년도 말 기준 직전 3개월간 그 개인정보가 저장·관리되고 있는 이용자 수가 일일평균 1천명 이상일 것 <p>② 가입 대상 개인정보처리자가 보험 또는 공제에 가입하거나 준비금을 적립할 경우 최저가입금액(준비금을 적립하는 경우 최소적립금액을 말한다. 이하 이 조에서 같다)의 기준은 별표 1의4와 같다. 다만, 가입 대상 개인정보처리자가 보험 또는 공제 가입과 준비금 적립을 병행하는 경우에는 보험 또는 공제 가입금액과 준비금 적립금액을 합산한 금액이 별표 1의4에서 정한 최저가입금액의 기준 이상이어야 한다.</p> <p>③ 가입 대상 개인정보처리자가 다른 법률에 따라 법 제39조 및 제39조의2에 따른 손해배상책임의 이행을 보장하는 보험 또는 공제에 가입하거나 준비금을 적립한 경우에는 법 제39조의9제1항에 따른 보험 또는 공제에 가입하거나 준비금을 적립한 것으로 본다.</p>

1. 일반규정과의 관계

정보주체가 개인정보 유출등으로 인하여 손해를 입은 경우 일반규정인 제39조 및 제39조의2에 따라 개인정보처리자에게 손해배상을 청구할 수 있다. 정보통신서비스 이용자 또한 자신의 개인정보를 처리하는 정보통신서비스 제공자등에게 위의 규정에 따라 손해배상을 청구할 수 있다. 이러한 손해배상책임의 이행의 보장을 위하여 특례규정인 제39조의9는 보험(공제) 가입 또는 준비금 적립 등의 조치 의무를 별도로 규정하고 있다.

이처럼 손해배상책임 보장제도는 특례규정에서만 규정하고 있으므로 정보통신서비스 제공자등에게만 적용된다. 이는 빅데이터·사물인터넷·인공지능 등 신기술의 확산, 사이버 공격의 대상과 규모의 증가 등으로 개인정보 유출로 인한 이용자 피해 사례가 증가하

고 있는 상황에서 정보통신서비스 제공자등이 배상능력이 없어 이용자가 손해를 배상받지 못하는 상황을 방지하기 위하여 도입되었다.

2. 이행이 보장되는 손해배상책임의 범위

제39조의9에 따라 그 이행이 보장되는 손해배상책임은 제39조 및 제39조의2에 따른 일반 손해배상책임, 법정손해배상책임 및 징벌적 손해배상책임이다(제39조의9제1항). 이들 손해배상 제도와 관련하여 자세한 내용은 제39조(손해배상책임) 및 제39조의2(법정손해배상의 청구) 해설을 참고하도록 한다.

3. 손해배상책임 보장 조치 적용 대상

정보통신서비스 제공자등은 전년도(법인의 경우 전 사업연도)의 매출액이 5천만원 이상이고 전년도말 기준 직전 3개월간 그 개인정보가 저장·관리되고 있는 이용자 수가 일일 평균 1천명 이상에 해당하는 경우 보험 또는 공제에 가입하거나 준비금을 적립하는 등 손해배상책임을 보장하기 위한 조치를 하여야 한다(영 제48조의7제1항).

매출액이란 보험 또는 공제에 가입하거나 준비금을 적립하여야 할 연도의 직전 사업연도의 매출액을 말한다. 또한, 그 범위는 정보통신서비스 부분에 한정되지 않으며 정보통신서비스 제공자등의 총 매출액을 의미한다.

이용자 수란 정보통신서비스 제공자등이 저장·관리하고 있는 개인정보 건수(이용자 수)를 의미한다. 따라서 정보통신서비스 제공자등이 저장·관리하고 있는 모든 개인정보 즉, 회원의 개인정보, 비회원의 개인정보, 다른 법령에 따라 보관하고 있는 탈퇴회원 또는 서비스 미이용자(휴면계정)의 개인정보도 이용자 수에 포함된다. 반면, 해당 정보통신서비스를 이용하지 않는 임직원의 경우에는 이용자가 아니므로 이용자 수에서 제외된다. 정보통신서비스를 제공하는 과정에서 수집한 이용자의 개인정보이지만 하면 수집한 경로가 온라인·오프라인인지 여부와는 무관하게 이용자 수에 포함하여야 한다.

한편, 전년도말 기준 직전 3개월간 일일평균 이용자 수는 손해배상책임 보장 조치를 해야 할 연도의 전년도 10월, 11월, 12월 전체 일일 이용자 수의 총합을 92(일)로 나누어 산정한다.

정보통신서비스 제공자등이 손해배상책임 보장 의무의 적용 대상이 되기 위해서는 위의 두가지 기준을 모두 충족하여야 하므로 전년도 매출액이 5천만원 미만이거나 일일평균 이용자수가 1천명 미만인 경우에는 대상에서 제외된다. 이처럼 손해배상책임 보장제도에

서 매출액 기준 및 이용자수 기준에 하한을 설정한 것은 신생기업 등과 같이 매출액이 거의 없거나 미미한 경우에는 사실상 규제 준수가 어려운 점(매출액 하한), 보유하고 있는 이용자 개인정보의 양이 적은 사업자의 경우 개인정보 유출 등 사고 발생 시 피해 및 배상액 규모 등이 상대적으로 크지 않아 손해배상책임의 이행을 보장하는 조치를 의무화할 필요성이 낮은 점(이용자수 하한) 등을 고려한 것이다.

4. 보험 최저가입금액(준비금 최소적립금액) 기준

적용 대상 사업자가 보험 또는 공제에 가입하거나 준비금을 적립할 때 최저가입금액(최소적립금액) 기준은 다음과 같다.

< 손해배상책임의 이행을 위한 최저가입금액(최소적립금액)의 기준(영 별표 1의4) >

가입 대상 개인정보처리자의 가입금액 산정요소		최저가입금액 (최소적립금액)
매출액	이용자 수	
800억원 초과	100만명 이상	10억원
50억원 초과 800억원 이하		5억원
5천만원 이상 50억원 이하		2억원
800억원 초과	10만명 이상 100만명 미만	5억원
50억원 초과 800억원 이하		2억원
5천만원 이상 50억원 이하		1억원
800억원 초과	1천명 이상 10만명 미만	2억원
50억원 초과 800억원 이하		1억원
5천만원 이상 50억원 이하		5천만원

보험 또는 공제 가입과 준비금 적립을 병행하는 경우에는 보험 또는 공제 가입금액과 준비금 적립금액을 합산한 금액이 위의 영 별표 1의4에서 정한 최저가입금액(최소적립금액) 기준 이상이어야 한다(영 제48조의7제2항 단서).

5. 다른 법률에 따른 손해배상의 보장과의 관계

다른 법률에 따라 가입한 보험(또는 공제) 또는 적립한 준비금이 제39조의9에 따른 손해배상책임의 이행을 보장하는 경우 동조에 따른 손해배상 보장 조치를 이행한 것으로 본다(영 제48조의7제3항).

여기서 제39조의9에 따른 손해배상책임의 이행을 보장하는 경우에 해당하는지 여부는 다른 법률에 따라 가입한 보험 등이 제39조 및 제39조의2에 따른 손해배상책임을 담보(보상)하는지, 영 별표 1의4에서 정한 최저가입금액기준(최저적립금액기준)을 준수하고 있는

지 등을 고려하여 개별적으로 판단하여야 한다.

6. 벌칙규정

위반행위	벌칙
보험 또는 공제 가입, 준비금 적립 등 필요한 조치를 하지 않은 자 (제39조의9제1항 위반)	2천만원 이하 과태료 (제75조제3항제1호)

7. 질의 응답

- Q** 위탁사(A사)를 대신하여 개인정보를 처리하는 수탁사(B)도 보험에 가입하거나 준비금을 적립해야 하는지(개인정보는 수탁사에 DB에 저장되고 위탁사는 접근 권한 등만 부여)?
- A** 정보통신서비스 제공자(A사)로부터 개인정보 업무를 위탁받은 수탁자(B사)의 경우에는 A사가 보험 등 가입 대상에 해당하므로 의무 적용 대상에 해당되지 않는다. 다만, 수탁사(B)도 개인정보를 활용한 고유의 정보통신서비스를 영위하는 경우에는 정보통신서비스 제공자로서 대상이 될 수 있다.
- Q** 당사는 글로벌 기업의 한국 지사로 대부분의 주된 사업(서비스)는 글로벌 본사를 통해 이루어지는데, 이 경우 본사와 한국 지사 모두 보험 등에 가입해야 하는가?
- A** 국내 이용자에게 서비스를 제공하는 주체가 해외 소재 본사인지, 국내 소재 지사 인지를 고려하여, 국내 이용자에게 본사와 지사가 각각 서비스를 제공하고 있다면 각각 보험 가입 등 조치를 해야 한다.
- Q** 당사는 여러 서비스를 제공하는 회사로, 한사람이 여러 개의 서비스를 구매하는 등 거래건수가 발생할 때마다 개인정보가 수집되는데 이 경우 이용자수는 어떻게 산정해야 하는가?
- A** 동일인은 중복을 제외하여 이용자수를 산정하면 되고, 동일인 여부에 대해서는 정보통신서비스 제공자가 합리적으로 추정하여 구분하면 되지만 입증책임은 해당 정보통신서비스 제공자에게 있다.

Q | 다른 계열사와 함께 단체로 보험에 가입하는 경우 법 제39조의9에 따른 보험에 가입하였다고 볼 수 있는지?

A | 원칙적으로 준수 의무는 손해배상책임의 귀속주체인 개별 법인(또는 자연인) 단위로 발생한다. 이에, 단체보험을 통한 가입 형태도 무방하나 법령 상 최저가입금액(보상한도액) 기준은 개별 기업별로 적용되므로 단체보험의 최저가입금액은 개별 기업별 준수해야 하는 가입금액을 합산한 금액이 되어야 법령 상 기준을 준수한 것으로 판단된다.

Q | 준비금을 적립하는 구체적인 방법은 어떻게 되는지?

A | 준비금은 임의적립금(자본계정)으로 적립하고 주주총회 결의 등을 통해 해당 임의적립금이 법 제39조의9의 의무이행을 위한 것임을 명확히 하여야 한다.

제39조의10 | 노출된 개인정보의 삭제·차단

법률	제39조의10 (노출된 개인정보의 삭제·차단) ① 정보통신서비스 제공자등은 주민등록번호, 계좌정보, 신용카드정보 등 이용자의 개인정보가 정보통신망을 통하여 공중에 노출되지 아니하도록 하여야 한다. ② 제1항에도 불구하고 공중에 노출된 개인정보에 대하여 보호위원회 또는 대통령령으로 지정한 전문기관의 요청이 있는 경우 정보통신서비스 제공자등은 삭제·차단 등 필요한 조치를 취하여야 한다.
시행령	제48조의8(노출된 개인정보의 삭제·차단 요청 기관) 법 제39조의10제2항에서 “대통령령으로 지정한 전문기관”이란 한국인터넷진흥원을 말한다.

1. 입법 취지

개인정보가 정보통신망을 통하여 공중에 노출되는 경우 사생활 침해, 명의도용, 불법스팸, 보이스 피싱 등에 의한 경제적·정신적 피해를 야기할 수 있으며 각종 범죄에 악용될 우려도 있다. 이에 따라 특례규정인 제39조의10은 정보통신서비스 제공자등에게 정보통신망을 통한 공중 노출 방지 의무 및 노출된 개인정보에 대한 삭제·차단 등 필요한 조치 의무를 규정함으로써 정보통신서비스 제공자등에게 개인정보 노출에 대한 경각심을 높임과 동시에 노출된 개인정보로 인한 2차 피해의 발생 가능성을 최소화하고자 하였다.

한편, 정보통신망을 통한 공중 노출 방지 의무 등은 특례규정인 제39조의10에서만 규정하고 있으므로 정보통신서비스 제공자등에게만 적용된다.

2. 정보통신망을 통한 공중 노출 방지 의무

정보통신서비스 제공자등은 주민등록번호, 계좌정보, 신용카드정보 등 이용자의 개인정보가 정보통신망을 통하여 공중에 노출되지 않도록 하여야 한다. 여기서 정보통신망을 통하여 공중(公衆)에 노출된 경우란 정보통신망 상에서 공중이 해킹 등 특별한 방법을 사용하지 않고도 정보통신망을 통해 이용자의 개인정보를 손쉽게 확인·조회하거나 취득할 수 있도록 개인정보가 공개 또는 방치되어 있는 상태를 의미한다.

3. 공중에 노출된 개인정보에 대한 삭제·차단 등 필요한 조치 의무

정보통신서비스 제공자등은 공중에 노출된 개인정보에 대하여 보호위원회 또는 한국인터넷진흥원의 요청이 있는 경우 삭제·차단 등 필요한 조치를 취하여야 한다. 이 경우 삭제·차단 등 필요한 조치로는 다음과 같은 것을 들 수 있다.

< 필요한 조치의 예시 >

개인정보 노출 원인	조치 내용 예시
관리자 부주의	<ul style="list-style-type: none"> · 마스킹 및 삭제 조치(공통) · 관리자 페이지에 대한 안전한 접속 수단 혹은 인증수단 적용 · 노출된 개인정보에 대한 접근 제어
이용자 부주의	<ul style="list-style-type: none"> · 마스킹 및 삭제 조치(공통) · 개인정보를 입력하지 않도록 안내 · 게시판 운영을 비공개로 전환
설계 및 개발 오류	<ul style="list-style-type: none"> · 마스킹 및 삭제 조치(공통) · 홈페이지 설계 변경, 디렉터리 설정 변경 등 조치
검색엔진 등을 통한 노출	<ul style="list-style-type: none"> · 마스킹 및 삭제 조치(공통) · 당해 검색엔진에 캐쉬 페이지 삭제 등 요청 · 노출된 개인정보에 로봇배제 규칙을 적용하여 외부 검색엔진의 접근 자체를 차단 · 시스템의 계정, 로그 등 점검 후 분석 결과에 따른 접속 경로 차단 조치

제39조의11 | 국내대리인의 지정

법률

- 제39조의11(국내대리인의 지정)** ① 국내에 주소 또는 영업소가 없는 정보통신서비스 제공자등으로서 이용자 수, 매출액 등을 고려하여 대통령령으로 정하는 기준에 해당하는 자는 다음 각 호의 사항을 대리하는 자(이하 “국내대리인”이라 한다)를 서면으로 지정하여야 한다.
1. 제31조에 따른 개인정보 보호책임자의 업무
 2. 제39조의4에 따른 통지·신고
 3. 제63조제1항에 따른 관계 물품·서류 등의 제출
- ② 국내대리인은 국내에 주소 또는 영업소가 있는 자로 한다.
- ③ 제1항에 따라 국내대리인을 지정한 때에는 다음 각 호의 사항 모두를 제30조에 따른 개인정보 처리방침에 포함하여야 한다.
1. 국내대리인의 성명(법인의 경우에는 그 명칭 및 대표자의 성명을 말한다)
 2. 국내대리인의 주소(법인의 경우에는 영업소 소재지를 말한다), 전화번호 및 전자우편 주소
- ④ 국내대리인이 제1항 각 호와 관련하여 이 법을 위반한 경우에는 정보통신서비스 제공자등이 그 행위를 한 것으로 본다.

시행령

- 제48조의9(국내대리인 지정 대상자의 범위)** ① 법 제39조의11제1항 각 호 외의 부분에서 “대통령령으로 정하는 기준에 해당하는 자”란 다음 각 호의 어느 하나에 해당하는 자를 말한다.
1. 전년도(법인인 경우에는 전 사업연도를 말한다) 매출액이 1조원 이상인 자
 2. 정보통신서비스 부문 전년도(법인인 경우에는 전 사업연도를 말한다) 매출액이 100억원 이상인 자
 3. 전년도 말 기준 직전 3개월간 그 개인정보가 저장·관리되고 있는 이용자 수가 일일평균 100만명 이상인 자
 4. 이 법을 위반하여 개인정보 침해 사건·사고가 발생하였거나 발생할 가능성이 있는 경우로서 법 제63조제1항에 따라 관계 물품·서류 등 자료의 제출을 요구받은 자
- ② 제1항제1호 및 제2호에 따른 매출액은 전년도(법인인 경우에는 전 사업연도를 말한다) 평균환율을 적용하여 원화로 환산한 금액을 기준으로 한다.

1. 입법 취지

글로벌 온라인 서비스 이용이 보편화되면서 국외(해외) 사업자가 우리 국민의 개인정보를 처리하는 경우가 증가함에 따라 우리 국민이 개인정보 관련 고충처리를 위해 언어 등의 어려움 없이 편리하게 연락할 수 있도록 하고 개인정보 침해 사고 발생 시 규제 집행력을 강화해야 할 필요성이 제기되었다.

이에 따라 특례규정인 제39조의11은 국내에 주소 또는 영업소를 두지 않고 정보통신서비스를 제공하는 국외(해외) 사업자에 대하여 국내대리인 지정을 의무화하여 개인정보 보호책임자의 업무, 자료제출 등의 업무를 대리하도록 규정하였다. 국내대리인 지정 제도는 특례규정인 제39조의11에서만 규정하고 있으므로 국외(해외) 정보통신서비스 제공자등에만 적용된다.

2. 적용 대상

국내에 주소 또는 영업소가 없는 정보통신서비스 제공자등으로서, 영 제48조의9 제1항 각 호의 어느 하나에 해당하는 자는 국내대리인을 지정하여야 한다.

먼저, 한국에 정보통신서비스를 제공하면서 국내에 주소 또는 영업소가 없는 정보통신서비스 제공자등이어야 한다(제39조의11제1항).

정보통신서비스 제공자등은 ① 전기통신사업법 규정에 의한 전기통신사업자와 ② 영리를 목적으로 전기통신사업자의 전기통신역무를 이용하여 정보를 제공하거나 정보의 제공을 매개하는 자 ③ 정보통신서비스 제공자로부터 이용자의 개인정보를 제공받은 자를 의미한다. 또한, 한국에 정보통신서비스를 제공하면서 국내에 주소 또는 영업소가 없어야 하고, 국내에 주소 또는 영업소가 있는지 여부는 입법 취지인 우리 국민의 개인정보 고충처리, 개인정보 침해신고 시 규제 집행 등을 고려하여 판단하여야 한다. 여기서 한국에 정보통신서비스를 제공하는지 여부는 한국어 서비스를 운영하고 있는지, 한국인을 이용 대상 중 하나로 상정하고 있는지, 국내에 사업 신고 등을 하였는지 등 여러 요소를 종합적으로 고려하여 판단한다.

다음으로 영 제48조의9 제1항 각 호의 어느 하나(아래의 ①~④ 기준 중 어느 하나)의 기준에 해당하여야 한다.

① 전년도(법인의 경우에는 전 사업연도) 매출액이 1조원 이상인 자(제1호)

매출액은 한국에서 발생한 매출액으로 한정하지 않으며 정보통신서비스 부문이 아닌

전 세계에서 발생하는 전체 매출액을 의미한다. 여기서 매출액은 전년도 평균환율을 적용하여 원화로 환산한 금액을 기준으로 한다(영 제48조의9제2항).

② 정보통신서비스 부문 전년도(법인의 경우에는 전 사업연도) 매출액이 100억원 이상인 자(제2호)

한국에 정보통신서비스를 제공하여 발생한 매출액의 합으로 산정하며, 여러 가지 정보통신서비스를 제공하는 경우에는 해당 서비스의 매출액을 모두 합하여 계산한다. 여기서 매출액은 전년도 평균환율을 적용하여 원화로 환산한 금액을 기준으로 한다(영 제48조의9제2항).

③ 전년도 말 기준 직전 3개월간 그 개인정보가 저장·관리되고 있는 이용자 수가 일일 평균 100만명 이상인 자(제3호)

이용자수는 정보통신서비스 제공자들이 그 개인정보를 저장·관리하고 있는 이용자의 수를 말한다. 전년도말 기준 직전 3개월간 일일평균 이용자 수는 국내대리인을 지정해야 할 연도의 전년도 10월, 11월, 12월 전체 일일 이용자 수의 총합을 92(일)로 나누어 산정한다.

④ 이 법을 위반하여 개인정보 침해 사건·사고가 발생하였거나 발생할 가능성이 있는 경우로서 법 제63조제1항에 따른 관계 물품·서류 등의 제출을 요구받은 자(제4호)

보호위원회는 제63조제1항 및 영 제60조제1항에 따라 법 위반 사항을 발견하거나 혐의가 있음을 알게 된 경우, 법 위반에 대한 신고를 받거나 민원이 접수된 경우, 개인정보 유출 등 정보주체의 개인정보에 관한 권리 또는 이익을 침해하는 사건·사고 등이 발생하였거나 발생할 가능성이 상당히 있는 경우 개인정보처리자에게 관계 물품·서류 등의 제출을 요구할 수 있다.

3. 국내대리인의 역할

국내대리인은 국외(해외) 정보통신서비스 제공자들을 대리하여 다음의 사항을 대리한다(제39조의11제1항).

첫째, 개인정보 처리와 관련한 불만의 처리 및 피해 구제 등 제31조에 따른 개인정보 보호 책임자의 업무를 국외(해외) 정보통신서비스 제공자들을 대리하여 수행해야 한다(제1호). 다만, 국내대리인은 개인정보 보호책임자가 아니라 그 업무를 대리하는 자이므로 국내대리인의 구체적인 업무 범위는 정보통신서비스 제공자들과의 세부적인 계약 내용에 따라 달라질 수 있다.

둘째, 국내대리인은 개인정보의 유출등 사실을 알게 된 경우 국외(해외) 정보통신서비스 제공자들을 대리하여 제39조의4에 따라 이용자에게 통지하고, 보호위원회 또는 한국인터넷

넷진흥원에 신고해야 한다(제2호).

셋째, 국내대리인은 제63조제1항에 따라 법 위반 등과 관련하여 보호위원회로부터 관계 물품·서류 등의 제출을 요구받은 경우 국외(해외) 정보통신서비스 제공자들을 대리하여 법령 등에서 요구하는 절차를 신속하게 진행해야 한다(제3호).

한편, 국내대리인이 위의 사항과 관련하여 이 법을 위반한 경우에는 정보통신서비스 제공자들이 그 행위를 한 것으로 본다(제39조의11제4항).

4. 국내대리인의 지정 절차

국내대리인은 서면으로 지정하여야 한다(제39조의11제1항). 또한, 국내대리인을 지정한 경우에는 국내대리인의 성명(법인의 경우에는 그 명칭 및 대표자의 성명)과 국내대리인의 주소(법인의 경우에는 영업소 소재지), 전화번호, 전자우편 주소 모두를 개인정보 처리방침에 포함하여야 한다(제39조의11제3항). 복수의 국내대리인을 지정한 경우에는 지정한 국내대리인 모두에 대한 관련 정보를 개인정보 처리방침을 통해 공개하여야 한다.

5. 벌칙규정

위반행위	벌칙
국내대리인을 지정하지 않은 자 (제39조의11제1항 위반)	2천만원 이하 과태료 (제75조제3항제2호)

제39조의12 | 국외 이전 개인정보의 보호

법률

제39조의12(국외 이전 개인정보의 보호) ① 정보통신서비스 제공자등은 이용자의 개인정보에 관하여 이 법을 위반하는 사항을 내용으로 하는 국제계약을 체결해서는 아니 된다.

② 제17조제3항에도 불구하고 정보통신서비스 제공자등은 이용자의 개인정보를 국외에 제공(조회되는 경우를 포함한다)·처리위탁·보관(이하 이 조에서 “이전”이라 한다)하려면 이용자의 동의를 받아야 한다. 다만, 제3항 각 호의 사항 모두를 제30조제2항에 따라 공개하거나 전자우편 등 대통령령으로 정하는 방법에 따라 이용자에게 알린 경우에는 개인정보 처리위탁·보관에 따른 동의절차를 거치지 아니할 수 있다.

③ 정보통신서비스 제공자등은 제2항 본문에 따른 동의를 받으려면 미리 다음 각 호의 사항 모두를 이용자에게 고지하여야 한다.

1. 이전되는 개인정보 항목
2. 개인정보가 이전되는 국가, 이전일시 및 이전방법
3. 개인정보를 이전받는 자의 성명(법인인 경우에는 그 명칭 및 정보관리책임자의 연락처를 말한다)
4. 개인정보를 이전받는 자의 개인정보 이용목적 및 보유·이용 기간

④ 정보통신서비스 제공자등은 제2항 본문에 따른 동의를 받아 개인정보를 국외로 이전하는 경우 대통령령으로 정하는 바에 따라 보호조치를 하여야 한다.

⑤ 이용자의 개인정보를 이전받는 자가 해당 개인정보를 제3국으로 이전하는 경우에 관하여는 제1항부터 제4항까지의 규정을 준용한다. 이 경우 “정보통신서비스 제공자등”은 “개인정보를 이전받는 자”로, “개인정보를 이전받는 자”는 “제3국에서 개인정보를 이전받는 자”로 본다.

시행령

제48조의10(개인정보 국외 이전 시 보호조치) ① 정보통신서비스 제공자 등이 법 제39조의12제2항 본문에 따라 개인정보를 국외로 이전하는 경우에 같은 조 제4항에 따라 해야 하는 보호조치는 다음 각 호와 같다.

1. 제48조의2제1항에 따른 개인정보 보호를 위한 안전성 확보 조치
2. 개인정보 침해에 대한 고충처리 및 분쟁해결에 관한 조치
3. 그 밖에 이용자의 개인정보 보호를 위하여 필요한 조치

② 정보통신서비스 제공자등이 법 제39조의12제2항 본문에 따라 개인정보를 국외에 이전하려는 경우에는 제1항 각 호의 사항에 관하여 이전받는 자와 미리 협의하고 이를 계약내용 등에 반영해야 한다.

③ 법 제39조의12제2항 단서에서 “전자우편 등 대통령령으로 정하는 방법”이란 서면등의 방법을 말한다.

1. 일반규정과의 관계

개인정보처리자는 일반규정인 제17조제3항에 따라 개인정보를 국외의 제3자에게 제공하는 경우 정보주체의 동의를 받아야 하며, 이 법을 위반하는 내용으로 개인정보의 국외 이전에 관한 계약을 체결하여서는 아니 된다.

한편, 특례규정인 제39조의12는 정보통신서비스 제공자등에게 국외 제3자 제공뿐만 아니라 개인정보 조회, 처리위탁 및 보관을 포함한 국외 이전 시 동의, 보호조치 의무 등을 별도로 규정하고 있으며, 국외 이전된 개인정보를 제3국으로 재이전하는 경우에 대해서도 규정하고 있다. 이처럼 특례규정은 일반규정에서 규정하고 있는 내용을 포함하여 국외 이전·재이전 시 보호 조치를 폭넓게 규정하고 있으므로 정보통신서비스 제공자등에 대해서는 특례규정이 적용된다.

개인정보의 국외 이전은 개인정보 보호에 대한 법적 체계가 우리나라와 다른 나라로 개인정보가 옮겨지는 것이므로 개인정보의 침해 위험성이 크다. 특히, 대량의 개인정보를 신속하게 전송할 수 있는 정보통신망의 특성, 사이버 공격의 대상과 규모의 증가 등을 고려할 때 정보통신망을 통한 이전은 그 위험성이 더욱 크다고 할 수 있다. 이에 따라 제39조의12는 정보통신서비스 제공자등의 개인정보 국외 이전에 대하여 강화된 보호 조치를 규정하고 있다.

2. 법 위반 사항을 내용으로 하는 국제계약의 체결 금지

정보통신서비스 제공자등은 이용자의 개인정보에 관하여 이 법을 위반하는 사항을 내용으로 하는 국제계약을 체결해서는 아니 된다. 이는 일반규정인 제17조제3항의 경우 이 법을 위반하는 내용으로 개인정보의 국외 이전에 관한 계약의 체결을 금지하고 있는 것과 구분된다.

3. 개인정보의 국외 이전에 대한 동의

가 국외 이전의 유형

특례규정에서는 법 해석 및 적용상의 혼란을 방지하기 위하여 국외 이전의 유형을 특정하고 있다. 즉, 개인정보 국외 이전의 유형으로 정보통신서비스 제공자등이 이용자의 개인정보를 국외에 제공(조회되는 경우를 포함한다)·처리위탁·보관하는 경우로 구분하고 있다(제2항 전단).

따라서 국외 이전은 일반규정인 제17조제3항에서 규정하고 있는 개인정보의 국외 제3자 제공보다 범위가 넓다.

참고 유형별 국외 이전 사례

- **(제공)** 다국적기업의 한국 법인이 수집한 고객정보를 해외 본사로 이전하는 경우, 다국적기업의 한국 법인의 고객DB를 해외 본사에서 조회하는 경우
- **(처리위탁)** 해외에 자회사인 콜센터를 설립하고 국내 고객DB를 이용해 고객대응 업무를 대행시키는 경우
- **(보관)** 해외 인터넷쇼핑몰 사업자가 국내 소비자의 개인정보를 해외에서 직접 수집·보관하는 경우, 국내 사업자가 국내에서 수집한 소비자의 개인정보를 해외 서버에 보관하는 경우

나 국외 이전 동의

정보통신서비스 제공자등이 이용자의 개인정보를 국외에 이전할 때에는 ① 이전되는 개인정보 항목 ② 개인정보가 이전되는 국가, 이전일시 및 이전방법 ③ 개인정보를 이전받는 자의 성명(법인인 경우에는 그 명칭 및 정보관리책임자의 연락처) ④ 개인정보를 이전받는 자의 개인정보 이용목적 및 보유·이용 기간 모두를 이용자에게 고지한 후 동의를 받아야 한다(제2항 본문 및 제3항).

다만, 국외 처리위탁 및 보관의 경우에는 위의 ①~④ 모두를 개인정보 처리방침에 공개하거나 서면, 전자우편, 팩스, 전화, 문자전송 또는 이에 상당하는 방법(서면등)으로 이용자에게 알린 경우에는 국외 이전 동의 절차를 거치지 아니할 수 있다(제2항 단서 및 제3항).

다 국외 이전 시 보호조치

정보통신서비스 제공자등은 이용자의 동의를 받아 개인정보를 국외로 이전하는 경우 ① 영 제48조의2에 따른 개인정보 보호를 위한 안전성 확보조치 ② 개인정보 침해에 대한 고충처리 및 분쟁해결에 관한 사항 ③ 그 밖에 이용자의 개인정보 보호를 위하여 필요한 조치를 하여야 한다(제4항, 영 제48조의10제1항).

또한, 정보통신서비스 제공자등은 위의 ①~③의 사항을 개인정보를 국외에서 이전받는 자와 미리 협의하고 이를 계약 내용 등에 반영하여야 한다(영 제48조의10제2항).

4. 개인정보의 국외 재이전에 대한 동의

국외 재이전이란 이용자의 개인정보를 국외 이전받는 자가 해당 개인정보를 제3국으로 이전하는 것을 말한다. 제5항은 글로벌 사업자가 대한민국 국민의 개인정보를 해외로 이전한 후 제3국으로 재이전하는 등 해외 시장에서 유통되고 있음을 고려하여 국외 재이전의 법적 근거를 마련한 것이다. 즉, 국외 재이전의 경우에도 국외 이전의 경우와 동일하게 제1항부터 제4항까지의 내용이 적용된다.

5. 벌칙규정

위반행위	벌칙 및 제재
이용자의 동의 없이 개인정보를 국외에 제공(재제공)한 경우 (제39조의12제2항 및 제5항 위반)	위반행위 관련 매출액의 100분의3 이하 과징금 (제39조의15제1항제7호)
국외 처리위탁·보관 시 고지사항 모두를 처리방침에 공개하지 않거나 이용자에게 알리지 않은 자 (제39조의12제2항 단서)	2천만원 이하 과태료 (제75조제3항제3호)
국외 이전(재이전) 시 보호조치를 하지 않은 자 (제39조의12제4항 및 제5항 위반)	3천만원 이하 과태료 (제75조제2항제12의8호)

제39조의13(상호주의) 제39조의12에도 불구하고 개인정보의 국외 이전을 제한하는 국가의 정보통신서비스 제공자등에 대하여는 해당 국가의 수준에 상응하는 제한을 할 수 있다. 다만, 조약 또는 그 밖의 국제협정의 이행에 필요한 경우에는 그러하지 아니하다.

1. 입법 취지

국가별로 개인정보를 보호하는 수준이 서로 다르고, 특히 우리나라보다 개인정보 보호 수준이 낮은 나라로의 이전에 대해서는 국제규범상 동등하게 보호하는 등 우리나라 국민의 개인정보가 해외에서도 안전하게 유통될 수 있는 방안을 마련할 필요가 있다. 이에 따라 특례규정인 제39조의13는 국가별 개인정보 보호 수준에 맞게 합리적이고 탄력적으로 대응할 수 있도록 하는 상호주의 규정을 도입하였다.

한편, 상호주의 규정은 특례규정인 제39조의13에서만 규정하고 있으므로 국외(해외) 정보통신서비스 제공자등을 대상으로 적용된다.

2. 상호주의

개인정보의 국외 이전을 제한하는 국가의 정보통신서비스 제공자등에 대하여는 해당 국가의 수준에 상응하는 제한을 할 수 있다. 다만, 조약 또는 그 밖의 국제협정의 이행에 필요한 경우에는 상호주의 적용이 배제된다.

제39조의14 | 방송사업자등에 대한 특례

법률

제39조의14(방송사업자등에 대한 특례) 「방송법」 제2조제3호가목부터 마목까지와 같은 조 제6호·제9호·제12호 및 제14호에 해당하는 자(이하 이 조에서 “방송사업자등”이라 한다)가 시청자의 개인정보를 처리하는 경우에는 정보통신서비스 제공자에게 적용되는 규정을 준용한다. 이 경우 “방송사업자등”은 “정보통신서비스 제공자” 또는 “정보통신서비스 제공자등”으로, “시청자”는 “이용자”로 본다.

제39조의14에 따른 방송사업자등에 대한 특례는 방송사업자등이 시청자의 개인정보를 처리하는 경우에 적용된다. 여기서 방송사업자등은 「방송법」 제2조제3호가목부터 마목까지와 같은 조 제6호·제9호·제12호 및 제14호에 해당하는 자를 말한다(방송사업자등의 구체적인 범위는 ‘개관’ 부분의 적용 대상 해설 참고).

방송사업자등은 정보통신서비스 제공자에게 적용되는 규정을 준용하므로 정보통신서비스 제공자에게 적용되는 일반규정과 특례규정이 동일하게 적용된다.

방송사업자등에 정보통신서비스 제공자에게 적용되는 규정이 준용되는 경우 방송사업자등은 정보통신서비스 제공자 또는 정보통신서비스 제공자등으로 시청자는 이용자로 보게 되므로 시청자 역시 특례규정에 따른 이용자의 권리를 동일하게 보장받는다.

제39조의15 | 과징금의 부과 등에 대한 특례

법률

제39조의15(과징금의 부과 등에 대한 특례) ① 보호위원회는 정보통신서비스 제공자등에게 다음 각 호의 어느 하나에 해당하는 행위가 있는 경우에는 해당 정보통신서비스 제공자등에게 위반행위와 관련한 매출액의 100분의 3 이하에 해당하는 금액을 과징금으로 부과할 수 있다.

1. 제17조제1항·제2항, 제18조제1항·제2항 및 제19조(제39조의14에 따라 준용되는 경우를 포함한다)를 위반하여 개인정보를 이용·제공한 경우
2. 제22조제6항(제39조의14에 따라 준용되는 경우를 포함한다)을 위반하여 법정대리인의 동의를 받지 아니하고 만 14세 미만인 아동의 개인정보를 수집한 경우
3. 제23조제1항제1호(제39조의14에 따라 준용되는 경우를 포함한다)를 위반하여 이용자의 동의를 받지 아니하고 민감정보를 수집한 경우
4. 제26조제4항(제39조의14에 따라 준용되는 경우를 포함한다)에 따른 관리·감독 또는 교육을 소홀히 하여 특례 수탁자가 이 법의 규정을 위반한 경우
5. 이용자의 개인정보를 분실·도난·유출·위조·변조 또는 훼손한 경우로서 제29조의 조치(내부 관리계획 수립에 관한 사항은 제외한다)를 하지 아니한 경우(제39조의14에 따라 준용되는 경우를 포함한다)
6. 제39조의3제1항(제39조의14에 따라 준용되는 경우를 포함한다)을 위반하여 이용자의 동의를 받지 아니하고 개인정보를 수집한 경우
7. 제39조의12제2항 본문(같은 조 제5항에 따라 준용되는 경우를 포함한다)을 위반하여 이용자의 동의를 받지 아니하고 이용자의 개인정보를 국외에 제공한 경우

② 제1항에 따른 과징금을 부과하는 경우 정보통신서비스 제공자등이 매출액 산정자료의 제출을 거부하거나 거짓의 자료를 제출한 경우에는 해당 정보통신서비스 제공자등과 비슷한 규모의 정보통신서비스 제공자등의 재무제표 등 회계자료와 가입자 수 및 이용요금 등 영업현황 자료에 근거하여 매출액을 추정할 수 있다. 다만, 매출액이 없거나 매출액의 산정이 곤란한 경우로서 대통령령으로 정하는 경우에는 4억원 이하의 과징금을 부과할 수 있다.

③ 보호위원회는 제1항에 따른 과징금을 부과하려면 다음 각 호의 사항을 고려하여야 한다.

1. 위반행위의 내용 및 정도
2. 위반행위의 기간 및 횟수
3. 위반행위로 인하여 취득한 이익의 규모

④ 제1항에 따른 과징금은 제3항을 고려하여 산정하되, 구체적인 산정기준과 산정절차는 대통령령으로 정한다.

⑤ 보호위원회는 제1항에 따른 과징금을 내야 할 자가 납부기한까지 이를 내지 아니하면 납부기한의 다음 날부터 내지 아니한 과징금의 연 100분의 6에 해당하는 가산금을 징수한다.

⑥ 보호위원회는 제1항에 따른 과징금을 내야 할 자가 납부기한까지 이를 내지 아니한 경우에는 기간을 정하여 독촉을 하고, 그 지정된 기간에 과징금과 제5항에 따른 가산금을 내지 아니하면 국세 체납처분의 예에 따라 징수한다.

⑦ 법원의 판결 등의 사유로 제1항에 따라 부과된 과징금을 환급하는 경우에는 과징금을 낸 날부터 환급하는 날까지의 기간에 대하여 금융회사 등의 예금이자율 등을 고려하여 대통령령으로 정하는 이자율에 따라 계산한 환급가산금을 지급하여야 한다.

⑧ 제7항에도 불구하고 법원의 판결에 의하여 과징금 부과처분이 취소되어 그 판결이유에 따라 새로운 과징금을 부과하는 경우에는 당초 납부한 과징금에서 새로 부과하기로 결정한 과징금을 공제한 나머지 금액에 대해서만 환급가산금을 계산하여 지급한다.

제48조의11(과징금의 산정기준 등에 관한 특례) ① 법 제39조의15제1항에 따른 매출액은 해당 정보통신서비스 제공자등의 위반행위와 관련된 정보통신서비스의 직전 3개 사업연도의 연평균 매출액으로 한다. 다만, 해당 사업연도 첫날 현재 사업을 개시한지 3년이 되지 않은 경우에는 그 사업개시일부터 직전 사업연도 말일까지의 매출액을 연평균 매출액으로 환산한 금액으로 하며, 해당 사업연도에 사업을 개시한 경우에는 사업개시일부터 위반행위일까지의 매출액을 연매출액으로 환산한 금액으로 한다.

② 법 제39조의15제2항 단서에서 “대통령령으로 정하는 경우”란 다음 각 호의 어느 하나에 해당하는 경우를 말한다.

1. 영업을 개시하지 않았거나 영업을 중단하는 등의 사유로 영업실적이 없는 경우
2. 재해 등으로 인하여 매출액 산정자료가 소멸되거나 훼손되는 등 객관적인 매출액의 산정이 곤란한 경우

③ 보호위원회는 제1항에 따른 매출액 산정을 위하여 재무제표 등 자료가 필요한 경우 20일 이내의 기간을 정하여 해당 정보통신서비스 제공자등에게 관련 자료의 제출을 요청할 수 있다.

④ 법 제39조의15제4항에 따른 과징금의 산정기준과 산정절차는 별표 1의5와 같다.

제48조의12(과징금의 부과 및 납부) ① 보호위원회가 법 제39조의15에 따라 과징금을 부과하려는 경우에는 해당 위반행위를 조사·확인한 후 위반사실·부과금액·이의제기 방법 및 이의제기 기간 등을 서면으로 명시하여 과징금 부과 대상자에게 통지해야 한다.

② 제1항에 따라 통지를 받은 자는 통지를 받은 날부터 30일 이내에 보호위원회가 지정하는 금융기관에 과징금을 납부해야 한다. 다만, 천재지변이나 그 밖의 부득이한 사유로 인하여 그 기간 내에 과징금을 납부할 수 없는 경우에는 그 사유가 없어진 날부터 7일 이내에 납부해야 한다.

③ 제2항에 따라 과징금의 납부를 받은 금융기관은 과징금을 납부한 자에게 영수증을 발급해야 한다.

제48조의13(환급가산금의 이자율) 법 제39조의15제7항에서 “대통령령으로 정하는 이자율” 이란 「국세기본법 시행령」 제43조의3제2항 본문에 따른 이자율을 말한다.

개인정보보호 법규 위반에 대한 과징금 부과기준(보호위원회 고시 제2020-6호)

제1조(목적) 이 고시는 「개인정보 보호법」(이하 “법” 이라 한다) 제39조의15 제4항, 같은 법 시행령(이하 “령” 이라 한다) 제48조의11제4항 및 [별표 1의5]에 따른 과징금 부과에 필요한 세부기준을 정함을 목적으로 한다.

제2조(과징금 산정 절차 및 기준) 과징금은 법 제39조의15제3항 각 호에서 정한 참작사유와 이에 영향을 미치는 행위를 고려하여 산정하되, 기준금액에 필수적 가중·감경, 추가적 가중·감경을 거쳐 과징금을 산정한다.

제3조(기준금액) ① 기준금액은 관련 매출액에 영 [별표 1의5] 2.가. 1)에 따른 부과기준율을 곱한 금액으로 정한다.

② 영 제48조의11제2항 각 호의 어느 하나에 해당하여 제1항을 적용할 수 없는 경우에는 아래 표에 따라 기준금액을 정한다.

위반행위의 중대성	기준금액
매우 중대한 위반행위	3억 6천만원
중대한 위반행위	2억 8천만원
보통 위반행위	2억

제4조(관련 매출액의 산정) ① 관련 매출액은 위반 정보통신서비스 제공자등의 위반행위로 인하여 직접 또는 간접적으로 영향을 받는 서비스의 직전 3개 사업년도의 연평균 매출액으로 한다.

② 제1항에 따른 관련 매출액 산정시 서비스의 범위는 「전기통신사업법」 제5조를 기준으로 판단하되, 구체적인 판단에 있어서는 다음 각 호의 사항을 고려하여야 한다.

1. 서비스 제공 방식
2. 서비스 가입 방법(서비스 가입시 온라인 가입인지 오프라인 가입인지 여부 및 하나의 사업자가 수 개의 웹사이트를 운영하는 경우 독립되어 각각 별개의 가입을 요구하는지 여부 등을 의미한다)
3. 이용약관에서 규정한 서비스 범위
4. 개인정보 데이터베이스 관리 조직·인력 및 시스템 운영 방식

고시

③ 서비스에 대한 매출액은 회계자료를 참고하여 정하되, 이를 통해 위반행위와 관련한 서비스의 매출액을 산정하기 곤란한 경우에는 해당 정보통신서비스 제공자등의 과거 실적, 동종 유사 역무제공사업자의 과거 실적, 사업계획, 그 밖에 시장상황 등을 종합적으로 고려하여 매출액을 산정할 수 있다.

제5조(중대성의 판단) ① 영 [별표 1의5] 2. 가. 1)에 따른 위반행위의 중대성의 판단기준 중 고의·중과실 여부는 영리 목적의 유무, 영 제48조의2에 따른 안전성 확보조치 이행 여부 등을 고려하여 판단한다.

② 위반 정보통신서비스 제공자등에게 고의·중과실이 없으면 위반행위의 중대성을 보통 위반행위로 판단한다.

③ 위반 정보통신서비스 제공자등에게 고의·중과실이 있으면 위반행위의 중대성을 매우 중대한 위반행위로 판단한다. 다만, 위반행위의 결과가 다음 각 호의 사항 중 모두 해당하는 경우에는 보통 위반행위로, 1개 이상 2개 이하에 해당하는 경우에는 중대한 위반행위로 감경한다.

1. 위반 정보통신서비스 제공자등이 위반행위로 인해 직접적으로 이득을 취득하지 않은 경우
2. 위반행위로 인한 개인정보의 피해규모가 위반 정보통신서비스 제공자등이 보유하고 있는 개인정보의 100분의 5 이내인 경우
3. 이용자의 개인정보가 공중에 노출되지 않은 경우

제6조(필수적 가중·감경) ① 위반기간을 고려하여 다음 각 호와 같이 과징금을 조정한다.

1. 단기 위반행위: 위반기간이 1년 이내인 경우는 기준금액을 유지한다.
2. 중기 위반행위: 위반기간이 1년 초과 2년 이내인 경우에는 기준금액의 100분의 25에 해당하는 금액을 가산한다.
3. 장기 위반행위: 위반기간이 2년을 초과하는 경우에는 기준금액의 100분의 50에 해당하는 금액을 가산한다.

② 위반횟수를 고려하여 다음 각 호와 같이 과징금을 조정한다.

1. 최초 위반행위: 위반 정보통신서비스 제공자등이 최근 3년간 법 제39조의15 제1항 각 호에 해당하는 행위로 과징금 처분을 받은 적이 없는 경우에는 제1항에 따른 조정을 거친 금액에서 기준금액의 100분의 50에 해당하는 금액을 감경한다.
2. 2회 이상의 위반행위: 위반 정보통신서비스 제공자등이 최근 3년간 법 제39조의15제1항 각 호에 해당하는 행위로 1회 이상의 과징금 처분을 받은 경우에는 제1항에 따른 조정을 거친 금액을 유지한다.

③ 제2항에서 과거 위반횟수를 산정할 때에는 시정조치 명령이나 과징금 부과 무효 또는 취소판결이 확정된 건을 제외한다.

제7조(위반기간의 산정) ① 제6조제1항에 따른 위반기간은 위반행위의 개시일부

터 종료일까지의 기간을 말한다. 다만, 위반행위가 과징금 부과처분을 명하는 개인정보보호위원회의 심의종결일까지 종료되지 아니한 경우에는 해당 사건에 대한 개인정보보호위원회의 심의종결일을 위반행위의 종료일로 본다.

② 제1항에 따른 위반기간을 산정하면서 위반행위의 개시일 또는 종료일이 불분명한 경우에는 위반 정보통신서비스 제공자등의 영업·재무관련 자료, 임직원·이용자 등의 진술, 동종 유사 정보통신서비스 제공자등의 영업 및 거래실태·관행 등을 고려하여 이를 산정할 수 있다.

제8조(추가적 가중·감경) 개인정보보호위원회는 사업자의 위반행위 주도 여부, 조사 협력 여부 등을 고려하여 필수적 가중·감경을 거친 금액의 100분의 50의 범위 내에서 [별표]에 따라 추가적으로 가중하거나 감경할 수 있다.

제9조(시정조치의 명령) 개인정보보호위원회는 과징금 부과와 함께 법 제64조제1항에 따라 해당 위반행위의 중지나 시정을 위하여 필요한 시정조치를 명할 수 있으며, 위반 정도가 경미하다고 판단되는 경우에는 과징금 부과를 시정조치의 명령으로 갈음할 수 있다.

제10조(재검토 기한) 개인정보보호위원회는 「훈령·예규 등의 발령 및 관리에 관한 규정」(대통령훈령 제394호)에 따라 이 고시에 대하여 2020년 8월 11일을 기준으로 매 3년이 되는 시점(매 3년째의 8월 10일까지를 말한다)마다 그 타당성을 검토하여 개선 등의 조치를 하여야 한다.

보호위원회는 정보통신서비스 제공자등이 이 법을 위반한 경우로서 일정한 경우 그 위반행위와 관련한 매출액의 100분의 3 이하에 해당하는 금액을 과징금으로 부과할 수 있으며, 다만 매출액이 없거나 매출액의 산정이 곤란한 경우에는 4억원 이하의 과징금을 부과할 수 있다(제39조의15제1항 및 제2항 단서).

과징금의 부과 등에 대한 특례를 규정하고 있는 제39조의15는 종전 「정보통신망법」에서 이관하여 규정한 것으로 정보통신서비스 제공자등에게만 적용된다. 이와 관련하여 개인정보보호 법규 위반에 대한 과징금 부과기준(보호위원회 고시 제2020-6호, 이하, ‘과징금 부과기준’이라 한다)은 과징금 부과에 필요한 세부 사항을 정하고 있다.

1. 과징금 부과 대상 행위

정보통신서비스 제공자등이 다음 중 어느 하나에 해당하는 위반행위를 한 경우 과징금 부과 대상이 될 수 있다(제39조의15제1항).

과징금 부과 대상 행위(제39조의15제1항)

1. 제17조제1항·제2항, 제18조제1항·제2항 및 제19조(제39조의14에 따라 준용되는 경우를 포함한다)를 위반하여 개인정보를 이용·제공한 경우
2. 제22조제6항(제39조의14에 따라 준용되는 경우를 포함한다)을 위반하여 법정대리인의 동의를 받지 아니하고 만 14세 미만인 아동의 개인정보를 수집한 경우
3. 제23조제1항제1호(제39조의14에 따라 준용되는 경우를 포함한다)를 위반하여 이용자의 동의를 받지 아니하고 민감정보를 수집한 경우
4. 제26조제4항(제39조의14에 따라 준용되는 경우를 포함한다)에 따른 관리·감독 또는 교육을 소홀히 하여 특례 수탁자가 이 법의 규정을 위반한 경우
5. 이용자의 개인정보를 분실·도난·유출·위조·변조 또는 훼손한 경우로서 제29조의 조치(내부 관리계획 수립에 관한 사항은 제외한다)를 하지 아니한 경우(제39조의14에 따라 준용되는 경우를 포함한다)
6. 제39조의3제1항(제39조의14에 따라 준용되는 경우를 포함한다)을 위반하여 이용자의 동의를 받지 아니하고 개인정보를 수집한 경우
7. 제39조의12제2항 본문(같은 조 제5항에 따라 준용되는 경우를 포함한다)을 위반하여 이용자의 동의를 받지 아니하고 이용자의 개인정보를 국외에 제공한 경우

2. 과징금 산정 기준 및 절차

과징금은 위반행위의 내용 및 정도, 위반행위의 기간 및 횟수, 위반행위로 인하여 취득한 이익의 규모, 이에 영향을 미치는 행위를 종합적으로 고려하여 기준금액에 필수적 가중·감경, 추가적 가중·감경을 순차적으로 거쳐 산정한다. 다만, 가중하는 경우에도 과징금 금액의 상한을 넘을 수 없다(제3항, 영 제48조의11과 별표 [1의5]).

가 기준금액의 산정

1) 원칙

기준금액은 위반행위와 관련한 매출액에 위반행위의 중대성에 따라 다음과 같이 구분된 과징금의 산정비율(부과기준율)을 곱하여 산출한 금액으로 한다(영 별표 [1의5]).

위반행위의 중대성	부과기준율
매우 중대한 위반행위	1천분의 27
중대한 위반행위	1천분의 21
보통 위반행위	1천분의 15

위반행위와 관련한 매출액이란 첫째, 정보통신서비스 제공자들의 위반행위에 직접·간접적으로 영향을 받는 서비스의 직전 3개 사업연도의 연평균 매출액을 말한다(영 제48조의11 제1항 본문, 과징금 부과기준 제4조제1항). 여기서 서비스의 범위는 「전기통신사업법」 제

5조를 기준으로 판단하되 구체적 판단에 있어서는 다음의 사항을 고려하여야 한다(과징금 부과기준 제4조제2항).

서비스 범위 판단 시 고려사항(과징금 부과기준 제4조제2항)

1. 서비스 제공 방식
2. 서비스 가입 방법(서비스 가입시 온라인 가입인지 오프라인 가입인지 여부 및 하나의 사업자가 수 개의 웹사이트를 운영하는 경우 독립되어 각각 별개의 가입을 요구하는지 여부 등을 의미)
3. 이용약관에서 규정한 서비스 범위
4. 개인정보 데이터베이스 관리 조직·인력 및 시스템 운영 방식

다만, 해당 사업연도 첫날 현재 사업을 개시한 지 3년이 되지 않은 경우에는 그 사업개시일부터 직전 사업연도 말일까지의 매출액을 연평균 매출액으로 환산한 금액으로, 해당 사업연도에 사업을 개시한 경우에는 사업개시일부터 위반행위일까지의 매출액을 연매출액으로 환산한 금액을 매출액으로 한다(영 제48조의11제1항 단서).

한편, 매출액은 재무제표 등 회계자료를 참고하여 산정하되, 이를 통해 위반행위와 관련한 서비스의 매출액을 산정하기 곤란한 경우에는 해당 정보통신서비스 제공자등의 과거 실적, 동종 유사 역무제공사업자의 과거 실적, 사업계획, 그 밖에 시장상황 등을 종합적으로 고려하여 산정할 수 있다(과징금 부과기준 제4조제3항).

보호위원회는 매출액 산정을 위하여 회계자료 등 자료가 필요한 경우 20일 이내의 기간을 정하여 해당 정보통신서비스 제공자등에게 관련 자료의 제출을 요청할 수 있으며(영 제48조의11제3항), 해당 정보통신서비스 제공자등이 자료의 제출을 거부하거나 거짓의 자료를 제출한 경우에는 비슷한 규모의 정보통신서비스 제공자등의 회계자료와 가입자 수 및 이용요금 등 영업현황 자료에 근거하여 매출액을 추정할 수 있다(제39조의15제2항 본문).

2) 매출액이 없거나 매출액 산정이 곤란한 경우

매출액이 없거나 매출액 산정이 곤란한 경우란 ① 영업을 개시하지 아니하거나 영업을 중단하는 등의 사유로 영업실적이 없거나 ② 재해 등으로 인하여 매출액 산정자료가 소멸되거나 훼손되는 등 객관적인 매출액의 산정이 곤란한 경우를 말한다(영 제48조의11제2항). 이 경우 기준금액은 위반행위의 중대성에 따라 다음과 같이 정한다(영 별표 [1의5]).

위반행위의 중대성	기준금액
매우 중대한 위반행위	3억 6천만원
중대한 위반행위	2억 8천만원
일반 위반행위	2억원

3) 위반행위의 중대성 판단

위반행위의 중대성은 ① 고의·중과실 여부 ② 영리 목적의 유무 ③ 위반행위로 인한 개인정보의 피해규모 ④ 개인정보의 공중에 노출 여부 ⑤ 위반행위로 인하여 취득한 이익의 규모 등을 종합적으로 고려하여 판단한다(영 별표 [1의5]). 여기서 고의·중과실 여부는 영리 목적의 유무, 법 제29조 및 영 제48조의2제1항에 따른 개인정보의 안전성 확보 조치에 관한 특례 이행 여부 등을 고려하여 판단한다(과징금 부과기준 제5조제1항). 위반행위의 중대성을 판단하는 기준은 다음과 같이 적용된다(과징금 부과기준 제5조제2항, 제3항).

위반행위의 중대성	판단 기준
매우 중대한 위반행위	· 고의·중과실이 있는 경우
중대한 위반행위	· 고의·중과실이 있으나, 위반행위의 결과가 과징금 부과기준 제5조제3항의 감경사유 중 1~2개에 해당하는 경우
일반 위반행위	· 고의·중과실이 없는 경우 · 고의·중과실이 있으나, 위반행위의 결과가 과징금 부과기준 제5조제3항의 감경사유 모두에 해당하는 경우
※ (과징금 부과기준 제5조제3항의 감경사유) 1. 위반행위로 인해 직접적으로 이득을 취득하지 않은 경우, 2. 위반행위로 인한 개인정보의 피해규모가 위반 정보통신서비스 제공자등이 보유하고 있는 개인정보의 5% 이내인 경우, 3. 이용자의 개인정보가 공중에 노출되지 않은 경우	

나 필수적 가중·감경

위반행위의 기간과 횟수 등을 고려하여 기준금액의 100분의 50의 범위에서 가중하거나 감경하여야 한다(영 별표 [1의5]). 위반 행위의 기간이 길거나 횟수가 빈번한 경우에는 당연히 이용자의 개인정보 침해로 인한 피해 규모 또한 매우 클 것이기 때문이다.

1) 위반기간을 고려한 조정

위반기간이란 위반행위의 개시일부터 종료일까지의 기간을 말하며, 위반행위가 과징금 부과처분을 명하는 심의종결일까지 종료되지 아니한 경우에는 해당 사건에 대한 심의종결일을 위반행위의 종료일로 본다(과징금 부과기준 제7조제1항).

위반행위의 개시일 또는 종료일이 불분명한 경우에는 위반 정보통신서비스 제공자등의 영업·재무관련 자료, 임직원·이용자 등의 진술, 동종 유사 정보통신서비스 제공자등의 영업 및 거래실태·관행 등을 고려하여 위반기간을 산정할 수 있다(과징금 부과기준 제7조제2항).

위반기간에 따른 과징금 조정 내용은 다음과 같다(과징금 부과기준 제6조제1항).

위반기간	조정 내용
단기 위반행위(위반기간 1년 이내)	기준금액 유지
중기 위반행위(위반기간 1년 초과 2년 이내)	기준금액의 100분의 25에 해당하는 금액 가산
장기 위반행위(위반기간 2년 초과)	기준금액의 100분의 50에 해당하는 금액 가산

2) 위반횟수를 고려한 조정

위반기간에 따른 조정을 거친 금액에서 위반횟수를 고려하여 다음과 같이 과징금을 조정한다. 위반횟수를 산정하는 경우에는 시정조치 명령이나 과징금 부과 무효 또는 취소 판결이 확정된 건은 제외한다(과징금 부과기준 제6조제3항).

위반횟수	조정 내용
최초 위반행위 (최근 3년 간 법 제39조의15에 따른 과징금 처분을 받은 적이 없는 경우)	위반기간에 따른 조정을 거친 금액에서 기준금액의 100분의 50에 해당하는 금액 감경
2회 이상의 위반행위 (최근 3년 간 1회 이상 법 제39조의15에 따른 과징금 처분을 받은 경우)	위반기간에 따른 조정을 거친 금액 유지

다 추가적 가중·감경

개인정보 보호를 위한 노력 정도, 위반행위에 대한 조사의 협조 여부, 위반행위의 주도 여부 등을 종합적으로 고려하여 필수적 가중·감경을 거친 금액의 100분의 50의 범위에서 가중하거나 감경할 수 있다(영 [별표] 1의5).

추가적 가중·감경 사유에 따른 과징금 가중·감경 비율은 다음과 같다(과징금 부과기준 [별표]).

구분	세부 내용	비율
가중사유	① 위반 정보통신서비스 제공자등 및 그 소속 임원·종업원이 법 제63조제1항 및 제3항에 따른 물품이나 서류의 제출요구 또는 검사를 거부하거나 증거인멸, 조작, 허위의 정보제공 등의 방법으로 조사를 방해하거나 관련 이용자에게 허위로 진술하도록 요청한 경우	100분의 30 이내
	② 다수의 사업자가 관련된 상황에서 위반행위를 주도 또는 선도한 경우	100분의 20 이내
	③ 기타 ①~②의 사항에 준하는 사유가 있는 경우	100분의 10 이내
감경사유	① 개인정보 보호를 위해 보호위원회가 인정하는 인증을 받은 경우	100분의 50 이내
	② 보호위원회의 조사에 적극 협력한 경우	100분의 30 이내
	③ 개인정보 유출 사실을 자진 신고한 경우	100분의 30 이내
	④ 기타 ① 또는 ②의 사항에 준하는 사유가 있는 경우	100분의 10 이내

3. 과징금의 납부 등

보호위원회가 과징금을 부과하는 경우에는 해당 위반행위를 조사·확인한 후 위반사실·부과금액·이의제기방법 및 이의제기기간 등을 서면으로 명시하여 이를 납부할 것을 과징금 부과대상자에게 통지하여야 한다(영 제48조의12제1항). 통지를 받은 자는 통지를 받은 날부터 30일 이내에 보호위원회가 지정하는 금융기관에 과징금을 납부하여야 하며, 다만 천재지변이나 그 밖에 부득이한 사유로 인하여 그 기간 내에 과징금을 납부할 수 없는 경우에는 그 사유가 없어진 날부터 7일 이내에 납부해야 한다(동조 제2항).

보호위원회는 과징금을 내야 할 자가 납부기한까지 이를 내지 아니하면 납부기한의 다음 날부터 내지 아니한 과징금의 연 100분의 6에 해당하는 가산금을 징수한다(제39조의15 제5항). 이 경우 보호위원회는 기간을 정하여 독촉을 하고 그 기간까지 과징금과 가산금을 내지 아니하면 국세 체납처분의 예에 따라 징수한다(동조 제6항).

법원의 판결 등의 사유로 부과된 과징금을 환급하는 경우에는 과징금을 낸 날부터 환급하는 날까지의 기간에 대하여 금융회사 등의 예금이자율 등을 고려하여 「국세기본법 시행령」 제43조의3제2항 본문에 따른 이자율에 따라 계산한 환급가산금을 지급하여야 한다(제39조의15제7항, 영 제48조의13). 참고로 2020년 기준 이자율은 연 1천분의 18이다(「국세기본법 시행규칙」 제19조의3).

다만, 법원의 판결에 의하여 과징금 부과처분이 취소되어 그 판결이유에 따라 새로운 과징금을 부과하는 경우에는 당초 납부한 과징금에서 새로 부과하기로 결정한 과징금을 공제한 나머지 금액에 대해서만 환급가산금을 계산하여 지급한다(제39조의15제8항).

제7장 개인정보 분쟁조정위원회

- 제40조 설치 및 구성
- 제41조 위원의 신분보장
- 제42조 위원의 제척·기피·회피
- 제43조 조정의 신청 등
- 제44조 처리기간
- 제45조 자료의 요청 등
- 제46조 조정 전 합의 권고
- 제47조 분쟁의 조정
- 제48조 조정의 거부 및 중지
- 제49조 집단분쟁조정
- 제50조 조정절차 등



제40조 | 설치 및 구성

법률

제40조(설치 및 구성) ① 개인정보에 관한 분쟁의 조정(調停)을 위하여 개인정보 분쟁조정위원회(이하 “분쟁조정위원회”라 한다)를 둔다.

② 분쟁조정위원회는 위원장 1명을 포함한 20명 이내의 위원으로 구성하며, 위원은 당연직위원과 위촉위원으로 구성한다.

③ 위촉위원은 다음 각 호의 어느 하나에 해당하는 사람 중에서 보호위원회 위원장이 위촉하고, 대통령령으로 정하는 국가기관 소속 공무원은 당연직위원이 된다.

1. 개인정보보호업무를 관장하는 중앙행정기관의 고위공무원단에 속하는 공무원으로 재직하였던 사람 또는 이에 상당하는 공공부문 및 관련 단체의 직에 재직하고 있거나 재직하였던 사람으로서 개인정보보호업무를 경험하는 사람

2. 대학이나 공인된 연구기관에서 부교수 이상 또는 이에 상당하는 직에 재직하고 있거나 재직하였던 사람

3. 판사·검사 또는 변호사로 재직하고 있거나 재직하였던 사람

4. 개인정보보호와 관련된 시민사회단체 또는 소비자단체로부터 추천을 받은 사람

5. 개인정보처리자로 구성된 사업자단체의 임원으로 재직하고 있거나 재직하였던 사람

④ 위원장은 위원 중에서 공무원이 아닌 사람으로 보호위원회 위원장이 임명한다.

⑤ 위원장과 위촉위원의 임기는 2년으로 하되, 1차에 한하여 연임할 수 있다.

⑥ 분쟁조정위원회는 분쟁조정 업무를 효율적으로 수행하기 위하여 필요하면 대통령령으로 정하는 바에 따라 조정사건의 분야별로 5명 이내의 위원으로 구성되는 조정부를 둘 수 있다. 이 경우 조정부가 분쟁조정위원회에서 위임받아 의결한 사항은 분쟁조정위원회에서 의결한 것으로 본다.

⑦ 분쟁조정위원회 또는 조정부는 재적위원 과반수의 출석으로 개의하며 출석위원 과반수의 찬성으로 의결한다.

⑧ 보호위원회는 분쟁조정 접수, 사실 확인 등 분쟁조정에 필요한 사무를 처리할 수 있다.

⑨ 이 법에서 정한 사항 외에 분쟁조정위원회 운영에 필요한 사항은 대통령령으로 정한다.

시행령

제48조의14(당연직위원) 분쟁위원회의 당연직위원은 보호위원회의 고위공무원단에 속하는 일반직공무원으로서 개인정보 보호에 관한 업무를 담당하는 사람 중 보호위원회 위원장이 지명하는 사람으로 한다.

제49조(조정부의 구성 및 운영) ① 법 제40조제6항에 따른 조정부(이하 “조정

부”라 한다)는 분쟁조정위원회 위원장이 지명하는 5명 이내의 위원으로 구성하되, 그 중 1명은 변호사 자격이 있는 위원으로 한다.

② 분쟁조정위원회 위원장은 조정부의 회의를 소집한다.

③ 분쟁조정위원회의 위원장은 조정부의 회의를 소집하려면 회의 날짜·시간·장소 및 안건을 정하여 회의 개최 7일 전까지 조정부의 각 위원에게 알려야 한다. 다만, 긴급한 사정이 있는 경우에는 그러하지 아니하다.

④ 조정부의 장은 조정부 위원 중에서 호선(互選)한다.

⑤ 제1항부터 제4항까지의 규정에서 정한 사항 외에 조정부의 구성 및 운영 등에 필요한 사항은 분쟁조정위원회의 의결을 거쳐 분쟁조정위원회의 위원장이 정한다.

제50조(사무기구) ① 법 제40조제8항에 따른 분쟁조정 접수 및 사실 확인 등 분쟁조정에 필요한 사무처리는 보호위원회의 사무기구가 수행한다.

② 사무기구는 분쟁조정 접수·진행 및 당사자 통지 등 분쟁조정에 필요한 사무를 전자적으로 처리하기 위하여 분쟁조정업무시스템을 구축하여 운영할 수 있다.

제51조(분쟁조정위원회 등의 운영) ① 분쟁조정위원회 위원장은 분쟁조정위원회의 회의를 소집하며, 그 의장이 된다.

② 분쟁조정위원회 위원장이 분쟁조정위원회의 회의를 소집하려면 회의 날짜·시간·장소 및 안건을 정하여 회의 개최 7일 전까지 각 위원에게 알려야 한다. 다만, 긴급한 사정이 있는 경우에는 그러하지 아니하다.

③ 분쟁조정위원회 및 조정부의 회의는 공개하지 아니한다. 다만, 필요하다고 인정되는 경우에는 분쟁조정위원회의 의결로 당사자 또는 이해관계인에게 방청을 하게 할 수 있다.

개인정보 유출, 오·남용 등으로 인한 손해는 정신적인 피해가 대부분이라서 소송을 통한 피해구제에는 한계가 있다. 소송에 의할 경우 고의·과실의 입증책임이 개인정보처리자에게 전환되어 있다고 하더라도 개인정보 침해사실, 손해 발생, 손해액, 손해와 침해 사이의 인과관계 등에 대한 입증책임을 여전히 정보주체가 부담해야 하기 때문에 승소할 가능성이 낮고, 소송에서 이기더라도 손해배상액(승소액)보다 소송에 소요되는 비용과 시간이 더 많은 사건이 대부분이라서 정보주체가 이를 감당하기 어렵다. 따라서 피해구제를 받는데 소요되는 비용과 시간을 획기적으로 절감하면서도 소송절차에 준해서 공정하게 피해구제를 받을 수 있는 장치로써 개인정보 피해구제 사건만을 전문적으로 다룰 객관적이고 독립적인 분쟁조정기구를 두도록 하고 있다.

1. 개인정보 분쟁조정위원회의 설치 및 구성

가 분쟁조정위원회의 설치

개인정보에 관한 분쟁의 조정(調停)을 위하여 개인정보 분쟁조정위원회를 두고 있다.

조정은 분쟁을 법원의 판결에 의하지 않고 조정위원회의 권고에 의하여 양당사자가 서로 양보하여 합의로서 해결하는 자주적 분쟁해결 절차로써 당사자의 자율성이 최대한 보장된다. 조정위원회는 권고만 하고 그 권고에 동의할 지 안 할지는 양 당사자의 자유이다. 하지만 당사자가 권고를 수락하여 조정이 성립되면 ‘재판상 화해’와 같이 법원의 확정 판결과 동일한 효력이 발생하게 된다.

나 분쟁조정위원회의 구성

분쟁조정위원회는 위원장 1명을 포함한 20명 이내의 위원으로 구성한다. 다만, 위원은 당연직위원과 위촉위원으로 구성한다(제2항). 당연직위원은 보호위원회의 고위공무원단에 속하는 일반직공무원으로서 개인정보 보호에 관한 업무를 담당하는 사람 중 보호위원회 위원장이 지명하는 사람으로 한다(영 제48조의14). 위촉위원은 분쟁조정위원의 자격에 해당하는 사람 중에서 보호위원회 위원장이 위촉한다(제3항). 공익 대표, 교수·법조인 등 전문가, 소비자(정보주체) 대표, 사업자(개인정보처리자) 대표 등 각계를 대표하는 전문가와 이해당사자가 참여하여 공정하고 객관적인 결정을 내릴 수 있도록 하기 위한 것이다. 위원장은 위원 중에서 공무원이 아닌 사람을 보호위원회 위원장이 임명하고(제4항), 위원장과 위촉위원의 임기는 2년으로 하되, 1차에 한하여 연임할 수 있다.

분쟁조정위원의 자격(제3항)

1. 개인정보보호업무를 관장하는 중앙행정기관의 고위공무원단에 속하는 공무원으로 재직 하였던 사람 또는 이에 상당하는 공공부문 및 관련 단체의 직에 재직하고 있거나 재직 하였던 사람으로서 개인정보 보호 업무의 경험이 있는 사람
2. 대학이나 공인된 연구기관에서 부교수 이상 또는 이에 상당하는 직에 재직하고 있거나 재직하였던 사람
3. 판사·검사 또는 변호사로 재직하고 있거나 재직하였던 사람
4. 개인정보보호와 관련된 시민사회단체 또는 소비자단체로부터 추천을 받은 사람
5. 개인정보처리자로 구성된 사업자단체의 임원으로 재직하고 있거나 재직하였던 사람

2. 조정부의 설치 및 구성

가 조정부의 설치

분쟁조정위원회는 분쟁조정 업무를 효율적으로 수행하기 위하여 필요하면 조정사건의 분야별로 5명 이내의 위원으로 구성되는 조정부를 둘 수 있다. 이 경우 조정부가 분쟁조정 위원회에서 위임받아 의결한 사항은 분쟁조정위원회에서 의결한 것으로 본다.

나 조정부의 구성

조정부는 분쟁조정위원회의 위원장이 지명하는 5명 이내의 위원으로 구성하되, 그 중 1명은 변호사의 자격이 있는 위원으로 한다(영 제49조제1항). 조정부의 장은 조정부의 위원 중에서 호선(互選)한다(영 제49조제4항).

다 조정부의 소집

조정부의 소집은 분쟁조정위원회 위원장이 한다(영 제49조제2항). 분쟁조정위원회의 위원장이 조정부의 회의를 소집하려면 회의 일시·장소 및 안건을 정하여 회의 개최 7일 전까지 조정부의 각 위원에게 알려야 한다. 다만, 긴급한 사정이 있는 경우에는 그러하지 아니할 수 있다(영 제49조제3항).

라 조정부의 구성·운영규칙

이 법과 시행령에서 정한 사항 외에 조정부의 구성 및 운영 등에 필요한 사항은 분쟁조정위원회의 의결을 거쳐 분쟁조정위원회의 위원장이 정한다.

3. 분쟁조정위원회 및 조정부의 개의 및 의결

분쟁조정위원회 또는 조정부는 재적위원 과반수의 출석으로 개의하며 출석위원 과반수의 찬성으로 의결한다(제7항).

4. 분쟁조정위원회 사무처리 및 조정부의 운영

가 분쟁조정위원회의 운영 지원

보호위원회는 분쟁조정 접수 및 사실 확인 등 분쟁조정에 필요한 사무를 처리할 수 있다(제40조제8항).

나 분쟁조정위원회의 사무처리

분쟁조정위원회의 분쟁조정 접수 및 사실 확인 등에 필요한 사무처리는 보호위원회의 사무기구가 수행한다(영 제50조제1항). 그 밖의 사무기구에서 수행하는 사무로는 분쟁조정 사건 접수창구의 운영, 조정전 합의권고, 조정결정서의 송달, 의사록의 작성·보관 등이 있다. 또한, 사무기구는 분쟁조정 접수·진행 및 당사자 통지 등 분쟁조정에 필요한 사무를 전자적으로 처리하기 위하여 분쟁조정업무시스템을 구축하여 운영할 수 있다(영 제50조제2항).

5. 분쟁조정위원회 등의 운영

분쟁조정위원회 회의의 소집은 분쟁조정위원회의 위원장이 하며, 그 의장이 된다(영 제51조제1항). 분쟁조정위원회의 위원장이 분쟁조정위원회의 회의를 소집하려면 회의 일시·장소 및 안건을 정하여 회의 개최 7일 전까지 각 위원에게 알려야 한다. 다만, 긴급한 사정이 있는 경우에는 그러하지 아니하다(영 제51조제2항).

분쟁조정위원회 및 조정부의 회의는 공개하지 아니한다. 다만, 필요하다고 인정되는 경우에는 분쟁조정위원회의 의결로 당사자 또는 이해관계인에게 방청을 하게 할 수 있다. 개인정보 분쟁조정 사건은 개인정보의 유출 또는 오·남용으로 인한 피해를 구제하고자 하는 것이므로 사생활 보호 차원에서 비공개를 원칙으로 한 것이다(영 제51조제3항).

제41조/제42조 | 위원의 신분보장

법률

제41조(위원의 신분보장) 위원은 자격정지 이상의 형을 선고받거나 심신상의 장애로 직무를 수행할 수 없는 경우를 제외하고는 그의 의사에 반하여 면직되거나 해촉되지 아니한다.

제42조(위원의 제척·기피·회피) ① 분쟁조정위원회의 위원은 다음 각 호의 어느 하나에 해당하는 경우에는 제43조제1항에 따라 분쟁조정위원회에 신청된 분쟁조정사건(이하 이 조에서 “사건”이라 한다)의 심의·의결에서 제척(除斥)된다.

1. 위원 또는 그 배우자나 배우자였던 자가 그 사건의 당사자가 되거나 그 사건에 관하여 공동의 권리자 또는 의무자의 관계에 있는 경우
2. 위원이 그 사건의 당사자와 친족이거나 친족이었던 경우
3. 위원이 그 사건에 관하여 증언, 감정, 법률자문을 한 경우
4. 위원이 그 사건에 관하여 당사자의 대리인으로서 관여하거나 관여하였던 경우

② 당사자는 위원에게 공정한 심의·의결을 기대하기 어려운 사정이 있으면 위원장에게 기피신청을 할 수 있다. 이 경우 위원장은 기피신청에 대하여 분쟁조정위원회의 의결을 거치지 아니하고 결정한다.

③ 위원이 제1항 또는 제2항의 사유에 해당하는 경우에는 스스로 그 사건의 심의·의결에서 회피할 수 있다.

분쟁조정제도는 준사법적 절차이기 때문에 조정의 독립성과 공정성이 보장되어야 한다. 이에 따라 법은 위원의 신분보장을 통해 분쟁조정 독립성을 보장하는 한편, 위원의 제척·기피·회피 제도를 도입하여 분쟁조정의 공정성을 확보하고 있다.

1. 분쟁조정의 독립성 보장

위원은 자격정지 이상의 형을 선고받거나 심신상의 장애로 직무를 수행할 수 없는 경우를 제외하고는 그의 의사에 반하여 면직되거나 해촉되지 아니한다. 자격정지 이상의 형의 종류에는 사형, 무기징역, 무기금고, 유기징역, 유기금고가 있다. 사형, 무기징역, 무기금고는 자격상실 사유에 해당하고, 유기징역 또는 유기금고는 그 형의 집행이 종료하거나 면제될 때까지 자격정지 사유에 해당한다(형법 제43조). 따라서 벌금, 구류, 과료, 몰수 등을 이유로 해당 위원을 면직하거나 해촉해서는 안 된다.

2. 분쟁조정 기 공정성 보장

가 제척사유

‘제척’이라 함은 분쟁조정사건의 심의·의결에서 배제되는 것을 의미한다. 분쟁조정위원회는 분쟁조정 제척사유에 해당하는 위원을 분쟁조정사건의 심의·의결에 포함시켜서는 안 된다.

분쟁조정 제척사유(제42조제1항)

1. 위원 또는 그 배우자나 배우자였던 자가 그 사건의 당사자가 되거나 그 사건에 관하여 공동의 권리자 또는 의무자의 관계에 있는 경우
2. 위원이 그 사건의 당사자와 친족이거나 친족이었던 경우
3. 위원이 그 사건에 관하여 증언, 감정, 법률자문을 한 경우
4. 위원이 그 사건에 관하여 당사자의 대리인으로서 관여하거나 관여하였던 경우

나 기피사유

‘기피’란 당사자의 일방 또는 쌍방이 분쟁조정사건의 심의·의결에서 특정 위원을 배제시켜 달라고 요구하는 것을 의미한다. 당사자는 특정 위원에게 공정한 심의·의결을 기대하기 어려운 사정이 있으면 위원장에게 기피신청을 할 수 있다. 이 경우 위원장은 기피신청에 대하여 단독으로 결정한다.

다 회피사유

‘회피’란 위원이 공정한 결정을 내리기 곤란하다고 인정할만한 상당한 사유가 있는 경우에 특정 분쟁조정사건의 심의·의결에서 스스로 빠지는 것을 말한다. 위원은 특정 사건이 제1항 또는 제2항의 사유에 해당하는 경우에는 스스로 그 사건의 심의·의결에 참여하지 않을 수 있다.

제43조(조정 신청 등) ① 개인정보와 관련한 분쟁의 조정을 원하는 자는 분쟁 조정위원회에 분쟁조정을 신청할 수 있다.

② 분쟁조정위원회는 당사자 일방으로부터 분쟁조정 신청을 받았을 때에는 그 신청내용을 상대방에게 알려야 한다.

③ 공공기관이 제2항에 따른 분쟁조정의 통지를 받은 경우에는 특별한 사유가 없으면 분쟁조정에 응하여야 한다.

제44조(처리기간) ① 분쟁조정위원회는 제43조제1항에 따른 분쟁조정 신청을 받은 날부터 60일 이내에 이를 심사하여 조정안을 작성하여야 한다. 다만, 부득이한 사정이 있는 경우에는 분쟁조정위원회의 의결로 처리기간을 연장할 수 있다.

② 분쟁조정위원회는 제1항 단서에 따라 처리기간을 연장한 경우에는 기간연장의 사유와 그 밖의 기간연장에 관한 사항을 신청인에게 알려야 한다.

제45조(자료의 요청 등) ① 분쟁조정위원회는 제43조제1항에 따라 분쟁조정 신청을 받았을 때에는 해당 분쟁의 조정을 위하여 필요한 자료를 분쟁당사자에게 요청할 수 있다. 이 경우 분쟁당사자는 정당한 사유가 없으면 요청에 따라야 한다.

② 분쟁조정위원회는 필요하다고 인정하면 분쟁당사자나 참고인을 위원회에 출석하도록 하여 그 의견을 들을 수 있다.

제46조(조정 전 합의 권고) 분쟁조정위원회는 제43조제1항에 따라 분쟁조정 신청을 받았을 때에는 당사자에게 그 내용을 제시하고 조정 전 합의를 권고할 수 있다.

제47조(분쟁의 조정) ① 분쟁조정위원회는 다음 각 호의 어느 하나의 사항을 포함하여 조정안을 작성할 수 있다.

1. 조사 대상 침해행위의 중지
2. 원상회복, 손해배상, 그 밖에 필요한 구제조치
3. 같거나 비슷한 침해의 재발을 방지하기 위하여 필요한 조치

② 분쟁조정위원회는 제1항에 따라 조정안을 작성하면 지체 없이 각 당사자에게 제시하여야 한다.

③ 제1항에 따라 조정안을 제시받은 당사자가 제시받은 날부터 15일 이내에 수락 여부를 알리지 아니하면 조정을 거부한 것으로 본다.

④ 당사자가 조정내용을 수락한 경우 분쟁조정위원회는 조정서를 작성하고, 분쟁조정위원회의 위원장과 각 당사자가 기명날인하여야 한다.

⑤ 제4항에 따른 조정의 내용은 재판상 화해와 동일한 효력을 갖는다.

- 제48조(조정)의 거부 및 중지** ① 분쟁조정위원회는 분쟁의 성질상 분쟁조정위원회에서 조정하는 것이 적합하지 아니하다고 인정하거나 부정한 목적으로 조정이 신청되었다고 인정하는 경우에는 그 조정을 거부할 수 있다. 이 경우 조정거부의 사유 등을 신청인에게 알려야 한다.
- ② 분쟁조정위원회는 신청된 조정사건에 대한 처리절차를 진행하던 중에 한쪽 당사자가 소를 제기하면 그 조정의 처리를 중지하고 이를 당사자에게 알려야 한다.

1. 분쟁조정 신청 등

가 분쟁조정 신청

개인정보와 관련한 분쟁의 조정을 원하는 자는 누구든지 분쟁조정위원회에 분쟁조정을 신청할 수 있다. 정보주체뿐만 아니라 개인정보처리자도 신청할 수 있다. 분쟁조정 신청은 분쟁조정위원회 홈페이지나 서면(방문, 팩스, 우편, 전자우편)으로 가능하다.

분쟁조정 신청사유에 대해서도 특별한 제한을 두고 있지 않으므로 신청사유는 개인정보 처리와 관련하여 당사자 사이에 분쟁이 있으면 충분하다.

신청의 내용은 법령 위반행위의 금지·중지 또는 손해배상의 청구 뿐만 아니라, 개인정보 열람, 정정, 삭제 등의 요구와 같은 적극적인 이행 청구도 포함된다.

나 조정신청사실의 통지 등

분쟁조정위원회는 당사자 일방으로부터 분쟁조정 신청을 접수 받았을 때에는 그 신청 내용을 상대방에게 알려야 한다. 정보주체가 신청한 경우에는 개인정보처리자에게, 개인정보처리자가 신청한 경우에는 정보주체에게 각각 통지하여 조정에 대비하도록 하여야 한다.

다 공공기관의 특례

분쟁조정은 강제적 조정절차가 아니므로 통지를 받은 상대방은 자유롭게 조정절차에 참여 여부를 결정할 수 있으나, 공공기관이 분쟁조정의 통지를 받은 경우에는 특별한 사유가 없는 한 분쟁조정 절차에 응해야 한다. 이는 민간 기업이나 단체와 달리 공공기관은 국민의 권리·

이익을 보호하기 위하여 존재하는 것이고, 행정기관의 장이 민원의 신청을 받았을 때 다른 법령에 특별한 규정이 있는 경우를 제외하고는 그 접수를 보류하거나 거부할 수 없도록 규정하고 있는 「민원 처리에 관한 법률」 제9조제1항의 취지를 고려한 것이다.

2. 분쟁조정외 처리 기간

분쟁의 신속한 해결을 위하여 분쟁조정위원회는 분쟁조정외 신청을 접수받은 날부터 60일 이내에 이를 심사하여 조정안을 작성하여야 한다. 다만, 부득이한 사정이 있는 경우에는 분쟁조정위원회의 의결로 처리기간을 연장할 수 있으나, 이 경우 분쟁조정위원회는 기간연장의 사유와 그 밖의 기간연장에 관한 사항을 신청인에게 알려야 한다.

3. 자료제출·출석 등의 요청

객관적 사실에 입각한 공정한 조정결정을 위하여 분쟁조정위원회는 분쟁조정외에 필요한 자료를 분쟁당사자에게 요청할 수 있고 분쟁당사자 또는 참고인을 위원회에 출석하게 하여 의견을 들을 수도 있다.

자료제출 요청을 받은 분쟁당사자는 정당한 사유가 없는 한 그 요청에 따라야 한다. 정당한 사유로는 영업비밀 보호, 타인의 사생활 보호, 국가 안보 및 외교상 이익 등이 있을 수 있다.

4. 조정 전 합의 권고

분쟁조정위원회는 분쟁조정 신청을 받았을 때에는 당사자에게 그 내용을 제시하고 조정 전 합의를 권고할 수 있다. 여기서 “그 내용을 제시” 라고 함은 당사자가 제시한 조건을 상대방에게 전달하고 합의 여부를 확인하는 것을 말한다. 위원회는 조정심의 전에 양 당사자가 합의에 이른 경우 신청 건에 대해 ‘조정 전 합의’ 로 종결할 수 있다. 분쟁은 당사자의 자발적 합의에 의해 스스로 처리하는 것이 가장 바람직하다는 점에서 이 제도의 의의가 있다.

5. 분쟁의 조정

가 조정안의 작성 및 제시

사실조사, 의견청취, 전문가 자문 등이 끝나면 분쟁조정위원회는 ① 조사 대상 침해행위의 중지(개인정보 열람, 정정, 삭제 등 적극적 조치 포함) ② 원상회복, 손해배상, 그 밖에 필요한 구제조치 ③ 같거나 비슷한 침해의 재발을 방지하기 위하여 필요한 조치 중 어느 사항의 하나를 포함한 조정안을 작성하고 이를 지체 없이 각 당사자에게 제시하여야 한다.

나 조정안의 수락 및 거부

분쟁당사자가 조정안을 제시받은 날부터 15일 이내에 수락 여부를 알리지 아니하면 조정안을 거부한 것으로 본다(제3항). 양 당사자 중 한 사람이라도 수락의 의사표시를 하지 않으면 조정안은 거부된 것으로 본다. 따라서 당사자가 조정 내용을 수락하고자 하는 경우에는 15일 이내에 분쟁조정위원회에 수락 의사를 알려야 한다. 당사자가 조정 내용을 수락한 경우 분쟁조정위원회는 조정서를 작성하고, 분쟁조정위원회의 위원장과 각 당사자가 이에 기명날인을 하여야 한다. 다만, 양 당사자가 분쟁조정위원회가 제시한 조정수락서에 기명날인한 것은 조정서에 기명날인한 것으로 본다.

다 분쟁조정 성립의 법적 효력

분쟁당사자가 조정안을 수락하여 분쟁조정이 성립되면 조정의 내용은 재판상 화해와 동일한 효력을 갖는다. 재판상 화해의 효력은 확정판결과 같은 효력을 의미하므로 조정안 수락으로 분쟁은 최종적으로 종료되고 조정조서에 의하여 강제집행도 가능하게 된다(「민사소송법」 제220조). 즉 추후에 조정 내용에 대해서 불복사유가 발견되더라도 소송을 통해 그 효력을 다툴 수 없고, 그 효력은 오로지 준재심의 절차에 의해서만 다툴 수 있다(「민사소송법」 제461조).

6. 조정의 진행 거부 및 중지

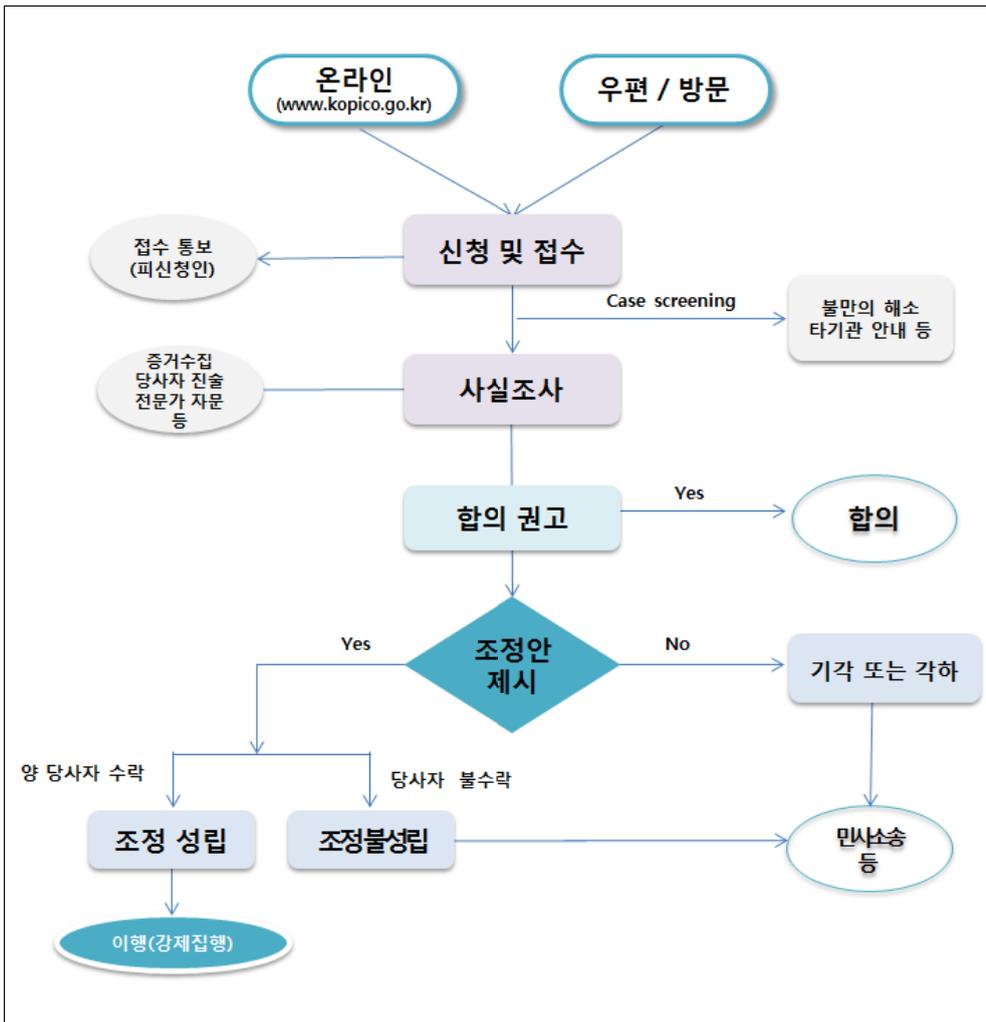
분쟁조정위원회는 분쟁의 성질상 분쟁조정위원회에서 조정하는 것이 적합하지 아니하다고 인정하거나 부정한 목적으로 조정이 신청되었다고 인정하는 경우에는 그 조정을 거부할 수 있다. 이 경우 조정거부의 사유 등을 신청인에게 알려야 한다.

사례 분쟁조정 거부 사유

1. 개인정보처리와 관련한 분쟁이 아닌 경우
2. 신청자가 악의적으로 같은 사건에 대해 계속적으로 분쟁조정을 신청하는 경우
3. 관계 법령 또는 객관적인 증빙 등에 의하여 조정의 실익이 없는 경우 등

분쟁조정위원회는 신청된 조정사건에 대한 처리절차를 진행하던 중에 한 쪽 당사자가 소를 제기하면 그 조정의 처리를 중지하고 이를 당사자에게 알려야 한다. 사실상 조정절차에 따를 의사가 없다고 보기 때문이다.

< 분쟁조정 절차도 >



제49조 | 집단분쟁조정

법률

제49조(집단분쟁조정) ① 국가 및 지방자치단체, 개인정보보호단체 및 기관, 정보주체, 개인정보처리자는 정보주체의 피해 또는 권리침해가 다수의 정보주체에 게 같거나 비슷한 유형으로 발생하는 경우로서 대통령령으로 정하는 사건에 대하여는 분쟁조정위원회에 일괄적인 분쟁조정(이하 “집단분쟁조정”이라 한다)을 의뢰 또는 신청할 수 있다.

② 제1항에 따라 집단분쟁조정을 의뢰받거나 신청받은 분쟁조정위원회는 그 의결로써 제3항부터 제7항까지의 규정에 따른 집단분쟁조정의 절차를 개시할 수 있다. 이 경우 분쟁조정위원회는 대통령령으로 정하는 기간 동안 그 절차의 개시를 공고하여야 한다.

③ 분쟁조정위원회는 집단분쟁조정의 당사자가 아닌 정보주체 또는 개인 정보처리자로부터 그 분쟁조정의 당사자에 추가로 포함될 수 있도록 하는 신청을 받을 수 있다.

④ 분쟁조정위원회는 그 의결로써 제1항 및 제3항에 따른 집단분쟁조정의 당사자 중에서 공동의 이익을 대표하기에 가장 적합한 1인 또는 수인을 대표 당사자로 선임할 수 있다.

⑤ 분쟁조정위원회는 개인정보처리자가 분쟁조정위원회의 집단분쟁조정의 내용을 수락한 경우에는 집단분쟁조정의 당사자가 아닌 자로서 피해를 입은 정보주체에 대한 보상계획서를 작성하여 분쟁조정위원회에 제출하도록 권고할 수 있다.

⑥ 제48조제2항에도 불구하고 분쟁조정위원회는 집단분쟁조정의 당사자인 다수의 정보주체 중 일부의 정보주체가 법원에 소를 제기한 경우에는 그 절차를 중지하지 아니하고, 소를 제기한 일부의 정보주체를 그 절차에서 제외한다.

⑦ 집단분쟁조정의 기간은 제2항에 따른 공고가 종료된 날의 다음 날부터 60일 이내로 한다. 다만, 부득이한 사정이 있는 경우에는 분쟁조정위원회의 의결로 처리기간을 연장할 수 있다.

⑧ 집단분쟁조정의 절차 등에 관하여 필요한 사항은 대통령령으로 정한다.

시행령

제52조(집단분쟁조정의 신청 대상) 법 제49조제1항에서 “대통령령으로 정하는 사건”이란 다음 각 호의 요건을 모두 갖춘 사건을 말한다.

1. 피해 또는 권리침해를 입은 정보주체의 수가 다음 각 목의 정보주체를 제외하고 50명 이상일 것
 - 가. 개인정보처리자와 분쟁해결이나 피해보상에 관한 합의가 이루어진 정보주체
 - 나. 같은 사안으로 다른 법령에 따라 설치된 분쟁조정기구에서 분쟁조정 절차가 진행 중인 정보주체

다. 해당 개인정보 침해로 인한 피해에 대하여 법원에 소(訴)를 제기한 정보주체

2. 사건의 중요한 쟁점이 사실상 또는 법률상 공통될 것

제53조(집단분쟁조정 절차의 개시) ① 법 제49조제2항 후단에서 “대통령령으로 정하는 기간” 이란 14일 이상의 기간을 말한다.

② 법 제49조제2항 후단에 따른 집단분쟁조정 절차의 개시 공고는 분쟁조정위원회의 인터넷 홈페이지 또는 「신문 등의 진흥에 관한 법률」에 따라 전국을 보급지역으로 하는 일반일간신문에 게재하는 방법으로 한다.

제54조(집단분쟁조정 절차에 대한 참가 신청) ① 법 제49조에 따른 집단분쟁조정(이하 “집단분쟁조정”이라 한다)의 당사자가 아닌 정보주체 또는 개인정보처리자가 법 제49조제3항에 따라 추가로 집단분쟁조정의 당사자로 참가하려면 법 제49조제2항 후단의 공고기간에 문서로 참가 신청을 하여야 한다.

② 분쟁조정위원회는 제1항에 따라 집단분쟁조정 당사자 참가 신청을 받으면 제1항의 신청기간이 끝난 후 10일 이내에 참가 인정 여부를 문서로 알려야 한다.

제55조(집단분쟁조정 절차의 진행) ① 집단분쟁조정 절차가 개시된 후 제52조제1호가목부터 다목까지의 어느 하나에 해당하게 된 정보주체는 당사자에서 제외된다.

② 분쟁조정위원회는 제52조 각 호의 요건을 모두 갖춘 사건에 대하여 집단분쟁조정 절차가 개시되고 나면 그 후 집단분쟁조정 당사자 중 일부가 같은 조 제1호가목부터 다목까지의 어느 하나에 해당하게 되어 같은 조 제1호의 요건을 갖추지 못하게 되더라도 집단분쟁조정 절차를 중지하지 아니한다.

개인정보 유출사고와 오·남용사고는 대부분 집단성을 띠고 있고, 유출되거나 오·남용된 개인정보의 항목이나 피해의 유형도 같거나 비슷하다. 이처럼 작게는 수천 건에서 많게는 수천만 건에 이르는 개인정보 유출 및 오남용 사건을 개별적인 분쟁조정절차를 통해서 처리하는 것은 시간적으로나 비용적으로 낭비이다. 따라서 이와 같은 집단적 분쟁사건에 대해서는 하나의 분쟁조정절차에서 일괄적으로 해결하는 것이 편리하고 효율적이다.

1. 집단분쟁조정 의뢰 및 신청

가 집단분쟁조정 의뢰자 및 신청자

분쟁조정위원회에 일괄적인 분쟁조정(집단분쟁조정)을 의뢰하거나 신청할 수 있는 자는 ① 국가 및 지방자치단체 ② 개인정보보호단체 및 기관 ③ 정보주체 ④ 개인정보처리자이다.

집단분쟁조정을 의뢰할 수 있는 개인정보보호단체 및 기관의 자격에는 제한이 없다. 따라서 개인정보 보호 업무를 수행하는 단체나 기관은 누구든지 집단분쟁조정을 의뢰할 수 있으며, 기업들이 설립한 개인정보 보호 단체나 국가·지자체 등이 설립한 공공기관도 가능하다.

나 집단분쟁조정 신청대상 사건

집단분쟁조정의 신청대상이 되기 위해서는 정보주체의 피해 또는 권리침해가 다수의 정보주체에게 같거나 비슷한 유형으로 발생했어야 하며(제49조제1항), 집단분쟁조정 신청 요건을 모두 갖춘 사건이어야 한다(영 제52조).

집단분쟁조정 신청요건(영 제52조)

1. 피해 또는 권리침해를 입은 정보주체의 수가 다음 각 목의 정보주체를 제외하고 50명 이상일 것
 - 가. 개인정보처리자와 분쟁해결이나 피해보상에 관한 합의가 이루어진 정보주체
 - 나. 같은 사안으로 다른 법령에 따라 설치된 분쟁조정기구에서 분쟁조정 절차가 진행 중인 정보주체
 - 다. 해당 개인정보 침해로 인한 피해에 대하여 법원에 소(訴)를 제기한 정보주체
2. 사건의 중요한 쟁점이 사실상 또는 법률상 공통될 것

2. 집단분쟁조정절차의 개시 및 공고

가 집단분쟁조정절차 개시·공고

집단분쟁조정을 의뢰받거나 신청받은 분쟁조정위원회는 그 의결로써 집단분쟁조정절차를 개시할 수 있다(제49조제2항 전단).

분쟁조정위원회가 집단분쟁조정절차를 개시하고자 하는 경우에는 14일 이상의 기간 동안 그 절차의 개시를 공고하여야 한다(제49조제2항 후단, 영 제53조제1항).

집단분쟁조정 절차의 개시 공고는 분쟁조정위원회의 인터넷 홈페이지 또는 「신문 등의 진흥에 관한 법률」에 따라 전국을 보급지역으로 하는 일반일간신문에 게재하는 방법으로 한다(영 제53조제2항).

나 집단분쟁조정의 추가신청

집단분쟁조정의 당사자가 아닌 정보주체 또는 개인정보처리자가 추가로 집단분쟁조정의 당사자로 참가하려면 집단분쟁조정절차 개시 공고기간 내에 문서로 참가 신청을 하여

야 한다. 분쟁조정위원회가 집단분쟁조정의 당사자 참가 신청을 받으면 집단분쟁조정절차 개시 공고기간(참가 신청기간)이 끝난 후 10일 이내에 참가인정 여부를 문서로 알려야 한다 (영 제54조제2항).

다 대표당사자의 선임

분쟁조정위원회는 그 의결로써 집단분쟁조정의 당사자 중에서 공동의 이익을 대표하기에 가장 적합한 1인 또는 다수를 대표당사자로 선임할 수 있다.

3. 당사자 이외의 자에 대한 보상

분쟁조정위원회는 개인정보처리자가 분쟁조정위원회의 집단분쟁조정의 내용을 수락한 경우에는 집단분쟁조정의 당사자가 아닌 자로서 피해를 입은 정보주체에 대한 보상계획서를 작성하여 분쟁조정위원회에 제출하도록 권고할 수 있다. 사업자가 권고를 수락하는 경우 15일 이내에 보상계획서를 제출하여야 하고, 위원회는 이를 홈페이지에 공개한다. 사업자는 보상계획서에 ‘피해자가 계획서에 동의하고 계획대로 집행될 경우 당해 피해자에 대한 보상은 종결된 것으로 본다’ 는 문구를 삽입할 수 있다. 다만, 사업자가 보상계획서의 보상을 피해자에게 하지 못할 경우 피해자는 금전 채권에 대한 강제 집행을 법원에 신청하여 해결할 수 있다.

4. 집단분쟁조정절차의 제외

법 제48조제2항(소제기에 따른 분쟁조정절차의 중지)에도 불구하고 분쟁조정위원회는 집단분쟁조정의 당사자인 다수의 정보주체 중 일부의 정보주체가 법원에 소를 제기한 경우에는 그 절차를 중지하지 아니하고 조정절차를 계속 진행하여야 한다. 다만, 소를 제기한 정보주체들은 그 절차에서 제외하여야 한다(제49조제6항).

집단분쟁조정 신청사건이 영 제52조 각 호의 요건을 모두 갖추어 집단분쟁조정 절차가 개시된 후에 집단분쟁조정 신청 당사자 중 일부가 집단분쟁조정 신청 결정사유(영 제52조제1호가목부터 다목까지에 해당하는 자)에 해당하더라도 나머지 사람들에게 대한 집단분쟁조정 절차는 중지되지 아니한다. 다만, 집단분쟁조정 절차가 개시된 후 집단분쟁조정 신청 결정사유에 해당하게 된 자는 당사자에서 제외하여야 한다(영 제55조제1항).

5. 집단분쟁조정 성립의 법적 효력

집단분쟁조정이 성립된 경우의 법적 효력은 일반 분쟁조정の場合와 같다. 즉 당사자가 조정안을 수락한 경우에는 재판상 화해와 동일한 효력이 발생한다. 다수의 정보주체 중 일부만이 조정안을 수락한 경우에는 수락한 사람에 한해서만 재판상 화해의 효력이 미친다.

6. 집단분쟁조정 기간

집단분쟁조정 기간은 집단분쟁조정절차 개시 공고기간이 종료된 날의 다음 날부터 60일 이내로 한다. 다만, 부득이 한 사정이 있는 경우에는 분쟁조정위원회의 의결로 처리기간을 연장할 수 있다.

참고 소비자기본법

제68조(분쟁조정특례) ① 제65조제1항의 규정에 불구하고, 국가·지방자치단체·한국소비자원·소비자단체·소비자 또는 사업자는 소비자의 피해가 다수의 소비자에게 같거나 비슷한 유형으로 발생하는 경우로서 대통령령이 정하는 사건에 대하여는 조정위원회에 일괄적인 분쟁조정(이하 “집단분쟁조정”이라 한다)을 의뢰 또는 신청할 수 있다.

②제1항의 규정에 따라 집단분쟁조정을 의뢰받거나 신청받은 조정위원회는 다음 각 호의 어느 하나에 해당하는 사건을 제외하고는 조정위원회의 의결로써 의뢰받거나 신청받은 날부터 60일 이내에 제4항부터 제7항까지의 규정에 따른 집단분쟁조정 절차를 개시하여야 한다. 이 경우 조정위원회는 대통령령이 정하는 기간동안 그 절차의 개시를 공고하여야 한다.

1. 제1항의 요건을 갖추지 못한 사건
2. 기존의 집단분쟁조정결정이 있는 사건으로서 개시의결을 반복할 필요가 없다고 인정되는 사건
3. 신청인의 신청내용이 이유가 없다고 명백하게 인정되는 사건

③ 제2항에도 불구하고 조정위원회는 다음 각 호의 어느 하나에 해당하는 사건에 대하여는 제2항에 따른 개시결정기간 내에 조정위원회의 의결로써 집단분쟁조정 절차개시의 결정을 보류할 수 있다. 이 경우 그 사유와 기한을 명시하여 의뢰 또는 신청한 자에게 통지하여야 하고, 그 보류기간은 제2항에 따른 개시결정기간이 경과한 날부터 60일을 넘을 수 없다.

1. 피해의 원인규명에 시험, 검사 또는 조사가 필요한 사건
2. 피해의 원인규명을 위하여 제68조의2에 따른 대표당사자가 집단분쟁조정 절차개시 결정의 보류를 신청하는 사건

④조정위원회는 집단분쟁조정 당사자가 아닌 소비자 또는 사업자로부터 그 분쟁조정 당사자에 추가로 포함될 수 있도록 하는 신청을 받을 수 있다.

⑤ 조정위원회는 사업자가 조정위원회의 집단분쟁조정 내용을 수락한 경우에는 집단분쟁조정 당사자가 아닌 자로서 피해를 입은 소비자에 대한 보상계획서를 작성하여 조

정위원회에 제출하도록 권고할 수 있다.

⑥ 제65조제5항의 규정에 불구하고 조정위원회는 집단분쟁조정 당사자인 다수의 소비자 중 일부의 소비자가 법원에 소를 제기한 경우에는 그 절차를 중지하지 아니하고, 소를 제기한 일부의 소비자를 그 절차에서 제외한다.

⑦ 제66조제1항에도 불구하고 집단분쟁조정은 제2항에 따른 공고가 종료된 날의 다음 날부터 30일 이내에 마쳐야 한다. 다만, 정당한 사유가 있는 경우로서 해당 기간 내에 분쟁 조정을 마칠 수 없는 때에는 2회에 한하여 각각 30일의 범위에서 그 기간을 연장할 수 있으며, 이 경우 그 사유와 기한을 구체적으로 밝혀 당사자 및 그 대리인에게 통지하여야 한다.

⑧ 집단분쟁조정의 절차 등에 관하여 필요한 사항은 대통령령으로 정한다.

제68조의2(대표당사자의 선임 등) ① 집단분쟁조정에 이해관계가 있는 당사자들은 그 중 3명 이하를 대표당사자로 선임할 수 있다.

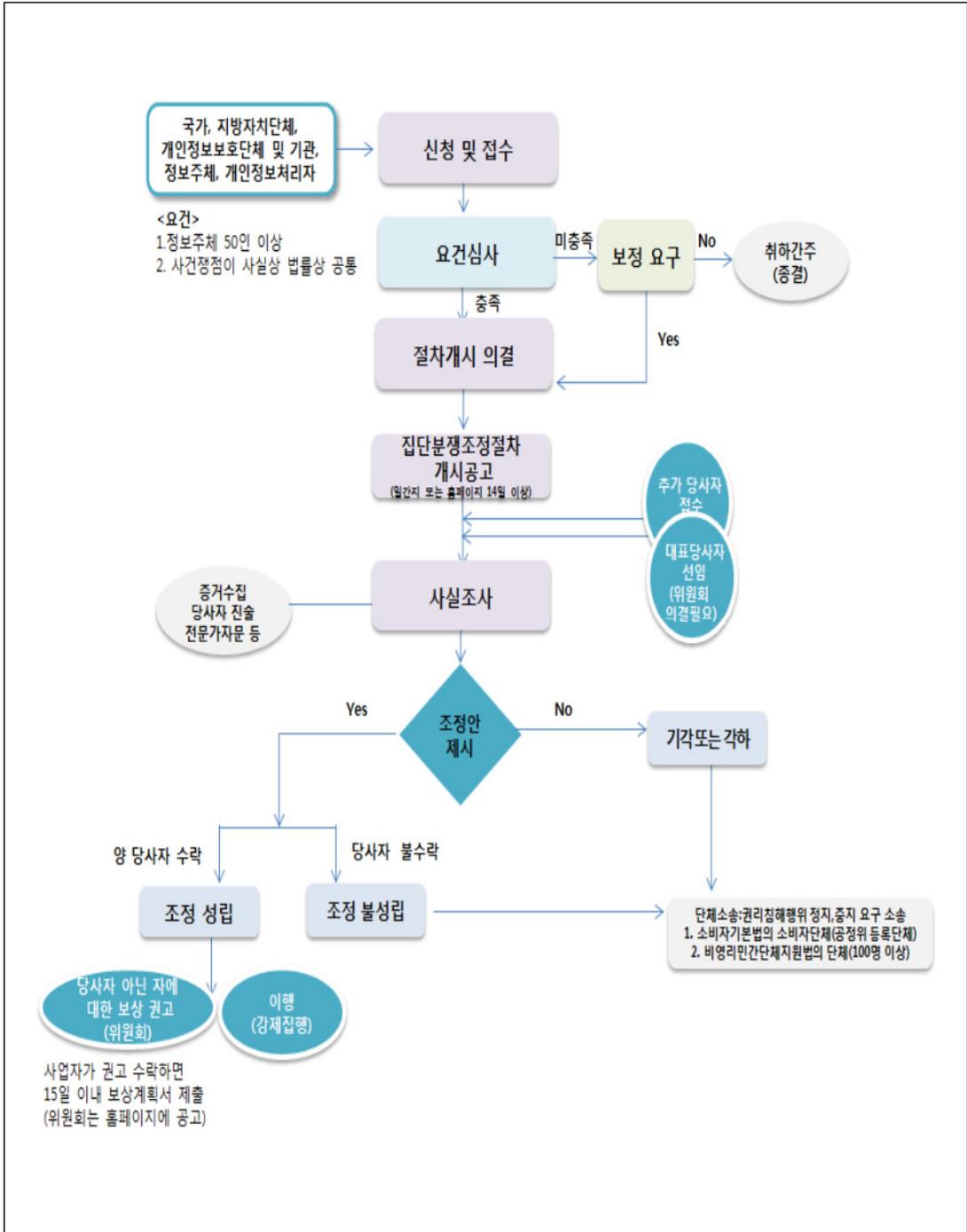
② 조정위원회는 당사자들이 제1항에 따라 대표당사자를 선임하지 아니한 경우에 필요하다고 인정하는 때에는 당사자들에게 대표당사자를 선임할 것을 권고할 수 있다.

③ 대표당사자는 자기를 선임한 당사자들을 위하여 그 사건의 조정에 관한 모든 행위를 할 수 있다. 다만, 조정신청의 철회 및 조정안의 수락·거부는 자기를 선임한 당사자들의 서면에 의한 동의를 받아야 한다.

④ 대표당사자를 선임한 당사자들은 대표당사자를 통하여서만 그 사건의 조정에 관한 행위를 할 수 있다.

⑤ 대표당사자를 선임한 당사자들은 필요하다고 인정하는 경우에는 대표당사자를 해임하거나 변경할 수 있다. 이 경우 당사자들은 그 사실을 지체 없이 조정위원회에 통지하여야 한다.

< 집단분쟁조정 절차도 >



제50조 | 조정절차 등

법률	<p>제50조(조정절차 등) ① 제43조부터 제49조까지의 규정에서 정한 것 외에 분쟁의 조정방법, 조정절차 및 조정업무의 처리 등에 필요한 사항은 대통령령으로 정한다.</p> <p>② 분쟁조정위원회의 운영 및 분쟁조정 절차에 관하여 이 법에서 규정하지 아니한 사항에 대하여는 「민사조정법」을 준용한다.</p>
시행령	<p>제56조(수당과 여비) 분쟁조정위원회 및 조정부의 회의에 출석한 위원 등에게는 예산의 범위에서 수당과 여비를 지급할 수 있다. 다만, 공무원인 위원이 그 소관 업무와 직접적으로 관련되어 출석하는 경우에는 그러하지 아니하다.</p> <p>제57조(분쟁조정 세칙) 법 및 이 영에서 규정한 사항 외에 분쟁조정위원회의 운영 및 집단분쟁조정을 위하여 필요한 사항은 분쟁조정위원회의 의결을 거쳐 분쟁조정위원회의 위원장이 정한다.</p>

1. 「민사조정법」의 준용

분쟁조정위원회의 운영 및 분쟁조정 절차에 관하여 이 법에서 규정하지 아니한 사항에 대하여는 「민사조정법」을 준용한다.

2. 조정위원회에 대한 수당 등의 지급

분쟁조정위원회 및 조정부의 회의에 출석한 위원 등에게는 예산의 범위에서 수당과 여비를 지급할 수 있다. 다만, 공무원인 위원이 그 소관업무와 직접적으로 관련되어 출석하는 경우에는 그러하지 아니하다(영 제56조).

3. 「분쟁조정세칙」의 제정

이 법 및 영에서 규정한 것 외에 분쟁조정위원회의 운영 및 집단분쟁조정을 위하여 필요한 사항은 분쟁조정위원회의 의결을 거쳐 위원장이 정한다(영 제57조).

< 유사분쟁조정위원회 현황 및 비교 >

구 분	개인정보분쟁조정위원회 (개인정보 보호법)	공공데이터제공분쟁조정위원회 (공공데이터법)	소비자분쟁조정위원회 (소비자기본법)
설립 목적	개인정보에 관한 분쟁의 조정	공공데이터 제공거부 및 제공중단에 관한 분쟁조정	소비자와 사업자 사이에 발생한 분쟁을 조정
위 상	보호위원회 산하	행정안전부장관 소속	한국소비자원
위원회 구성	위원장 1명을 포함한 20명 이내의 위원	위원장 1인 포함 25명 이내	위원장 1인을 포함한 150인 이내의 위원
위원 임기	2년(1차에 한하여 연임) * 공무원은 보직 기간동안 재임	2년(1차에 한하여 연임)	3년으로 하며, 연임가능
위원 임명	보호위원회 위원장이 위촉	행정안전부장관이 위촉	공정거래위원회위원장이 임명 또는 위촉
위원장 임명	위원중 공무원이 아닌 사람으로, 보호위원회 위원장이 위촉	위원중 공무원이 아닌 사람으로 행정안전부장관이 임명	상임위원 중 공정거래위원장이 임명
상임 여부	1명은 상임위원	1명은 상임위원	위원장을 포함한 5인은 상임
조정 의 효력	재판상 화해	재판상 화해	재판상 화해
조정 전 합의 권고	有	有	無(소비자원 등의 합의 권고가 전제된 사건에 한 해 신청 가능)
사무국	보호위원회	공공데이터활용지원센터 (한국정보화진흥원)	한국소비자원
기타	- 조정기간 : 60일 - 조정의 거부 및 중지 - 위원의 신분보장, 제척·기피·회피	- 조정기간 : 30일 - 조정의 거부 및 중지 - 위원의 신분보장, 제척·기피·회피	- 조정기간 : 30일 - 조정의 중지 - 위원의 신분보장, 제척·기피·회피

제8장 개인정보 단체소송

- 제51조 단체소송의 대상 등
- 제52조 전속관할
- 제53조 소송대리인의 선임
- 제54조 소송허가신청
- 제55조 소송허가요건 등
- 제56조 확정판결의 효력
- 제57조 「민사소송법」의 적용 등



제51조(단체소송의 대상 등) 다음 각 호의 어느 하나에 해당하는 단체는 개인 정보처리자가 제49조에 따른 집단분쟁조정을 거부하거나 집단분쟁조정 결과에 수락하지 아니한 경우에는 법원에 권리침해 행위의 금지·중지를 구하는 소송(이하 “단체소송”이라 한다)을 제기할 수 있다.

1. 「소비자기본법」 제29조에 따라 공정거래위원회에 등록된 소비자단체로서 다음 각 목의 요건을 모두 갖춘 단체
 - 가. 정관에 따라 상시적으로 정보주체의 권익증진을 주된 목적으로 하는 단체일 것
 - 나. 단체의 정회원수가 1천명 이상일 것
 - 다. 「소비자기본법」 제29조에 따른 등록 후 3년이 경과하였을 것
2. 「비영리민간단체 지원법」 제2조에 따른 비영리민간단체로서 다음 각 목의 요건을 모두 갖춘 단체
 - 가. 법률상 또는 사실상 동일한 침해를 입은 100명 이상의 정보주체로부터 단체소송의 제기를 요청받을 것
 - 나. 정관에 개인정보보호를 단체의 목적으로 명시한 후 최근 3년 이상 이를 위한 활동 실적이 있을 것
 - 다. 단체의 상시 구성원수가 5천명 이상일 것
 - 라. 중앙행정기관에 등록되어 있을 것

제52조(전속관할) ① 단체소송의 소는 피고의 주된 사무소 또는 영업소가 있는 곳, 주된 사무소나 영업소가 없는 경우에는 주된 업무담당자의 주소가 있는 곳의 지방법원 본원 합의부의 관할에 전속한다.

- ② 제1항을 외국사업자에 적용하는 경우 대한민국에 있는 이들의 주된 사무소·영업소 또는 업무담당자의 주소에 따라 정한다.

제53조(소송대리인의 선임) 단체소송의 원고는 변호사를 소송대리인으로 선임하여야 한다.

1. 개인정보 단체소송의 의의

시장경제의 지속적인 발전, IT의 급격한 발달 등으로 인해 개인정보 침해로 인한 피해의 확산속도는 빨라져 가고 그 피해규모 또한 점차 대형화되고 있음에 반해 피해를 입은 불특정 다수의 개인들은 여전히 비조직화·파편화된 상황에 머물러 있다. 이와 같이 개인정보 침해유발자와 침해피해자 사이의 비대칭성으로 인해 개인정보 침해에 대한 피해구제를 정보주체인 개인에게만 맡겨두면 실질적인 피해구제가 이루어지기 어려운 문제점이 발생할 수 있다. 이러한 문제점을 보완하여 집단적 피해의 발생·확대 방지 및 집단적 해결을 위한 소송제도로는 크게 미국식의 ‘집단소송제도’와 유럽식의 ‘단체소송제도’가 있다.

집단소송(Class Action)은 피해 집단에 속해 있는 개인에게 당사자 적격을 인정하여 그로 하여금 집단구성원 전원을 위하여 소송을 수행할 수 있게 하는 제도이고, 단체소송(Verbandsklage)은 일정한 자격을 갖춘 단체로 하여금 전체 피해자들의 이익을 위해 소송을 제기할 수 있는 권한을 부여하는 제도이다. 집단소송은 주로 소액다수의 피해구제를 위한 손해배상청구 소송으로 그 장점을 발휘해 왔고, 단체소송은 사업자들의 위법행위를 금지·중단시키기 위한 금지·중지청구소송제도로 발전해 왔다. 그러나 최근에는 단체소송에서도 소비자단체가 사업자의 위법행위에 의해 손해를 입은 소비자를 대표하여 손해배상소송을 제기하는 입법례도 나타나는 등 두 제도의 차이가 좁혀지고 있다.

단체소송은 우리나라에서 2006년 「소비자기본법」에 처음 도입하였다. 2011년 「개인정보 보호법」을 제정하면서 단체소송을 도입하였는데, 이는 개인정보처리자로 하여금 개인정보의 수집, 이용, 제공 등에 대한 준법정신과 경각심을 높이고, 동일, 유사 개인정보 소송에 따른 사회적 비용을 절감하기 위한 것이다. 「개인정보 보호법」은 유럽식의 단체소송제도를 도입하여 일정한 자격요건을 갖춘 단체에게만 개인정보 단체소송을 제기할 권한을 부여하고 있으며 단체소송의 청구범위도 권리침해행위의 금지·중지에 한정하고 금전적 피해 구제는 제외하고 있다.

이처럼 단체는 단체소송을 통하여 권리침해행위의 금지·중지를 청구할 수 있을 뿐이므로 단체가 집행정지 또는 가처분 등을 통하여 권리침해행위의 금지·중지를 청구할 수 없다. 다만, 개인정보처리자의 위법행위를 발견한 경우에 보호위원회에 「개인정보 보호법」 위반으로 신고하여 그 조사절차 등을 통하여 개인정보처리자의 권리침해행위를 금지 또는 중지하게 할 수 있다. 한편, 자신의 권리가 침해된 정보주체는 그 권리침해행위에 관하여 단체소송이 제기되었는지 여부와 관계없이 직접 「민사소송법」에 따라 개인정보처리자를 피고로 하여 권리침해행위의 금지·중지를 구하는 소송을 제기할 수 있다.

〈 단체소송과 집단소송의 차이 〉

구 분	단체소송(Verbandsklage)	집단소송(Class Action)
청구권자	일정 요건을 구비한 소비자단체 등 (단체가 소송수행)	이해관계가 밀접한 다수의 피해자집단 (대표당사자가 소송수행)
소송목적	위법행위의 금지·중지	금전적 피해구제(손해배상청구)
기대효과	피해의 확산방지 및 예방	피해의 사후적 구제
판결의 효과	다른 단체에게도 판결의 효력이 미침	모든 피해자에게 판결의 효과가 미침 (단, 제외 신청을 한 사람은 제외)

개인정보침해 단체소송의 대상 및 절차 등에 관해서는 법 제51조부터 제57조에 규정되어 있고 이를 구체화하기 위해 「개인정보 단체소송규칙(대법원 규칙 제2358호, 2011. 9. 28. 제정, 2011. 9. 30. 시행)」이 제정되어 시행 중에 있다.

2. 분쟁조정 전치주의

개인정보단체소송을 제기하기 위해서는 반드시 개인정보 집단분쟁조정 절차를 거쳐야 한다. 불필요한 소송의 남발을 막기 위한 것이다. 개인정보처리자가 조정위원회의 집단분쟁조정을 거부하거나 집단분쟁조정 결과 수락하지 아니한 경우에만 개인정보단체소송을 제기할 수 있다.

3. 개인정보단체소송의 대상 및 청구범위

가 개인정보단체소송의 대상

개인정보단체소송의 대상이 되는 개인정보처리자의 행위는 개인정보 처리와 관련한 정보주체의 권리를 침해하는 행위이다. 반드시 이 법 위반에 따른 권리침해 행위에 한정하지 않고 개인정보처리와 관련해서 발생한 권리침해행위는 모두 단체소송의 대상이 된다. 다만 청구취지 자체가 법원에 권리침해 행위의 금지·중지를 구하는 내용이기 때문에 최소한 소제기 당시 권리침해 행위가 계속되고 있어야 하고 과거의 행위로서 소제기 당시 종료된 권리침해행위는 특별한 사정이 없는 한 단체소송의 대상이 되지 못한다. 또한, 단체소송이 진행되고 있는 중에 개인정보처리자의 권리침해행위가 금지 또는 중지되었다면 그 단체소송은 더 이상 보호할 권리가 없으므로 특별한 사정이 없으면 소송의 이익을 상실하여 각하된다.

나 개인정보단체소송의 청구범위

개인정보단체소송은 개인정보의 목적 외 이용 및 제공, 개인정보 열람요구에 대한 금지 등과 같이 권리침해행위의 금지 또는 중지를 청구하는 소송을 말한다(제51조 본문). 따라서 개인정보 유출 또는 오·남용으로 인한 손해배상을 청구하는 소송과 같이 금전을 청구하는 소송이나 권리침해 이전으로의 원상회복을 구하는 취지의 소송은 단체소송을 통해서 제기할 수 없다. 정보주체가 손해배상 또는 원상회복을 청구하기 위해서는 개별적으로 별도의 민사소송을 제기해야 한다.

4. 개인정보단체소송의 원고적격

개인정보단체소송을 제기할 수 있는 자는 등록 소비자단체와 비영리민간단체로 한정되어 있다.

소비자단체가 개인정보단체소송을 제기하기 위해서는 「소비자기본법」 제29조에 따라 공정거래위원회에 등록된 소비자단체로서 ① 정관에 따라 상시적으로 정보주체의 권익증진을 주된 목적으로 하는 단체이며 ② 단체의 정회원수가 1천명 이상이고 ③ 「소비자기본법」 제29조에 따른 등록 후 3년이 경과하여야 한다.

비영리민간단체가 개인정보단체소송을 제기하기 위해서는 「비영리민간단체 지원법」 제2조에 따른 비영리민간단체로서 ① 법률상 또는 사실상 동일한 침해를 입은 100명 이상의 정보주체로부터 단체소송의 제기를 요청받고 ② 정관에 개인정보보호를 단체의 목적으로 명시한 후 최근 3년 이상 이를 위한 활동 실적이 있으며 ③ 단체의 상시 구성원수가 5천명 이상으로 ④ 중앙행정기관에 등록되어 있어야 한다.

법 명	조문 내용
비영리민간단체 지원법	<p>제2조(정의) 이 법에 있어서 “비영리민간단체”라 함은 영리가 아닌 공익활동을 수행하는 것을 주된 목적으로 하는 민간단체로서 다음 각호의 요건을 갖춘 단체를 말한다.</p> <ol style="list-style-type: none"> 1. 사업의 직접 수혜자가 불특정 다수일 것 2. 구성원 상호간에 이익분배를 하지 아니할 것 3. 사실상 특정정당 또는 선출직 후보를 지지·지원 또는 반대할 것을 주된 목적으로 하거나, 특정 종교의 교리전파를 주된 목적으로 설립·운영되지 아니할 것 4. 상시 구성원수가 100인 이상일 것 5. 최근 1년 이상 공익활동실적이 있을 것 6. 법인이 아닌 단체일 경우에는 대표자 또는 관리인이 있을 것

5. 개인정보단체소송의 전속관할

개인정보단체소송은 피고의 주된 사무소 또는 영업소가 있는 곳의 지방법원 본원 합의부의 관할에 전속한다. 그러나 주된 사무소나 영업소가 없는 경우에는 주된 업무담당자의 주소가 있는 곳의 지방법원 본원 합의부의 관할에 전속한다. 피고가 외국사업자인 경우에는 대한민국에 있는 이들의 주된 사무소·영업소 또는 업무담당자의 주소에 따라 전속관할을 정한다.

6. 소송대리인의 선임

원고가 개인정보단체소송을 제기하기 위해서는 변호사를 소송대리인으로 선임하여야 한다. 집단분쟁조정인 경우에는 청구인 중에서 대표당사자를 선임하도록 하였으나(제49조제4항) 단체소송의 경우에는 변호사를 소송대리인으로 선임하도록 하고 있다. 그러므로 변호사가 소송대리인으로 선임되어 있지 않은 경우에는 소각하 사유가 된다.

한편, 원고의 소송대리인 전원이 사망 또는 사임하거나 해임된 때에는 원고가 새로운 소송대리인을 선임할 때까지 소송절차가 중지된다. 이 경우 법원은 원고에게 1개월 이상의 기간을 정하여 변호사를 선임할 것을 명하게 되는데, 원고가 정해진 기간 내에 변호사를 선임하지 아니한 때에는 법원은 소각하 결정을 하여야 한다. 당해 각하 결정에 대해 원고는 즉시항고를 할 수 있다(「개인정보 단체소송규칙」 제11조제4항).

참고 즉시항고(「민사소송법」 제444조)

항고란 소송절차에 관한 신청을 기각한 결정이나 명령에 대한 불복신청을 말한다. 통상의 항고는 불복신청 기간에 대한 제한이 없는 반면에, 즉시항고는 재판의 신속한 확정을 위하여 불복신청기간을 기각결정을 고지 받은 날부터 1주일로 제한하고 있다.

제54조(소송허가신청) ① 단체소송을 제기하는 단체는 소장과 함께 다음 각 호의 사항을 기재한 소송허가신청서를 법원에 제출하여야 한다.

1. 원고 및 그 소송대리인
2. 피고
3. 정보주체의 침해된 권리의 내용

② 제1항에 따른 소송허가신청서에는 다음 각 호의 자료를 첨부하여야 한다.

1. 소제기단체가 제51조 각 호의 어느 하나에 해당하는 요건을 갖추고 있음을 소명하는 자료
2. 개인정보처리자가 조정을 거부하였거나 조정결과를 수락하지 아니하였음을 증명하는 서류

제55조(소송허가요건 등) ① 법원은 다음 각 호의 요건을 모두 갖춘 경우에 한하여 결정으로 단체소송을 허가한다.

1. 개인정보처리자가 분쟁조정위원회의 조정을 거부하거나 조정결과를 수락하지 아니하였을 것
2. 제54조에 따른 소송허가신청서의 기재사항에 흠결이 없을 것

② 단체소송을 허가하거나 불허가하는 결정에 대하여는 즉시항고할 수 있다.

1. 단체소송허가의 신청

개인정보단체소송을 제기하려는 단체는 소장과 함께 ① 원고 및 그 소송대리인 ② 피고 ③ 정보주체의 침해된 권리의 내용을 기재한 소송허가신청서를 관할 법원에 제출하여야 한다.

2. 단체소송허가 신청시 첨부서류

개인정보단체소송을 제기하려는 단체가 관할 법원에 소송허가신청서를 제출하고자 하는 경우에는 소송허가신청서에는 ① 소제기단체가 제51조 각 호의 어느 하나에 해당하는 요건(단체소송 원고적격)을 갖추고 있음을 소명하는 자료와 ② 개인정보처리자가 조정을 거부하였거나 조정결과를 수락하지 아니하였음을 증명하는 서류를 첨부하여야 한다.

단체소송 원고적격 소명자료는 단체소송을 제기하는 단체가 누구냐에 따라 아래와 같이 다르다.

< 소송허가 신청시 첨부서류(개인정보 단체소송 규칙 제6조) >

구분	소비자단체	비영리민간단체
소명 자료	<ol style="list-style-type: none"> 1. 단체의 정관 2. 단체의 정회원수가 1천명 이상임을 소명할 수 있는 자료 3. 「소비자기본법」 제29조에 따라 소비자단체로 등록된 사실 및 등록일자를 소명하는 서면 	<ol style="list-style-type: none"> 1. 단체의 정관 2. 개인정보보호와 관련된 최근 3년간의 활동실적 3. 단체의 상시 구성원수가 5천명 이상임을 소명할 수 있는 자료 4. 중앙행정기관에 등록되어 있음을 소명하는 서면 5. 단체소송의 제기를 요청한 정보주체의 이름·주소와 연락처(전화번호·팩시밀리번호 또는 전자우편주소 등을 말한다) 6. 제5호의 정보주체들이 단체소송의 제기를 요청한 서면(각 정보주체별 침해의 내용과 서명 또는 날인을 포함하여야 한다)

참고 1 청구의 변경

원고는 청구의 기초가 바뀌지 아니하는 한도 안에서 청구의 취지 또는 원인을 변경할 수 있다. 이때에는 법 제54조 및 제55조의 규정이 적용되지 않으므로 별도로 단체소송 허가신청을 하여 허가결정을 다시 받을 필요가 없다(「개인정보 단체소송규칙」 제13조).

참고 2 변론의 병합

동일한 법원에 청구의 기초와 피고인 개인정보처리자가 같은 여러 개의 개인정보 단체소송이 계속 중인 때에는 원칙적으로 이를 병합하여 심리하게 된다. 다만, 심리상황이나 그 밖의 사정을 고려하여 병합심리가 타당하지 아니한 때에는 분리하여 심의한다(「개인정보 단체소송규칙」 제14조).

3. 소송허가의 요건

신청서의 기재내용이나 첨부서류에 흠결이 있는 경우 법원은 상당한 기간을 정하여 흠결의 보정을 명하여야 한다. 이러한 보정명령에도 불구하고 보정이 이루어지지 않는 경우 법원은 결정으로 단체소송을 불허하게 된다. 소송불허가결정서의 이유에는 흠결이 있는 소송허가요건이 명시된다.

법원은 ① 소송허가신청서의 기재사항에 흠결이 없고 ② 개인정보처리자가 분쟁조정위원회의 조정을 거부하거나 조정결과를 수락하지 아니한 사실을 확인한 경우에는 결정으로

단체소송을 허가하여야 한다. 법원은 소송허가 여부를 결정하기 위해 필요하다고 인정하는 때에는 원고의 대표자, 피용자, 회원 또는 구성원, 피고 및 정보주체 등을 심문할 수 있다.

소송허가결정 및 소송불허가결정의 경우 그 결정등본이 원고와 피고에게 송달되는데, 소송불허가결정이 확정된 때에는 단체소송이 제기되지 아니한 것으로 보게 된다. 이와 같이 단체소송을 허가하거나 불허가하는 결정에 대하여는 즉시항고할 수 있다.

- 제56조(확정판결의 효력)** 원고의 청구를 기각하는 판결이 확정된 경우 이와 동일한 사안에 관하여는 제51조에 따른 다른 단체는 단체소송을 제기할 수 없다. 다만, 다음 각 호의 어느 하나에 해당하는 경우에는 그러하지 아니하다.
1. 판결이 확정된 후 그 사안과 관련하여 국가·지방자치단체 또는 국가·지방자치단체가 설립한 기관에 의하여 새로운 증거가 나타난 경우
 2. 기각판결이 원고의 고의로 인한 것임이 밝혀진 경우

1. 청구기각 판결의 효력

원고의 청구를 기각하는 판결이 확정된 경우, 이와 동일한 사안에 관하여는 다른 소비자 단체나 비영리단체도 다시 단체소송을 제기할 수 없다. 즉 단체소송의 확정판결 효과는 다른 단체에게까지 미친다(제56조 본문). 그러나 개별 정보주체들은 개인정보 단체소송의 결과에 관계 없이 권리침해 행위의 금지·중지를 구하는 소송 또는 손해배상 청구를 구하는 소송을 제기할 수 있다.

2. 확정판결 효력의 정지

원고가 청구 기각 판결을 받았더라도 ① 판결이 확정된 후 그 사안과 관련하여 국가·지방자치단체 또는 국가·지방자치단체가 설립한 기관에 의하여 새로운 증거가 나타나거나 ② 기각판결이 원고의 고의로 인한 것임이 밝혀진 경우에는 다른 단체가 동일 사안에 대하여 다시 단체소송을 제기할 수 있다(제56조 단서).

제57조 | 민사소송법 적용 등

법률

- 제57조(「민사소송법」의 적용 등)** ① 단체소송에 관하여 이 법에 특별한 규정이 없는 경우에는 「민사소송법」을 적용한다.
- ② 제55조에 따른 단체소송의 허가결정이 있는 경우에는 「민사집행법」 제4편에 따른 보전처분을 할 수 있다.
- ③ 단체소송의 절차에 관하여 필요한 사항은 대법원규칙으로 정한다.

1. 「민사소송법」의 적용

단체소송에 관하여 이 법에 특별한 규정이 없는 경우에는 「민사소송법」을 적용한다. 따라서 즉시항고의 기간·방법 등 다수의 민사소송 규정이 개인정보 단체소송 절차에도 그대로 적용된다.

2. 「민사집행법」의 적용

법원의 단체소송 허가결정이 있는 경우에는 「민사집행법」 제4편에 따른 보전처분을 할 수 있다. 그러나 개인정보 단체소송은 권리침해 행위의 금지·중지만 청구할 수 있기 때문에 금전채권의 보전을 목적으로 하는 가압류 관련 규정은 활용될 여지가 없고 가처분 관련 규정만 활용이 가능하다.

3. 「개인정보 단체소송규칙」의 제정·운동

단체소송 절차는 대법원규칙에 규정되어 있다. 「개인정보 단체소송규칙」에는 소의 제기 및 소송허가신청의 방법, 소장의 기재사항, 소송허가신청서의 기재사항, 소송허가신청서에 붙일 자료, 소송허가신청서의 심사, 소송허가신청서부분의 송달, 소송허가신청의 심리, 소송허가여부에 대한 결정, 소송대리인의 사임, 공동소송참가, 청구의 변경, 변론의 병합 등이 포함되어 있다.

< 개인정보 단체소송규칙 (대법원규칙 제2358호, 2011.9.28 제정) >

제1조(목적) 이 규칙은 「개인정보 보호법」(다음부터 “법”이라고 한다) 제51조에 따라 제기된 금지·중지 청구에 관한 소송(다음부터 ‘개인정보 단체소송’이라고 한다)의 절차에 관하여 필요한 사항을 정하는 것을 목적으로 한다.

제2조(「민사소송규칙」의 적용) 개인정보 단체소송에 관하여 이 규칙에 특별한 규정이 없는 때에는 「민사소송규칙」을 적용한다.

제3조(소의 제기 및 소송허가신청의 방법) 소장과 소송허가신청서는 별개의 서면으로 작성하여 제출하여야 한다.

제4조(소장의 기재사항) 소장에는 다음 각 호의 사항을 적어야 한다.

1. 원고 및 그 소송대리인
2. 피고
3. 청구의 취지와 원인

제5조(소송허가신청서의 기재사항) 소송허가신청서에는 다음 각 호의 사항을 적어야 한다.

1. 원고 및 그 소송대리인
2. 피고
3. 허가신청의 취지와 원인
4. 정보주체의 침해된 권리의 내용

제6조(소송허가신청서에 붙일 자료) ① 법 제51조제1호에 규정된 단체는 소송허가신청서에 다음 각 호의 자료 등을 붙여야 한다.

1. 단체의 정관
2. 단체의 정회원수가 1천명 이상임을 소명할 수 있는 자료
3. 「소비자기본법」 제29조에 따라 소비자단체로 등록된 사실 및 등록일자를 소명하는 서면

② 법 제51조제2호에 규정된 단체는 소송허가신청서에 다음 각 호의 자료 등을 붙여야 한다.

1. 단체의 정관
2. 개인정보보호와 관련된 최근 3년간의 활동실적
3. 단체의 상시 구성원수가 5천명 이상임을 소명할 수 있는 자료
4. 중앙행정기관에 등록되어 있음을 소명하는 서면
5. 단체소송의 제기를 요청한 정보주체의 이름·주소와 연락처(전화번호·팩시밀리번호 또는 전자우편주소 등을 말한다)
6. 제5호의 정보주체들이 단체소송의 제기를 요청한 서면(각 정보주체별 침해의 내용과 서명 또는 날인을 포함하여야 한다)

③ 소제기단체는 소송허가신청서에 법 제54조제2항제2호에 따라 개인정보처리자가 법 제49조에 따른 집단분쟁조정을 거부하거나 집단분쟁조정 결과 수락하지 아니하였음을 증명하는 서류를 붙여야 한다.

제7조(소송허가신청서의 심사) ① 소송허가신청서의 기재사항 및 소송허가신청서에 붙일 서류에 흠이 있는 때에는 재판장은 상당한 기간을 정하여 그 기간 이내에 흠을 보정하도록 명하여야 한다.

② 원고가 제1항에 따른 재판장의 명령에도 불구하고 흠을 보정하지 아니한 때에는 법원은 결정으로 단체소송을 불허한다.

제8조(소송허가신청서 부분의 송달) 소송허가신청서의 부분은 소장부분과 함께 피고에게 송달한다.

제9조(소송허가신청의 심리) 법원은 소송허가 여부를 결정하기 위하여 필요하다고 인정하는 때에는 원고의 대표자, 피용자, 회원 또는 구성원, 피고 및 정보주체 등을 심문할 수 있다.

제10조(소송허가 여부에 대한 결정) ① 소송허가결정서 및 소송불허가결정서에는 다음 각 호의 사항을 기재하고 결정을 한 법관이 기명날인하여야 한다.

1. 원고 및 그 소송대리인
2. 피고
3. 주문

4. 이유

- ② 소송불허가결정서의 이유에는 흠결이 있는 소송허가요건을 명시하여야 한다.
- ③ 소송허가결정 및 소송불허가결정은 그 결정등본을 원고와 피고에게 송달하여야 한다.
- ④ 소송불허가결정이 확정된 때에는 단체소송이 제기되지 아니한 것으로 본다.

제11조(소송대리인의 사임 등) ① 원고의 소송대리인 전원이 사망 또는 사임하거나 해임된 때에는 원고가 새로운 소송대리인을 선임할 때까지 소송절차가 중지된다.

- ② 제1항에 따라 소송절차가 중지된 경우 법원은 원고에게 1개월 이상의 기간을 정하여 변호사를 선임할 것을 명하여야 한다.
- ③ 원고가 제2항에 따른 명령을 받고도 정해진 기간 내에 변호사를 선임하지 아니한 때에는 법원은 결정으로 소를 각하하여야 한다.
- ④ 제3항의 결정에 대하여는 즉시항고를 할 수 있다.

제12조(공동소송참가) ① 법 제51조 각 호의 어느 하나에 해당하는 단체는 법 제55조제1항에 따른 법원의 허가를 받아 다른 단체와 개인정보처리자 사이에 계속 중인 개인정보 단체소송에 「민사소송법」 제83조에 따른 공동소송인으로 참가할 수 있다. 이 때 공동소송참가신청서와 공동소송참가허가신청서는 법 제54조제1항의 소장과 소송허가신청서로 본다.

- ② 제1항의 경우 법 제54조제2항제2호, 제55조제1항제1호의 규정은 적용하지 아니한다.

제13조(청구의 변경) 원고가 청구의 기초가 바뀌지 아니하는 한도 안에서 청구의 취지 또는 원인을 바꿀 때에는 법 제54조 및 제55조의 규정을 적용하지 아니한다.

제14조(변론의 병합) 동일한 법원에 청구의 기초와 피고인 개인정보처리자가 같은 여러 개의 개인정보 단체소송이 계속 중인 때에는 이를 병합하여 심리하여야 한다. 다만, 심리상황이나 그 밖의 사정을 고려하여 병합심리가 타당하지 아니한 때에는 그러하지 아니하다.

제9장 보칙

- 제58조 적용의 일부 제외
- 제58조의2 적용제외
- 제59조 금지행위
- 제60조 비밀유지 등
- 제61조 의견제시 및 개선권고
- 제62조 침해 사실의 신고 등
- 제63조 자료제출 요구 및 검사
- 제64조 시정조치 등
- 제65조 고발 및 징계권고
- 제63조 결과의 공표
- 제67조 연차보고
- 제68조 권한의 위임·위탁
- 제69조 벌칙 적용 시의 공무원 의제



제58조 | 적용의 일부 제외

법률

제58조(적용의 일부 제외) ① 다음 각 호의 어느 하나에 해당하는 개인정보에 관하여는 제3장부터 제7장까지를 적용하지 아니한다.

1. 공공기관이 처리하는 개인정보 중 「통계법」에 따라 수집되는 개인정보
2. 국가안전보장과 관련된 정보 분석을 목적으로 수집 또는 제공 요청되는 개인정보
3. 공중위생 등 공공의 안전과 안녕을 위하여 긴급히 필요한 경우로서 일시적으로 처리되는 개인정보
4. 언론, 종교단체, 정당이 각각 취재·보도, 선교, 선거 입후보자 추천 등 고유 목적을 달성하기 위하여 수집·이용하는 개인정보

② 제25조제1항 각 호에 따라 공개된 장소에 영상정보처리기를 설치·운영하여 처리되는 개인정보에 대하여는 제15조, 제22조, 제27조제1항·제2항, 제34조 및 제37조를 적용하지 아니한다.

③ 개인정보처리자가 동창회, 동호회 등 친목 도모를 위한 단체를 운영하기 위하여 개인정보를 처리하는 경우에는 제15조, 제30조 및 제31조를 적용하지 아니한다.

④ 개인정보처리자는 제1항 각 호에 따라 개인정보를 처리하는 경우에도 그 목적을 위하여 필요한 범위에서 최소한의 기간에 최소한의 개인정보만을 처리하여야 하며, 개인정보의 안전한 관리를 위하여 필요한 기술적·관리적 및 물리적 보호조치, 개인정보의 처리에 관한 고충처리, 그 밖에 개인정보의 적절한 처리를 위하여 필요한 조치를 마련하여야 한다.

이 법에서 보호하고자 하는 프라이버시권은 누구나 누려야 할 기본권이자 민주주의 사회의 초석이다. 또한 프라이버시권은 정치적 자유, 표현의 자유, 집회의 자유, 종교의 자유, 신체의 자유, 사유재산 보호 그 밖에 우리 사회가 개인의 자유 및 사적 자치에 부여하고 있는 모든 가치의 토대를 이루고 있다.

그러나 개인정보 보호를 지나치게 강조하면 국가안전보장, 공공의 안녕과 질서 등 헌법의 기본적인 가치와 언론의 자유, 선교활동의 자유, 정당활동의 자유 등 다른 헌법상의 권리들이 오히려 위축되는 결과를 초래할 수 있다. 따라서 개인정보를 적절히 보호하면서도 다른 헌법적 가치들과 균형을 위하여 일정한 목적과 유형의 개인정보 처리에 대해서는 법률의 일부 적용을 제외할 필요가 있다.

1. 통계법에 따라 수집되는 개인정보에 대한 적용 제외

공공기관이 처리하는 개인정보 중 「통계법」에 따라 수집되는 개인정보에 대해서는 법 제3장부터 제8장이 적용되지 않는다. 「통계법」에 따라 작성된 통계는 국가는 물론 민간에서도 각종 의사결정을 하는데 기본적인 데이터로 활용되는 공공재로서의 역할을 수행하고 있고 경제·사회 발전의 기초가 되므로 시의적절하고 정확한 통계의 작성은 매우 중요하다.

다만 「통계법」에 따라 통계종사자, 통계종사자이었던 자 또는 통계작성기관으로부터 통계 작성업무의 전부 또는 일부를 위탁받아 그 업무에 종사하거나 종사하였던 자는 직무상 알게 된 사항을 업무 외의 목적으로 사용하거나 다른 자에게 제공하여서는 안 되고(「통계법」 제34조), 통계의 작성과정에서 알려진 사항으로서 개인이나 법인 또는 단체 등의 비밀에 속하는 사항은 보호되어야 하고 통계의 작성을 위하여 수집된 개인이나 법인 또는 단체 등의 비밀에 속하는 자료는 통계작성 외의 목적으로 사용되어서는 아니 되며(「통계법」 제33조), 통계작성기관의 장이 다른 통계작성기관의 장에게 통계자료를 제공하는 때에는 특정의 개인이나 법인 또는 단체 등을 식별할 수 없는 형태로 통계자료를 처리한 후 제공하여야 한다(「통계법」 제30조제2항).

결정례 「통계법」에 따라 승인을 받지 않은 통계작성을 위하여 제공받은 개인정보의 적용 제외에 해당 여부

「통계법」 제18조제1항에 따른 통계청장의 승인을 받지 아니한 장애인 관련 통계작성을 위하여 보건복지부로부터 장애인의 주민등록번호, 장애종류, 장애등급 정보를 제공받으려 할 경우, 위 정보는 「개인정보 보호법」 제58조제1항제1호에 정한 「통계법」에 따라 수집되는 개인정보에 해당하지 않으므로 개인정보 보호법 제3장부터 제8장까지의 적용이 제외되지 아니한다(보호위원회 결정 제2017-23-176호).

2. 국가안보 관련 정보 분석을 목적으로 처리되는 개인정보에 대한 적용 제외

국가안전보장과 관련된 정보 분석을 목적으로 수집 또는 제공이 요청되는 개인정보에 대해서도 법 제3장부터 제8장까지를 적용하지 아니한다. 이 경우 수집 또는 제공에는 이용이 포함된다(보호위원회 결정 제2019-04-044호 참고). 테러분자의 추적, 간첩 색출, 국가전복 기도 방지, 국가기밀 누출방지 등 국가안보를 위한 정보·수사기관들의 정보 수집, 분석 및 관리 업무는 비밀리에 수행되어야 하기 때문에 국가안보를 목적으로 하는 개인정보 수집·제공 행위 등에 대해서는 이 법의 일부 적용을 배제하고 있다.

결정례1 제58조제1항제2호에 따른 '수집 또는 제공'의 범위

법 제15조제1항이 개인정보의 '수집'의 요건을 규정함에 있어 '이용'을 전제로 하고 있는 점, 법 제58조제1항제2호의 '국가안전보장과 관련된 정보 분석'은 그 자체가 '이용'에 해당되고 동 호가 개인정보의 제3자 제공까지 허용하고 있는 점 등을 고려할 때, 제58조제1항제2호의 '수집 또는 제공 요청'에는 '이용'이 포함되는 것으로 해석하는 것이 「개인정보 보호법」의 전체 체계 및 입법 취지에 부합한다(보호위원회 결정 제2019-04-044호).

결정례2 코로나19 관련 재난지원금 지원을 위한 국민건강보험공단 보유 개인정보 제공

「개인정보 보호법」 제18조제2항제5호는 공공기관인 개인정보처리자가 개인정보를 목적 외의 용도로 이용하거나 이를 제3자에게 제공하지 아니하면 다른 법률에서 정하는 소관업무를 수행할 수 없는 경우로서 보호위원회의 심의·의결을 거친 경우에는 정보주체 또는 제3자의 이익을 부당하게 침해할 우려가 있는 경우를 제외하고는 개인정보를 목적 외의 용도로 이용하거나 이를 제3자에게 제공할 수 있다고 규정하고 있다.

「재난 및 안전관리기본법」과 지방자치단체의 조례 등 관계 법령의 지원기준에 따라 국가 및 지방자치단체가 코로나19 관련 긴급재난지원금을 지급하는 것은 법률에서 정하는 소관 업무에 해당한다 할 것이다.

따라서 국민건강보험공단은 「개인정보 보호법」 제18조제2항제5호에 따라 본 건 정보를 지방자치단체와 보건복지부에 제공할 수 있다(보호위원회 결정 제2020-07-105호).

결정례3 관악구 CCTV 영상정보 제공

「개인정보 보호법」 제18조제1항의 규정에 따라 개인정보처리자는 개인정보를 목적 외 용도로 이용하거나 제3자에게 제공하여서는 아니 된다. 따라서 지자체가 설치한 CCTV의 영상정보를 군사 작전 및 재난대응 용도로 군부대에서 상시 사용할 수는 없으며 보안 대책이 마련되었다고 하더라도 수도방위사령부 병커에서 구청의 CCTV 영상정보를 상시 관제하는 것은 「개인정보 보호법」 위반에 해당한다.

다만, 「개인정보 보호법」 제58조제1항제2호에서 '국가안전보장과 관련된 정보 분석을 목적으로 수집 또는 제공 요청되는 개인정보'에 대해서는 이 법의 일부 내용을 적용하지 아니하도록 예외를 인정 하고 있으므로 수방사가 이에 해당되는 사유로 구청의 CCTV 영상정보를 요청하는 경우에는 제공이 가능하다 할 것이다.

이 경우, 개인정보자기결정권 보호를 위해 '국가안전보장과 관련된 정보 분석의 목적'은 '구체적' 이고 '명확한' 경우로 엄격하게 해석 되어야 할 것이다. 따라서 단순히 훈련을 위한 목적으로 CCTV 영상정보를 제공하여서는 안 되며, 구청 내에 설치된 통합방위지원본부에서 군부대 요원 등이 CCTV 영상을 관제하는 것도 개인정보의 목적 외 이용 및 제3자 제공에 해당되므로 상기한 바와 같이 '국가안전보장과 관련된 정보 분석을 목적'으로 하는 예외적 사유에 해당되지 않는 한 허용되지 않는다고 보아야 한다(보호위원회 의결, 2012. 11. 12.).

3. 공중위생등 목적으로 처리되는 개인정보에 대한 적용 제외

공중위생 등 공공의 안전과 안녕을 위하여 긴급히 필요한 경우로서 일시적으로 처리되는 개인정보에 대해서도 법 제3장부터 제8장이 적용되지 않는다. 각종 전염병의 확산방지를 위한 환자 격리, 감염원 추적 등의 활동과 천재지변·긴급재난 등으로부터 이재민을 구조·구호하기 위한 활동은 존각을 다투는 경우가 많고 국민의 생명·신체 및 재산의 안전이 위협을 받고 있는 상황이므로 이 법령에 의한 기준·절차에 따라 개인정보 처리가 곤란하기 때문이다. 다만, 이 경우에도 남용을 방지하기 위하여 해당 개인정보를 일시적으로 처리하는 경우에 한해서 법 적용을 제외하고 있다.

4. 언론, 종교단체, 정당 등에 대한 적용 제외

언론, 종교단체, 정당이 각각 취재·보도, 선교, 선거 입후보자 추천 등 그 고유 목적을 달성하기 위하여 수집·이용하는 개인정보에 대해서는 제3장부터 제8장을 적용하지 아니한다.

그 고유 목적을 달성하기 위하여 처리되는 개인정보에 한하여 이 법의 일부가 적용 배제되며, 언론기관, 종교단체, 정당 등이 처리하는 모든 개인정보에 대해서 이 법의 적용이 제외되는 것은 아니다. 예컨대 언론기관의 인물DB사업, 종교단체의 사회복지사업, 정당의 여성정치인 육성사업은 언론기관·종교단체·정당 등의 고유 목적이라고 할 수 없다.

언론의 취재 또는 보도 등 고유목적의 달성하기 위한 활동으로 취재란 언론이 보도·논평 및 여론 등을 전파할 목적으로 기사작성에 필요한 기초자료 또는 정보를 수집하는 행위를 말하며, 보도란 언론이 취재를 통하여 얻어진 것을 신문, 잡지, 방송 또는 인터넷 등의 매체를 통해 일반인에게 전달하는 행위를 말한다.

< 간행물의 종류 >

종류	내용
신문	「신문 등의 진흥에 관한 법률」 제9조제1항에 따라 등록된 신문으로서 일반일간신문, 특수일간신문, 일반주간신문, 특수주간신문 등 정치·경제·사회·문화·산업·과학·종교·교육·체육 등 전체 분야 또는 특정 분야에 관한 보도·논평·여론 및 정보 등을 전파하기 위하여 같은 명칭으로 월 2회 이상 발행하는 간행물

인터넷 신문	<p>「언론중재 및 피해구제 등에 관한 법률」 제2조제10호, 「신문 등의 진흥에 관한 법률」 제2조제2호 및 「신문 등의 진흥에 관한 법률 시행령」 제2조가 규정한 컴퓨터 등 정보처리능력을 가진 장치와 통신망을 이용하여 정치·경제·사회·문화·시사 등에 관한 보도·논평·여론 및 정보 등을 전파하기 위해 간행하는 전자간행물로서 독자적 기사 생산과 지속적인 발행 등 다음의 기준을 모두 충족하는 것</p> <ul style="list-style-type: none"> • 독자적인 기사 생산을 위한 요건으로서 취재 인력 3인 이상을 포함하여 취재 및 편집 인력 5인 이상을 상시적으로 고용하고, 주간 게재 기사 건수의 30% 이상을 자체적으로 생산한 기사로 게재할 것 • 지속적인 발행요건으로서 주간 단위로 새로운 기사를 게재할 것
잡지	<p>「잡지 등 정기간행물의 진흥에 관한 법률」 제2조제1호 가목에서 규정한 동일한 제호로 월 1회 이하 정기적으로 발행하는 책자 형태의 간행물로서 「신문 등의 진흥에 관한 법률」 제2조에 따른 신문을 제외한 잡지 및 기타간행물</p>

‘언론’ 이라 함은 다음의 기관들을 말한다.

1. 「신문 등의 진흥에 관한 법률」 제9조제1항에 따라 등록된 일간신문·주간신문·인터넷신문 및 「잡지 등 정기간행물의 진흥에 관한 법률」 제15조제1항에 따라 등록된 월간잡지를 발행하는 자
2. 「방송법」 제2조제3호에 따른 방송사업자로 지방파방송사업자, 종합유선방송사업자, 위성방송사업자, 방송채널사용사업자, 공동체라디오방송사업자
3. 「뉴스통신 진흥에 관한 법률」 제8조에 따라 등록된 뉴스통신사업을 하려는 법인
 - ※ 뉴스통신이라 함은 「전파법」에 따라 무선국의 허가를 받거나 그 밖의 정보통신기술을 이용하여 외국의 뉴스통신사와 뉴스통신계약을 체결하고 국내외의 정치·경제·사회·문화·시사 등에 관한 보도·논평 및 여론 등의 전파를 목적으로 행하는 유무선을 포괄한 송수신 또는 이를 목적으로 발행하는 간행물
4. 그밖에, 「공직선거법」 제8조의5제1항이 규정한 정치·경제·사회·문화·시사 등에 관한 보도·논평·여론 및 정보 등을 전파할 목적으로 취재·편집·집필한 기사를 인터넷을 통해 보도·제공하거나 매개하는 인터넷홈페이지를 경영·관리하는 자와 이와 유사한 언론의 기능을 행하는 인터넷홈페이지를 경영·관리하는 자

‘종교단체’에는 천주교, 개신교, 대종교, 불교, 원불교, 유교, 이슬람교, 천도교 등 종교의 보급, 기타 교화를 목적으로 설립된 종단·교단·유지재단 또는 이와 유사한 연합종교단체, 종교단체에 소속된 법인 또는 단체로서 종교의 보급, 기타 교화를 목적으로 설립된 개별단체로서 「민법」 제32조에 근거하여 문화체육관광부에 등록을 한 법인인 단체 또는 관할 시·군·구청에 종교단체로 등록하여 고유번호를 부여받고 관할세무서에 사업자 등록을 한 단체 등이 해당될 수 있다.

종교단체가 선교 등 고유목적의 달성을 위한 활동으로는 ① 교단정리, 교단내부규율정리, 소속종교단의 등록, 교역자의 신상관리, 소식지 제작, 홍보, 종교단체가 의사결정을 하거나 자문을 위하여 행하는 각종 회의소집, 교단 홈페이지 관리 등 종교단체의 교단유지업무

② 종교단체의 교리를 전파하거나 전쟁이나 재해를 입은 주민의 재건과 화해를 위한 선교활동(헌재 2008.6.26. 2007헌마1366) ③ 종교의 교리를 전달하고 종교를 전파할 목적을 행하는 교육, 그밖에 종교를 선교하기 위한 부수적인 활동으로 행하는 청소년운동, 부정부패추방 시민운동, 환경운동 등과 같은 공익활동이나 자원봉사활동 등이 있다.

‘정당’이라 함은 국민의 이익을 위하여 책임 있는 정치적 주장이나 정책을 추진하고 공식 선거의 후보자를 추천 또는 지지함으로써 국민의 정치적 의사형성에 참여함을 목적으로 하는 국민의 자발적 조직으로서 「정당법」 제4조제1항에 의하여 중앙선거관리위원회에 등록된 단체를 말한다. 정당이 선거 입후보자 추천 등 고유목적 달성을 위한 활동에는 정당이 공식선거의 후보자(후보자가 되고자 하는 자를 포함한다)를 지지·추천하는 행위, 정당의 정책이나 정치적 현안에 대한 입장을 인쇄물·시설물·광고 등을 이용하여 홍보하는 행위, 정당이 당원을 모집하기 위한 활동(호별방문을 제외한다) 등이 포함된다.

5. 동창회, 동호회 등 친목단체에 대한 적용 제외

개인정보처리자가 동창회, 동호회 등 친목 도모를 위한 단체를 운영하기 위하여 개인정보를 처리하는 경우에는 제15조(개인정보의 수집·이용), 제30조(개인정보 처리방침의 수립 및 공개) 및 제31조(개인정보 보호책임자의 지정)를 적용하지 아니한다. 친목단체는 업무적 성격보다는 사적 모임의 성격이 강하기 때문에 이 법의 일부 적용을 배제한 것이다.

따라서 친목단체는 정보주체의 동의 없이 회원의 개인정보를 수집·이용하는 것이 가능하다. 다만, 친목단체의 설립 목적을 벗어난 이용·제공에 대해서는 제15조, 제30조, 제31조에 따라 처리하여야 한다.

현행법은 일정한 법정 단체(법령상 친목 단체)에 대해 친목도모를 목적으로 한다거나 친목단체의 회비에 대하여는 「기부금품의 모집 및 사용에 관한 법률」상의 기부금으로 보지 아니한다거나 「공직선거법」상의 규제대상인 기부금으로 보지 아니한다는 내용만 규정하고 있고, 친목단체와 관련하여 별도의 개념 정의조항을 두고 있지 않다. 사전적으로는 ‘학교, 지역, 기업, 인터넷 커뮤니티 등을 단위로 구성되는 것으로서 자원봉사, 취미, 정치, 종교 등 공통의 관심사나 목표를 가진 사람간의 친목도모를 위한 모임’으로 볼 수 있고, 영리를 목적으로 하는 단체는 친목단체가 될 수 없다고 보아야 한다. 다만, 해당 영리단체 등 친목단체가 아닌 단체의 구성원도 단체 내에서는 자유롭게 친목단체를 구성할 수 있다고 볼 수 있다.

< 법령 상 친목단체 관련 규정 >

법 명	내 용
고엽제후유의증 환자지원 등에 관한 법률	제9조제1항은 ‘고엽전우회’를 고엽제후유증의 환자 등 상호간의 친목을 도모하고 상부상조함을 목적으로 하는 법인임을 명시
공무원행동강령	제17조제1항은 공무원으로 하여금 직무관련자나 직무관련공무원에게 경조사를 알리지 못하도록 함. 예외적으로 “공무원 자신이 소속된 종교 단체·친목단체 등의 회원에 대한 통지”는 허용
공직선거법	제112조 제2항제2호 마목은 “친목회·향우회·종친회·동창회 등 각종 사교·친목단체 및 사회단체의 구성원으로서 당해 단체의 정관·규약 또는 운영관계상의 의무에 기하여 종전의 범위안에서 회비를 납부하는 행위”를 기부금에서 제외
기부금품의 모집 및 사용에 관한 법률	“법인, 정당, 사회단체, 종친회(宗親會), 친목단체 등이 정관, 규약 또는 회칙 등에 따라 구성원으로부터 가입금, 일시금, 회비 또는 그 구성원의 공동이익을 위하여 모은 금품”은 위 법률의 적용대상인 기부금품에서 배제

< 친목단체 관련 판례 >

판례 구분	내용
대법원 2010.10.28. 선고 2010두14084 판결	친목단체가 구성원에 대하여 행하는 강제통제의 성격을 갖는 외부 활동행위에 대한 규제는 친목도모의 범위를 벗어나는 행위라 보아야 한다.
대법원 2010.9.30. 선고 2010도5954 판결	친목단체의 구성원이 해당 친목단체의 정관이나 규약 등 자치규범에 따라 납부하게 되는 회비 등에 대하여는 「기부금품의 모집 및 사용에 관한 법률」상의 기부금으로 보지 아니한다.
대법원 2010.6.24. 선고 2007두18000 판결	일정한 비용의 지출이 내부구성원을 상대로 하여 구성원간 원활한 관계를 목적으로 한 것이면 친목도모를 위한 비용으로 과세의 대상이 되지 아니하나 외부인을 대상으로 하는 경우에는 친목도모의 범위를 벗어난 것으로서 광고선전비에 해당한다.

친목단체의 설립 목적 범위 내에서 개인정보를 처리하는 경우에도 개인정보의 최소수집 원칙, 개인정보의 기술적·관리적 보호조치, 고유식별정보 및 민감정보의 처리 제한, 수탁자에 대한 관리·감독, 개인정보 유출 통지 및 신고 의무, 개인정보 파기, 정보주체의 권리 보호 등의 규정은 모두 그대로 적용된다.

6. 기술적·관리적 보호조치 등의 강구

개인정보처리자가 제1항 각 호에 따라 개인정보를 처리하는 경우에도 그 목적을 위하여 필요한 범위에서 필요한 최소한의 개인정보만을 처리하여야 한다. 또한, 개인정보의 안전한 관리를 위하여 필요한 기술적·관리적 및 물리적 보호조치를 취해야 하고, 개인정보처리에 관한 고충처리를 포함하여 그 밖에 개인정보의 적절한 처리를 위하여 필요한 조치를 마련하여야 한다.

< 외국 개인정보 보호법 적용 제외 사례 >

구분	내용
OECD 프라이버시 가이드라인	<ul style="list-style-type: none"> • 순수하게 사적인 목적으로 처리되는 경우 • 국가주권, 국가안보, 공공정책(Public Policy)을 위한 경우
EU 일반 개인정보 보호법(GDPR)	<ul style="list-style-type: none"> • 순수하게 사적이고 가사목적의 활동을 위한 경우 • 공공의 안전, 방위, 국가안보를 위한 활동의 경우 • 형사법 영역의 국가활동(수사 등) • 보도 목적, 문학·예술적 창작활동이나 표현을 위한 경우
독일 연방 개인정보 보호법	<ul style="list-style-type: none"> • 개인정보의 수집, 생산, 이용이 오직 개인적이거나 가족적인 활동 영역에 속하는 경우(제3조제3항) • 법률의 규정, 정보주체의 동의, 공공복리 및 공공안전침해 방지, 형사상·행정상 집행을 위한 경우(제14조제2항) • 계약목적, 정보주체의 중요한 법적 이익, 광고·시장조사· 여론조사, 학문연구, 과학적 연구(정보주체의 이익보다 크고, 기타 방법이 없는 경우), 제3자의 법적 이익 또는 공익보호, 정치·철학·종교 또는 노동조합 목적(제28조)
일본 개인정보 보호법 (제76조)	<ul style="list-style-type: none"> • 보도 목적(방송기관, 신문사, 통신사 기타 보도기관) • 저술활동 목적(저술을 업으로 하는 자) • 학술연구 목적(대학 기타 학술연구를 목적으로 하는 기관, 단체 또는 그 구성원) • 종교활동 목적(종교단체) • 정치활동 목적(정치단체)

7. 질의 응답

Q | 인터넷 커뮤니티 사이트도 친목단체에 포함되나?

A | 해당 블로그의 운영형태, 회원규약 등으로 판단하여 볼 때, 순수하게 친목을 목적으로 하거나 취미를 공유하기 위한 목적으로 운영되면 친목단체로 볼 수 있다. 그러나 형식상으로는 친목, 취미를 표방하면서 실질적으로 상품판매, 공동구매, 수강생 모집, 광고 수수 등 영리수단으로 이용되고 있다면 친목단체로 볼 수 없다.

제58조의2 | 적용제외

법률

제58조의2(적용제외) 이 법은 시간·비용·기술 등을 합리적으로 고려할 때 다른 정보를 사용하여도 더 이상 개인을 알아볼 수 없는 정보에는 적용하지 아니한다.

1. 「개인정보 보호법」의 적용제외

시간·비용·기술 등을 합리적으로 고려할 때 다른 정보를 사용하여도 더 이상 개인을 알아볼 수 없는 정보는 더 이상 개인정보에 해당되지 않는 바, 해당 정보는 「개인정보 보호법」이 적용되지 않음을 명시하는 규정이다.

여기서 말하는 시간·비용·기술 등을 합리적으로 고려한다거나 다른 정보를 사용하여 개인을 알아볼 수 없다(또는 있다)는 점 등에 대해서는 법 제2조제1호가 적용되며, 「신용정보법」 제2조제17호의 익명처리 개념이 적용된다.

한편, 「개인정보 보호법」의 적용이 제외되는 범위는 제58조의2에 따른 정보를 처리하는 경우 뿐 아니라 개인정보를 다른 정보를 사용하여도 더 이상 개인을 알아볼 수 없도록 처리하는 경우까지 포함한다. 따라서 개인정보처리자가 이러한 정보 생성을 위해 개인정보를 처리하는 경우에는 정보주체의 동의를 받을 필요가 없다.

2. 관련 법률

「신용정보법」에서는 익명처리에 대해 별도의 정의 규정을 두고 있다. 익명처리된 개인신용정보는 개인정보에 해당하지 않기 때문에 「개인정보 보호법」의 적용도 제외된다.

신용정보법

제2조 (정의) 이 법에서 사용하는 용어의 뜻은 다음과 같다.

17. “익명처리”란 더 이상 특정 개인인 신용정보주체를 알아볼 수 없도록 개인신용정보를 처리하는 것을 말한다.

제59조 | 금지행위

법률

제59조(금지행위) 개인정보를 처리하거나 처리하였던 자는 다음 각 호의 어느 하나에 해당하는 행위를 하여서는 아니 된다.

1. 거짓이나 그 밖의 부정한 수단이나 방법으로 개인정보를 취득하거나 처리에 관한 동의를 받는 행위
2. 업무상 알게 된 개인정보를 누설하거나 권한 없이 다른 사람이 이용하도록 제공하는 행위
3. 정당한 권한 없이 또는 허용된 권한을 초과하여 다른 사람의 개인정보를 훼손, 멸실, 변경, 위조 또는 유출하는 행위

1. 금지행위의 의무대상자

금지행위의 의무대상자는 ‘개인정보를 처리하거나 처리하였던 자’이다. 여기서 ‘개인정보를 처리하거나 처리하였던 자’는 ‘개인정보처리자’에 한정되지 않고 업무상 알게 된 개인정보를 제2조제2호의 방법으로 처리하거나 처리하였던 자도 포함된다. 따라서 개인정보처리자에게 소속되어 개인정보를 처리하고 있거나 처리한 적이 있는 전·현직 임직원, 파견직, 수탁자 등이 ‘개인정보를 처리하거나 처리하였던 자’에 해당된다.

판례1 법 제59조제2호의 개인정보를 처리하거나 처리하였던 자의 범위

「개인정보 보호법」 제71조제5호의 적용대상자로서 제59조제2호의 의무주체인 ‘개인정보를 처리하거나 처리하였던 자’는 제2조제5호의 ‘개인정보처리자’ 즉 업무를 목적으로 개인정보파일을 운용하기 위하여 스스로 또는 다른 사람을 통하여 개인정보를 처리하는 공공기관, 법인, 단체 및 개인 등에 한정되지 않고, 업무상 알게 된 제2조 제1호의 ‘개인정보’를 제2조 제2호의 방법으로 ‘처리’하거나 ‘처리’하였던 자를 포함한다(대법원 2016. 3. 10. 선고 2015도8766 판결).

판례2 제71조 제5호의 ‘개인정보를 제공받은 자’에 해당하는지 여부

「개인정보 보호법」 제59조제2호는 ‘개인정보를 처리하거나 처리하였던 자는 업무상 알게 된 개인정보를 누설하거나 권한 없이 다른 사람이 이용하도록 제공하는 행위를 하여서는 아니 된다’고 규정하고 있고, 제71조제5호는 ‘제59조제2호를 위반하여 업무상 알게 된 개인정보를 누설하거나 권한 없이 다른 사람이 이용하도록 제공한 자 및 그 사정을 알면서도 영리 또는 부정한 목적으로 개인정보를 제공받은 자’를 처벌하는 것으로 규정하고 있다. 위에서 보듯이 「개인정보 보호법」 제71조제5호 후단은 그 사정을 알면서도 영리 또는 부정한 목적으로 개인정보를 제공받은 자를 처벌하도록 규정하고 있을 뿐 개인정보를 제공하는 자가 누구인지에 관하여는 문언상 아무런 제한을 두지 않고 있는 점과 개인정보 보호법의 입법 목적 등을 고려할 때, 개인정보를 처리하거나 처리하였던 자가 업무상 알게 된 개인정보를 누설하거나 권한 없이 다른 사람이 이용하도록 제공한 것이라는 사정을 알면서도 영리 또는 부정한 목적으로 개인정보를 제공받은 자라면, 개인정보를 처리하거나 처리하였던 자로부터 직접 개인정보를 제공받지 아니하더라도 「개인정보 보호법」 제71조제5호의 ‘개인정보를 제공받은 자’에 해당된다고 볼 것이다(대법원 2018. 1. 24. 선고, 2015도16508 판결).

< 제59조 각 호 적용 대상 관련 사례 >

사례1

아파트 관리소장이 보관 중이던 동대표 해임서(입주민의 이름 등 기재)를 해임대상자인 동대표에게 열람하게 한 경우

일부 입주민들의 동·호수, 이름, 전화번호, 서명 등이 기재된 동대표 해임서를 보관하던 아파트 관리소장이 이를 해임대상자인 동대표에게 열람하도록 제공한 사안에서, 원심은 아파트 관리소장은 개인정보처리자가 아니므로 법률위반의 책임이 없다고 보았으나 대법원은 이를 파기하면서 개인정보처리자가 아니더라도 개인정보를 실제로 처리하거나 처리하였던 자는 법 제71조 제5호의 형사책임을 부담한다고 판시하였다(대법원 2016. 3. 10. 선고 2015도8766 판결).

사례2

인터넷 신문 기자가 취재 활동 중 알게 된 취재원의 개인정보를 누설한 경우

인터넷 신문 기자인 피고인이 뉴스 사이트에 甲에 관한 기사를 게재하면서 취재 활동 중에 알게 된 甲의 성명, 지위, 주소 등의 개인정보를 누설하였다고 하여 개인정보 보호법 제71조 제5호, 제59조 위반으로 기소된 사안에서, 피고인은 개인정보처리자가 아니라는 이유로 무죄를 주장하였으나 법원은 피고인이 개인정보처리자가 아니더라도 제71조 제5호 위반으로 처벌할 수 있다고 판시하였다(서울서부지방법원 2015. 12. 18. 선고 2015고정1144 판결).

참고로 이 사안에서 피고인은 법 제58조 제1항 제4호에서 언론이 취재, 보도 등 고유 목적을 달성하기 위하여 수집·이용하는 개인정보에 관하여는 법 제3장부터 제7장까지를 적용하지 아니한다고 규정하고 있고, 언론의 특성상 개인정보의 ‘이용’이라는 것은 취재 과정상 수집한 개인정보를 ‘보도’하는 것을 의미하므로 개인정보 보호법이 적용되지 아니한다고 주장하였다. 그러나 법원은 ① 법 제58조 제1항 제4호의 예외 규정은 법 제3장에서부터 제7장까지 적용하지 아니함에 반하여 피고인에 대한 처벌규정인 법 제58조 제1항 제4호는 제8장에 속하는 규정인 점, ② 법 제58조 제1항 제4호의 예외 규정은 개인정보의 ‘수집’, ‘이용’에 한정하여 예외 규정을 두고 있는데, 개인정보 보호법에서는 ‘수집’, ‘이용’과 ‘제공’, ‘공개’를 구별하여 규정하고 있는 점, ③ 「개인정보 보호법」의 취지에 비추어 언론이 취재·보도를 위하여 개인정보를 이용한다고 하더라도 그 이용에 개인정보를 일반 공중에게 보도하는 것이 포함된다고 보기 어려운 점 등을 이유로 이 주장을 받아들이지 아니하였다.

사례3

경찰공무원이 피고인의 부탁을 받고 신고자의 전화번호 뒷자리 4자를 알려준 경우

경찰공무원인 피고인 甲이 피해자 乙의 신고에 따라 피고인 丙등의 도박 현장을 단속한 다음 훈방 조치하였는데, 그 후 피고인 丙으로부터 신고자의 전화번호를 알려달라는 부탁을 받고 ‘乙의 휴대전화번호 뒷자리 4자’를 알려 주었다고 하여 개인정보 보호법 위반으로 기소된 사안에서, 피고인 甲은 개인정보를 처리한 자로서 업무상 알게 된 개인정보를 누설하였다는 이유로, 피고인 丙은 피고인 甲으로부터 이러한 사정을 알면서도 부정확한 목적으로 개인정보를 제공받았다는 이유로 각각 개인정보 보호법 제71조 제5호 위반으로 처벌할 수 있다고 판시하였다(대전지방법원 논산지원 2013. 8. 9. 선고 2013고단17 판결).

2. 부정한 방법에 의한 개인정보 취득 및 처리동의 획득

개인정보를 처리하거나 처리하였던 자는 ‘거짓이나 그 밖의 부정한 수단이나 방법’으로 개인정보를 취득하거나 처리에 관한 동의를 받는 행위를 하여서는 아니 된다.

‘거짓이나 그 밖의 부정한 수단이나 방법’이란 개인정보를 취득하거나 또는 그 처리에 관한 동의를 받기 위하여 사용하는 위계 기타 사회통념상 부정한 방법이라고 인정되는 것으로서 개인정보 취득 또는 그 처리에 동의할지 여부에 관한 정보주체의 의사결정에 영향을 미칠 수 있는 적극적 또는 소극적 행위를 말한다. 구체적으로, ‘거짓’에는 사기 또는 기망과 같은 의미로 사람을 속이는 행위가 포함되며, ‘그 밖의 부정한 수단이나 방법’에는 공갈·협박 및 그 외 착오·오인 유발행위가 포함된다. 언어·문서에 의하든 적극적인 동작이나 소극적인 부작위(不作爲)에 의하든 이를 불문한다. 최근 금융기관, 경찰청, 세무서, 우체국, 법원, 국민연금관리공단 등을 사칭하여 정보주체로부터 카드번호, 주민번호, 비밀번호 등의 개인정보를 빼내가는 인터넷 피싱(인터넷 사기)과 보이스피싱(전화사기)이 대표적인 사례라고 할 수 있다.

판례1 법 제59조제1호, 제72조제2호의 “거짓이나 그 밖의 부정한 수단이나 방법”의 의미(1)

「개인정보 보호법」 제72조 제2호에 규정된 ‘거짓이나 그 밖의 부정한 수단이나 방법’이란 개인정보를 취득하거나 또는 그 처리에 관한 동의를 받기 위하여 사용하는 위계 기타 사회통념상 부정한 방법이라고 인정되는 것으로서 개인정보 취득 또는 그 처리에 동의할지에 관한 정보주체의 의사결정에 영향을 미칠 수 있는 적극적 또는 소극적 행위를 뜻한다. 그리고 거짓이나 그 밖의 부정한 수단이나 방법으로 개인정보를 취득하거나 그 처리에 관한 동의를 받았는지를 판단할 때에는 개인정보처리자가 그에 관한 동의를 받는 행위 자체만을 분리하여 개별적으로 판단하여서는 안 되고, 개인정보처리자가 개인정보를 취득하거나 처리에 관한 동의를 받게 된 전 과정을 살펴보아 거기에서 드러난 개인정보 수집 등의 동기와 목적, 수집 목적과 수집 대상인 개인정보의 관련성, 수집 등을 위하여 사용한 구체적인 방법, 개인정보 보호법 등 관련 법령을 준수하였는지 및 취득한 개인정보의 내용과 규모, 특히 민감정보·고유식별정보 등의 포함 여부 등을 종합적으로 고려하여 사회통념에 따라 판단하여야 한다.

피고인들이 이 사건 광고 및 경품행사의 주된 목적을 숨긴 채 사은행사를 하는 것처럼 소비자들을 오인하게 한 다음 경품행사와는 무관한 고객들의 개인정보까지 수집하여 이를 제3자에게 제공한 점, 피고인들이 이와 같은 행위를 하면서 「개인정보 보호법」상의 개인정보 보호 원칙 및 제반 의무를 위반한 점, 피고인들이 수집한 개인정보에는 사생활의 비밀에 관한 정보나 심지어는 고유식별정보 등도 포함되어 있는 점 및 피고인들이 수집한 개인정보의 규모 및 이를 제3자에게 판매함으로써 얻은 이익 등을 종합적으로 고려하여 보면, 피고인들은 개인정보 보호법 제72조 제2호에 규정된 ‘거짓이나 그 밖의 부정한 수단이나 방법으로 개인정보를 취득하거나 개인정보 처리에 관한 동의를 받는 행위를 한 자’에 해당한다고 보는 것이 옳다(대법원 2017. 4. 7. 선고 2016도13263 판결).

판례2 법 제72조제2호의 “거짓 그 밖의 부정한 수단이나 방법”의 의미(2)

구 공공기관의 개인정보보호에 관한 법률 제23조 제3항의 “거짓 그 밖의 부정한 방법”이란 법에 따른 절차에 의해서는 처리정보 보유기관으로부터 처리정보를 열람 또는 제공받을 수 없음에도 이를 열람 또는 제공받기 위하여 행하는 위계 기타 사회통념상 부정한 방법이라고 인정되는 것으로서 처리정보 열람 또는 제공에 관한 의사결정에 영향을 미칠 수 있는 적극적 및 소극적 행위를 뜻한다고 봄이 타당하며, 따라서 법 제23조 제3항 위반죄는 처리정보 보유기관의 장이 처리정보를 이용하게 하거나 제공할 수 있는 경우(법 제10조 제3항 각 호)와 관련하여 ‘거짓 그 밖의 부정한 방법’을 사용하여 처리정보를 열람 또는 제공받을 때에만 성립하는 것은 아니다(대법원 2014. 2. 27. 선고 2013도10461 판결).

3. 업무상 알게 된 개인정보의 무단 이용·제공

개인정보를 처리하거나 처리하였던 자는 ‘업무상 알게 된 개인정보를 누설하거나 권한 없이 다른 사람이 이용하도록 제공하는 행위’를 하여서는 아니 된다.

‘업무상 알게 된 개인정보’란 넓게 업무를 처리하는 과정에서 우연히 알게 된 것으로 충분하고 반드시 자신에게 부여된 업무를 처리하는 과정에서 적법하게 알게 된 것이어야 할 필요는 없다. ‘누설’이란 아직 이를 알지 못하는 타인에게 알려주는 일체의 행위이다(대법원 2015.7.9. 선고 2013도13070 판결 참고).

판례 법 제59조제2호의 “누설”과 “제공”, 같은 조 제3호의 “유출”의 상대방의 의미

「개인정보 보호법」 제71조 제5호 및 제59조 제2호에서 금지하고 있는 “누설” 또는 “제공”이나 같은 법 제71조 제6호 및 제59조 제3호에서 금지하고 있는 “유출”의 상대방은 “당해 개인정보를 처리하거나 처리하였던 사람을 제외한 모든 사람”을 의미함이 그 구성요건상 명백하다(서울고등법원 2013. 5. 30. 선고 2013노613 판결).

사례

경찰공무원이 업무 관련 시스템을 통해 알아낸 연락처를 고소장에 기재하여 이를 알지 못하는 수사기관에 제출한 경우

경찰공무원 A가 경찰이라는 직업상 지위에 기하여 업무 관련 시스템인 e-사람 조화를 통하여 경찰공무원 B 등의 휴대전화번호를 검색하여 알아낸 것은 업무상 알게 된 개인정보를 처리한 것으로서 경찰공무원 A는 「개인정보 보호법」 제59조제2호의 의무주체에 해당하며, 경찰공무원 B 등의 휴대전화번호를 고소장에 기재하여 이를 알지 못하는 수사기관에 제출한 본 건 행위는 업무상 알게 된 개인정보를 누설한 것에 해당한다. 그리고 경찰공무원 B 등의 휴대전화번호를 고소장에 기재하여 수사기관에 제출함으로써 개인정보가 개인정보처리자인 경찰청의 관리범위를 벗어나 개인정보처리자 이외의 제3자에게 제공된 결과가 되었으므로 이는 개인정보의 유출에도 해당한다(보호위원회 결정 제 2019-13-212호).

4. 정당한 권한 없이 타인 정보의 훼손·멸실·변경·위조·유출

개인정보를 처리하거나 처리하였던 자는 ‘정당한 권한 없이 또는 허용된 권한을 초과하여 다른 사람의 개인정보를 훼손, 멸실, 변경, 위조 또는 유출하는 행위’를 하여서는 아니 된다. ‘정당한 권한 없이’란 처음부터 권한을 부여받지 못하였거나 부여받은 권한을 박탈당한 상태에서 마치 권한이 있는 것처럼 한 행위를 말하고, ‘허용된 권한을 초과하여’란 권한을 부여받기는 하였으나 부여받은 권한을 넘어서서 행사하는 것을 말한다.

참고 용어해설

- 훼손 : 타인의 개인정보를 조작하거나 일부를 지우거나 다르게 만들어서 본래의 개인정보의 특성, 효용 및 사회적 가치를 손상시키거나 침해하는 행위
- 멸실 : 개인정보를 삭제·폐기·소각 등을 하여 없애버리는 행위
- 변경 : 개인정보의 내용을 본래의 것과 다르게 바꾸는 행위
- 위조 : 다른 사람을 속일 목적으로 꾸며 진짜처럼 만드는 행위
- 유출 : 법령이나 개인정보처리자의 자유로운 의사에 의하지 않고, 정보주체의 개인정보에 대하여 개인정보처리자가 통제를 상실하거나 권한 없는 자의 접근을 허용하는 행위

5. 다른 법률과의 관계

「신용정보법」은 신용정보회사등과 신용정보의 처리를 위탁받은 임직원 또는 임직원이었던 자는 업무상 알게 된 타인의 신용정보 및 사생활 등 개인적 비밀을 업무목적 외에 누설하거나 이용하는 것을 금지하는 규정을 두고 있다. 따라서 신용정보회사등은 「신용정보법」에 의한 누설금지 의무를 준수하여야 한다. 다만 「개인정보 보호법」에서는 이 외에도 개인정보를 처리하거나 처리하였던 자가 정당한 권한 없이 개인정보를 훼손하거나 거짓이나 그 밖의 부정한 수단으로 개인정보 처리 동의를 얻는 것을 금지하고 있는데 반하여, 「신용정보법」에서는 이에 대하여 규정하고 있지 않으므로, 신용정보회사등과 신용정보의 처리를 위탁받은 임직원 또는 임직원이었던 자는 이에 대하여 「개인정보 보호법」에 따른 금지의무를 준수하여야 한다.

신용정보법

제42조(업무 목적 외 누설금지 등) ① 신용정보회사등과 제17조제2항에 따라 신용정보의 처리를 위탁받은 자의 임직원이거나 임직원이었던 자(이하 “신용정보법관련자”라 한다)는 업무상 알게 된 타인의 신용정보 및 사생활 등 개인적 비밀(이하 “개인비밀”이라 한다)을 업무 목적 외에 누설하거나 이용하여서는 아니 된다.

6. 벌칙규정

위반행위	벌칙
<p>거짓 그 밖에 부정한 수단이나 방법에 의하여 개인정보를 취득하거나 개인정보 처리에 관한 동의를 얻는 행위를 한 자 및 그 사정을 알면서도 영리 또는 부정한 목적으로 개인정보를 제공받은 자 (제59조제11호 위반)</p>	<p>3년 이하의 징역 또는 3천만원 이하의 벌금 (제72조제2호)</p>
<p>업무상 알게 된 개인정보를 누설하거나 다른 사람의 이용에 제공한 자 및 그 사정을 알면서도 영리 또는 부정한 목적으로 개인정보를 제공받은 자 (제59조제2호 위반)</p>	<p>5년 이하의 징역 또는 5천만원 이하의 벌금 (제71조제5호)</p>
<p>다른 사람의 개인정보를 훼손, 멸실, 변경, 위조 또는 유출하는 행위를 한 자 (제59조제3호 위반)</p>	<p>5년 이하의 징역 또는 5천만원 이하의 벌금 (제71조제6호)</p>

제60조 | 비밀유지 등

법률

제60조(비밀유지 등) 다음 각 호의 업무에 종사하거나 종사하였던 자는 직무상 알게 된 비밀을 다른 사람에게 누설하거나 직무상 목적 외의 용도로 이용하여서는 아니 된다. 다만, 다른 법률에 특별한 규정이 있는 경우에는 그러하지 아니하다.

1. 제7조의8 및 제7조의9에 따른 보호위원회의 업무
- 1의2. 제32조의2에 따른 개인정보 보호 인증 업무
2. 제33조에 따른 영향평가 업무
3. 제40조에 따른 분쟁조정위원회의 분쟁조정 업무

이 법에 따른 조사, 검사, 심의, 인증, 평가, 조정 등의 업무에 종사하는 사람들은 다른 사람의 사생활이나 영업비밀을 다룰 기회가 많다. 따라서 본 조는 그들에게 업무상 비밀보장 의무를 부과하여 국민들이 안심하고 자료제출, 의견개진, 시설공개 등에 협력하도록 하기 위한 것이다.

1. 비밀유지 등의 의무대상자

이 조에 따른 비밀유지 등의 의무대상자는 보호위원회 업무, 개인정보 보호 인증 업무, 개인정보 영향평가 업무, 분쟁조정위원회 분쟁조정 업무에 종사하거나 종사하였던 자이다. 예컨대 보호위원회 또는 분쟁조정위원회의 전·현직 위원 및 임직원, 개인정보 보호 인증 전문기관의 전·현직 임직원, 개인정보 영향평가기관의 전·현직 임직원 등이 해당된다. 이들 기관의 전·현직 위원이나 임직원은 아니지만 이들 기관에서 자문위원, 전문위원 등의 신분으로 업무에 참여하거나 감정평가, 기술자문, 법률자문 등의 업무에 참여한 사람도 포함된다.

2. 직무상 알게 된 비밀

‘직무상 알게 된 비밀’에는 각종 법령에 의하여 비밀로 분류된 것은 물론 사회통념상 비밀로 인식될 수 있는 모든 사항이 포함된다. 즉 해당 개인·기업·국가의 입장에서 비밀로 보호할 만한 가치가 있는 것이면 된다.

예컨대 개인의 사생활, 기업의 영업비밀, 그밖에 정치·군사·외교·경제·사회적 필요에 따라 비밀로 취급해야 할 사항은 모두 이에 포함될 수 있다. 개인정보 영향평가 업무에

종사한 사람이 그 조직의 정보시스템의 보안상 취약점을 알아내 강연·발표 등에서 이를 누설하거나 해킹·협박의 수단으로 악용하는 행위는 이 법 위반에 해당한다.

3. 다른 법률에 특별한 규정

‘다른 법률에 특별한 규정’이 있는 경우에는 직무상 비밀누설 및 목적 외 이용이 예외적으로 허용된다. 예컨대 「국회에서의 증언·감정 등에 관한 법률」(제2조)에 의하여 증인 또는 참고인으로 출석 또는 감정을 요구받은 경우, 「형사소송법」(제146조, 제221조)에 의하여 증인 또는 참고인으로 소환을 받은 경우 등이다.

참고 1 국회에서의 증언·감정 등에 관한 법률

- 제4조(공무상 비밀에 관한 증언·서류등의 제출)** ① 국회로부터 공무원 또는 공무원이었던 자가 증언의 요구를 받거나, 국가기관이 서류등의 제출을 요구받은 경우에 증언할 사실이나 제출할 서류등의 내용이 직무상 비밀에 속한다는 이유로 증언이나 서류등의 제출을 거부할 수 없다. 다만, 군사·외교·대북관계의 국가기밀에 관한 사항으로서 그 발표로 말미암아 국가안위에 중대한 영향을 미친다는 주무부장관(대통령 및 국무총리의 소속기관에서는 당해 관서의 장)의 소명이 증언등의 요구를 받은 날로부터 5일 이내에 있는 경우에는 그러하지 아니하다.
- ② 국회가 제1항 단서의 소명을 수락하지 아니할 경우에는 본회의의 의결로, 폐회중에는 해당위원회의 의결로 국회가 요구한 증언 또는 서류등의 제출이 국가의 중대한 이익을 해친다는 취지의 국무총리의 성명을 요구할 수 있다.
- ③ 국무총리가 제2항의 성명의 요구를 받은 날로부터 7일 이내에 그 성명을 발표하지 아니하는 경우에는 증언이나 서류등의 제출을 거부할 수 없다.

참고 2 형사소송법

- 제147조 (공무상비밀과 증인자격)** ① 공무원 또는 공무원이었던 자가 그 직무에 관하여 알게 된 사실에 관하여 본인 또는 당해공무소가 직무상 비밀에 속한 사항을 신고한 때에는 그 소속공무소 또는 감독관공서의 승락 없이는 증인으로 신문하지 못한다.
- ② 그 소속공무소 또는 당해감독관공서는 국가에 중대한 이익을 해하는 경우를 제외하고는 승낙을 거부하지 못한다.
- 제149조 (업무상비밀과 증언거부)** 변호사, 변리사, 공증인, 공인회계사, 세무사, 대서업자, 의사, 한의사, 치과의사, 약사, 약종상, 조산사, 간호사, 종교의 직에 있는 자 또는 이러한 직에 있던 자가 그 업무상 위탁을 받은 관계로 알게 된 사실로서 타인의 비밀에 관한 것은 증언을 거부할 수 있다. 단, 본인의 승낙이 있거나 중대한 공익상 필요 있는 때에는 예외로 한다.

4. 벌칙규정

위반행위	벌칙
직무상 비밀 누설 또는 직무상 목적 외 사용 (제60조 위반)	3년 이하의 징역 또는 3천만원 이하의 벌금 (제72조제3호)

5. 질의응답

Q | '직무상 알게 된 비밀'이란?

A | 보호위원회의 심의과정에서 알게 된 국가정보기관이 보유하는 개인정보파일 현황이나 수사과정이 진행 중인 수사 관련 내용, 분쟁조정위원회의 조정과정에서 알게 된 개인의 민감한 사생활에 관한 정보, 개인정보 보호 인증 업무 또는 개인정보 영향평가 업무 수행과정에서 알게 된 기업의 영업비밀 또는 정보시스템에 관한 사항 등을 말한다.

제61조 | 의견제시 및 개선권고

<p>법률</p>	<p>제61조(의견제시 및 개선권고) ① 보호위원회는 개인정보보호에 영향을 미치는 내용이 포함된 법령이나 조례에 대하여 필요하다고 인정하면 심의·의결을 거쳐 관계 기관에 의견을 제시할 수 있다.</p> <p>② 보호위원회는 개인정보보호를 위하여 필요하다고 인정하면 개인정보처리자에게 개인정보 처리 실태의 개선을 권고할 수 있다. 이 경우 권고를 받은 개인정보처리자는 이를 이행하기 위하여 성실하게 노력하여야 하며, 그 조치 결과를 보호위원회에 알려야 한다.</p> <p>③ 관계 중앙행정기관의 장은 개인정보보호를 위하여 필요하다고 인정하면 소관 법률에 따라 개인정보처리자에게 개인정보 처리 실태의 개선을 권고할 수 있다. 이 경우 권고를 받은 개인정보처리자는 이를 이행하기 위하여 성실하게 노력하여야 하며, 그 조치 결과를 관계 중앙행정기관의 장에게 알려야 한다.</p> <p>④ 중앙행정기관, 지방자치단체, 국회, 법원, 헌법재판소, 중앙선거관리위원회는 그 소속 기관 및 소관 공공기관에 대하여 개인정보보호에 관한 의견을 제시하거나 지도·점검을 할 수 있다.</p>
<p>시행령</p>	<p>제58조(개선권고 및 징계권고) ① 법 제61조제2항·제3항에 따른 개선권고 및 법 제65조제2항·제3항에 따른 징계권고는 권고 사항, 권고 사유 및 조치 결과 회신기간 등을 분명하게 밝힌 문서로 하여야 한다.</p> <p>② 제1항에 따른 권고를 받은 자는 권고 내용에 따라 필요한 조치를 하고, 그 결과를 보호위원회 또는 관계 중앙행정기관의 장에게 문서로 통보해야 한다. 다만, 권고 내용대로 조치하기 곤란하다고 판단되는 특별한 사정이 있는 경우에는 그 사유를 통보해야 한다.</p>

1. 법령·조례에 대한 의견제시

보호위원회는 개인정보 보호에 영향을 미치는 내용이 포함된 법령이나 조례에 대하여 필요하다고 인정하면 보호위원회의 심의·의결을 거쳐 관계 기관에 의견을 제시할 수 있다. 의견제시의 예로는 타부처 법령 제·개정안, 지자체 조례 및 부처별 소관분야 지침 등에 대한 의견제시, 조약 및 협약의 제·개정에 대한 의견제시 등이 있다.

의견제시의 상대방은 관계 중앙행정기관, 지방자치단체 등 관계기관이다. 권력분립의 원칙상 국회, 법원, 헌법재판소, 중앙선거관리위원회 등 헌법기관에 대하여는 의견제시를 할 수 없다고 보아야 할 것이다.

2. 개인정보 처리실태 개선권고

가 「개인정보 보호법」에 의한 개선권고

보호위원회는 개인정보 보호를 위하여 필요하다고 인정하면 개인정보처리자에게 개인정보 처리 실태의 개선을 권고할 수 있다. 개인정보처리자의 업무관행, 내부규칙, 개인정보처리 동의서, 개인정보 처리방침, 거래약관, 안내문, 내부교육자료 등이 개선권고의 대상이 될 수 있다. 보호위원회는 「개인정보 보호법」 위반이 인정되지 않더라도 개인정보보호를 위하여 필요하다고 인정하면 개선권고를 할 수 있다. 뿐만 아니라 법 집행의 통일성과 일관성을 유지하기 위하여 공공기관은 물론 민간 기업이나 단체에 대해서도 개선권고를 할 수 있고, 금융기관, 의료기관, 교육기관, 통신사업자 등 다른 부처 소관의 민간 기업이나 단체에 대해서도 개선권고를 할 수 있다. 개선권고는 권고 사항, 권고 사유 및 조치 결과의 회신기간 등을 명시한 문서로 하여야 한다(영 제50조제1항).

나 ‘소관 법률’에 의한 개선권고

개인정보 보호와 관련한 개별법이 있는 경우 관계 중앙행정기관의 장은 소관 법률에 따라 개인정보처리자에게 개인정보 처리 실태의 개선을 권고할 수 있다. 관계 중앙행정기관의 장이 개선권고를 하려면 개인정보 보호와 관련하여 별도의 소관 법률이 있어야 하므로 「개인정보 보호법」에 의한 개선권고는 할 수 없다. 관계 중앙행정기관의 장에게 개선 권고를 부여한 것은 그 분야만의 특수성과 자율성을 존중하기 위한 것이다. 소관 법률에 의한 개선권고 또한 권고 사항, 권고 사유 및 조치 결과의 회신기간 등을 명시한 문서로 하여야 한다(영 제58조제1항).

다 조치결과의 통보의무

보호위원회 또는 관계 중앙행정기관의 장으로부터 개선권고를 받은 개인정보처리자는 이를 이행하기 위하여 성실하게 노력하여야 하며, 그 조치 결과를 개선권고를 했던 기관의 장에게 알려야 한다. 개인정보처리자가 개선권고에 따라 필요한 조치를 하고 그 결과를 통보할 때에는 문서로 하여야 한다. 다만, 권고 내용대로 조치하기 곤란하다고 판단되는 특별한 사정이 있는 경우에는 그 사유를 통보하여야 한다(영 제58조제2항).

3. 소속기관 등에 대한 의견제시 및 지도·점검

중앙행정기관, 지방자치단체, 국회, 법원, 헌법재판소, 중앙선거관리위원회는 그 소속 기관 및 소관 공공기관에 대하여 개인정보 보호에 관한 의견을 제시하거나 지도·점검을 할 수 있다.

제62조 | 침해 사실의 신고 등

<p style="text-align: center;">법률</p>	<p>제62조(침해 사실의 신고 등) ① 개인정보처리자가 개인정보를 처리할 때 개인정보에 관한 권리 또는 이익을 침해받은 사람은 보호위원회에 그 침해 사실을 신고할 수 있다.</p> <p>② 보호위원회는 제1항에 따른 신고의 접수·처리 등에 관한 업무를 효율적으로 수행하기 위하여 대통령령으로 정하는 바에 따라 전문기관을 지정할 수 있다. 이 경우 전문기관은 개인정보침해 신고센터(이하 “신고센터”라 한다)를 설치·운영하여야 한다.</p> <p>③ 신고센터는 다음 각 호의 업무를 수행한다.</p> <ol style="list-style-type: none"> 1. 개인정보 처리와 관련한 신고의 접수·상담 2. 사실의 조사·확인 및 관계자의 의견 청취 3. 제1호 및 제2호에 따른 업무에 딸린 업무 <p>④ 보호위원회에 제3항제2호의 사실 조사·확인 등의 업무를 효율적으로 하기 위하여 필요하면 「국가공무원법」 제32조의4에 따라 소속 공무원을 제2항에 따른 전문기관에 파견할 수 있다.</p>
<p style="text-align: center;">시행령</p>	<p>제59조(침해 사실의 신고 등) 보호위원회는 법 제62조제2항에 따라 개인정보에 관한 권리 또는 이익 침해 사실 신고의 접수·처리 등에 관한 업무를 효율적으로 수행하기 위한 전문기관으로 한국인터넷진흥원을 지정한다.</p>
<p style="text-align: center;">표준지침</p>	<p>제30조(개인정보 침해 사실의 신고 처리 등) ① 개인정보처리자의 개인정보 처리로 인하여 개인정보에 관한 권리 또는 이익을 침해받은 사람은 법 제62조제2항에 따른 개인정보침해 신고센터에 침해 사실을 신고할 수 있다.</p> <p>② 제1항에 따른 개인정보침해 신고센터는 다음 각 호의 업무를 수행한다.</p> <ol style="list-style-type: none"> 1. 개인정보 처리와 관련한 신고의 접수·상담 2. 개인정보 침해 신고에 대한 사실 조사·확인 및 관계자의 의견 청취 3. 개인정보처리자에 대한 개인정보 침해 사실 안내 및 시정 유도 4. 사실 조사 결과가 정보주체의 권리 또는 이익 침해 사실이 없는 것으로 판단되는 경우 신고의 종결 처리 5. 법 제43조에 따른 개인정보 분쟁조정위원회 조정 안내 등을 통한 고충 해소 지원

1. 개인정보 침해 신고

개인정보처리자의 개인정보 처리로 인해 개인정보에 관한 권리 또는 이익을 침해받은 사람은 보호위원회에 그 침해 사실을 신고할 수 있다. 권리·이익을 침해받은 정보주체 자신 뿐만 아니라 그의 법정대리인이나 임의대리인도 정보주체를 대신하여 신고할 수 있다.

2. 개인정보 침해 신고센터의 설치·운영

보호위원회는 개인정보 침해 신고의 접수·처리 등에 관한 업무를 효율적으로 수행하기 위하여 한국인터넷진흥원(KISA)을 전문기관으로 지정하고 있으며(영 제59조), 이에 따라 한국인터넷진흥원은 개인정보침해 신고센터(<http://privacy.kisa.or.kr>)를 설치·운영하고 있다. ‘개인정보침해 신고센터’는 개인정보 처리와 관련한 신고의 접수·상담, 접수된 사건에 대한 사실의 조사·확인 및 관계자 의견청취, 그 밖에 이들 업무에 딸린 부수적 업무를 수행한다.

3. 소속 공무원의 파견

보호위원회는 접수된 사건에 대한 사실 조사·확인 등의 업무(제3항제2호)를 효율적으로 수행하기 위하여 필요한 경우 「국가공무원법」 제32조의4에 따라 소속 공무원을 한국인터넷진흥원에 파견할 수 있다.

< 개인정보침해 신고센터 홈페이지 (<http://privacy.kisa.or.kr>) >

제63조(자료제출 요구 및 검사) ① 보호위원회는 다음 각 호의 어느 하나에 해당하는 경우에는 개인정보처리자에게 관계 물품·서류 등 자료를 제출하게 할 수 있다.

1. 이 법을 위반하는 사항을 발견하거나 혐의가 있음을 알게 된 경우
2. 이 법 위반에 대한 신고를 받거나 민원이 접수된 경우
3. 그 밖에 정보주체의 개인정보 보호를 위하여 필요한 경우로서 대통령령으로 정하는 경우

② 보호위원회는 개인정보처리자가 제1항에 따른 자료를 제출하지 아니하거나 이 법을 위반한 사실이 있다고 인정되면 소속 공무원으로 하여금 개인정보처리자의 사무소나 사업장에 출입하여 업무 상황, 장부 또는 서류 등을 검사하게 할 수 있다. 이 경우 검사를 하는 공무원은 그 권한을 나타내는 증표를 지니고 이를 관계인에게 내보여야 한다.

③ 관계 중앙행정기관의 장은 소관 법률에 따라 개인정보처리자에게 제1항에 따른 자료제출을 요구하거나 개인정보처리자 및 해당 법 위반사실과 관련한 관계인에 대하여 제2항에 따른 검사를 할 수 있다.

④ 보호위원회는 이 법을 위반하는 사항을 발견하거나 혐의가 있음을 알게 된 경우에는 관계 중앙행정기관의 장(해당 중앙행정기관의 장의 지휘·감독을 받아 검사권한을 수행하는 법인이 있는 경우 그 법인을 말한다)에게 구체적인 범위를 정하여 개인정보처리자에 대한 검사를 요구할 수 있으며, 필요시 보호위원회의 소속 공무원이 해당 검사에 공동으로 참여하도록 요청할 수 있다. 이 경우 그 요구를 받은 관계 중앙행정기관의 장은 특별한 사정이 없으면 이에 따라야 한다.

⑤ 보호위원회는 관계 중앙행정기관의 장(해당 중앙행정기관의 장의 지휘·감독을 받아 검사권한을 수행하는 법인이 있는 경우 그 법인을 말한다)에게 제4항에 따른 검사 결과와 관련하여 개인정보처리자에 대한 시정조치를 요청하거나, 처분 등에 대한 의견을 제시할 수 있다.

⑥ 제4항 및 제5항에 대한 방법과 절차 등에 관한 사항은 대통령령으로 정한다.

⑦ 보호위원회는 개인정보 침해사고의 예방과 효과적인 대응을 위하여 관계 중앙행정기관의 장과 합동으로 개인정보 보호실태를 점검할 수 있다.

⑧ 보호위원회와 관계 중앙행정기관의 장은 제1항 및 제2항에 따라 제출받거나 수집한 서류·자료 등을 이 법에 따른 경우를 제외하고는 제3자에게 제공하거나 일반에 공개해서는 아니 된다.

⑨ 보호위원회와 관계 중앙행정기관의 장은 정보통신망을 통하여 자료의 제출 등을 받은 경우나 수집한 자료 등을 전자화한 경우에는 개인정보·영업비밀 등이 유출되지 아니하도록 제도적·기술적 보완조치를 하여야 한다.

제60조(자료제출 요구 및 검사) ① 법 제63조제1항제3호에서 “대통령령으로 정하는 경우”란 개인정보 유출 등 정보주체의 개인정보에 관한 권리 또는 이익을 침해하는 사건·사고 등이 발생하였거나 발생할 가능성이 상당히 있는 경우를 말한다.

② 보호위원회는 법 제63조제1항 및 제2항에 따른 자료의 제출 요구 및 검사 등을 위하여 한국인터넷진흥원의 장에게 기술적인 사항을 자문하는 등 필요한 지원을 요청할 수 있다.

③ 보호위원회는 법 제63조제4항 전단에 따라 관계 중앙행정기관의 장(해당 중앙행정기관의 장의 지휘·감독을 받아 검사권한을 수행하는 법인이 있는 경우 그 법인을 말한다. 이하 이 조에서 같다)에게 검사 대상 및 사유를 정하여 개인정보처리자에 대한 검사를 요구할 수 있으며, 필요 시 보호위원회의 소속 공무원을 지정하여 해당 공무원이 검사에 공동으로 참여하도록 요청할 수 있다.

④ 제3항에 따른 요구를 받은 관계 중앙행정기관의 장은 검사 일정, 검사 범위 및 방법 등을 포함한 검사 계획을 수립하여 요구를 받은 날부터 15일 이내에 보호위원회에 통보해야 한다.

⑤ 관계 중앙행정기관의 장은 제4항에 따른 검사 계획을 통보한 날부터 60일 이내에 검사를 완료하고, 검사 결과를 보호위원회에 통보해야 한다. 다만, 검사 기간은 보호위원회와 협의하여 30일 이내의 범위에서 연장할 수 있다.

⑥ 관계 중앙행정기관의 장은 법 제63조제5항에 따라 개인정보처리자에 대한 시정조치를 요청받거나 처분 등에 대한 의견을 제시받은 경우에는 그 내용을 이행하도록 노력해야 한다.

⑦ 보호위원회는 법 제63조제7항에 따라 개인정보 침해사과의 예방과 효과적인 대응이 필요한 경우에는 보호위원회가 정하는 바에 따라 관계 중앙행정기관의 장에게 공동대응을 요청할 수 있다.

제63조의 자료제출 요구는 법 위반행위 등을 조사·확인하기 위한 것으로 법 제11조의 개인정보 보호 기본계획·실시계획 등 정책수립을 위한 자료제출과 구분된다.

1. 물품·서류 등 자료제출 요구

가 「개인정보 보호법」에 의한 자료제출 요구

보호위원회는 이 법 위반사항을 발견하거나 위반 혐의를 포착한 경우, 법 위반에 대한 신고·민원을 접수한 경우, 정보주체의 권리 또는 이익을 침해하는 사건·사고 등의 발생 또는

발생할 상당한 가능성이 있는 경우에 개인정보처리자에게 관계 물품·서류 등 자료를 제출하게 할 수 있다. 보호위원회는 공공기관은 물론 민간 기업이나 단체에 대해서도 자료제출을 요구할 수 있으며, 금융기관, 의료기관, 교육기관, 통신사업자 등 다른 부처 소관의 민간 기업이나 단체에 대해서도 자료제출을 요구할 수 있다. 이는 법 집행의 통일성과 일관성을 유지하기 위한 것이다.

나 '소관 법률' 에 의한 자료제출 요구

관계 중앙행정기관의 장은 개인정보 보호와 관련한 개별법(「신용정보법」 등)이 있는 경우에는 소관 법률에 따라 개인정보처리자에게 제1항에 따른 자료제출을 요구할 수 있다. 다만, 관계 중앙행정기관의 장은 「개인정보 보호법」에 의한 자료제출 요구는 할 수 없다. 관계 중앙행정기관의 장에게 자료제출 요구권을 부여한 것은 그 분야만의 특수성과 자율성을 존중하기 위한 것이다.

2. 사무소·사업장 등의 출입 및 검사

가 「개인정보 보호법」에 의한 출입 및 검사

보호위원회는 개인정보처리자가 자료를 제출하지 아니하거나 이 법을 위반한 사실이 있다고 인정되면 소속 공무원으로 하여금 개인정보처리자의 사무소나 사업장에 출입하여 업무 상황, 장부 또는 서류 등을 검사하게 할 수 있다. 또한 보호위원회는 공공기관은 물론 민간 기업이나 단체에 대해서도 출입 및 검사를 요구할 수 있고, 금융기관, 의료기관, 교육기관, 통신사업자 등 다른 부처 소관의 민간 기업이나 단체에 대해서도 출입 및 검사를 요구할 수 있다. 이는 법 집행의 통일성과 일관성을 유지하기 위한 것이다.

나 '소관 법률' 에 의한 출입 및 검사

관계 중앙행정기관의 장은 개인정보 보호와 관련한 소관법률(「신용정보법」 등)이 있는 경우에는 소관 법률에 따라 개인정보처리자 및 해당 법 위반사실과 관련한 관계인의 사무소나 사업장에 출입하여 업무 상황, 장부 또는 서류 등을 검사하게 할 수 있다. 다만, 관계 중앙행정기관의 장은 「개인정보 보호법」에 근거한 출입 및 검사를 할 수는 없다. 관계 중앙행정기관의 장에게 자료제출 요구권을 부여한 것은 그 분야만의 특수성과 자율성을 존중하기 위한 것이다.

다 관계인에 대한 증표제시 의무

공무원이 개인정보처리자 및 해당 법 위반사실과 관련한 관계인의 사무소나 사업장에 출입하여 업무 상황, 장부 또는 서류 등을 검사하고자 하는 경우에는 그 권한을 나타내는 증표를 지니고 이를 관계인에게 내보여야 한다.

3. 개인정보처리자에 대한 검사요구 등

보호위원회의 검사 요구 등은 2020. 2. 4. 이 법의 개정(2020. 8. 5. 시행)에 따라 새롭게 도입된 것으로 분산된 개인정보 보호 감독기능을 보호위원회로 일원화하여 개인정보 보호 컨트롤 타워 기능을 강화하기 위한 수단 중 하나이다.

가 보호위원회의 검사요구

1) 검사의 요구

보호위원회는 이 법의 위반 사항을 발견하거나 혐의가 있음을 알게 된 경우 관계 중앙행정기관의 장(해당 중앙행정기관의 장의 지휘·감독을 받아 검사권한을 수행하는 법인이 있는 경우 그 법인을 말한다)에게 개인정보처리자에 대한 검사를 요구할 수 있다. 이 경우 보호위원회는 검사 대상 및 사유를 정하여 관계 중앙행정기관의 장에게 검사를 요구할 수 있으며, 요구를 받은 관계 중앙행정기관의 장은 특별한 사정이 없으면 이에 따라야 한다. 한편, 보호위원회는 필요한 경우 보호위원회의 소속 공무원을 지정하여 해당 공무원이 검사에 공동으로 참여하도록 요청할 수 있다.

2) 검사계획의 수립·통보

검사요구를 받은 관계 중앙행정기관의 장은 검사 일정, 검사 범위 및 방법 등을 포함한 검사 계획을 수립하여 요청을 받은 날로부터 15일 이내에 보호위원회에 통보하여야 한다.

3) 검사 결과의 통보

관계 중앙행정기관의 장은 검사 계획을 통보한 날로부터 60일 이내(보호위원회와 협의하여 30일 이내 범위에서 연장 가능)에 검사를 완료하고, 그 결과를 보호위원회에 통보하여야 한다.

나 시정조치 요청 등

보호위원회는 관계 중앙행정기관의 장(해당 중앙행정기관의 장의 지휘·감독을 받아 검사권한을 수행하는 법인이 있는 경우 그 법인을 말한다)에게 제4항에 따른 검사 결과와 관련하여 개인정보처리자에 대한 시정조치를 요청하거나 처분 등에 대한 의견을 제시할 수 있다(제5항). 이 경우 시정조치 요청이나 처분 등에 대한 의견을 제시받은 관계 중앙행정기관의 장은 그 내용을 이행하도록 노력해야 한다(영 제60조제6항).

4. 개인정보 침해사고 공동 대응

보호위원회는 개인정보 침해사고의 예방과 효과적인 대응을 위하여 관계 중앙행정기관의 장과 합동으로 개인정보 보호 실태를 점검할 수 있다(제7항). 또한 보호위원회는 개인정보 침해사고의 예방과 효과적인 대응이 필요한 경우에는 관계 중앙행정기관의 장에게 공동대응을 요청할 수 있다(영 제60조제7항). 이는 부처간 중복 규제를 최소화하기 위한 것이다.

5. 서류·자료 등의 제공·공개 금지

보호위원회와 관계 중앙행정기관의 장은 개인정보처리자로부터 제출받거나 수집한 서류·자료 등을 이 법에 따른 경우를 제외하고는 제3자에게 제공하거나 일반에게 공개하여서는 아니 된다.

6. 개인정보·영업비밀 등의 보호

보호위원회와 관계 중앙행정기관의 장은 정보통신망을 통하여 자료의 제출 등을 받은 경우나 수집한 자료 등을 전자화한 경우에는 개인정보·영업비밀 등이 유출되지 아니하도록 제도적·기술적 보완조치를 하여야 한다.

7. 기술자문 등 전문기관의 지원

보호위원회는 자료의 제출 요구 및 검사 등을 위하여 필요한 경우 한국인터넷진흥원장에게 기술적인 사항에 관하여 자문하는 등 필요한 지원을 요청할 수 있다.

8. 다른 법률과의 관계

금융위원회는 신용정보회사등이 「신용정보법」 또는 「신용정보법」에 따른 명령을 준수하고 있는지 감독할 수 있고, 이를 위하여 신용정보회사등의 업무와 재산상황에 관한 보고 등을 명할 수 있으며, 금융위원회의 검사 및 요구를 거부·방해 또는 기피하는 경우에 5천만원 미만의 과태료를 부과하고 있다.

또한, 「신용정보법」은 금융위원회가 신용정보주체를 보호하고 건전한 신용질서를 확립하기 위하여 신용정보회사등에게 신용정보회사등이 보유하는 신용정보에 관한 사항, 신용정보의 처리에 관한 사항, 신용정보회사등의 업무 개선에 관한 사항, 신용정보활용체제의 공시에 관한 사항 등에 관하여 자료제출, 처리중단, 시정조치, 공시 등 필요한 조치를 명할 수 있도록 규정하고 있다.

다만, 이 경우에도 신용정보회사등이 「개인정보 보호법」을 위반한 경우에는 보호위원회가 이 법에 따라 자료제출 요구 및 검사를 할 수 있다.

한편, 「신용정보법」은 금융회사가 아닌 일반 상거래기업 및 법인에 대해서는 보호위원회에게 자료제출요구권, 검사권, 출입권, 시정명령, 과징금 및 과태료 부과 등의 권한을 부여하였다. 이에 따라, 보호위원회는 상거래기업 및 법인이 상거래정보보호규정을 위반하는 사항을 발견하거나 혐의가 있음을 알게 된 경우, 상거래정보보호규정 위반에 대한 신고·민원이 접수된 경우, 신용정보주체의 개인신용정보에 관한 권리 또는 이익을 침해하는 사건·사고 등의 발생 또는 발생할 가능성이 높은 경우 등에는 「신용정보법」에 따라 자료제출을 요구할 수 있다.

신용정보법	<p>제45조(감독·검사 등) ① 금융위원회는 신용정보회사등(데이터전문기관을 포함하며, 다음 각 호에 해당하는 자 외의 자로서 대통령령으로 정하는 자는 제외한다. 이하 이 조 및 제45조의2에서 같다)에 대하여 이 법 또는 이 법에 따른 명령의 준수 여부를 감독한다.</p> <ol style="list-style-type: none"> 1. 신용정보회사 및 채권추심회사 2. 본인신용정보관리회사 3. 신용정보집중기관 4. 신용정보제공·이용자로서 「금융위원회의 설치 등에 관한 법률」 제38조 각 호의 어느 하나에 해당하는 자 5. 제4호 외의 자로서 대통령령으로 정하는 금융업 또는 보험업을 하는 자 <p>제45조의2(금융위원회의 조치명령권) 금융위원회는 신용정보주체를 보호하고 건전한 신용질서를 확립하기 위하여 신용정보회사등에 다음 각 호의 사항에 관하여 자료제출, 처리중단, 시정조치, 공시 등 필요한 조치를 명할 수 있다.</p> <ol style="list-style-type: none"> 1. 신용정보회사등이 보유하는 신용정보에 관한 사항 2. 신용정보의 처리에 관한 사항 3. 신용정보회사등의 업무 개선에 관한 사항
-------	--

- 4. 신용정보활용체제의 공시에 관한 사항
- 5. 그 밖에 신용정보주체 보호 또는 건전한 신용질서 확립을 위하여 필요한 사항으로서 대통령령으로 정하는 사항

제45조의3(보호위원회의 자료제출 요구·조사 등) ① 보호위원회는 다음 각 호의 어느 하나에 해당하는 경우에는 제45조에 따라 금융위원회의 감독을 받지 아니하는 신용정보제공·이용자(이하 “상거래기업 및 법인”이라 한다)에게 관계 물품·서류 등 자료를 제출하게 할 수 있다.

- 1. 상거래기업 및 법인이 다음 각 목의 규정(이하 “상거래정보보호규정”이라 한다)을 위반하는 사항을 발견하거나 혐의가 있음을 알게 된 경우
 - 가. 제15조 및 제17조
 - 나. 제19조 및 제20조의2
 - 다. 제32조·제33조·제34조·제36조·제37조·제38조·제38조의3·제39조의4·제40조의2 및 제42조
 - 2. 상거래기업 및 법인의 상거래정보보호규정 위반에 대한 신고를 받거나 민원이 접수된 경우
 - 3. 그 밖에 개인신용정보 보호를 위하여 필요한 경우로서 대통령령으로 정하는 경우
- ② 보호위원회는 상거래기업 및 법인이 제1항에 따른 자료를 제출하지 아니하거나 상거래정보보호규정을 위반한 사실이 있다고 인정되면 소속 공무원으로 하여금 상거래기업 및 법인 및 상거래정보보호규정 위반사실과 관련한 관계인의 사무소나 사업장에 출입하여 업무 상황, 장부 또는 서류 등을 조사하게 할 수 있다. 이 경우 검사를 하는 공무원은 그 권한을 나타내는 증표를 지니고 이를 관계인에게 내보여야 한다.
- ③ 보호위원회는 제1항에 따라 제출받거나 수집한 서류·자료 등을 이 법에 따른 경우를 제외하고는 제3자에게 제공하거나 일반에게 공개하여서는 아니 된다.
 - ④ 보호위원회는 정보통신망을 통하여 자료의 제출 등을 받은 경우나 수집한 자료 등을 전자화한 경우에는 개인신용정보·영업비밀 등이 유출되지 아니하도록 제도적·기술적 보안조치를 하여야 한다.

제52조(과태료) ④ 다음 각 호의 어느 하나에 해당하는 자에게는 5천만원 이하의 과태료를 부과한다.

- 7. 제45조제2항부터 제4항까지의 규정에 따른 명령에 따르지 아니하거나 검사 및 요구를 거부·방해 또는 기피한 자

제64조(시정조치 등) ① 보호위원회는 개인정보가 침해되었다고 판단할 상당한 근거가 있고 이를 방지할 경우 회복하기 어려운 피해가 발생할 우려가 있다고 인정되면 이 법을 위반한 자(중앙행정기관, 지방자치단체, 국회, 법원, 헌법재판소, 중앙선거관리위원회는 제외한다)에 대하여 다음 각 호에 해당하는 조치를 명할 수 있다.

1. 개인정보 침해행위의 중지
2. 개인정보 처리의 일시적인 정지
3. 그 밖에 개인정보의 보호 및 침해 방지를 위하여 필요한 조치

② 관계 중앙행정기관의 장은 개인정보가 침해되었다고 판단할 상당한 근거가 있고 이를 방지할 경우 회복하기 어려운 피해가 발생할 우려가 있다고 인정되면 소관 법률에 따라 개인정보처리자에 대하여 제1항 각 호에 해당하는 조치를 명할 수 있다.

③ 지방자치단체, 국회, 법원, 헌법재판소, 중앙선거관리위원회는 그 소속 기관 및 소관 공공기관이 이 법을 위반하였을 때에는 제1항 각 호에 해당하는 조치를 명할 수 있다.

④ 보호위원회는 중앙행정기관, 지방자치단체, 국회, 법원, 헌법재판소, 중앙선거관리위원회가 이 법을 위반하였을 때에는 해당 기관의 장에게 제1항 각 호에 해당하는 조치를 하도록 권고할 수 있다. 이 경우 권고를 받은 기관은 특별한 사유가 없으면 이를 존중하여야 한다.

제65조(고발 및 징계권고) ① 보호위원회는 개인정보처리자에게 이 법 등 개인정보보호와 관련된 법규의 위반에 따른 범죄혐의가 있다고 인정될 만한 상당한 이유가 있을 때에는 관할 수사기관에 그 내용을 고발할 수 있다.

② 보호위원회는 이 법 등 개인정보보호와 관련된 법규의 위반행위가 있다고 인정될 만한 상당한 이유가 있을 때에는 책임이 있는 자(대표자 및 책임있는 임원을 포함한다)를 징계할 것을 해당 개인정보처리자에게 권고할 수 있다. 이 경우 권고를 받은 사람은 이를 존중하여야 하며 그 결과를 보호위원회에 통보하여야 한다.

③ 관계 중앙행정기관의 장은 소관 법률에 따라 개인정보처리자에 대하여 제1항에 따른 고발을 하거나 소속 기관·단체 등의 장에게 제2항에 따른 징계권고를 할 수 있다. 이 경우 제2항에 따른 권고를 받은 사람은 이를 존중하여야 하며 그 결과를 관계 중앙행정기관의 장에게 통보하여야 한다.

제66조(결과의 공표) ① 보호위원회는 제61조에 따른 개선권고, 제64조에 따른 시정조치 명령, 제65조에 따른 고발 또는 징계권고 및 제75조에 따른 과태료 부과 내용 및 결과에 대하여 공표할 수 있다.

② 관계 중앙행정기관의 장은 소관 법률에 따라 제1항에 따른 공표를 할 수 있다.

	<p>③ 제1항 및 제2항에 따른 공표의 방법, 기준 및 절차 등은 대통령령으로 정한다.</p>
<p style="text-align: center;">시행령</p>	<p>제61조(결과의 공표) ① 보호위원회 및 관계 중앙행정기관의 장은 법 제66조제1항 및 제2항에 따라 다음 각 호의 사항을 인터넷 홈페이지 또는 「신문 등의 진흥에 관한 법률」에 따라 전국을 보급지역으로 하는 일반일간신문 등에 게재하여 공표할 수 있다.</p> <ol style="list-style-type: none"> 1. 위반행위의 내용 2. 위반행위를 한 자 3. 개선권고, 시정조치 명령, 고발, 징계권고 및 과태료 부과の内容 및 결과 <p>② 보호위원회 및 관계 중앙행정기관의 장은 법 제66조제1항 및 제2항에 따라 제1항 각 호의 사항을 공표하려는 경우에는 위반행위의 내용 및 정도, 위반기간 및 횟수, 위반행위로 인하여 발생한 피해의 범위 및 결과 등을 고려하여야 한다.</p> <p>③ 보호위원회 및 관계 중앙행정기관의 장은 보호위원회의 심의·의결 전에 공표대상자에게 공표대상자라는 사실을 알려 소명자료를 제출하거나 의견을 진술할 수 있는 기회를 주어야 한다.</p>

이 법은 신고, 조사 등을 통해 개인정보처리자의 법 위반사실이 확인된 경우 시정명령 등을 통해 위법행위를 바로 잡고, 범칙행위 등에 대해서는 고발·징계하게 함으로써 법 위반행위가 반복되지 않도록 하기 위해 다양한 사후 구제 및 제재 조치를 마련하고 있다.

1. 시정조치 명령

보호위원회 또는 관계 중앙행정기관의 장은 신고, 조사 등을 통해 개인정보처리자의 법 위반사실이 확인된 경우 당해 위법행위를 바로잡기 위해 시정조치 등을 명할 수 있다. 시정조치 등을 명하기 위해서는 이 법 위반으로 인해 개인정보가 침해되었다고 판단할 만한 상당한 근거가 있고 이를 방지할 경우 회복하기 어려운 피해가 발생할 우려가 있다고 인정되어야 한다.

보호위원회는 또는 관계 중앙행정기관의 장은 개인정보 침해행위의 중지, 개인정보 처리의 일시적인 정지, 그밖에 개인정보의 보호 및 침해방지를 위하여 필요한 조치를 명할 수 있다. ‘그 밖에 개인정보의 보호 및 침해 방지를 위하여 필요한 조치’에는 개인정보 유출사이트 차단, 기술적·관리적 보호조치, 개인정보 처리방침 또는 약관의 개정 등이 포함될 수 있다.

보호위원회는 공공기관은 물론 민간 기업이나 단체·개인에 대해서도 시정조치를 명할

수 있으나 중앙행정기관, 지방자치단체, 국회, 법원, 헌법재판소, 중앙선거관리위원회에 대하여는 시정조치를 명할 수 없다(제64조제1항). 또한 보호위원회는 지방자치단체에 대해서는 시정조치 명령을 내릴 수 없으나 해당 지방자치단체의 지방공기업, 지방공단 등에 대해서는 시정조치를 명할 수 있다.

관계 중앙행정기관의 장은 개인정보가 침해되었다고 판단할 만한 상당한 근거가 있고 이를 방지할 경우 회복하기 어려운 피해가 발생할 우려가 있다고 인정되면 개인정보보호와 관련한 개별법이 있는 경우에는 소관 법률에 따라 제1항 각 호에 해당하는 조치를 명할 수 있다(제64조제2항).

지방자치단체, 국회, 법원, 헌법재판소, 중앙선거관리위원회는 그 소속 기관 및 소관 공공기관이 이 법을 위반하였을 때에는 제1항 각 호에 해당하는 조치를 명할 수 있다(제64조제3항).

2. 시정조치 권고

중앙행정기관, 지방자치단체, 국회, 법원, 헌법재판소, 중앙선거관리위원회가 이 법을 위반하였을 때에는 보호위원회가 해당 기관의 장에게 개인정보 침해해위의 중지, 개인정보 처리의 일시적인 정지, 그밖에 개인정보의 보호 및 침해방지를 위하여 필요한 조치를 하도록 권고할 수 있다. 보호위원회의 시정조치 권고를 받은 기관은 특별한 사유가 없으면 이를 존중하여야 한다. 보호위원회가 중앙행정기관, 지방자치단체 등에 대하여 시정조치를 권고하기 위해서는 제8조에 따라 심의·의결을 거쳐야 한다.

3. 법 위반자의 고발 및 징계권고

가 수사기관에 고발

보호위원회는 개인정보처리자에게 이 법 등 개인정보 보호와 관련된 법규의 위반에 따른 범죄혐의가 있다고 인정될 만한 상당한 이유가 있을 때에는 관할 수사기관에 그 내용을 고발할 수 있다(제1항).

관계 중앙행정기관의 장도 소관 법률에 따라 개인정보처리자에 대하여 제1항에 따른 고발을 할 수 있다. 다만, 관계 중앙행정기관의 장은 ‘소관 법률’에 따라 고발을 할 수 있을 뿐이므로 별도의 소관 법률에 관련 규정이 없으면 고발할 수 없다(제3항).

나 소속기관 등에 대한 징계권고

보호위원회는 이 법 등 개인정보 보호와 관련된 법규의 위반행위가 있다고 인정될 만한 상당한 이유가 있을 때에는 책임이 있는 자(대표자 및 책임 있는 임원을 포함한다)를 징계할 것을 그 소속 기관·단체 등의 장에게 권고할 수 있다(제2항).

관계 중앙행정기관의 장도 그 소관 법률에 따라 소속 기관·단체 등의 장에게 징계를 권고할 수 있다(제3항). 관계 중앙행정기관의 장은 ‘소관 법률’에 따라 징계를 권고할 수 있을 뿐이므로 별도의 소관 법률에 관련 규정이 없으면 징계를 권고할 수 없다.

제65조제2항·제3항에 따른 징계권고는 권고 사항, 권고 사유 및 조치 결과의 회신기간 등을 명시한 문서로 하여야 한다(영 제58조제1항). 징계권고를 받은 자는 이를 존중하여야 하며 권고 내용에 따라 필요한 조치를 하고 그 결과를 보호위원회 또는 관계 중앙행정기관의 장에게 문서로 통보하여야 한다. 다만, 권고 내용대로 조치하기 곤란하다고 판단되는 특별한 사정이 있는 경우에는 그 사유를 통보하여야 한다(영 제58조제2항).

4. 시정조치 명령 등의 결과 공표

보호위원회는 이 법에 따른 개선권고(제61조), 시정조치 명령(제64조), 고발 또는 징계권고(제65조), 과태료 부과(제75조)의 내용과 결과를 인터넷 홈페이지 등에 공표할 수 있다(제66조제1항). 행정처분 결과 공표제도는 「개인정보 보호법」 위반에 대한 행정처분 결과를 공개해 경각심을 고취하기 위해 도입된 제도이다.

관계 중앙행정기관의 장은 소관 법률에 따라 개선권고(제61조), 시정조치 명령(제64조), 고발 또는 징계권고(제65조), 과태료 부과(제75조)의 내용과 결과를 인터넷 홈페이지 등에 공표할 수 있다(제66조제2항). 관계 중앙행정기관의 장은 ‘소관 법률’에 따라 시정조치 명령 등의 결과를 공표할 수 있을 뿐이므로 소관 법률에 이 법에 따른 개선권고(제61조), 시정조치 명령(제64조), 고발 또는 징계권고(제65조), 과태료 부과(제75조)의 내용에 준하는 별도의 규정이 없으면 결과를 공표할 수 없다.

5. 결과 공표의 방법·절차 등

가 결과 공표의 방법

보호위원회 또는 관계 중앙행정기관의 장이 시정조치 명령 등의 결과를 공표하고자 하는 경우에는 위반행위의 내용, 위반행위를 한 자, 개선권고, 시정조치 명령, 고발, 징계권고

및 과태료 부과 내용 및 결과를 인터넷 홈페이지 또는 「신문 등의 진흥에 관한 법률」에 따라 전국을 보급지역으로 하는 일반일간신문 등에 게재하여 공표할 수 있다.

나 결과 공표시 고려사항

보호위원회 또는 관계 중앙행정기관의 장이 시정조치 명령 등의 결과를 공표하고자 하는 경우에 위반행위의 내용 및 정도, 위반 기간 및 횟수, 위반행위로 인하여 발생한 피해의 범위 및 결과 등을 고려하여야 한다.

다 결과 공표의 절차

시정조치 명령 등의 결과 공표는 보호위원회의 심의·의결 사항에 해당하므로(제7조의9 제1항제12호 참고), 보호위원회 및 관계 중앙행정기관의 장은 보호위원회의 심의·의결 전에 공표대상자에게 공표대상자임을 알리고 소명자료를 제출하거나 의견을 진술할 수 있는 기회를 주어야 한다(영 제61조제3항).

6. 다른 법률과의 관계

「신용정보법」은 금융위원회와 금융감독원으로 하여금 신용정보회사등이 이 법 또는 이 법에 따른 명령을 위반하여 신용정보업의 건전한 경영과 신용정보주체의 권익을 해칠 우려가 있다고 인정되는 경우 신용정보회사등에 대한 주의 또는 경고, 임원에 대한 주의 또는 경고, 직원에 대한 주의 및 정직, 감봉, 견책 등의 문책 요구, 임원에 대한 해임권고, 직무정지 요구 또는 직원에 대한 면직 요구, 위반행위에 대한 시정명령, 신용정보제공의 중지 등의 조치를 취할 수 있다.

또한, 「신용정보법」은 금융위원회가 신용정보주체를 보호하고 건전한 신용질서를 확립하기 위하여 신용정보회사등에게 신용정보회사등이 보유하는 신용정보에 관한 사항, 신용정보의 처리에 관한 사항, 신용정보회사등의 업무 개선에 관한 사항, 신용정보활용체제의 공시에 관한 사항 등에 관하여 자료제출, 처리중단, 시정조치, 공시 등 필요한 조치를 명할 수 있도록 규정하고 있다.

다만, 이 경우에도 신용정보회사등이 「개인정보 보호법」을 위반한 경우에는 보호위원회가 「개인정보 보호법」에 따라 시정조치 등을 명할 수 있다.

한편, 「신용정보법」은 금융회사가 아닌 일반 상거래기업 및 법인에 대해서는 보호위원회에게 자료제출요구권, 검사권, 출입권, 시정명령, 과징금 및 과태료 부과 등의 권한을

부여하였다. 이에 따라, 보호위원회는 상거래정보보호규정과 관련하여 개인신용정보가 침해되었다고 판단할 상당한 근거가 있고 이를 방지할 경우 회복하기 어려운 피해가 발생할 우려가 있다고 인정되면 상거래기업 및 법인에 대하여 「신용정보법」에 따라 개인신용정보 침해행위의 중지, 개인신용정보 처리의 일시적인 정지 등의 조치를 명할 수 있다.

신용정보법	<p>제45조(감독·검사 등) ⑦ 금융위원회는 신용정보회사등이 이 법(채권추심회사의 경우에는 「채권의 공정한 추심에 관한 법률」을 포함한다. 이하 이 항에서 같다) 또는 이 법에 따른 명령을 위반하여 신용정보 관련 산업의 건전한 경영과 신용정보주체의 권익을 해칠 우려가 있다고 인정하면 다음 각 호의 어느 하나에 해당하는 조치를 하거나, 금융감독원장으로 하여금 제1호부터 제3호까지의 규정에 해당하는 조치를 하게 할 수 있다.</p> <ol style="list-style-type: none"> 1. 신용정보회사등에 대한 주의 또는 경고 2. 임원에 대한 주의 또는 경고 3. 직원에 대한 주의 및 정직, 감봉, 견책 등의 문책 요구 4. 임원에 대한 해임권고, 직무정지 또는 직원에 대한 면직 요구 5. 위반행위에 대한 시정명령 6. 신용정보제공의 중지 <p>제45조의2(금융위원회의 조치명령권) 금융위원회는 신용정보주체를 보호하고 건전한 신용질서를 확립하기 위하여 신용정보회사등에 다음 각 호의 사항에 관하여 자료제출, 처리중단, 시정조치, 공시 등 필요한 조치를 명할 수 있다.</p> <ol style="list-style-type: none"> 1. 신용정보회사등이 보유하는 신용정보에 관한 사항 2. 신용정보의 처리에 관한 사항 3. 신용정보회사등의 업무 개선에 관한 사항 4. 신용정보활용체제의 공시에 관한 사항 5. 그 밖에 신용정보주체 보호 또는 건전한 신용질서 확립을 위하여 필요한 사항으로서 대통령령으로 정하는 사항 <p>제45조의4(보호위원회의 시정조치) 보호위원회는 상거래정보보호규정과 관련하여 개인신용정보가 침해되었다고 판단할 상당한 근거가 있고 이를 방지할 경우 회복하기 어려운 피해가 발생할 우려가 있다고 인정되면 상거래기업 및 법인에 대하여 다음 각 호에 해당하는 조치를 명할 수 있다.</p> <ol style="list-style-type: none"> 1. 개인신용정보 침해행위의 중지 2. 개인신용정보 처리의 일시적인 정지 3. 그 밖에 개인정보의 보호 및 침해 방지를 위하여 필요한 조치
-------	--

제67조(연차보고) ① 보호위원회는 관계 기관 등으로부터 필요한 자료를 제출 받아 매년 개인정보보호정책의 수립 및 시행에 관한 보고서를 작성하여 정기국회 개회 전까지 국회에 제출(정보통신망에 의한 제출을 포함한다)하여야 한다.

② 제1항에 따른 보고서에는 다음 각 호의 내용이 포함되어야 한다.

1. 정보주체의 권리침해 및 그 구제현황
2. 개인정보 처리에 관한 실태조사 등의 결과
3. 개인정보보호정책의 추진현황 및 실적
4. 개인정보 관련 해외의 입법 및 정책 동향
5. 주민등록번호 처리와 관련된 법률·대통령령·국회규칙·대법원규칙·헌법재판소규칙·중앙선거관리위원회규칙 및 감사원규칙의 제정·개정 현황
6. 그 밖에 개인정보 보호정책에 관하여 공개 또는 보고하여야 할 사항

연차보고서란 개인정보 보호정책의 수립 및 시행에 관하여 매년 작성되는 보고서를 말한다. 연차보고서에는 정보주체의 권리침해 및 그 구제 현황, 개인정보 처리에 관한 실태조사 등의 결과, 개인정보보호정책의 추진현황 및 실적, 개인정보 관련 해외의 입법 및 정책 동향, 주민등록번호 처리와 관련된 법률·대통령령·국회규칙·대법원규칙·헌법재판소규칙·중앙선거관리위원회규칙 및 감사원규칙의 제정·개정 현황, 그 밖에 개인정보보호정책에 관하여 공개 또는 보고하여야 할 사항이 포함되어야 한다.

연차보고서는 보호위원회가 관계기관 등(행정안전부 등 관계 중앙행정기관, 지방자치단체, 헌법기관, 분쟁조정위원회 등)으로부터 필요한 자료를 제출 받아 작성하여 정기국회 개회 전까지 국회에 제출한다.

제68조 | 권한의 위임·위탁

법률	<p>제68조(권한의 위임·위탁) ① 이 법에 따른 보호위원회 또는 관계 중앙행정기관의 장의 권한은 그 일부를 대통령령으로 정하는 바에 따라 특별시장, 광역시장, 도지사, 특별자치도지사 또는 대통령령으로 정하는 전문기관에 위임하거나 위탁할 수 있다.</p> <p>② 제1항에 따라 보호위원회 또는 관계 중앙행정기관의 장의 권한을 위임 또는 위탁받은 기관은 위임 또는 위탁받은 업무의 처리 결과를 보호위원회 또는 관계 중앙행정기관의 장에게 통보하여야 한다.</p> <p>③ 보호위원회는 제1항에 따른 전문기관에 권한의 일부를 위임하거나 위탁하는 경우 해당 전문기관의 업무 수행을 위하여 필요한 경비를 출연할 수 있다.</p>
시행령	<p>제62조(권한의 위탁) ① <삭제></p> <p>② 보호위원회는 법 제24조의2제4항에 따른 대체가입수단 제공의 지원에 관한 권한을 다음 각 호의 어느 하나의 기관에 위탁할 수 있다.</p> <ol style="list-style-type: none">1. 「전자정부법」 제72조제1항에 따른 한국지역정보개발원2. 한국인터넷진흥원3. 대체가입수단의 개발·제공·관리 업무를 안전하게 수행할 수 있는 기술적·재정적 능력과 설비를 보유한 것으로 인정되어 행정자치부장관이 고시하는 법인·기관·단체 <p>③ 보호위원회는 다음 각 호의 권한을 한국인터넷진흥원에 위탁한다.</p> <ol style="list-style-type: none">1. 법 제13조제1호에 따른 개인정보보호에 관한 교육·홍보2. 법 제33조제5항에 따른 관계 전문가의 육성 및 영향평가 기준의 개발3. 법 제35조제2항에 따른 열람 요구의 접수 및 처리4. 법 제63조에 따른 자료제출 요구 및 검사(법 제62조에 따라 개인정보침해 신고센터에 접수된 신고의 접수·처리 및 상담과 관련된 사항만 해당한다)5. 제37조제2항에 따른 평가기관 지정신청서의 접수 및 같은 조 제6항에 따른 신고 사항의 접수 <p>④ 보호위원회는 제2항에 따라 권한을 위탁하는 경우에는 그 수탁자 및 위탁 업무를 고시해야 한다.</p>

1. 지방자치단체에 대한 권한 위임

보호위원회 또는 관계 중앙행정기관의 장의 권한은 그 일부를 대통령령으로 정하는 바에 따라 특별시장, 광역시장, 도지사, 특별자치도지사에게 위임할 수 있다.

2. 전문기관에 대한 권한 위탁

보호위원회는 한국지역정보개발원, 한국인터넷진흥원 등 전문기관에 다음의 권한을 위탁한다. 다만, 법 제24조의2제4항에 따른 대체가입수단 제공의 지원은 현재는 한국지역정보개발원에 대해서만 위탁되어 있다.

보호위원회는 권한의 일부를 위임하거나 위탁하는 경우에는 해당 전문기관의 업무 수행을 위하여 필요한 경비를 출연할 수 있다.

전문기관	위탁 권한 내용
한국지역정보개발원	· 제24조의2제4항에 따른 대체가입수단 제공의 지원
한국인터넷진흥원	· 제13조제1호에 따른 개인정보보호에 관한 교육·홍보 · 제33조제5항에 따른 관계 전문가의 육성 및 영향평가 기준의 개발 · 제35조제2항에 따른 열람 요구의 접수 및 처리 · 제63조에 따른 자료제출 요구 및 검사(법 제62조에 따라 개인정보침해 신고센터에 접수된 신고의 접수·처리 및 상담과 관련된 사항만 해당한다) · 제37조제2항에 따른 평가기관 지정신청서의 접수 및 같은 조 제6항에 따른 신고 사항의 접수

3. 위임·위탁업무 처리 결과의 통보

보호위원회 또는 관계 중앙행정기관의 장의 권한을 위임 또는 위탁받은 기관은 위임 또는 위탁받은 업무의 처리 결과를 보호위원회 또는 관계 중앙행정기관의 장에게 통보하여야 한다.

제69조 | 벌칙 적용 시의 공무원 의제

법률

- 제69조(벌칙 적용 시의 공무원 의제)** ① 보호위원회의 위원 중 공무원이 아닌 위원 및 공무원이 아닌 직원은 「형법」이나 그 밖의 법률에 따른 벌칙을 적용할 때에는 공무원으로 본다.
- ② 보호위원회 또는 관계 중앙행정기관의 장의 권한을 위탁한 업무에 종사하는 관계 기관의 임직원은 「형법」 제129조부터 제132조까지의 규정을 적용할 때에는 공무원으로 본다.

보호위원회의 위원 중 공무원이 아닌 위원 및 공무원이 아닌 직원에게 「형법」 제129조(수뢰, 사전수뢰), 제130조(제삼자뇌물제공), 제131조(수뢰후부정처사, 사후수뢰), 제132조(알선수뢰)의 규정을 적용함에 있어서는 그를 공무원으로 본다. 보호위원회 또는 관계 중앙행정기관의 장의 권한을 위탁한 업무에 종사하는 관계 기관의 임직원 또한 마찬가지이다. 그 업무의 특성상 공무원에 준하는 청렴의무가 부과되기 때문이다. ‘공무원으로 본다’는 것은 일반인의 경우에는 처벌 받지 않을 행위일지라도 그를 공무원으로 보아 처벌하겠다는 의미이다.

형법

- 제129조(수뢰, 사전수뢰)** ① 공무원 또는 중재인이 그 직무에 관하여 뇌물을 수수, 요구 또는 약속한 때에는 5년 이하의 징역 또는 10년 이하의 자격정지에 처한다.
- ② 공무원 또는 중재인이 될 자가 그 담당할 직무에 관하여 청탁을 받고 뇌물을 수수, 요구 또는 약속한 후 공무원 또는 중재인이 된 때에는 3년 이하의 징역 또는 7년 이하의 자격정지에 처한다.
- 제130조(제삼자뇌물제공)** 공무원 또는 중재인이 그 직무에 관하여 부정한 청탁을 받고 제3자에게 뇌물을 공여하게 하거나 공여를 요구 또는 약속한 때에는 5년 이하의 징역 또는 10년 이하의 자격정지에 처한다.
- 제131조(수뢰후부정처사, 사후수뢰)** ① 공무원 또는 중재인이 전2조의 죄를 범하여 부정한 행위를 한 때에는 1년 이상의 유기징역에 처한다.
- ② 공무원 또는 중재인이 그 직무상 부정한 행위를 한 후 뇌물을 수수, 요구 또는 약속하거나 제삼자에게 이를 공여하게 하거나 공여를 요구 또는 약속한 때에도 전항의 형과 같다.
- ③ 공무원 또는 중재인이었던 자가 그 재직 중에 청탁을 받고 직무상 부정한 행위를 한 후 뇌물을 수수, 요구 또는 약속한 때에는 5년 이하의 징역 또는 10년 이하의 자격정지에 처한다.
- ④ 전3항의 경우에는 10년 이하의 자격정지를 병과할 수 있다.
- 제132조(알선수뢰)** 공무원이 그 지위를 이용하여 다른 공무원의 직무에 속한 사항의 알선에 관하여 뇌물을 수수, 요구 또는 약속한 때에는 3년 이하의 징역 또는 7년 이하의 자격정지에 처한다.

제10장 벌칙

제70조 벌칙

제71조 벌칙

제72조 벌칙

제73조 벌칙

제74조 양벌규정

제74조의2 몰수·추징 등

제75조 과태료

제76조 과태료에 관한 규정 적용의 특례



제70조(벌칙) 다음 각 호의 어느 하나에 해당하는 자는 10년 이하의 징역 또는 1억원 이하의 벌금에 처한다.

1. 공공기관의 개인정보 처리업무를 방해할 목적으로 공공기관에서 처리하고 있는 개인정보를 변경하거나 말소하여 공공기관의 업무 수행의 중단·마비 등 심각한 지장을 초래한 자
2. 거짓이나 그 밖의 부정한 수단이나 방법으로 다른 사람이 처리하고 있는 개인정보를 취득한 후 이를 영리 또는 부정한 목적으로 제3자에게 제공한 자와 이를 교사·알선한 자

제71조(벌칙) 다음 각 호의 어느 하나에 해당하는 자는 5년 이하의 징역 또는 5천만원 이하의 벌금에 처한다.

1. 제17조제1항제2호에 해당하지 아니함에도 같은 항 제1호를 위반하여 정보주체의 동의를 받지 아니하고 개인정보를 제3자에게 제공한 자 및 그 사정을 알고 개인정보를 제공받은 자
2. 제18조제1항·제2항(제39조의14에 따라 준용되는 경우를 포함한다), 제19조, 제26조제5항, 제27조제3항 또는 제28조의2를 위반하여 개인정보를 이용하거나 제3자에게 제공한 자 및 그 사정을 알면서도 영리 또는 부정한 목적으로 개인정보를 제공받은 자
3. 제23조제1항을 위반하여 민감정보를 처리한 자
4. 제24조제1항을 위반하여 고유식별정보를 처리한 자
- 4의2. 제28조의3을 위반하여 가명정보를 처리하거나 제3자에게 제공한 자 및 그 사정을 알면서도 영리 또는 부정한 목적으로 가명정보를 제공받은 자
- 4의3. 제28조의5제1항을 위반하여 특정 개인을 알아보기 위한 목적으로 가명정보를 처리한 자
- 4의4. 제36조제2항(제27조에 따라 정보통신서비스 제공자등으로부터 개인정보를 이전받은 자와 제39조의14에 따라 준용되는 경우를 포함한다)을 위반하여 정정·삭제 등 필요한 조치(제38조제2항에 따른 열람등요구에 따른 필요한 조치를 포함한다)를 하지 아니하고 개인정보를 이용하거나 이를 제3자에게 제공한 정보통신서비스 제공자등
- 4의5. 제39조의3제1항(제39조의14에 따라 준용되는 경우를 포함한다)을 위반하여 이용자의 동의를 받지 아니하고 개인정보를 수집한 자
- 4의6. 제39조의3제4항(제39조의14에 따라 준용되는 경우를 포함한다)을 위반하여 법정대리인의 동의를 받지 아니하거나 법정대리인이 동의하였는지를 확인하지 아니하고 만 14세 미만인 아동의 개인정보를 수집한 자
5. 제59조제2호를 위반하여 업무상 알게 된 개인정보를 누설하거나 권한 없

이 다른 사람이 이용하도록 제공한 자 및 그 사정을 알면서도 영리 또는 부정한 목적으로 개인정보를 제공받은 자

6. 제59조제3호를 위반하여 다른 사람의 개인정보를 훼손, 멸실, 변경, 위조 또는 유출한 자

제72조(벌칙) 다음 각 호의 어느 하나에 해당하는 자는 3년 이하의 징역 또는 3천만원 이하의 벌금에 처한다.

1. 제25조제5항을 위반하여 영상정보처리기기의 설치 목적과 다른 목적으로 영상정보처리기기를 임의로 조작하거나 다른 곳을 비추는 자 또는 녹음기능을 사용한 자
2. 제59조제1호를 위반하여 거짓이나 그 밖의 부정한 수단이나 방법으로 개인정보를 취득하거나 개인정보 처리에 관한 동의를 받는 행위를 한 자 및 그 사정을 알면서도 영리 또는 부정한 목적으로 개인정보를 제공받은 자
3. 제60조를 위반하여 직무상 알게 된 비밀을 누설하거나 직무상 목적 외에 이용한 자

제73조(벌칙) 다음 각 호의 어느 하나에 해당하는 자는 2년 이하의 징역 또는 2천만원 이하의 벌금에 처한다.

1. 제23조제2항, 제24조제3항, 제25조제6항, 제28조의4제1항 또는 제29조를 위반하여 안전성 확보에 필요한 조치를 하지 아니하여 개인정보를 분실·도난·유출·위조·변조 또는 훼손당한 자
2. 제21조제1항(제39조의14에 따라 준용되는 경우를 포함한다)을 위반하여 개인정보를 파기하지 아니한 정보통신서비스 제공자등
3. 제36조제2항을 위반하여 정정·삭제 등 필요한 조치를 하지 아니하고 개인정보를 계속 이용하거나 이를 제3자에게 제공한 자
3. 제37조제2항을 위반하여 개인정보의 처리를 정지하지 아니하고 계속 이용하거나 제3자에게 제공한 자

이 법 위반행위에 대해서는 보호 법익의 중요성, 예상되는 피해의 규모 및 사회적 비용 등에 따라 4단계로 나누어 형사벌을 부과하도록 규정하고 있다.

조문	위반행위	벌칙수준	제재이유
제70조	<ol style="list-style-type: none"> 1. 공공기관의 개인정보처리 업무를 방해할 목적으로 공공기관에서 처리하는 개인정보를 변경 또는 말소하여 공공기관의 업무수행에 심각한 지장을 초래한 자 2. 거짓 기타 부정한 수단·방법으로 개인정보를 취득한 후 영리 또는 부정한 목적으로 제3자에게 제공하거나 이를 알선한 자 	10년 이하 징역 또는 1억원 이하 벌금	<ul style="list-style-type: none"> ☞ 행정기관의 각종 공적 업무수행에 차질이 발생할 수 있고, 행정처리의 오류 발생으로 일반 국민의 권익침해 가능성이 매우 높을 뿐 아니라, 행정기관의 업무 방해라는 고의적·악의적 목적이 있으므로 강력 제재 ☞ 다른 사람이 처리하고 있는 개인정보를 부당하게 취득하여 불법 유통시킴으로 인해 막대한 부당이익을 얻는 행위를 엄중하게 처벌할 필요성 제기

조문	위반행위	벌칙수준	제재이유
제71조	<p>1. 정보주체의 동의없이 개인정보를 제3자에게 제공한 자 (그 사정을 알고 제공받은 자 포함)</p> <p>2. 불법정보인 사정을 알고 개인정보를 이용하거나 제공한 자 (그 사정을 알고 영리 또는 부정한 목적으로 제공 받은 자 포함)</p> <p>3. 민감정보 처리기준을 위반한 자</p> <p>4. 고유식별정보 처리기준을 위반한 자</p> <p>4의2. 가명정보 결합 제한기준을 위반하여 가명정보를 처리하거나 제공한 자 (그 사정을 알고 영리 또는 부정한 목적으로 제공받은 자 포함)</p> <p>4의3. 특정 개인을 알아보기 위한 목적으로 가명정보를 처리한 자</p> <p>4의4. 개인정보 정정·삭제요청에 따라 필요한 조치를 취하지 아니하고 개인정보를 계속 이용하거나 제3자에게 제공한 정보통신서비스 제공자등</p> <p>4의5. 이용자 동의없이 개인정보를 수집한 정보통신서비스 제공자</p> <p>4의6. 법정대리인의 동의를 받지 아니하거나 법정대리인이 동의하였는지를 확인하지 아니하고 만 14세 미만인 아동의 개인정보를 수집한 정보통신서비스 제공자</p> <p>5. 업무상 알게 된 개인정보의 누설하거나 권한 없이 타인이 이용하도록 제공한 자(그 사정을 알고 영리 또는 부정한 목적으로 제공 받은 자 포함)</p> <p>6. 다른 사람의 개인정보를 훼손, 멸실, 변경, 위조, 유출한 자</p>	<p>5년 이하 징역 또는 5천만원 이하 벌금</p>	<p>☞ 개인정보의 목적 외 이용·제공, 유출, 누설 등은 정보주체가 합리적으로 예상할 수 있는 범위를 초과하여 개인정보가 처리되어 정보주체가 적절한 대응조치를 취할 수 없고, 개인정보의 전전유통 등이 발생할 우려가 크므로 엄격히 규제할 필요</p> <p>☞ 민감정보, 고유식별정보는 유출시 정보주체의 사생활 등 권의 침해 가능성이 매우 높으므로 엄격히 규제할 필요</p> <p>☞ 가명정보의 재식별행위 등 의무위반 발생시 정보주체의 권리 침해 가능성이 크고, 개인정보처리자의 도덕적 해이 발생을 방지하고 책임성을 강화하기 위하여 엄격히 규제할 필요</p> <p>☞ 정보통신망에 기반한 서비스의 경우 대량의 개인정보 수집이 가능하고 주로 비대면으로 이루어지는 등을 고려할 때 이용자 보호 필요성이 크므로 보다 엄격히 규제할 필요</p>
제72조	<p>1. 영상정보처리기기 설치목적과 다른 목적으로 임의조작하거나 다른 곳을 비추는 자 또는 녹음기능을 사용한 자</p>	<p>3년 이하 징역 또는 3천만원 이하 벌금</p>	<p>☞ 영상정보처리기기를 확대·회전하거나 녹음할 경우 개인의 민감한 사생활을 침해할 우려가 높으므로 규제 필요</p>

조문	위반행위	벌칙수준	제재이유
	2. 거짓 그 밖에 부정한 수단이나 방법에 의하여 개인정보를 취득하거나 개인정보처리에 관한 동의를 얻는 행위를 한 자 (그 사정을 알고 영리 또는 부정한 목적으로 제공받은 자를 포함)		☞ 피싱 등 부정한 방법으로 개인정보를 취득하거나 동의를 얻는 행위는 목적 외 이용·제공보다는 가벌성이 약하나 정보주체의 개인정보자기결정권을 중대하게 제한한다는 점에서 3년 이하 징역 등으로 규정함
	3. 직무상 알게 된 비밀을 누설하거나 직무상 목적 외에 이용한 자		☞ 이 법의 규율대상인 개인정보처리자의 비밀누설 등 행위와는 달리, 위원회 위원 등의 행위를 규율하는 것으로 유사 입법례를 참조하여 규정
제73조	1. 안전성 확보에 필요한 보호조치를 취하지 아니하여 개인정보를 분실·도난·유출·위조·변조·훼손당한 자	2년 이하의 징역 또는 2천만원 이하의 벌금	☞ 개인정보 보호는 사전 예방이 중요하므로 안전조치의무 위반으로 누출 등이 된 경우 형사처벌로 엄격 제재
	1의2. 개인정보 미파기 정보통신서비스 제공자등(방송사업자 등 포함)		☞ 정보통신망의 파급력 및 전파력을 고려할 때 정보통신서비스 제공자등의 개인정보 미파기에 대해서는 형사처벌로 엄격 제재
	2. 개인정보의 정정·삭제요청에 따라 필요한 조치를 취하지 아니하고 개인정보를 계속 이용하거나 제3자에게 제공한 자		☞ 정보주체의 정정·삭제요청, 보유기관 경과에 따른 필요조치를 취하지 않고 잘못된 정보를 이용·제공할 경우, 정보주체가 예상치 못한 피해를 입을 수 있으므로 엄격 규제
3. 개인정보의 처리정지 요구에 따라 처리를 중단하지 아니하고 계속 이용하거나 제3자에게 제공한 자		☞ 정보주체가 개인정보처리자의 처리행위에 반대하여 처리정지를 요구하였음에도 계속 이용·제공할 경우 정보주체의 권익 침해가 크므로 엄격 규제	

이 법은 원칙적으로 의무의 수범자를 개인정보처리자로 하고 이들에게 법률위반과 관련된 법적 책임을 묻고 있는데 예외적으로 개인정보처리자가 법인 등일 것을 감안하여 담당 업무로 개인정보를 실제 처리한 자에게도 형사처벌을 부과하고 있다(개인정보를 처리하거나 처리하였던자의 제59조 각 호 위반행위에 대하여 형사처벌을 부과하는 경우가 이에 해당하며, 이와 관련한 자세한 설명은 제59조(금지행위) 해설 참고).

한편, 정보통신망의 파급력 및 전파력, 대량의 개인정보 수집이 가능하고 주로 비대면으로 이루어지는 정보통신서비스의 특성 등을 감안하여 정보통신서비스 이용자의 개인정보를 처리하는 정보통신서비스 제공자등의 위반행위에 대하여 개인정보처리자의 위반행위보다 강화된 제재(형사처벌)를 부과하는 경우도 존재한다(제71조제4호의4, 제4호의5, 4호의6, 제73조제1호의2 참고). 이 경우 정보통신서비스 제공자등에게 적용되는 규정이 준용되는 방송사업자등의 위반행위에 대해서도 동일한 제재를 적용하고 있다(제39조의14 참고).

제74조 | 양벌규정

법률

제74조(양벌규정) ① 법인의 대표자나 법인 또는 개인의 대리인, 사용인, 그 밖의 종업원이 그 법인 또는 개인의 업무에 관하여 제70조에 해당하는 위반행위를 하면 그 행위자를 벌하는 외에 그 법인 또는 개인을 7천만원 이하의 벌금에 처한다. 다만, 법인 또는 개인이 그 위반행위를 방지하기 위하여 해당 업무에 관하여 상당한 주의와 감독을 게을리하지 아니한 경우에는 그러하지 아니하다.

② 법인의 대표자나 법인 또는 개인의 대리인, 사용인, 그 밖의 종업원이 그 법인 또는 개인의 업무에 관하여 제71조부터 제73조까지의 어느 하나에 해당하는 위반행위를 하면 그 행위자를 벌하는 외에 그 법인 또는 개인에게도 해당 조문의 벌금형을 과(科)한다. 다만, 법인 또는 개인이 그 위반행위를 방지하기 위하여 해당 업무에 관하여 상당한 주의와 감독을 게을리하지 아니한 경우에는 그러하지 아니하다.

법인의 대표자나 법인 또는 개인의 대리인, 사용인, 그 밖의 종업원이 그 법인 또는 개인의 업무에 관하여 제70조부터 제73조까지에 해당하는 위반행위를 하면 그 행위자를 처벌할 뿐만 아니라 그 법인 또는 개인에 대해서도 벌금을 부과한다.

이는 임직원, 대리인 등의 법 위반행위에 대하여 해당 행위자뿐만 아니라 개인정보처리자도 처벌함으로써 임직원, 대리인 등의 업무 처리에 대한 개인정보처리자의 경각심을 높이고 관리·감독을 강화하기 위한 것이다.

사례1 수탁자의 법 위반행위에 대한 위탁자의 형사책임

법원은 A택배회사(이하 'A社')와 택배위수탁계약을 체결하고 위 회사로부터 위탁받은 택배화물을 고객들에게 운송하는 일을 담당한 甲이 A社가 관리하는 개인정보를 유출한 사안에서, 甲은 「정보통신망법」 제66조에서 정한 '법인의 사용인이 법인의 업무에 관하여' 위반행위를 한 것이고, A社가 甲의 위반행위를 방지하기 위하여 당해 업무에 대하여 상당한 주의와 감독을 하였다고 보기 어려우므로 동법 제24조제2항 및 제62조제2호의 규정에 의하여 A社의 형사책임을 인정하였다.(수원지법 2005. 7. 29. 선고 2005고합160 판결)

제74조에 따라 개인정보처리자의 임직원, 대리인 등의 법 위반행위에 의하여 개인정보처리자(법인 또는 개인)를 처벌하기 위한 요건으로서 '업무에 관하여' 위반행위를 한 것으로 보기 위해서는 객관적으로 개인정보처리자의 업무를 위하여 하는 것으로 인정할 수 있는 행위가 있어야 하고, 주관적으로는 그 임직원 등이 개인정보처리자의 업무를 위하여 한다는 의사를 가지고 행위를 하였어야 한다(대법원 1983. 3. 22. 선고 80도1591 판결 등 참고).

사례2 종업원의 개인정보 목적 외 이용행위에 대한 회사의 형사책임

회사 종업원이 제품 수리를 위해 수집한 고객의 개인정보를 이용하여 고객이 운영하는 사업장에 대한 인터넷 블로그 이용후기 글에 악의적 댓글을 게시한 사안에서, 회사 종업원의 개인정보 목적 외 이용행위는 객관적 외형상으로 회사의 업무를 위하여 한 것이라고 볼 수 없고, 주관적으로도 회사 종업원이 회사의 업무 처리를 위하여 한다는 의사를 가지고 고객 개인정보를 목적 외로 이용하였다고 볼 수 없으며, 회사 종업원의 행위가 회사의 인식 하에 일어난 행위로 보기 어렵고, 따라서 회사에게 개인정보 보호법 제74조 제2항의 양벌규정과 제71조 제2호의 벌칙규정을 적용할 수 없다고 의결하였다(보호위원회 결정 제2018-22-246호)

판례 법인에 형사처벌을 부과하기 위한 업무 관련성 판단 요건

「관세법」 제196조에 따라 법인의 임, 직원 또는 피용자의 범칙행위에 의하여 법인을 처벌하기 위한 요건으로서 “법인의 업무에 관하여” 행한 것으로 보기 위해서는 객관적으로 법인의 업무를 위하여 하는 것으로 인정할 수 있는 행위가 있어야 하고 주관적으로는 피용자등이 법인의 업무를 위하여 한다는 의사를 가지고 행동함을 요한다고 함이 당원의 판례취지이며(당원 1979.9.13. 선고 77도 2055 판결 참조), 위 요건을 판단함에 있어서는 법인의 적법한 업무의 범위, 피용자 등의 직책이나 직위, 피용자 등의 범법행위와 법인의 적법한 업무사이의 관련성, 피용자 등이 행한 범법행위의 동기와 사후처리, 피용자 등의 범법행위에 대한 법인의 인식여부 또는 관여정도, 피용자 등이 범법행위에 사용한 자금의 출처와 그로 인한 손익의 귀속 여하 등 여러 사정을 심리하여 결정하여야 할 것이다(대법원 1983. 3. 22. 선고 80도1591 판결 참조).

한편, 개인정보처리자의 임직원, 대리인 등의 위반행위에 대해 무조건 개인정보처리자(법인 또는 개인)에게도 형사벌을 부과할 경우 과중한 제재가 될 수 있으므로, 개인정보처리자가 그 위반행위를 방지하기 위하여 해당 업무에 관하여 상당한 주의와 감독을 게을리하지 아니한 경우에는 형사책임을 지지 않는다.

제74조의 2 | 몰수·추징 등

법률

제74조의2(몰수·추징 등) 제70조부터 제73조까지의 어느 하나에 해당하는 죄를 지은 자가 해당 위반행위와 관련하여 취득한 금품이나 그 밖의 이익은 몰수할 수 있으며, 이를 몰수할 수 없을 때에는 그 가액을 추징할 수 있다. 이 경우 몰수 또는 추징은 다른 벌칙에 부가하여 과할 수 있다.

법 위반행위로 취득한 부정한 이익을 적극적으로 환수하기 위한 제도로 몰수와 추징 제도를 도입하였다(2015. 7.).

몰수(沒收)라 함은 범죄의 재발 방지나 범죄로 인한 부당이득의 금지를 목적으로 범죄 행위와 관련된 재산을 박탈하는 것을 내용으로 하는 재산형을 말한다. 몰수의 종류에는 임의적 몰수와 필요적 몰수가 있으며, 몰수는 임의적 몰수를 원칙으로 한다(「형법」 제48조). 특별법의 각 규정에 따른 몰수·추징의 요건이 충족되지 아니한 경우에도 「형법」 제48조의 요건이 충족되는 경우에는 형법의 일반규정에 따른 임의적 몰수·추징도 가능하다(대법원 1974. 6. 11. 선고 74도352 판결 등).

추징(追徵)은 몰수의 대상인 물건이 몰수하기 어려울 때에 몰수에 갈음하여 그 가액의 납부를 명하는 사법처분을 말한다(「형법」 제48조제2항). 추징의 법적 성격에 관하여는 이를 몰수의 취지를 관철시키기 위한 일종의 “사법처분” 이나 실질적으로는 몰수에 갈음하는 “부가형”의 성격을 가진다고 본다(대법원 1988. 6. 21. 선고 88도551 판결 등).

판례 몰수 요건 및 한계

「형법」 제48조 제1항 제1호에 의한 몰수는 임의적인 것이므로 그 몰수의 요건에 해당되는 물건이라도 이를 몰수할 것인지의 여부는 일응 법원의 재량에 맡겨져 있다할 것이나, 형벌 일반에 적용되는 비례의 원칙에 의한 제한을 받으며, 이러한 법리는 범죄수익은닉의 규제 및 처벌 등에 관한 법률 제8조 제1항의 경우에도 마찬가지로 적용된다. 그리고 몰수가 비례의 원칙에 위반되는 여부를 판단하기 위해서는, 몰수 대상물건(이하 ‘물건’이라 한다)이 범죄 실행에 사용된 정도와 범위 및 범행에서의 중요성, 물건의 소유자가 범죄 실행에서 차지하는 역할과 책임의 정도, 범죄 실행으로 인한 법익 침해의 정도, 범죄 실행의 동기, 범죄로 얻은 수익, 물건 중 범죄 실행과 관련된 부분의 별도 분리 가능성, 물건의 실질적 가치와 범죄와의 상관성 및 균형성, 물건이 행위자에게 필요불가결한 것인지 여부, 물건이 몰수되지 아니할 경우 행위자가 그 물건을 이용하여 다시 동종 범죄를 실행할 위험성 유무 및 그 정도 등 제반 사정이 고려되어야 한다(대법원 2013. 5. 23. 선고 2012도11586 판결).

제75조(과태료) ① 다음 각 호의 어느 하나에 해당하는 자에게는 5천만원 이하의 과태료를 부과한다.

1. 제15조제1항을 위반하여 개인정보를 수집한 자
2. 제22조제6항을 위반하여 법정대리인의 동의를 받지 아니한 자
3. 제25조제2항을 위반하여 영상정보처리기기를 설치·운영한 자

② 다음 각 호의 어느 하나에 해당하는 자에게는 3천만원 이하의 과태료를 부과한다.

1. 제15조제2항, 제17조제2항, 제18조제3항 또는 제26조제3항을 위반하여 정보주체에게 알려야 할 사항을 알리지 아니한 자
2. 제16조제3항 또는 제22조제5항을 위반하여 재화 또는 서비스의 제공을 거부한 자
3. 제20조제1항 또는 제2항을 위반하여 정보주체에게 같은 항 각 호의 사실을 알리지 아니한 자
4. 제21조제1항·제39조의6(제39조의14에 따라 준용되는 경우를 포함한다)을 위반하여 개인정보의 파기 등 필요한 조치를 하지 아니한 자
- 4의2. 제24조의2제1항을 위반하여 주민등록번호를 처리한 자
- 4의3. 제24조의2제2항을 위반하여 암호화 조치를 하지 아니한 자
5. 제24조의2제3항을 위반하여 정보주체가 주민등록번호를 사용하지 아니할 수 있는 방법을 제공하지 아니한 자
6. 제23조제2항, 제24조제3항, 제25조제6항, 제28조의4제1항 또는 제29조를 위반하여 안전성 확보에 필요한 조치를 하지 아니한 자
7. 제25조제1항을 위반하여 영상정보처리기기를 설치·운영한 자
- 7의2. 제28조의5제2항을 위반하여 개인을 알아볼 수 있는 정보가 생성되었음에도 이용을 중지하지 아니하거나 이를 회수·파기하지 아니한 자
- 7의3. 제32조의2제6항을 위반하여 인증을 받지 아니하였음에도 거짓으로 인증의 내용을 표시하거나 홍보한 자
8. 제34조제1항을 위반하여 정보주체에게 같은 항 각 호의 사실을 알리지 아니한 자
9. 제34조제3항을 위반하여 조치 결과를 신고하지 아니한 자
10. 제35조제3항을 위반하여 열람을 제한하거나 거절한 자
11. 제36조제2항을 위반하여 정정·삭제 등 필요한 조치를 하지 아니한 자
12. 제37조제4항을 위반하여 처리가 정지된 개인정보에 대하여 파기 등 필요한 조치를 하지 아니한 자
- 12의2. 제39조의3제3항(제39조의14에 따라 준용되는 경우를 포함한다)을 위

반하여 서비스의 제공을 거부한 자

12의3. 제39조의4제1항(제39조의14에 따라 준용되는 경우를 포함한다)을 위반하여 이용자·보호위원회 및 전문기관에 통지 또는 신고하지 아니하거나 정당한 사유 없이 24시간을 경과하여 통지 또는 신고한 자

12의4. 제39조의4제3항을 위반하여 소명을 하지 아니하거나 거짓으로 한 자

12의5. 제39조의7제2항(제39조의14에 따라 준용되는 경우를 포함한다)을 위반하여 개인정보의 동의 철회·열람·정정 방법을 제공하지 아니한 자

12의6. 제39조의7제3항(제39조의14에 따라 준용되는 경우와 제27조에 따라 정보통신서비스 제공자등으로부터 개인정보를 이전받은 자를 포함한다)을 위반하여 필요한 조치를 하지 아니한 정보통신서비스 제공자등

12의7. 제39조의8제1항 본문(제39조의14에 따라 준용되는 경우를 포함한다)을 위반하여 개인정보의 이용내역을 통지하지 아니한 자

12의8. 제39조의12제4항(같은 조 제5항에 따라 준용되는 경우를 포함한다)을 위반하여 보호조치를 하지 아니한 자

13. 제64조제1항에 따른 시정명령에 따르지 아니한 자

③ 다음 각 호의 어느 하나에 해당하는 자에게는 2천만원 이하의 과태료를 부과한다.

1. 제39조의9제1항을 위반하여 보험 또는 공제 가입, 준비금 적립 등 필요한 조치를 하지 아니한 자

2. 제39조의11제1항을 위반하여 국내대리인을 지정하지 아니한 자

3. 제39조의12제2항 단서를 위반하여 제39조의12제3항 각 호의 사항 모두를 공개하거나 이용자에게 알리지 아니하고 이용자의 개인정보를 국외에 처리위탁·보관한 자

④ 다음 각 호의 어느 하나에 해당하는 자에게는 1천만원 이하의 과태료를 부과한다.

1. 제21조제3항을 위반하여 개인정보를 분리하여 저장·관리하지 아니한 자

2. 제22조제1항부터 제4항까지의 규정을 위반하여 동의를 받은 자

3. 제25조제4항을 위반하여 안내판 설치 등 필요한 조치를 하지 아니한 자

4. 제26조제1항을 위반하여 업무 위탁 시 같은 항 각 호의 내용이 포함된 문서에 의하지 아니한 자

5. 제26조제2항을 위반하여 위탁하는 업무의 내용과 수탁자를 공개하지 아니한 자

6. 제27조제1항 또는 제2항을 위반하여 정보주체에게 개인정보의 이전 사실을 알리지 아니한 자

6의2. 제28조의4제2항을 위반하여 관련 기록을 작성하여 보관하지 아니한 자

7. 제30조제1항 또는 제2항을 위반하여 개인정보 처리방침을 정하지 아니하

	<p>거나 이를 공개하지 아니한 자</p> <p>8. 제31조제1항을 위반하여 개인정보 보호책임자를 지정하지 아니한 자</p> <p>9. 제35조제3항·제4항, 제36조제2항·제4항 또는 제37조제3항을 위반하여 정보주체에게 알려야 할 사항을 알리지 아니한 자</p> <p>10. 제63조제1항에 따른 관계 물품·서류 등 자료를 제출하지 아니하거나 거짓으로 제출한 자</p> <p>11. 제63조제2항에 따른 출입·검사를 거부·방해 또는 기피한 자</p> <p>⑤ 제1항부터 제4항까지의 규정에 따른 과태료는 대통령령으로 정하는 바에 따라 보호위원회와 관계 중앙행정기관의 장이 부과·징수한다. 이 경우 관계 중앙행정기관의 장은 소관 분야의 개인정보처리자에게 과태료를 부과·징수한다.</p>
시행령	<p>제63조(과태료의 부과기준) 법 제75조제1항부터 제4항까지의 규정에 따른 과태료의 부과기준은 별표 2와 같다.</p>

1. 과태료와 벌칙의 차이점

‘과태료’란 일정한 기준이나 질서를 위반한 행위에 대해 행정관청이 직접 부과하는 ‘행정질서벌’로서 이는 형벌이 아니기 때문에 전과기록이 남지 않는다. ‘벌칙’(형벌)은 형법이나 기타 법률에 규정된 범죄행위에 대해 법원의 재판절차를 거쳐 부과하는 형사벌로서 전과기록이 남으며, 여기에는 징역, 벌금 등이 있다.

형사처벌의 대상이 되는 범죄의 구성요건과 과태료 부과대상은 처벌 내지 제재대상이 되는 기본적 사실관계로서의 행위를 달리하고 있고, 형사처벌은 행위 자체를 위법한 것으로 보아 처벌하는 것인데 반하여 과태료는 행정행위의 실효성을 확보하기 위하여 제재를 과하는 것이므로 그 보호법익과 목적에서도 차이가 있으므로 형사처벌과 과태료의 부과는 일반적으로 「헌법」 제13조제1항이 금지하는 이중처벌에 해당한다고 할 수 없다.

이 법은 정보주체의 개인정보자기결정권 구현을 위해 개인정보의 처리 단계마다 정보주체의 동의를 근간으로 하고 있다. 이에 따라 동의 없는 개인정보 목적 외 이용 및 제3자 제공 등으로 정보주체의 권리침해를 초래하는 행위에는 벌칙을 부과하고 있다. 한편, 개인정보 보호책임자 미지정, 개인정보 처리방침 미공개 등 이 법이 정한 절차나 기준을 위반한 경우에는 과태료 등을 부과하고 있다.

「헌법」 제13조 제1항이 정한 “이중처벌금지(二重處罰禁止)의 원칙(原則)”은 동일한 범죄행위에 대하여 국가가 형벌권(刑罰權)을 거듭 행사할 수 없도록 함으로써 국민의 기본권 특히 신체의 자유를 보장하기 위한 것이므로, 그 “처벌(處罰)”은 원칙으로 범죄에 대한 국가의 형벌권 실행으로서의 과벌(課罰)을 의미하는 것이고, 국가가 행하는 일체의 제재(制裁)나 불이익처분(不利益處分)이 모두 그에 포함된다고 할 수는 없다(헌법재판소 1994. 6. 30.자 92헌바38 결정).

2. 과태료 부과 · 징수

법 위반에 따른 과태료의 부과 · 징수는 보호위원회와 관계 중앙행정기관의 장이 한다. 공공기관도 과태료 부과 대상이다. 과태료의 부과 · 징수, 재판 및 집행 등의 절차에 관하여는 이 법에서 정한 것을 제외하고는 「질서위반행위규제법」에 따른다.

3. 과태료 내용

조문	위반행위	벌칙수준	제재이유
제75조 제1항	1. 개인정보의 수집기준을 위반한 자 2. 만 14세 미만 아동의 개인정보 수집 시 법정대리인의 동의를 받지 않은 자 3. 탈의실·목욕실 등 영상정보처리기기 설치 금지의무를 위반한 자	5천만원 이하 과태료	☞ 개인정보처리자의 안전한 개인정보 처리 질서확립 및 정보주체의 개인정보자기결정권 보장을 위하여 중요한 사항이므로 5천만원 이하 과태료 부과
제75조 제2항	1. 개인정보 수집·이용·제공 동의획득 시, 목적 외 이용·제공 동의획득 시, 직접마케팅 업무위탁으로 인한 개인정보 제공시 정보주체에게 알려야 할 사항을 알리지 아니한 자 2. 필요최소한의 개인정보 이외의 개인정보 수집에 동의하지 않는다는 이유로 재화 또는 서비스의 제공을 거부한 자 3. 정보주체 외로부터 수집한 개인정보를 고지하지 아니한 자 4. 개인정보를 파기 등 필요한 조치를 하지 아니한 자 (미이용기간 경과 개인정보를 파기 등 필요한 조치 하지 아니한 자 포함) 4-2. 법을 위반하여 주민등록번호를 처리한 자	3천만원 이하 과태료	☞ 개인정보 파기의무, 안전조치 의무, 주민등록번호 대체가입수단 제공의무, 정보주체의 열람등 요청시 필요조치 이행의무는 정보주체의 개인정보보호를 강화하고 권리 행사를 보장하기 위해 부과된 의무사항이므로 단순한 절차규정 위반행위보다 높은 과태료 부과 ☞ 법집행의 실효성과 집행력을 담보하기 위해 시정조치 불응은 단순절차규정 위반보다 높은 과태료 부과 ☞ 개인정보의 유출로 인한 피해를 방지하고 정보주체로 하여금 유출에 대응할 수 있도록 하기 위해서는 유출 통지·신고가 필수적이므로 3천만원 이하 과태료 부과

조문	위반행위	벌칙수준	제재이유
	<p>4-3. 암호화조치를 하지 아니한 자</p> <p>5. 주민등록번호 대체가입수단을 제공하지 아니한 자</p> <p>6. 안전성 확보에 필요한 조치의무를 이행하지 아니한 자</p> <p>7. 영상정보처리기기 설치·운영기준 위반한 자</p> <p>7-2. 가명정보 처리 중 개인을 알아볼 수 있는 정보가 생성되었음에도 이용 중지·회수·파기를 하지 아니한 자</p> <p>7-3. 거짓으로 인증내용을 표시 또는 홍보한 자</p> <p>8. 개인정보 유출사실 통지하지 아니한 자</p> <p>9. 개인정보 유출에 따른 조치 결과를 신고하지 아니한 자</p> <p>10. 정보주체의 열람 요구를 부당하게 제한·거절한 자</p> <p>11. 정보주체의 개인정보 정정·삭제요청에 따라 필요한 조치를 취하지 아니한 자</p> <p>12. 처리 정지된 개인정보에 대하여 파기 등 필요한 조치를 하지 아니한 자</p> <p>12-2. 필요최소한의 개인정보 이외의 개인정보를 제공하지 아니한다는 이유로 서비스 제공을 거부한 자</p> <p>12-3. 유출등 통지·신고를 하지 아니하거나 정당한 사유 없이 24시간을 경과하여 통지·신고한 자</p> <p>12-4. 24시간을 경과하여 유출등 통지·신고 또는 통지·신고에 갈음한 조치를 한 정당한 사유를 소명하지 아니하거나 거짓으로 소명한 자</p> <p>12-5. 수집방법보다 쉬운 개인정보 동의 철회·열람·정정 방법을 제공하지 아니한 자</p> <p>12-6. 개인정보 동의 철회에 따른 파기 등 필요한 조치를 하지 아니한 정보통신서비스 제공자등</p> <p>12-7. 개인정보의 이용내역을 통지하지 아니한 자</p> <p>12-8. 개인정보 국외 이전시 보호조치를 하지 아니한 자</p> <p>13. 시정명령에 따르지 아니한 자</p>		<p>☞ 이용내역 통지는 정보통신망의 전파력 및 파급력 등을 감안하여 정보통신서비스 이용자에게 대하여 그 정보의 이용내역을 주기적으로 알리도록 함으로써 이용자의 권리를 두텁게 보장하기 위해 부과된 의무사항이므로 단순한 절차규정 위반행위보다 높은 과태료 부과</p> <p>☞ 법집행의 실효성과 집행력을 담보하기 위해 시정조치 불응은 단순절차규정 위반보다 높은 과태료 부과</p>

조문	위반행위	벌칙수준	제재이유
제75조 제3항	<ol style="list-style-type: none"> 1. 보험 또는 공제 가입, 준비금 적립 등 손해배상 보장조치를 하지 아니한 자 2. 국내대리인을 지정하지 아니한 자 3. 국외 처리위탁·보관 시 고지사항을 공개하지 않거나 이용자에게 통지하지 아니한 자 	2천만원 이하 과태료	<ul style="list-style-type: none"> ☞ 정보통신망을 통한 개인정보 유출 등으로 이용자 피해사례가 증가하는 상황에서는 정보통신서비스 제공자들의 이용자 손해배상 능력을 확보하는 것이 중요하므로 2천만원 이하 과태료 부과 ☞ 글로벌 온라인 서비스 이용의 보편화로 해외 정보통신서비스 제공자로부터 우리 국민의 개인정보를 보호하는 것이 중요해지고 있으므로 단순한 절차 규정 위반행위보다 높은 과태료 부과
제75조 제4항	<ol style="list-style-type: none"> 1. 미파기 개인정보의 별도 보존의무를 위반한 자 2. 동의획득 방법을 위반하여 동의받은 자 3. 영상정보처리기기 안내판 설치 등 필요조치 이행하지 아니한 자 4. 적법한 문서에 의하지 않고 업무를 위탁한 자 5. 업무위탁시 공개의무를 위반한 자 6. 영업양도 등으로 인한 개인정보 이전사실을 통지하지 아니한 자 6-2. 가명정보 처리 관련 기록을 작성하여 보관하지 아니한 자 7. 개인정보처리방침을 수립하지 않거나 공개하지 아니한 자 8. 개인정보보호책임자를 지정하지 아니한 자 9. 정보주체의 열람, 정정·삭제, 처리정지 요구 거부시 통지의무를 이행하지 아니한 자 10. 관계물품·서류 등의 미제출 또는 허위로 제출한 자 11. 출입·검사를 거부·방해 또는 기피한 자 	1천만원 이하 과태료	<ul style="list-style-type: none"> ☞ 고지·공개·통지의무, 지정의무 등 단순 절차사항을 위반한 행위이므로 1천만원 이하의 과태료 부과

4. 과태료 부과기준

과태료 부과에 공정성과 투명성을 보장하기 위해 범위반 횡수 등을 고려하여 과태료 부과에 세부적인 기준을 아래와 같이 규정하고 있다(영 제63조).

과태료의 부과기준은 「과징금·과태료 합리화 방안」(법제처, 법무부, 국가경쟁력강화위원회, 2009년)에 따라 위반횡수 3차, 횡수에 따른 가중비율 1:2:4로 정하였다.

< 과태료 부과기준(영 제63조 관련) >

1. 일반기준

- 가. 위반행위의 횟수에 따른 과태료의 가중된 부과기준은 최근 3년간 같은 위반행위로 과태료 부과처분을 받은 경우에 적용한다. 이 경우 기간의 계산은 위반행위에 대하여 과태료 부과처분을 받은 날과 그 처분 후 다시 같은 위반행위를 하여 적발된 날을 기준으로 한다.
- 나. 가목에 따라 가중된 부과처분을 하는 경우 가중처분의 적용 차수는 그 위반행위 전 부과처분 차수(가목에 따른 기간 내에 과태료 부과처분이 둘 이상 있었던 경우에는 높은 차수를 말한다)의 다음 차수로 한다.
- 다. 부과권자는 다음의 어느 하나에 해당하는 경우에는 제2호의 개별기준에 따른 과태료의 2분의 1 범위에서 그 금액을 줄일 수 있다. 다만, 과태료를 체납하고 있는 위반행위자에 대해서는 그렇지 않다.
 - 1) 위반행위가 사소한 부주의나 오류로 인한 것으로 인정되는 경우
 - 2) 위반의 내용·정도가 경미하다고 인정되는 경우
 - 3) 위반행위자가 법 위반상태를 시정하거나 해소하기 위하여 노력한 것이 인정되는 경우
 - 4) 위반행위자가 「중소기업기본법」 제2조에 따른 중소기업자인 경우
 - 5) 그 밖에 위반행위의 정도, 위반행위의 동기와 그 결과 등을 고려하여 줄일 필요가 있다고 인정되는 경우
- 라. 부과권자는 다음의 어느 하나에 해당하는 경우에는 제2호의 개별기준에 따른 과태료의 2분의 1 범위에서 그 금액을 늘려 부과할 수 있다. 다만, 늘려 부과하는 경우에도 법 제 75조제1항부터 제4항까지의 규정에 따른 과태료 금액의 상한을 넘을 수 없다.
 - 1) 위반의 내용·정도가 중대하여 소비자 등에게 미치는 피해가 크다고 인정되는 경우
 - 2) 법 위반상태의 기간이 3개월 이상인 경우
 - 3) 그 밖에 위반행위의 정도, 위반행위의 동기와 그 결과 등을 고려하여 과태료를 늘릴 필요가 있다고 인정되는 경우

2. 개별기준

위반행위	근거 법조문	과태료 금액		
		1회 위반	2회 위반	3회 이상 위반
가. 법 제15조제1항을 위반하여 개인정보를 수집한 경우	법 제75조 제1항제1호	1,000	2,000	4,000
나. 법 제15조제2항, 제17조제2항, 제18조제3항 또는 제26조제3항을 위반하여 정보주체에게 알려야 할 사항을 알리지 않은 경우	법 제75조 제2항제1호	600	1,200	2,400
다. 법 제16조제3항 또는 제22조제5항을 위반하여 재화 또는 서비스의 제공을 거부한 경우	법 제75조 제2항제2호	600	1,200	2,400
라. 법 제20조제1항 또는 제2항을 위반하여 정보주체에게 같은 항 각 호의 사실을 알리지 않은 경우	법 제75조 제2항제3호	600	1,200	2,400

위반행위	근거 법조문	과태료 금액		
		1회 위반	2회 위반	3회 이상 위반
마. 법 제21조제1항·제39조의6(제39조의14에 따라 준용되는 경우를 포함한다)을 위반하여 개인정보의 파기 등 필요한 조치를 하지 않은 경우	법 제75조 제2항제4호	600	1,200	2,400
바. 법 제21조제3항을 위반하여 개인정보를 분리하여 저장·관리하지 않은 경우	법 제75조 제4항제1호	200	400	800
사. 법 제22조제1항부터 제4항까지의 규정을 위반하여 동의를 받은 경우	법 제75조 제4항제2호	200	400	800
아. 법 제22조제6항을 위반하여 법정대리인의 동의를 받지 않은 경우	법 제75조 제1항제2호	1,000	2,000	4,000
자. 법 제23조제2항, 제24조제3항, 제25조제6항, 제28조의4제1항 또는 제29조를 위반하여 안전성 확보에 필요한 조치를 하지 않은 경우	법 제75조 제2항제6호	600	1,200	2,400
차. 법 제24조의2제1항을 위반하여 주민등록번호를 처리한 경우	법 제75조 제2항제4호의2	600	1,200	2,400
카. 법 제24조의2제2항을 위반하여 암호화 조치를 하지 않은 경우	법 제75조 제2항제4호의3	600	1,200	2,400
타. 법 제24조의2제3항을 위반하여 정보주체가 주민등록번호를 사용하지 않을 수 있는 방법을 제공하지 않은 경우	법 제75조 제2항제5호	600	1,200	2,400
파. 법 제25조제1항을 위반하여 영상정보처리기를 설치·운영한 경우	법 제75조 제2항제7호	600	1,200	2,400
하. 법 제25조제2항을 위반하여 영상정보처리기를 설치·운영한 경우	법 제75조 제1항제3호	1,000	2,000	4,000
거. 법 제25조제4항을 위반하여 안내판 설치 등 필요한 조치를 하지 않은 경우	법 제75조 제4항제3호	200	400	800
너. 법 제26조제1항을 위반하여 업무 위탁 시 같은 항목 호의 내용이 포함된 문서에 의하지 않은 경우	법 제75조 제4항제4호	200	400	800
더. 법 제26조제2항을 위반하여 위탁하는 업무의 내용과 수탁자를 공개하지 않은 경우	법 제75조 제4항제5호	200	400	800
러. 법 제27조제1항 또는 제2항을 위반하여 정보주체에게 개인정보의 이전 사실을 알리지 않은 경우	법 제75조 제4항제6호	200	400	800
머. 법 제28조의4제2항을 위반하여 관련 기록을 작성하여 보관하지 않은 경우	법 제75조 제4항 제6호의2	200	400	800

위반행위	근거 법조문	과태료 금액		
		1회 위반	2회 위반	3회 이상 위반
버. 법 제28조의5제2항을 위반하여 개인을 알아볼 수 있는 정보가 생성되었음에도 이용을 중지하지 않거나 이를 회수·파기하지 않은 경우	법 제75조 제2항제7호의2	600	1,200	2,400
서. 법 제30조제1항 또는 제2항을 위반하여 개인정보 처리방침을 정하지 않거나 이를 공개하지 않은 경우	법 제75조 제4항제7호	200	400	800
어. 법 제31조제1항을 위반하여 개인정보 보호책임자를 지정하지 않은 경우	법 제75조 제4항제8호	500		
저. 법 제32조의2제6항을 위반하여 인증을 받지 않았음에도 거짓으로 인증의 내용을 표시하거나 홍보한 경우	법 제75조 제2항제7호의3	600	1,200	2,400
처. 법 제34조제1항을 위반하여 정보주체에게 같은 항 각 호의 사실을 알리지 않은 경우	법 제75조 제2항제8호	600	1,200	2,400
거. 법 제34조제3항을 위반하여 조치 결과를 신고하지 않은 경우	법 제75조 제2항제9호	600	1,200	2,400
터. 법 제35조제3항을 위반하여 열람을 제한하거나 거절한 경우	법 제75조 제2항제10호	600	1,200	2,400
퍼. 법 제35조제3항·제4항, 제36조제2항·제4항 또는 제37조제3항을 위반하여 정보주체에게 알려야 할 사항을 알리지 않은 경우	법 제75조 제4항제9호	200	400	800
허. 법 제36조제2항을 위반하여 정정·삭제 등 필요한 조치를 하지 않은 경우	법 제75조 제2항제11호	600	1,200	2,400
고. 법 제37조제4항을 위반하여 처리가 정지된 개인정보에 대하여 파기 등 필요한 조치를 하지 않은 경우	법 제75조 제2항제12호	600	1,200	2,400
노. 법 제39조의3제3항(제39조의14에 따라 준용되는 경우를 포함한다)을 위반하여 서비스의 제공을 거부한 경우	법 제75조 제2항 제12호의2	600	1,200	2,400
도. 법 제39조의4제1항(제39조의14에 따라 준용되는 경우를 포함한다)을 위반하여 이용자·보호위원회 및 전문기관에 통지 또는 신고하지 않거나 정당한 사유 없이 24시간을 경과하여 통지 또는 신고한 경우	법 제75조 제2항 제12호의3	600	1,200	2,400
로. 법 제39조의4제3항을 위반하여 소명을 하지 않거나 거짓으로 한 경우	법 제75조 제2항 제12호의4	600	1,200	2,400

위반행위	근거 법조문	과태료 금액		
		1회 위반	2회 위반	3회 이상 위반
모. 법 제39조의7제2항(제39조의14에 따라 준용되는 경우를 포함한다)을 위반하여 개인정보의 동의 철회·열람·정정 방법을 제공하지 않은 경우	법 제75조 제2항 제12호의5	600	1,200	2,400
보. 법 제39조의7제3항(제39조의14에 따라 준용되는 경우와 제27조에 따라 정보통신서비스 제공자등으로부터 개인정보를 이전받은 경우를 포함한다)을 위반하여 필요한 조치를 하지 않은 경우	법 제75조 제2항 제12호의6	600	1,200	2,400
소. 법 제39조의8제1항 본문(제39조의14에 따라 준용되는 경우를 포함한다)을 위반하여 개인정보의 이용내역을 통지하지 않은 경우	법 제75조 제2항 제12호의7	600	1,200	2,400
오. 법 제39조의9제1항을 위반하여 보험 또는 공제 가입, 준비금 적립 등 필요한 조치를 하지 않은 경우	법 제75조 제3항제1호	400	800	1,600
조. 법 제39조의11제1항을 위반하여 국내대리인을 지정하지 않은 경우	법 제75조 제3항제2호	2,000		
초. 법 제39조의12제2항 단서를 위반하여 같은 조 제3항 각 호의 사항 모두를 공개하지 않거나 이용자에게 알리지 않고 이용자의 개인정보를 국외에 처리위탁·보관한 경우	법 제75조 제3항제3호	400	800	1,600
코. 법 제39조의12제4항(같은 조 제5항에 따라 준용되는 경우를 포함한다)을 위반하여 보호조치를 하지 않은 경우	법 제75조 제2항 제12호의8	600	1,200	2,400
토. 법 제63조제1항에 따른 관계 물품·서류 등 자료를 제출하지 않거나 거짓으로 제출한 경우 1) 자료를 제출하지 않은 경우 2) 자료를 거짓으로 제출한 경우	법 제75조 제4항제10호	100 200	200 400	400 800
포. 법 제63조제2항에 따른 출입·검사를 거부·방해 또는 기피한 경우	법 제75조 제4항제11호	200	400	800
호. 법 제64조제1항에 따른 시정명령에 따르지 않은 경우	법 제75조 제2항제13호	600	1,200	2,400

제76조 | 과태료에 관한 규정 적용의 특례

법률

제76조(과태료에 관한 규정 적용의 특례) 제75조의 과태료에 관한 규정을 적용할 때 제34조의2에 따라 과징금을 부과한 행위에 대하여는 과태료를 부과할 수 없다.

주민등록번호에 대한 안전성 확보 조치를 하지 아니하여 주민등록번호가 분실·도난·유출·위조·변조 또는 훼손 경우와 관련된 처벌은 아래와 같다.

구분	제재 내용
안전성 확보 조치 미이행 및 주민번호를 분실·도난·유출·위조·변조 또는 훼손당한 경우	2년 이하의 징역 또는 2천만원 이하 벌금 3천만원 이하 과태료 5억원 이하의 과징금

제76조에서는 개인정보처리자가 주민등록번호에 대한 안전성 확보 조치 미이행으로 인해 주민등록번호를 분실·도난·유출·위조·변조 또는 훼손당하여 과징금을 부과받는 경우에는 과태료를 부과 받지 않도록 하는 특례규정을 신설하였다.

참고 건강기능식품에 관한 법률

제48조(과태료에 관한 규정 적용의 특례) 제47조의 과태료에 관한 규정을 적용할 때 제37조에 따라 과징금을 부과한 행위에 대해서는 과태료를 부과할 수 없다.

2020 개인정보 보호 법령 해설서 집필진·감수위원

집필진	고환경	법무법인 광장 변호사
	권건보	아주대학교 교수
	김도엽	법무법인 태평양 변호사
	김진환	김·장 법률사무소 변호사
	김현경	서울과학기술대학교 교수
	박민철	김·장 법률사무소 변호사
	손도일	법무법인 율촌 변호사
	이상직	법무법인 태평양 변호사
	이성엽	고려대학교 교수
	이원우	서울대학교 교수
	장준영	법무법인 세종 변호사
	채성희	법무법인 광장 변호사
	허성욱	서울대학교 교수
감수위원	김일재	(전) 개인정보보호위원회 상임위원
	백대용	법무법인 세종 변호사
	서종식	법무법인 선우 변호사
	최정열	법무법인 율촌 변호사
	홍대식	서강대학교 교수
	황성기	한양대학교 교수
개인정보 보호위원회	이병남	개인정보보호정책과장
	나일청	개인정보보호정책과 사무관
	임종철	개인정보보호정책과 사무관
	강이석	개인정보보호정책과
한국인터넷 진흥원	봉기환	개인정보제도팀장
	박수현	개인정보제도팀
	박미사	개인정보제도팀

2020년 개인정보 보호 법령 및 지침·고시 해설

발행일	2020년 12월
발행처	개인정보보호위원회
홈페이지	www.pipc.go.kr
제작·편집	한국인터넷진흥원

**개인정보 보호
법령 및 지침·고시
해설**

2020. 12



개인정보보호위원회
Personal Information Protection Commission