2020 vol.5

KISA 한국인터넷진흥원
KOREA INTERNET & SECURITY AGENCY

KISA REPORT

CONTENTS

주제 제안 및 정기 메일 신청 | kisareport@kisa.or.kr

인터넷 정보보호 관련 이슈, 현안 등 궁금한 내용을 보내주시면 선별 후 보고서 주제로 선정됩니다.

또한, KISA Report 온라인 서비스 제공을 원하실 경우 신청해주시면 매월 받아보실 수 있습니다.

가명정보에 있어서 “다른 정보”와 “추가 정보”의 차이 및 가명처리의 대상과 범위

이창범 (miso4all@naver.com)

연세대학교 법무대학원 겸임교수

Ⅰ. 들어가는 글

개정 개인정보 보호법의 시행을 앞두고 가명정보의 개념과 가명처리의 범위에 대해서 논란이 많다. 특히 개인정보 보호법 제2조제1호 “나목의 정보(간접식별정보)”와 “다목의 정보(가명정보)”가 어떻게 다른 것인지에 대하여 의문이 제기된다.[1] 개인정보 보호법상 “간접식별정보”는 ‘다른 정보와 쉽게 결합하여 (특정 개인을) 알아볼 수 있는 정보’이고, “가명정보”는 ‘추가 정보의 사용·결합 없이는 특정 개인을 알아볼 수 없는 정보’이다.

전자는 긍정형으로 기술되어 있고 후자는 부정형으로 기술되어 있으며, 전자는 “다른 정보”와 결합을 전제로 하고 후자는 “추가 정보”와 결합을 전제로 하고 있다는 점에서 차이가 있을 뿐, 그 밖의 정보와 결합하여 특정 개인을 식별할 수 있는 정보라는 점에서 양자 사이에 차이가 없다. 따라서 “간접식별정보”와 “가명정보”를 명확히 구분하기 위해서는 “다른 정보”가 “추가 정보”와 어떻게 다른지를 알아야 한다. 또한 “추가 정보”의 의미를 명확히 이해하지 않으면 가명처리의 대상과 범위에 대해서도 계속 혼란을 초래하기 쉽다.

1) 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)

* 본 내용은 이창범 교수(E-Mail : miso4all@naver.com)에게 문의하시기 바랍니다.

Ⅱ. 가명정보의 의미

1. 가명정보의 정의

개인정보 보호법상 “가명정보”란 ‘개인정보를 가명처리함으로써 원래의 상태로 복원하기 위한 “추가정보”의 사용·결합 없이는 특정 개인을 알아볼 수 없는 정보’를 의미하고, 이 경우 “가명처리”란 ‘개인정보의 일부를 삭제하거나 일부 또는 전부를 대체하는 등의 방법으로 추가 정보가 없이는 특정 개인을 알아볼 수 없도록 처리하는 것’을 의미한다.[2] 바꿔 말하면 “가명정보”란 개인정보의 일부를 삭제하거나 일부 또는 전부를 대체하는 등의 방법으로 특정 개인을 알아볼 수 없도록 처리함으로써 특정 개인을 알아볼 수 있는 원래의 상태로 복원하기 위해서는 추가 정보의 사용·결합이 필요한 정보를 의미한다. 따라서 가명정보가 되기 위해서는 첫째, 복원할 수 있는 원래의 개인정보가 존재해야 하고, 둘째, 해당 개인정보의 일부를 삭제하거나 전부 또는 일부를 대체하는 등의 방법으로 특정 개인을 알아볼 수 없게 해야 하며, 셋째, 원래의 상태로 복원하기 위한 추가 정보가 존재해야 한다.

첫째, 복원할 수 있는 원래의 개인정보가 존재해야 하므로 기존의 정보가 없다면 가명정보도 존재할 수 없다. 최초 수집할 때부터 특정 개인을 식별할 수 없게 수집했다면 그 정보는 “간접식별정보”이거나 후술하게 될 “익명정보”에 해당할 것이다. 다른 정보와 결합해서 특정 개인을 식별할 수 있으면 “간접식별정보”에 해당하고, 다른 정보와 결합해도 특정 개인을 식별할 수 없으면 “익명정보”에 해당한다. 다만, 복원할 수 있는 원래의 개인정보가 없더라도 최초 가명정보를 수집·생성하면서 복원을 위한 추가 정보와 함께 원본정보(예컨대 이름, 연락처 등)를 별도로 남겨두고 있다면 그 정보는 가명정보로 볼 수 있다.

둘째, 개인정보의 일부를 삭제 또는 대체하여 특정 개인을 알아볼 수 없게 해야 한다. 개인정보의 일부를 삭제 또는 대체했더라도 나머지 정보만으로 특정 개인을 알아볼 수 있다면 “가목의 정보(직접식별정보)”에 해당할 것이고, “추가 정보” 이외의 다른 정보(제3자가 보유하고 있거나 공개된 정보)와 결합하여 특정 개인을 알아볼 수 있다면 “간접식별정보”에 해당할 것이며, 다른 정보와 결합해도 특정 개인을 알아볼 수 없다면 “익명정보”에 해당한다.

셋째, 원래의 상태로 복원하기 위한 추가 정보가 존재해야 하므로 추가 정보가 존재하지 않으면 가명정보라 할 수 없다. 추가 정보가 존재하지 아니하여 원래의 상태로 복원할 수는 없으나 다른 정보와 결합하여 특정 개인을 알아볼 수 있는 상태라면 “간접식별정보”에 해당하고, 추가 정보가 존재하지 아니하여 원래의 상태로 복원할 수 없고 “다른 정보”와 결합하여 특정 개인을 알아볼 수도 없다면 그 정보는 “익명정보”에 해당할 것이다.

참고로, 개인정보 보호법상 “가명처리”의 정의에는 개인정보를 대체하는 것 이외에 “삭제 등”을 하는 것

2) 제2조(정의) 이 법에서 사용하는 용어의 뜻은 다음과 같다.
1의2. "가명처리"란 개인정보의 일부를 삭제하거나 일부 또는 전부를 대체하는 등의 방법으로 추가 정보가 없이는 특정 개인을 알아볼 수 없도록 처리하는 것을 말한다.

도 포함하는 것으로 규정되어 있으나, 기술상으로 가명처리의 방법에는 대체(Counter, Random number generator, Cryptographic hash function, Message authentication code, Encryption 등)만 포함되고 삭제 등은 포함되지 않는다.[3] 즉, 기술적으로 보면 가명처리는 삭제, 랜덤화(Noise addition, Permutation, Differential privacy), 일반화(Aggregation, K-anonymity, L-diversity, T-closeness), 아웃라이어(outlier) 등과 함께 개인정보를 "비식별 조치"하기 위한 여러 기술적 방법의 하나일 뿐이다.[4] 다만, 개인정보 보호법상으로는 대체, 삭제 등을 포함한 넓은 의미로 사용되고 있으므로 본고에서 가명처리라고 하면 개인정보를 가명화하기 위해 사용될 수 있는 모든 비식별 기법을 의미하는 것으로 한다.

2. "간접식별정보"와의 차이

"간접식별정보"란 "다른 정보"와 쉽게 결합하여 특정 개인을 알아볼 수 있는 정보를 의미한다. "다른 정보"란 해당 정보를 제외한 그밖의 모든 정보를 의미하므로 개인정보처리자가 현재 보관하고 있는 정보는 물론 합리적으로 입수 가능한 정보까지 포함한다. 반면, "추가 정보"는 아래 제3장(Ⅲ)에서 설명하고 있는 바와 같이 넓게 보아도 개인정보처리자가 현재 보관하고 있는 정보로 한정되어야 하며(연계정보 및 원본정보), 좁게 보면 개인정보처리자가 별도 보관 중인 "연계정보"만을 의미한다고 보아야 한다. 따라서 어떤 데이터셋이 가명정보로 인정받기 위해서는 적어도 개인정보처리자가 별도로 보관하고 있는 "추가 정보" 이외의 다른 정보와 결합해서 특정 개인을 식별할 수 없게 조치하여야 한다.

예컨대, 생년월일은 그 자체만으로는 정보주체를 식별할 수 없으나 일반적으로 여러 사람이 이용하는 정보이므로 제3자가 보유하고 있거나 SNS, 공문서 등에 공개된 다른 정보와 결합하면 쉽게 정보주체를 식별할 수 있으므로 아래 [표1]의 정보는 이름을 이니셜로 대체하고 전화번호와 주소 일부를 삭제했음에도 불구하고 생년월일을 통해 개인 식별이 가능하므로 간접식별정보로 보아야 한다. 그러나 이름과 주소 일부를 삭제하고 생년월일을 나이로 대체해 버리면 나이와 남겨진 주소만으로는 개인을 식별할 수 없다. 다만, 개인정보처리자가 보유하고 있는 추가 정보(암호화된 휴대전화번호와 연계할 수 있는 정보)를 이용하면 원래의 상태로 복원이 가능하므로 [표2]는 가명정보에 해당한다.

[표 1] 간접식별정보의 예시

이 름	생년월일	전화번호	주소	직장/직업	고객등급	가입기간	월평균 사용액(원)	연체 횟수	연체 금액(원)
홍길동	88.6.30	010-1234-5678	서울시 종로구 혜화동 123-45번지	한국기업	골드	25년 6개월	5,327,650	4회	8,473,900
HGD	88.6.30	삭제	서울시 종로구 혜화동	회사원	골드	25년 6개월	5,327,650	4회	8,473,900

3) ENISA, Pseudonymisation techniques and best practices, 2019.11
4) WP29, Opinion 05/2014 on Anonymisation Techniques, 2014.4

[표 2] 가명정보의 예시

이 름	생년월일	전화번호	주소	직장/직업	고객등급	가입기간	월평균 사용액(원)	연체 횟수	연체 금액(원)
홍길동	88.6.30	010-1234-5678	서울시 종로구 혜화동 123-45번지	한국기업	골드	25년 6개월	5,327,650	4회	8,473,900
삭 제	42세	q371f8324k	서울시 종로구	회사원	골드	25년 6개월	5,327,650	4회	8,473,900

이 경우 간접식별정보와 다른 정보와의 결합 가능성은 '다른 정보의 입수 가능성 등 개인을 알아보는 데 소요되는 시간, 비용, 기술 등을 합리적으로 고려'해서 판단하게 되지만(제2조제1호 나목), 가명정보와 추가 정보의 결합 가능성은 기술적으로 결합이 가능한지 여부보다는 오히려 기술적으로는 결합이 가능한 상태에 있지만 다른 기술적·관리적 조치를 통해서 또는 법률의 규정에 의해서 이들의 결합이 차단되고 금지된다는 점에 초점을 두고 있다(제2조제1의2호 및 제28조의4).

예컨대, 회사 내에서 고객정보에 접근할 수 있도록 허락받은 사람이라면 누구든지 접근이 가능한 고객의 생년월일은 언제든지 다른 정보와 결합해서 특정 개인을 식별할 수 있으므로 생년월일을 그대로 담고 있는 데이터셋<표1>은 간접식별정보에 해당하지만, 고객정보에 접근할 수 있도록 허락을 받은 사람이라도 고객의 생년월일에 접근하지 못하도록 나이로 대체해버렸다면 해당 데이터셋<표2>은 가명정보에 해당한다.

3. "익명정보"와의 차이

익명정보와 가명정보는 둘 다 특정 개인을 알아 볼 수 없는 정보라는 점에서는 공통적이다. 그러나 "가명정보"는 '추가 정보의 사용·결합 없이는 특정 개인을 알아볼 수 없는 정보'임에 비해서(제2조제1호다목), "익명정보"는 '시간·비용·기술 등을 합리적으로 고려할 때 다른 정보를 사용하여도 더 이상 개인을 알아볼 수 없는 정보'이다(제58조의2)[5].

개인정보 보호법 제58조의2는 식별성의 판단주체를 특정하고 있지 아니하므로 임의의 제3자는 물론 개인정보처리자 자신도 더 이상 특정 개인을 알아볼 수 없도록 비식별 조치가 되어 있어야 비로소 익명정보가 된다. 즉, 익명정보는 개인정보를 제공받은 제3자를 포함하여 임의의 제3자는 물론 개인정보처리자 자신도 합리적으로 더 이상 특정 개인을 알아 볼 수 없어야 한다. 아래 [표 3]의 데이터셋은 이름과 전화번호를 삭제해 버렸기 때문에 복원할 수 있는 연계정보가 존재하지 않고 나머지 정보들도 일부를 삭제하거나 다른 정보로 대체하거나 범주화하여 제3자는 물론 개인정보처리자 자신도 재식별이 불가능하므로 익명정보에 해당한다.

5) 개인정보 보호법은 "익명정보"의 개념을 정의하고 있지도 않고 "익명정보"라는 용어를 사용하고 있지도 않지만 제58조의2에 해당하는 정보를 일반적으로 "익명정보"로 부르고 있다.

[표 3] 익명정보의 예시

이 름	생년월일	전화번호	주소	직장/직업	고객등급	가입기간	월평균 사용액(원)	연체 횟수	연체 금액(원)
홍길동	88.6.30	010-1234-5678	서울시 종로구 혜화동 123-45번지	한국 기업	골드	25년 6개월	5,327,650	4회	8,473,900
삭 제	40-45세	삭 제	서울시 종로구	회사원	골드	25~30년	500~600 만원	1~5회	500~999 만원

반면, 가명정보는 별도로 보관된 추가 정보의 사용·결합 없이는 특정 개인을 알아볼 수 없는 정보이므로 식별성의 판단주체는 "추가 정보"를 보유하고 있는 개인정보처리자가 되어야 한다. 즉, 개인정보처리자 자신은 추가 정보와 결합하여 특정 개인을 알아볼 수 있으나 해당 정보를 제공받은 자 또는 임의의 제3자는 특정 개인을 알아볼 수 없어야 한다.

예컨대, 개인정보처리자로부터 데이터를 제공받은 자(수령자)는 제공받은 데이터를 다른 정보와 결합해도 특정 개인을 식별할 수 없을지라도, 그 정보를 제공한 개인정보처리자 그 자신은 추가 정보(연계정보 등)와 결합해서 특정 개인을 식별할 수 있다면 그 정보는 익명정보가 아니라 가명정보에 해당하고, 추가정보 이외의 다른 정보와 결합해서 개인 식별이 가능하다면 간접식별정보에 해당한다.

Ⅲ. "다른 정보"와 "추가 정보"의 차이

1. "다른 정보"의 의미

개인정보 보호법 제2조 제1호 나목에서 규정하고 있는 "다른 정보"란 해당 정보(간접식별정보)를 제외한 그 밖의 모든 정보를 의미한다. 개인정보처리자 자신이 1) 현재 보유하고 있는 정보는 물론이고, 2) 합리적으로 입수할 수 있는 정보, 3) 더 나아가 임의의 제3자가 보유하고 있거나 공개되어 있는 정보까지 포함한다. 이는 개인정보 보호법상 개인정보의 정의에서 도출되는 당연한 결과이다.

앞에서 언급한 바와 같이 개인정보 보호법은 개인정보의 개념을 정의함에 있어서 식별성의 판단주체를 특정하고 있지 않으며(제2조제1호), "가명정보"와 "익명정보"를 정의함에 있어서도 비식별성의 판단주체를 특정하고 있지 않다(제2조제1의2호, 제58조의2). 이는 식별성 또는 비식별성의 판단주체를 현재 개인정보를 보유하고 있는 개인정보처리자로 한정하지 않고 임의의 제3자까지 포함하겠다는 취지로 해석해야 한다.

따라서 간접식별정보가 다른 정보와 결합하여 특정 개인을 알아볼 수 있는지 여부를 판단함에 있어서도 개인정보처리자는 현재 해당 간접식별정보를 처리하는 자의 입장에서뿐만 아니라 임의의 3자의 입장에서 자신이 현재 보유하고 있는 간접식별정보를 다른 정보와 결합하여 식별성이 있는지 여부를 고려해야 한다. 유럽연합 GDPR도 식별성의 판단 주체를 특정하지 않고 있으며 임의의 제3자까지 포함하고 있다.[6)]

6) EU GDPR 제4조제1호 및 Recital 26 ; WP29, Opinion 4/2007 on the concept of personal data. 2007.4

2. “추가 정보”의 의미

개인정보 보호법상 “가명정보”란 개인정보를 가명처리함으로써 원래의 상태로 복원하기 위한 추가 정보의 사용·결합 없이는 특정 개인을 알아볼 수 없는 정보를 의미하고(제2조제1호 다목), 개인정보처리자가 가명정보를 처리하는 경우에는 원래의 상태로 복원하기 위한 “추가 정보”를 별도로 분리해서 보관·관리해야 한다(제28조의4). 따라서 “추가 정보”는 개인정보처리자가 현재 보관하고 있는 정보로 한정해야 한다는 것은 자명하다. 이점 제3자가 보유하고 있는 정보 및 공개된 정보까지 포함하는 “다른 정보”와 확실히 구분된다.

그러나 개인정보 보호법은 “추가 정보”에 대한 설명이 없어 추가 정보의 범위를 개인정보처리자가 가명정보를 생산하면서 가명정보와 원본정보를 연결하기 위해서 생성한 “연계정보”만을 의미하는 것으로 보아야 할지(key code, 매칭 테이블 등), 아니면 원본정보(원장정보, 정보계정보, 개발정보 등)까지 포함되는 것으로 보아야 할지 분명하지 않다. 연계정보만을 추가정보로 본다면 연계정보를 이용하지 않고는 가명정보를 원본정보와 결합하거나 매칭할 수 없도록 후술하게 될 “속성정보”까지 가명처리를 해야 하는 것으로 해석될 수 있다. 반면, 원본정보도 추가 정보에 포함되는 것으로 본다면 “연계정보”를 이용하지 않고도 원본정보와 직접 결합해서 원래의 상태로 복원할 수 있어야 하므로 속성정보는 가명처리를 할 필요가 없다고 해석하게 될 것이다.

유럽연합 GDPR도 “가명처리”란 추가 정보(additional information)의 이용 없이는 더 이상 특정 정보주체에 귀속될 수 없는 방식으로 개인정보를 처리하는 것이라고 정의하고, 이 경우 가명 처리된 정보가 식별 가능한 자연인에 귀속하지 않도록 보장하기 위해 추가 정보를 별도로 안전하게 보관할 것을 요구하고 있다. 이 경우 추가 정보는 일반적으로 “연계정보”만을 의미하는 것으로 보인다. 그럼에도 불구하고 가명처리의 대상 및 범위에 대해서는 직접식별자만 가명처리하면 된다는 주장부터, 준식별자까지 가명처리를 해야 한다는 주장, 더 나아가 속성정보까지 가명처리를 해야 한다는 주장까지 다양하다.[7] 연계정보만을 추가 정보로 보면서 속성정보는 가명처리하지 않아도 된다는 주장이 논리 모순처럼 보일 수도 있지만 이에 대한 깊은 논의는 전개되고 있지 않다.

사견으로, 가명정보를 원래의 상태로 복원하기 위한 “대상”인 원본정보(즉 원래의 상태)와 가명정보를 원래의 상태로 복원하기 위한 “연결수단 또는 연결매체”로 생성·보관 중인 연계정보는 구분되어야 하고 따라서 추가 정보는 연계정보만을 의미하는 것으로 본다. 논리적으로도 대상과 수단이 동일하게 취급될 수는 없다. 연계정보(추가 정보)를 이용하지 않고 원본정보와 가명정보를 다이렉트로 결합해서 가명정보를 원래의 상태로 복원하는 것은 일반적으로 이용되거나 허용되지 않는 방법이고, 가명정보는 추가정보뿐만 아니라 원본정보와도 분리해서 보관해야 하므로 IT시스템이 가명정보를 원본정보와 다이렉트로 결합·대조할 수 있게 구축되어 있다면 그 자체 법 위반이 된다. 가명정보를 원본정보와 직접 결합할 수 있게 시스템이

7) 제4장의 각주 9)~14) 참조

구축되어 있다면 그 가명정보는 가명정보라 할 수 없고 간접식별정보에 불과하여 가명정보의 정의에 반하기 된다.

결론적으로 가명정보는 “규범적으로” 추가 정보(연계정보)를 이용해서만 원래의 상태로 복원해야 한다는 것을 의미할 뿐 “기술적으로” 추가 정보(연계정보)를 이용하지 않으면 원래의 상태로 복원할 수 없는 상태여야 한다는 것을 의미하는 것은 아니다. 이와 같은 입장에 서면 연계정보만 추가 정보가 될 수 있다고 보더라도 논리적으로 속성정보까지 가명처리를 해야 한다고 보아야 할 필요는 없게 된다.

Ⅳ. 가명처리의 대상 및 범위

1. 개인정보의 유형 분류

가명정보 또는 익명정보에 있어서 비식별 조치를 어느 대상 또는 어느 범위로까지 할 것인지를 판단함에 있어서 자주 활용되는 개인정보의 유형 분류법으로, 어떤 데이터셋에 저장되어 있는 각각의 정보들을 식별의 용이성에 따라 ①직접식별자(고유식별자), ②간접식별자(준식별자), ③속성정보, ④특이정보의 4가지 유형으로 구분하는 방법이 있다. 국내 실무자 사이에서는 특이정보를 민감정보라고 부르는 경우도 있으나, 이는 개인정보 보호법 제23조의 민감정보와 혼동할 우려가 있으므로 사용하지 않는 것이 바람직하다.

일반적으로 “직접식별자”란 해당 정보주체에게만 고유하게 부여되어 있는 정보로써 그 자체만으로 개인식별성이 강한 정보이고(이름, 사진, 주민등록번호, 전화번호, 이메일주소, IP주소, 차량의 번호판정보 등)[8], “준식별자”는 정보주체에게만 고유하게 부여된 정보는 아니지만 보편적으로 널리 이용되고 있는 정보이어서 다른 정보와 결합하면 특정 개인을 식별하기 쉬운 정보이며(생년월일, 사망일, 결혼기념일, 직업, 성별, 신용등급, 주소, 우편번호 등), “속성정보”는 주로 해당 개인정보처리자만 보유하고 있어 개인정보처리자 이외의 자는 다른 정보와 결합해도 특정 개인을 식별하기 어려운 정보이고(상품 구매이력, 월별 전화사용액, 대출 총액, 예금 총액, 보험 구좌수, 고객고유번호 등), “특이정보”는 해당 정보주체에게 고유하게 부여된 정보는 아니지만 해당 정보주체에 대해서만 해당되는 정보여서 누구든지 쉽게 식별이 가능한 정보(특이 질환자, 초고소득자, 초고령 연령자, 특이 직업, 이동 동선 등)를 의미한다.

[표 4] 개인정보의 유형분류

직접 식별자	준식별자	직접 식별자	준식별자	준 식별자	속성정보				
이 름	생년월일	전화번호	주소	직장/ 직업	고객 등급	가입 기간	월평균 사용액(원)	연체 횟수	연체 금액(원)
홍길동	88.6.30	010-1234-5678	서울시 종로구 혜화동 123-45번지	한국 기업	골드	25년 6개월	5,327,650	4회	8,473,900

8) 정보주체에게 고유하게 부여된 정보라도 고객고유번호, 사번, 직번 등과 같이 해당 개인정보처리자 내에서만 이용되는 정보는 식별정보로 보지 아니한다.

그러나 식별성의 정도에 따라 개인정보를 직접식별자, 간접식별자, 속성정보, 특이정보 등으로 구분한다고 해도 그 안에 포함시킬 개인정보의 항목은 논자에 따라 각기 다르다. 예컨대, 어떤 이는 직업을 준식별자로 보지만 다른 이는 준식별자로 보지 아니한다. 또한 동일하거나 유사한 개인정보라고 해서 항상 동일한 유형에 속하는 것도 아니다. 예를 들어, 누군가의 생년월일과 회의참석일은 둘 다 날짜로 표시되는데, 일반적으로 생년월일은 준식별자에 해당하는 것으로 보지만 회의 참석일은 속성정보에 해당하는 것으로 보게 된다. 또한, 일반적으로 회의 참석일자는 속성정보로 보지만 정보주체가 유명한 사람이어서 그 사람이 참석한 회의의 내용과 일자가 매번 언론 등을 통해 공개되어 누구든지 쉽게 검색해 볼 수 있다면 그 참석일자는 특이정보에 해당할 수도 있다.

2. 가명처리의 대상 및 범위

개인정보를 가명화함에 있어서 각각의 개인정보 항목을 어느 대상, 어느 범위까지 가명처리를 해야 하는지에 대해서는 논자마다 입장이 다르다. 유럽연합 WP29는 기록에 포함되어 있는 고유식별자(unique attribute)를 가명화하면 된다고 설명하고 있지만[9], Mike Hintze와 Khaled El Eman은 가명처리를 기본 가명처리(Basic Pseudonymization)와 고도 가명처리(Strong Pseudonymization)로 나누면서 전자는 직접식별자(direct identifiers)를 다른 정보로 대체하는 방법이고 후자는 간접식별자(indirect identifiers)까지 비식별 조치하는 방법이라고 소개하고 있으며[10], 유럽연합 ENISA는 고유식별자(unique identifier)를 포함한 모든 식별자(identifiers)를 가명처리의 대상으로 보고 있다.[11] 한편, Karolina Lubowicka는 GDPR의 가명처리 규정을 준수하기 위해서는 모든 개인정보(every piece of personal data)가 가명처리의 대상이 되어야 한다고 주장하고 있고,[12] Clyde Williamson도 가명처리란 식별가능한 정보(identifiable data)를 복원 가능하고 일관된 정보로 대체하는 것이라고 설명하고 있으며[13], John Noltensmeyer도 가명처리란 식별가능한 정보 또는 민감성 정보(identifying or sensitive data)를 가명으로 대체하는 것이라고 설명하고 있다.[14]

이상과 같은 이론상의 차이에도 불구하고 개인정보 보호법은 가명처리의 대상 및 범위에 대해서 비교적 명확한 기준을 제시하고 있다고 생각한다. 즉, 개인정보 보호법은 '추가 정보가 없이는 특정 개인을 알아볼 수 없도록 처리'할 것을 요구하고 있으므로 국내법상 가명정보는 아래의 두 가지 요건을 모두 충족하여야 한다. 첫째, 내부적으로는 가명처리된 정보만으로는 (추가 정보를 이용하지 않고는) 내부 직원이라도 "시스

9) WP29는 "가명처리"란 일반적으로 고유식별자(unique attribute)를 다른 정보로 대체하는 것이라고 설명하면서 가명처리의 기술로 암호화, 해쉬화, 토큰화 등의 방법을 제시하고 있다. WP29, Opinion 05/2014 on Anonymisation Techniques, 2014.4, pp.20-21 참조. 다만, GDPR 제89조는 가명정보는 정보주체의 동의없이 통계, 연구 등의 목적으로 이용·제공할 수 있다고 규정하면서도 목적 달성이 가능한 경우에는 정보주체의 식별이 허용되지 않는 추가적인 안전조치를 취할 것을 요구하고 있다.

10) Mike Hintze/Khaled El Emam, Comparing the Benefits of Pseudonymization and Anonymization Under the GDPR, 2018. 2

11) ENISA, Pseudonymisation techniques and best practices, 2019.11, p.21

12) Karolina Lubowicka, Data Pseudonymization in Web Analytics : The Ultimate Guide, 2018. 9

13) Clyde Williamson, Pseudonymization vs. Anonymization and How They Help With GDPR, 2017.1

14) John Noltensmeyer, Pseudonymization vs. Anonymization : GDPR, 2018.6

템적으로" 정보주체를 식별할 수 없을 정도로 가명처리가 되어 있어야 한다. 둘째, 외부적으로는 개인정보처리자 이외에 임의의 제3자 또는 제공받은 자가 가명처리된 해당 정보와 "다른 정보"를 결합하여 정보주체를 식별할 수 없을 정도로 "기술적으로" 가명처리가 되어 있어야 한다.

따라서 가명처리에서 주로 논의가 되고 있는 "속성정보"는 개인정보처리자 자신도 추가 정보를 이용하지 않고는 정보주체의 식별이 어렵고(원본정보와 직접 결합하면 식별이 가능할 수 있지만 그와 같은 행위는 기술적·관리적으로뿐만 아니라 법률적으로 결합이 금지됨), 제3자에게는 개인 식별성이 없거나 극히 낮으므로 굳이 가명처리를 할 필요가 없다고 본다. 그러나 속성정보가 특이성을 띄는 경우에는 내부 직원도 "추가 정보"와 결합 없이 특정 개인을 식별할 수 있을 뿐만 아니라 제3자도 특정 개인을 식별할 수 있으므로 가명처리를 해야 한다.

가명처리의 대상 및 범위가 논자마다 다른 이유는 가명처리를 보는 시각에 차이가 있기 때문이 아닌가 한다. 가명처리의 대상 또는 범위를 식별정보 또는 준식별정보로 한정하는 논자들은 주로 가명처리를 개인정보를 안전하게 이용하기 위한 보호수단의 하나로 파악한 반면, 가명정보의 이용, 제공 등 활용을 고려하는 논자는 가명정보의 전전유통에 따른 위험을 우려하여 직접식별자와 준식별자 이외에 속성정보와 민감정보의 가명처리까지 요구하고 있는 것으로 보인다. GDPR에서도 가명정보를 통계, 연구 등의 목적 이외로 이용·제공하고자 할 때에는 정보주체의 동의가 필요 없지만 제6조제4항에 따라 양립성 평가를 해야 하므로 가명처리의 수준 및 범위에 있어서 신중한 입장을 취하는 것은 당연하다고 할 수 있다.

Ⅴ. 맺음말

가명정보는 개인정보를 안전하게 이용하기 위한 기술적 조치의 하나에 불과할 뿐 개인정보가 아닌 것은 아니다. 따라서 익명정보와 같이 임의의 제3자를 포함해 누구도 재식별이 불가능할 정도로까지 비식별 조치를 엄격하게 적용해야 할 필요가 없지만, 역으로 간접식별정보와 같이 누구든지 다른 정보와 결합해서 개인 식별성이 가능할 정도로 느슨하게 비식별 조치를 적용해서도 안 된다. 추가 정보(연계정보)의 사용 없이는 개인정보처리자의 내부 직원이라도 개인 식별이 불가능하게 IT시스템적으로 조치하면 된다.

이처럼 가명정보는 개인 식별성을 제거하는데 목적이 있는 것이 아니라, 식별 가능성 그 자체는 어느 정도로 남겨두되 안전하게 이용하고자 하는 것이 목적이므로 가명처리의 대상 또는 범위에 대한 절대적 기준을 설정하는 것은 기술적으로 쉽지 않다. 가명정보의 활용 목적 및 데이터의 속성에 따라 평가를 달리해야 할 필요가 있기 때문이다. 따라서 가명정보의 적법성을 판단할 때에는 재식별이 가능한지 여부보다는 가명처리의 과정과 목적에 좀 더 주목할 필요가 있다. 즉, 가명처리의 목적이 정당하였는지, 목적에 부합할 정도로 충분히 가명처리가 되었는지, 심각한 사생활 침해로 이어지거나 차별로 이어질 수 있는 민감성 정보가 포함되어 있지 않는지, 가명처리의 과정에서 객관적이고 공정하게 개인정보 영향평가를 수행하였는지, 원본정보, 가명정보 및 추가정보가 기술적·관리적으로 안전하게 분리 보관되고 있는지, 가명정보를

이용하는 내부 직원이 원본정보 및 추가정보에 접근하지 못하도록 접근 통제가 되어 있고 접근통제 위반시 충분할 정도의 법적 제재수단이 마련되어 있는지 등을 종합적으로 고려해서 판단해야 한다.

그럼에도 불구하고 가명정보를 제3자에게 제공하는 경우에는 특정 개인을 알아보기 위하여 사용될 수 있는 정보를 포함해서는 안 되고(제28조의2 제2항), 특정 개인을 알아보기 위한 목적으로 가명정보를 처리해서는 안 되며(제18조의5 제1항), 가명정보를 처리하는 과정에서 특정 개인을 알아볼 수 있는 정보가 생성된 경우에는 즉시 해당 정보의 처리를 중지하고 지체 없이 회수·파기해야 하므로(제28조의5 제2항), 법률을 준수하고 집행하기 위한 기준으로 가명처리의 대상 및 범위의 객관화는 불가피하다.

일반적으로 개인정보처리자 자신은 물론 제3자도 합리적으로 재식별이 가능한 직접식별자, 준식별자 및 특이정보에 대해서는 모두 가명처리를 적용해야 한다는 것에 대해서는 어느 정도 의견의 일치가 있다고 할 수 있다. 문제는 속성정보인데 속성정보는 원본정보를 가지고 있지 않은 제3자는 물론 개인정보처리자의 내부 직원도 추가 정보를 이용하지 않고는 시스템적으로 복원이 어려우므로 가명처리의 대상에서 제외될 수 있다고 생각한다. 그렇다고 해서 속성정보는 항상 가명처리를 할 필요가 없다는 것을 의미하는 것으로 해석되어서는 안 된다. 속성정보와 원본정보의 결합이 가능하도록 시스템을 구성하고 있거나 가명정보를 처리하는 자에게 원본정보에 대한 접근권한이 부여되어 있다면 그 자체 가명처리의 정의에 반하는 것이므로 허용되지 않는다. 또한, 가명정보의 활용 목적을 달성하는데 문제가 없다면 개인정보 보호법 제3조의 개인정보보호원칙에 따라 속성정보도 가명처리를 해야 한다.

[참고문헌]

1. WP29, Opinion 4/2007 on the concept of personal data. 2007.4
2. WP29, Opinion 05/2014 on Anonymisation Techniques, 2014.4
3. ENISA, Pseudonymisation techniques and best practices, 2019.11
4. Pete Jones, Development of pseudonymised matching methods for linking multiple administrative datasets
5. Mike Hintze/Khaled El Emam, Comparing the Benefits of Pseudonymization and Anonymization Under the GDPR, 2018. 2
6. NHS, Guidance on the Pseudonymisation and Anonymisation of Data - Procedure, 2019. 1
7. Karolina Lubowicka, Data Pseudonymization in Web Analytics : The Ultimate Guide, 2018. 9
8. John Noltensmeyer, Pseudonymization vs. Anonymization : GDPR, 2018.6

〈 KISA 주요 활동 안내 〉

Untact 시대를 선도하는 모바일 전자고지 서비스
- 모바일 전자고지 사업 현황 -

□ 사업현황 및 도입효과

o **(현황)** 2018년 행정·공공기관 대상 모바일 전자고지 시스템 구축 도입을 지원한 이래, 민간분야로 대상을 확대하여 공모를 통한 전자화 지원 추진

- 현재 101개 기관(행정·공공기관 및 민간법인)에서 카카오페이(카카오톡), KT(문자), 네이버(앱) 등 공인전자문서중계자를 통한 모바일 전자고지를 실시('20.4월)

※ 발송기관은 공인전자문서중계자간 연계정보를 활용하여, 수신자 식별, 사전안내 및 전자고지 동의 획득 후 본 고지서를 발송

< 주요 도입기관 >

기관명	대상문서	기관명	대상문서
국세청	국세납입 안내문 등	국민연금공단	국민연금 가입내역 안내 등
여성가족부	성범죄자 알림e	한국주택금융공사	주택담보대출 만기도래 안내 등
외교부	여권 유효기간 만료 사전안내문	한국교통안전공단	자동차검사 사전안내
병무청	입영 통지서 등	주택도시보증공사	보증료 납입 영수증
경기도 성남시	지방세 환급금 수령 안내문 등	근로복지공단	고용보험 취득·상실안내
서울특별시	민방위교육훈련 안내문 등	한국소비자원	소비자 민원·분쟁관련 조정문
제주도 자치경찰단	도로교통법 위반 사전통지서	LH한국토지주택공사	임대료 고지서
대한산업보건협회	근로자 건강검진 및 헌혈 결과지	한국도로공사	하이패스 통행료 미납 안내문
충청북도 진천군	지방세 환급금 수령 안내문 등	건설근로자공제회	건설근로자 퇴직공제 수급 안내문

o **(효과)** 종이우편 고지의 낮은 수신율, 발송비용·행정력 과다 소요 등에 의한 국민 불편 해소 및 사회 전반의 효율 증진

〈 모바일 전자고지 도입 사례 및 효과 〉

국민 권익 증진	• 건설근로자공제회는 약 5만 명의 일용직 건설근로자 대상 퇴직공제금 수급요건 충족사실 안내문 및 생활안정 대부사업 안내문의 모바일 전자고지를 통해 주소, 전화번호가 부정확하여 고자안내가 원활하지 않는 문제의 해소 및 건설근로자의 알권리 충족
국민 부담 경감	• 한국교통안전공단은 자동차검사 사전안내문의 모바일 전자고지를 통해 검사경과 과태료 부과건이 전년 대비 약 3.6만 건 감소(최대 90억 원의 과태료 부과액 감소(19년 기준)
행정 효율 제고 & 국민 편의 증진	• 서울특별시는 지방세 과오납 환급금 안내문의 모바일 전자고지를 통해 환급율이 5%→ 30%로 증가하였으며, 안편등기로 전달되는 민방위 교육 훈련 통지서(약 110만 건, '18년 기준)의 모바일 전자고지를 통해 행정 효율 제고 및 국민 편의 증진 기대
국가 예산 절감	• 국민연금공단은 연금가입내역 안내문의 모바일 전자고지를 통해 약 11.3억 원('19년)의 우편발송 비용을 절감하였으며, 국세청은 약 2,600만 건('20년 목표)의 안내문을 모바일 전자고지로 추진하여, 약 50억 원의 우편 발송비용 절감을 기대

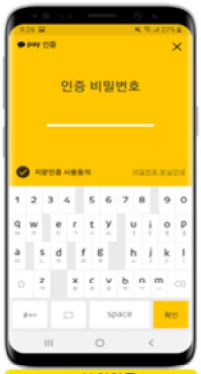
※ 문의: 한국인터넷진흥원 전자문서확산팀(paperless@kisa.or.kr)

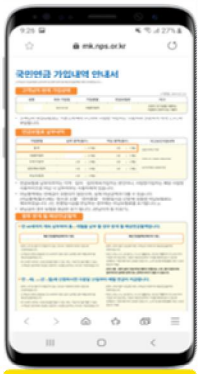
참고 모바일 전자고지 이용방법

KISA 한국인터넷진흥원 KOREA INTERNET & SECURITY AGENCY

카카오페이 이용방법 pay

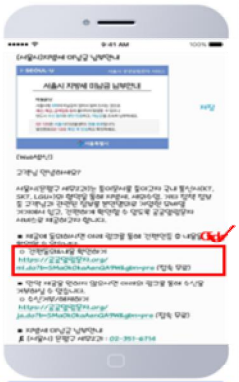
1. 카카오 알림톡 | 2. 전자문서 도착



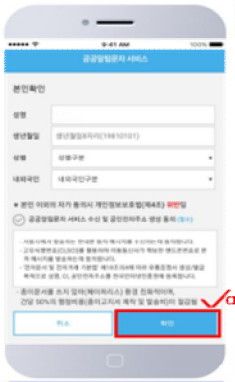


3. 본인인증 (카카오페이 인증서) | 4. 전자문서 열람

KT 이용방법 kt



1. 통합 안내 MMS

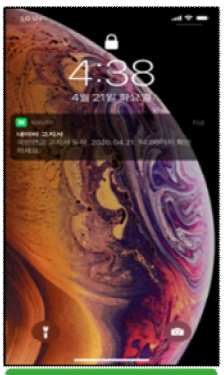


2. 본인확인 & 동의 하기 (서비스 동의는 미동의 회원만 표기)

3. 안내문 상세내용 (미납금 납부 안내)

3.1. 안내문 상세내용 (미납금 상세 보기)

네이버 이용방법 NAVER



1. 전자문서 도착 알림

2. 고지서 요약 페이지 (인증 요청 화면)

3. 본인 인증 완료

4. 고지서 열람

정보보호 혁신기술 스타트업 지원사업 안내

정보보호 부문 예비창업자부터 초기창업·성장기업까지
성장단계별 맞춤형 스타트업 지원사업 운영

□ 지원사업 개요

o **(사업목적)** 국내 정보보호산업의 지속 성장 및 新성장 동력 창출을 위해 혁신기술을 보유한 정보보호 스타트업 발굴 및 육성

※ 2017년 판교 정보보호 클러스터 개소 이래로 정보보호 스타트업 지원사업 운영 中

o **(사업기간)** 약 6개월 (2020. 6. ~ 2020. 12.)

o **(사업예산)** 총 650백만원 (초기창업 100백만원 / 성장기업 550백만원)

o **(지원대상)** 총 25개社 내외 (초기창업 5개社 / 성장기업 20개社)

o **(지원내용)** 성장단계별(창업 3년 기준) 맞춤형 지원

구 분	초기창업기업	성장기업
사업목적	정보보호 유망 스타트업 발굴 및 역량강화 지원	정보보호 스타트업 가치향상 및 투자유치 성공
모집대상	예비창업자 ~ 3년 이하 정보보호 스타트업(5개社 or 팀)	3년 이상 ~ 7년 이하 정보보호 스타트업(20개社)
모집기간	2020. 4. 13. ~ 2020. 5. 15. (약 한달간)	
주요 지원내용	▲**(트렌드 제공)** 최신 산업 및 기술 트렌드 동향 ▲**(교육 및 멘토링)** 보안 관련 인증(CC 등) 및 교육, 기술 지원 및 판로개척 등 멘토링 ▲**(컨설팅)** BM 진단·개선 및 법인설립 등 ▲**(테스트랩 이용)** R&D 개발을 위한 인프라 지원 ▲**(모의피칭 대회)** 기업 및 VC 대상 개최 ▲**(개발지원금)** 우수 3개社 대상 총 3천만원 제공 ※ (1등) 1,500만원 (2등) 1,000만원 (3등) 500만원	▲**(엑셀러레이팅)** 기업 진단 및 맞춤형 엑셀러레이팅 프로그램 운영 ▲**(분야별 멘토링)** 기업성장, 투자, 기술 등 ▲**(사업화 지원)** 지재권 취득 및 홍보물 제작 등 ▲**(협업 네트워크 구축)** 보안산업 생태계 이해 관계자와 스타트업간 협업 기회 제공 ▲**(투자유치 유도)** VC 및 기업 등 연계를 통한 투자상담회 및 혁신 경연대회* 개최 * 총 3천만원 규모의 IR 피칭 발표 경연대회

o **(사업성과)** 투자유치 170.59억 원, 수출액 819.5억 원 달성('17~'19년 누적 기준)

□ 관련 문의

o 한국인터넷진흥원 보안산업단 보안산업진흥팀 황도연 선임연구원 (☎ 061-820-1217)

2020 Vol.1

이슈&트렌드

2020 Vol.2

이슈&트렌드

2020 Vol.3

이슈&트렌드

2020 Vol.4

이슈&트렌드

KISA 한국인터넷진흥원
KOREA INTERNET & SECURITY AGENCY

발 행 일	2020년 5월
발 행 처	한국인터넷진흥원 (전라남도 나주시 진흥길 9)
기 획	한국인터넷진흥원 ICT미래연구소
편 집	㈜ 해리