

가명정보 열람권 등 정보주체 권리 보장을 위한 토론회

일시: 2020년 12월 7일(월) 오후 2시
주최: 국회의원 민병덕, 사단법인 오픈넷

가명정보 열람권 등 정보주체 권리 보장을 위한 토론회



일시 2020년 12월 7일(월) 오후 2시

주최 국회의원 민병덕, 사단법인 오픈넷

프로그램

발제 “가명정보에 대한 열람권 등 정보주체
권리 보장을 위한 개인정보보호법 개정 방향”

박경신 교수(고려대, 오픈넷 이사)

토론 좌장 : 유승희 전 국회의원(17, 19, 20대)

토론 : 김선희 변호사(법무법인 이공, 참여연대 공익법센터)

오병일 대표(진보네트워크센터)

이한샘 과장(개인정보보호위원회 데이터안전정책과)

최경진 교수(가천대)



※ 본 토론회는 온라인으로만 시청하실 수 있으며, 유튜브 오픈넷 채널에서 라이브 방송으로 진행됩니다.



문의

오픈넷 사무국

Tel. 02-581-1643 / Mail. master@opennet.or.kr

국회의원 민병덕

 opennet

가명정보 열람권 등 정보주체 권리 보장을 위한 토론회

지난 2월 개인정보보호법이 개정되면서 유럽의 GDPR처럼 “통계작성, 과학적 연구, 공익적 기록보존 등” 공공의 이익을 위해서는 “가명처리”라는 안전조치를 취하면 정보주체에게 일일이 동의를 얻지 않아도 개인정보를 활용할 수 있는 길이 열렸습니다. 그러나 정보주체에게 보장되었던 개인정보 열람권, 정정·삭제권, 처리거부권 등 정보주체의 권리를 가명처리된 개인정보인 “가명정보”에 대해서는 인정하지 않으면서 부당한 사례가 발생하고 있습니다(개인정보보호법 제28조의7). 개인정보처리자 입장에서도 가명처리된 개인정보, 즉 가명정보의 재식별화가 예외없이 금지되어 있기 때문에 정보주체가 열람권 등 자신의 권리를 행사하고자 할 때도 재식별화를 할 수 없어 권리의 보장을 해주지 못하게 되었습니다(개인정보보호법 제28조의5). 예를 들어, 병원은 개인정보 유출시의 피해를 최소화하기 위해 입원기록을 가명처리하여 보관할 수도 있는데, 환자가 자신의 입원기록을 보여달라고 해도 가명처리를 한 이상 재식별화해서 보여줄 수 없는 상황입니다.

이에 비해 GDPR에서는 ‘과학적 연구, 통계, 공익적 기록 등의 목적’을 위해서 이용된 경우에만 열람권, 정정권, 처리거부권 등이 제한되고 있고, 해석상 정보주체의 권리 보장을 위한 가명정보의 재식별화는 자유롭게 허용하고 있습니다. 관련 법개정을 위한 논의를 다음과 같이 하고자 합니다.

일시: 2020년 12월 7일(월) 오후 2시

주최: 국회의원 민병덕, 사단법인 오픈넷

<인사말씀> 더불어민주당 국회의원 민병덕

<발제>

“가명정보에 대한 열람권 등 정보주체 권리 보장을 위한 개인정보보호법 개정 방향”

- 박경신 교수(고려대, 오픈넷 이사)

<토론>

좌장: 유승희 전 국회의원(17, 19, 20대)

김선희 변호사(법무법인 이공, 참여연대 공익법센터)

오병일 대표(진보네트워크센터)

이한샘 과장(개인정보보호위원회 데이터안전정책과)

최경진 교수(가천대)

인사말씀

더불어민주당 국회의원 민병덕
(경기 안양시동안구갑)



안녕하십니까? 더불어민주당 민병덕 의원
입니다.

오늘 ‘가명정보 열람권 등 정보주체 권리
보장을 위한 토론회’에 참석해주신 여러
분께 진심으로 감사의 말씀을 드립니다.
더불어 발제를 맡아주신 박경신 교수님,
오늘 토론회의 좌장을 맡으신 유승희 전
국회의원님을 비롯한 토론자 여러분께도
노고의 말씀을 전합니다. 특히 오늘 토론회는 코로나19 확산으로 인해
부득이 온라인으로 진행하게 되었습니다. 다소의 불편함이 있더라도
양해해주시기 바랍니다.

지난 2월 개인정보보호법이 개정되면서, 과학적 연구·통계·공익적
기록 등의 목적에 대해서는 ‘가명처리’라는 안전조치를 취하면 개인
들에게 일일이 동의를 얻지 않아도 개인정보를 이용할 수 있도록 제도
가 바뀌었습니다. 하지만 정작 정보주체인 당사자에게는 개인정보 열
람권, 정정·삭제권, 처리거부권 등이 보장되지 않고 있습니다. 그 이
유는 개인정보가 ‘가명처리’가 아닌 ‘익명처리화’ 되어 활용되고 있
어, 정보주체가 자신의 정보를 열람하고자 해도 재식별화가 불가능하
기 때문입니다.

이에 비해 유럽의 GDPR에서는 정보주체의 권리 보장을 위한 가명정보
의 재식별화는 자유롭게 허용하고 있습니다. 자신의 정보를 스스로 열
람하고 정정·삭제할 권리는 어찌보면 개인의 당연한 권리가기 때문입

니다.

오늘 토론회가 정보주체의 권리보장을 위해 개인정보보호법이 올바른 방향으로 개정될 수 있도록 하는 논의의 장이 되기를 희망합니다. 토론회 이후에도 계속적으로 전문가들의 의견을 듣고, 상임위에서도 결과물을 만들기 위해 노력하겠습니다.

긴급하게 준비한 토론회인데도 여러분들께서 어렵게 시간을 내주셨습니다. 정책의 성패는 디테일에 달려있다는 말이 있습니다. 발제, 토론자를 비롯한 참석자 분들이 적극적으로 토론에 참여해주셔서 더욱 알찬 토론회가 될 수 있도록 해주시길 당부드립니다.

다시 한 번 오늘 토론회에 오신 분들, 그리고 온라인으로 토론회에 참여주신 여러분들 진심으로 환영합니다.

감사합니다.

가명정보에 대한 정보주체의 권리 보장을 위한 개인정보보호법 개정 제안

박경신 교수

고려대학교 법학전문대학원

(사)오픈넷 이사

개인정보보호법이 지난2월 개정되면서 유럽의 GDPR처럼 <과학적 연구, 통계, 공익적 기록 등의 목적> 등에 대해서는 <가명처리>라는 안전조치를 취하면 개인들에게 일일이 동의를 얻지 않아도 공공의 이익을 위해 개인정보를 이용할 수 있는 길이 열렸다. 그러나 이때 각 개인들에게 원래 보장되었던 열람권, 정정권, 처리거부권 등을 <가명정보>에 대해서 제한하면서 부당한 사례가 발생하고 있다(개인정보보호법 제28조의 7). 개인정보처리자 입장에서도 가명처리된 정보의 재식별화를 예외 없이 금지하고 있어 개인이 열람권, 정정권, 처리거부권 등을 행사하고자 할 때 권리보호를 해주지 못하고 있는 형편이다(개인정보보호법 제28조의5). 예를 들어, 병원은 개인정보 유출시의 피해를 최소화하기 위해 입원기록을 가명화하여 (즉 식별정보를 암호로 바꿔어) 보관할 수도 있는데, 환자가 입원기록을 보여달라고 해도 가명화했다는 이유로 재식별화할 수 없는 상황이다.

이에 비해 GDPR에서는 모든 가명정보에 대해서 권리제한을 하는 것이 아니라 <과학적 연구, 통계, 공익적 기록 등의 목적>을 위해서 이용된 경우에만 열람권, 정정권, 처리거부권등이 제한되고 있고 또 회원국들의 해석상 정보주체의 권리보장을 위한 가명정보의 재식별화는 자유롭게 허용되고 있다. 우리나라 개인정보보호법도 보안목적의 가명처리는 자유롭게 하되 동의없는 이용은 ‘과학적 연구, 통계 작성, 공익적 기록보관’의 공공성 등이 확보되는지 엄격하게 관리하고, 가명화된 정보에 대해서도 정보주체의 의사에 따라 재식별화할 수 있는 길을 열어 정보주체의 권리 보장을 할 필요가 있다.

I. 개인정보보호법의 연혁 및 개요¹⁾

1. 현대의 개인정보자기결정권의 시초

1) 이 장의 내용의 일부는 다음 논문에 게재된 것을 요약하고 강화하여 논의의 흐름을 유지하기 위해 여기에 전재한 것이다. 박경신. (2016). 독일개인정보보호법. 「강원법학」 49, 103-135면.

가. 정보감시의 방지책 필요

개인에 대한 정보를 수집할 때 그 개인으로부터 동의를 얻어야 한다거나 이를 수집목적에 따라서만 사용해야 한다거나 하는 현대의 개인정보보호법 상의 의무들은 정보주체가 물건들을 소유하듯이 자신에 대한 정보를 소유한다고 보는 시각과 합치한다.²⁾ 즉 타인의 물건을 빌리려면 그 물건의 소유자에게 동의를 얻어야 하고 빌리는 목적을 말하고 그 목적에 부합하게 물건을 사용해야 하며 그렇게 하지 못할 경우 물건의 소유자는 그 물건을 반환받을 수 있다는 등의 규범은 개인정보보호법 상의 개인정보처리자의 의무에 좋은 유비를 제시한다. 즉 내가 타인의 개인정보를 수집하는 것은 그의 자동차를 빌려온 것과 마찬가지로이다. 자동차를 빌릴 때 합의한 목적 외로 이용하거나 -병원에 가족 내 환자를 이동하기 위해 빌린다고 한 후 교외로 소풍을 떠나는 데에 이용하는 경우-합의되지 않은 제3자에게 재임대해줄 때는 자동차 소유자의 동의를 얻어야 할 것이다(처리동의권). 자동차 소유자가 원한다면 자동차가 잘 있는지 확인을 시켜줄 수 있어야 할 것이다(열람권). 또 자동차를 온전히 잘 보관해야 할 의무가 있어 자동차에 결함이 발생하거나 할 경우 이를 수리할 의무가 있다(삭제 및 정정권). 또 자동차를 빌리기로 한 기간이 끝나기 전이라도 소유자가 원한다면 임대료를 삭감하는 한이 있더라도 자동차는 우선 반환되어야 한다(동의취소권).

현대의 개인정보자기결정권은 어디에서부터 시작되었을까? 정보주체가 자신에 대한 정보에 대해 ‘소유권적’ 통제권을 가져야 한다는 주장은 1967년 알란 웨스틴(Alan Westin)의 <Privacy and Freedom>이라는 책을 통해 처음 시작되었다.³⁾ 이 책은 책의 제목 “프라이버시와 자유”에서 알 수 있듯이 처음으로 권력에 의한 사회적 통제 즉 정보보유자가 정보주체에 대해 자신도 모르는 규모와 내용의 정보를 가지고 있을 수 있다는 위협만으로 정보주체의 활동 및 자유를 위축시킬 수 있다는 점을 널리 알린 것이었다. 웨스틴의 연구결과는 영미계에서는 미국, 영국 등 각국의 정부들의 연구를 촉발시켰고 소위 공정한 정보처리의 원리(fair information practice principles)이라는 이름으로 각국의 법으로 또는 정책으로 퍼져나갔다. 대륙법계에서는 개인정보자기결정권을 새로운 기본권으로 천명한 1983년 서독연방 헌법재판소의 인구조사결정⁴⁾으로 계승되었다. 오늘날의 개인정보자기결정권의 세계적 흐름에 이르게 되었다. 당시 독일연방헌재는 인구조사법이 인구조사가 개인의 습관, 출근 교통수단, 부업 내역, 학력 등 매우 자세한 정보를 국민들에게 요청하

2) 개인정보에 대해 정보주체가 가진 권리를 재산권으로 다루어야 한다는 견해는 Lawrence Lessig, <Code>, 160-163면.

3) Westin, A., <Privacy and Freedom>, New York: Atheneum, 1967.

4) 독일연방헌법재판소, 15.12.1983 - 1BvR 209/83; 1BvR 269/83; 1BvR 362/83; 1BvR 420/83; 1BvR 440/83; 1BvR 484/83BVerfGE 65, page 1 ff. 독일의 개인정보보호규제의 발전과정에 대해서는 <http://www.iitr.us/publications/13-privacy-laws-in-germany-developments-over-three-decades.html>

도록 하고 이 정보를 원활한 지방행정을 목적으로 지방정부들과 공유할 수 있도록 한 것에 대하여 위헌결정을 내렸다. 그 이유는 개인에 대하여 국가가 수집한 많은 정보들을 조합하여 개인의 “인격” 전체를 구성해낼 가능성을 그 개인이 통제할 수 있어야 한다고 하며 이를 ‘정보자기결정권’ 이라고 명명하였다. 그 이유는 정보의 그와 같은 축적이 개인의 행동의 자유에 위축효과를 미치기 때문이다. 바로 16년전 웨스틴의 발견이었다. 그후 ‘정보자기결정권’ 은 발전을 거듭하여 지금에 이르게 되었다.

위 책 <Privacy and Freedom>에서 웨스틴은 전화 등의 통신기기가 발전한 사회에서의 프라이버시 침해를 고발하며 이에 대한 해법을 제시하였는데 책은 크게 나누어 (1) 감청 (2) 심문 (3) 정보의 대량수집 및 처리에서 발생할 수 있는 프라이버시 침해를 다루었다. 여기서 그는 (3)의 맥락에서 발생하는 프라이버시 침해를 예방하기 위해서는 ‘각 개인이 자신에 대한 모든 정보를 통제할 필요가 있다’ 고 주장하였다. 그 이유는 개인이 자발적으로 타인에게 공개하는 정보라고 할지라도 공개의 조건이 제대로 지켜지지 않아 원래 합의한 목적을 넘어서서 이용되거나 원래 합의한 공개의 범위를 넘어서는 사람에게 정보가 공개되는 것은, 자신이 전혀 공개를 원치 않는 정보가 외부에 공개되는 것과 똑같은 프라이버시 침해라고 볼 수 있다고 보았기 때문이다. 이와 같이 정보공개의 조건이 지켜지지 않아서 ‘자신에 대한 정보의 원치않는 공개’ 가 이루어진 상황을 웨스틴은 “정보감시(data surveillance)” 라고 불렀다. 이와 같은 정보감시 즉 의사에 반하는 자기 자신에 대한 정보공개는 피감시자를 위축시켜 사생활의 자유도 제약하는 피해까지 발생시킨다고 하였다.

다시 말해서 정보감시란, 사람이 살아가면서 자신에 대한 여러 정보를 정부기관이나 업체에 제공할 때, 이 정보가 자신도 모르게 원래의 제공목적과 달리 이용되거나 원래 수집기관이나 업체 밖으로 유출되어 이용되거나 다른 정보들과 합해지는 것을 말한다. 이렇게 될 경우 정보보유자나 처리자들은 정보제공자에 대해 직접 제공받은 정보 이상의 그 무엇을 알게 될 것이다. 이를테면 정보제공자의 다음 행동을 예측하거나 정보제공자 스스로도 몰랐던 자신의 성향을 추출해낼 수도 있을 것이다. ‘감시’ 란 물론 도청, 압수수색, 미행과 같이 개인이 자발적으로 제공하지 않은 정보를 타인이 취득하는 것을 말하지만, 개인이 자발적으로 타인에게 제공한 정보가 축적되는 것만으로도 ‘감시’ 와 비슷한 결과가 나타나는 현상을 웨스틴은 ‘정보감시’ 라고 부른 것이다.

정보감시가 이루어지지 않으려면 개인정보를 수집할 때 정보제공자가 정보제공의 조건으로 제시한 정보의 이용목적과 제3자 제공범위를 준수해야 한다. 이렇게 되면 자신이 제공한 정보의 축적과 이용은 자신이 동의한 범위 내에서만 이루어지게 되므로 원치 않는 ‘감시’ 는 사라지게 된다. 이를 준수하지 않으면 정보제공의 조건

을 위반한 것이므로 타인에 의한 원하지 않는 정보취득이 이루어진 것이므로 “감시”가 된다.

나. 계약법으로는 불충분하다

그런데 많은 경우 정보제공자는 정보의 이용목적과 제3자 제공범위를 구체적으로 정보제공의 조건으로 제시하지 못하여 정보수집자가 준수해야 할 정보제공의 조건이 없거나 불분명한 경우가 많이 있다. 즉 정보제공 시의 약속을 지키도록 하는 접근방식 즉 계약법적(contractual) 접근법이 적용조차 될 수 없는 사례들이 존재한다. 특히 힘없는 개인들이 거대한 기업이나 정부에게 재화나 서비스 수령을 위해 자신의 개인정보를 제공할 때 정보제공의 조건을 협상하거나 그 조건을 나중에 집행할 힘이나 지식이 없는 경우가 허다하다.

바로 이러한 이유로 웨스틴은 물권법적(property-based) 접근법을 선택한 것으로 보인다. 즉 정보주체에 대한 정보를 원칙상(as a default) 그의 소유물로 간주할 경우 정보제공의 조건에 대한 정확한 협상 없이 정보가 제공되었다손 치더라도 정보수집자는 그 정보를 마음대로 할 수 없다는 규범이 성립된다. 정보제공자가 아무런 정보제공의 조건을 제시하지 않았다고 할지라도 정보수집자는 정보제공자(정보주체)에게 정보의 이용목적과 제3자 제공범위를 알려줄 적극적인 의무를 가지게 된다. 쉽게 말해 정보주체는 자신에 대한 정보를 소유한 것으로 인정받게 되면 자신의 의사에 대해 더욱 강하게 존중받게 된다.

길을 지나가다 물건을 발견했다고 치자. 남의 물건으로 보이는 경우, 우리는 소유자와의 아무런 약속 없이도 그 물건을 함부로 다루어서는 안 된다고 생각하게 될 것이다. 이와 같은 디폴트룰이 없다면 우리는 타인에 대한 정보를 우연히 또는 아무런 조건 없이 취득하게 되는 경우 정보주체의 ‘감시로부터 자유로울 권리’를 존중하지 않게 될 것이다.

물권법적 접근은 정보가 제3자에게 양도된 후에도 빛을 발한다. 계약법에만 의존하게 되면, 정보주체로부터 정보를 취득하면서 정보제공의 조건으로서 특정 목적과 특정 공개범위에 합의한 정보처리자는 그 조건에 구속되지만 그 정보처리자로부터 정보를 넘겨받은 제3자는 정보주체와 직접 합의를 한 바가 없기 때문에 그 조건에 구속되지 않는다. 하지만 개인정보를 정보주체의 ‘소유물’로 본다면 - 자동차를 차주의 소유물로 보듯이 - 정보주체는 정보제공의 조건에 대해 자신과 직접 합의를 한 바 없는 제3자에 대해서도 우선하여 정보의 이용에 대한 권리를 행사할 수 있게 된다.

2. 정보소유권의 상대성 - 인상정보의 문제, ‘개인정보처리자’ 및 ‘개인정보파일’의 문제

우리는 여기서 ‘정보주체가 자신에 대한 정보를 소유한다’ 는 명제 즉 정보소유권론은 그 자체로 참이라기 보다는 ‘정보주체가 자신에 대한 정보를 소유한 것처럼 통제권을 가져야만 정보주체의 프라이버시가 효율적으로 보호된다’ 라는 좀 더 복잡한 명제를 은유적이고 표현한 것임을 알 수 있다.

그렇지 않을 경우, 개인정보를 모두 정보주체의 소유물로 보기에 상당한 논리적인 어려움이 뒤따르는데 대표적으로 인상정보의 문제가 있다. 예를 들어 필자가 평소에 알던 정보주체X에 대해 “X는 정치적으로 보수적이다” 라는 평소 감상을 내 노트북에 적어두고 있다고 하자. 그 정보를 정보주체는 정작 접해본 적이 없는데 어떻게 소유권적 통제권을 행사할 수 있겠는가? 또는 X에 대해서 필자가 꿈을 꿔다거나 점을 쳐봤다거나 기타 비과학적인 방법으로 “X가 정치적으로 보수적이다” 라는 확신을 갖게 되었다고 하자. 과연 이 확신에 대해서 X가 통제권을 행사한다는 기획은 현실적이지 않다.

이에 대한 반론으로 혹자는 ‘위 가상상황에서는 X로부터 정보를 “수집” 한 것이 아니라서 원래부터 개인정보보호법이 적용되지 않아 정보소유권론 자체에는 문제가 없다’ 주장할 수 있다. 그러나 평소감상을 적은 경우라도 ‘X는 정치적 보수’ 라는 생각의 토대가 된 정보는 X로부터 수집한 것이므로 개인정보자기결정권이 적용된다. 꿈이나 점의 경우에도 이미 개인정보보호법에 따르면 정보주체가 아닌 다른 소스로부터 정보를 수집하는 경우까지 규제하고 있으므로 역시 개인정보자기결정권이 적용되고 있다고 보아야 한다. 즉 위의 가상상황 모두에서도 정보소유권론은 X가 ‘X는 정치적 보수’ 라는 정보를 ‘소유’ 하고 있다고 볼 것을 요구한다. 하지만 이 당위는 실제로 X는 위 정보와 아무런 물리적 접촉이 없었다는 사실과 격렬하게 충돌한다.

이런 이유로 개인정보자기결정권은 그 문구에 담긴 원대한 희망과는 달리 실제로는 주관적인 공권이라기 보다는 개인정보처리자가 정보주체에 대해 가지는 의무를 통해 실현된다. 즉 정보처리자 - 예를 들어 우리 법 상으로는 ‘개인정보파일을 업무상 운용하는 자’ 가 아닌 이상(여기서 ‘개인정보파일’ 은 검색이 용이하게 개인 정보를 집합화한 것 ‘으로 정의된다) - 가 아닌 이상 타인의 개인정보를 수집 및 이용함에 있어서 아무런 제약이 없다. 보통 기본권은 개인과 외부세계 사이에서 외부세계 전체에 대해 주장할 수 있는 즉 외부세계 전체에 의무를 부과할 수 있는 규범을 의미한다. 예를 들어 사람이 죽음을 당한다면 살인자의 신분과 관계없이 우리는 똑같이 생명권이 침해된 것으로 본다. 그런데 개인정보자기결정권은 개인정보처리자의 행위가 개입되어 있지 않다면 전혀 침해가 발생하지 않는다.

즉 개인정보보호법은 정보주체의 동의 없는 정보이용행위에 있어 선악을 판정하여 규제하려는 ‘행위규제’ 가 아니고 특정인들 즉 여러 사람들에게 한꺼번에 영향을 줄 수 있는 자들을 선정하여 이들에게 의무를 부과하여 목표법익이 침해될 위험

을 최대한 낮추는 ‘위험규제’ 라고 볼 수 있다. 특히 위에서 말했듯이 정보를 제공하는 쪽이 정보를 수집하는 쪽에게 당당하게 정보제공의 조건을 제안하거나 협상할 수 없는 비대칭 상황에서 ‘정보감시’ 가 발생할 수 있는 위험을 낮추려는 것이다.

II. GDPR의 동의없는 2차 처리 관련 조항들

개인정보보호법의 ‘위험규제’ 적인 성격에 맞게 개인정보보호법의 바이블이라고 할 수 있는 GDPR도 처리동의권은 절대적이지 않고 상대적으로 내용이 구성된다. GDPR의 처리동의권과 관련된 조항들을 살펴본다.

1. 양립가능성(부합성) 요건

GDPR의 “목적의 제한성” 요건 즉 개인정보는 수집시에 정보주체가 동의한 목적으로만 이용되어야 한다는 요건은 상당히 완화된 편으로 “양립불가능성 금지”(not incompatible)요건으로 조문화되어 있다.⁵⁾ 이와 같은 연원은 2014년부터 영국개인정보보호기구인 ICO는 “우리는 개인정보보호원칙이 빅데이터라는 목적에 부합하지 않는다는 주장을 거부한다. . . 개인정보보호원칙에 내재하는 어떤 유연함이 있다. 그 원칙은 발전에 대한 걸림돌이 아니라 프라이버시권을 보호하는 틀이자 공중에게 지식을 교환하는 혁신적인 방법을 개발하는 자극제이다”⁶⁾라고 선언한 것과도 연관이 있다.

필자는 ‘양립성’ 이라는 어휘로 목적제한성 요건을 묘사하는 것은 ‘서로 충돌하지만 않으면 허용된다’ 는 어감을 포함할 수 있어 이 장에서만 ‘부합한다’ 는 표현을 쓰고자 한다. Graham Greenleaf의 조사에 따르면⁷⁾ 아시아 지역의 개인정보보호법들을 보면 목적제한성을 얼마나 엄격하게 요구하는가에 따라 편차가 있다고 한다. 아래 표를 보듯이 가장 엄격하게는 베트남법처럼 수집 시에 ‘천명된 목적’에 한정하는 경우도 있지만 마카오처럼 원목적과 충돌하지 않는 목적까지 확장된 경우도 있다.

5) **Article 5 Principles relating to processing of personal data** 1. Personal data shall be (a) processed lawfully, fairly and in a transparent manner in relation to the data subject ('lawfulness, fairness and transparency'); (b) collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes; . . . ('purpose limitation'); . . .

6) 전개서, ICO 제17문단

7) Graham Greenleaf, Asian Data Privacy Laws (2017).

	문구	번역
GDPR	compatible with	원목적과 부합하는
마카오	not incompatible with	원목적과 충돌하지 않는
싱가포르	reasonably expected from	원목적으로부터 합리적으로 기대되는
일본	duly related to	원목적과 적절하게 연관된
필리핀	compatible with but for legitimate interest	원목적과 부합하되 정당한 이익 보호를 위해
홍콩	directly related to	원목적과 직접 연관된
타이완	in conformity with	원목적과
한국	within the scope of	원목적의 범위 내에서
인도	for the purpose collected	수집의 목적을 위해서
베트남	for the purpose announced	천명된 목적을 위해서

Article 29 Working Party는 “우리는 새로운 목적에의 이용이 허용된다거나 새로운 목적이 원래 [수집시의] 목적과 동일해야 한다거나 심지어 새로운 목적이 원래 목적과 양립해야 한다고 요구하지 않으며 단지 원래 목적과 ‘양립불가능’ 해서는 아니된다고 요구할 뿐이다. . . 추가처리는 원래의 목적에 밀접하게 부합할 수도 있고 다를 수도 있다. 추가처리가 수집목적과 다르다고 해서 자동적으로 양립불가능한 것이 아니라 사안별로 평가되어야 한다” 고 하였다.⁸⁾ 그리고 이 개념은 GDPR의 핵심조항인 목적의 제한성 조항에서 명시되어 양립가능한 범위 내에서의 목적변경은 허용되는 것으로 간주되었다.⁹⁾

원래 목적과의 양립가능한 추가처리가 기존의 데이터베이스가 축적될 때 관련 정보처리자나 관련 정보주체가 전혀 예기치 않았던 방향의 연구일 경우에 위 조항의 효용성은 어떨까?¹⁰⁾ 예를 들어 도서관의 데이터베이스는 도서대출의 목적(더욱 정확히는 도서대출이후 도서반환청구권의 확보를 위하여)으로 ‘아무개가 어떤 책을 빌렸다’ 라는 정보들을 축적함으로써 이루어진 것인데 독서습관과 건강의 관계에 대한 연구를 들을 수 있다. 이와 같은 연구에의 이용은 정보주체의 동의범위를 벗어나는 것이 된다. 개인정보보호법을 엄격히 따르려면 결국 수백만 수천만의 기존

8) Article 29 Data Protection Working Party. Opinion 03/2013 on purpose limitation. European Commission 2 April 2013. http://ec.europa.eu/justice/dataprotection/article-29/documentation/opinionrecommendation/files/2013/wp203_en.pdf, 제21쪽

9) GDPR Article 5(1)(b)

10) 전게서, ICO 제115문단 (“The ability to analyze the data for different purposes, such as using the location of mobile phones to plot movements of people or traffic is an important characteristic - and a benefit - of big data analytics.”)

도서대출자에게 일일이 새로운 연구목적으로의 이용에 대한 동의를 얻어야 하겠지만 이는 우선 엄청난 노력과 비용을 필요로 할 뿐 아니라 동의를 해준 사람들의 데이터만으로 진행된 연구의 결과는 편향될 수 밖에 없다. 그렇다고 과연 GDPR이 ‘양립가능성’을 통해 허용하고자 하는 추가처리에 포함될지 의심스럽다. GDPR은 목적제한성 원칙을 밝힌 조항과 별도로 “추가처리” - 즉 원목적과 다른 목적으로 개인정보를 이용할 때는 몇가지 요소들을 고려하도록 되어 있다. 가명화가 이루어질 경우 추가처리가 가능한 양립가능한 목적의 범위가 다소 넓어질 수 있다. 6조4항은 양립가능성 판단에 있어서 고려할 요소로 원처리와 추가처리 사이의 연관성, 정보가 수집된 맥락, 정보주체에 미치는 영향, 그리고 암호화 및 가명화 등의 안전 조치를 거론하고 있다.¹¹⁾ 원처리와 추가처리의 연관성만을 고려한다면 많은 2차처리들이 제한될 것으로 보인다.

2. 기록/연구/통계 목적

GDPR은 위에서 말했듯 목적의 제한성에 대한 예외로서 양립가능한 목적의 추가처리를 언급한 후 그 구체적인 예로서 공익적 기록목적 (archiving purposes in the public interest), 과학적 또는 역사적 연구목적 (scientific and historical research purposes) 및 통계목적(statistical purpose)을 인정하고 있으며 이 때는 위에서 언급했던 6조4항의 원처리와 추가처리의 연관성 등과 같은 요소의 고려를 배제한다.¹²⁾ GDPR 제89조1항에서 이와 같은 기록, 연구, 및 통계목적으로 이용할 정보처리자들은 정보주체를 위한 적절한 안전조치를 취하도록 하고 있으며 특히 정보최소화원칙(data minimization principle)을 존중할 것을 요구하고 있다.¹³⁾

11) Article 6 Lawfulness of processing. . .

4. Where the processing for a purpose other than that for which the personal data have been collected is not based on the data subject's consent or on a Union or Member State law which constitutes a necessary and proportionate measure in a democratic society to safeguard the objectives referred to in Article 23(1), the controller shall, in order to ascertain whether processing for another purpose is compatible with the purpose for which the personal data are initially collected, take into account, inter alia:
- (a) any link between the purposes for which the personal data have been collected and the purposes of the intended further processing;
 - (b) the context in which the personal data have been collected, in particular regarding the relationship between data subjects and the controller;
 - (c) the nature of the personal data, in particular whether special categories of personal data are processed, pursuant to Article 9, or whether personal data related to criminal convictions and offences are processed, pursuant to Article 10;
 - (d) the possible consequences of the intended further processing for data subjects;
 - (e) the existence of appropriate safeguards, which may include encryption or pseudonymisation.

12) **Article 5 Principles relating to processing of personal data** 1. . .(b) . . .further processing for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes shall, in accordance with Article 89(1), not be considered to be incompatible with the initial purposes;

13) **Article 89 Safeguards and derogations relating to processing for archiving purposes in the**

공익목적의 기록은 다음과 같이 정의된다.¹⁴⁾

공익을 위한 기록을 보유한 공공기관, 공공기구 또는 민간기구는, 유럽연합이나 회원국 법률에 따라, 일반적인 공익을 위해 지속적 가치가 있는 열람을 획득, 보존, 평가, 조성, 기술(describe), 전달, 증진, 유포 및 제공할 법적 의무가 있는 (공공)서비스여야 한다. 회원국은 예를 들어, 과거 전체주의 국가 체제 하의 정치적 행위, 집단 학살, 홀로코스트 등의 비인도적 범죄, 또는 전쟁 범죄에 관한 특정 정보를 제공할 목적으로, 유지보존의 목적을 위한 개인정보의 추가적 처리를 규정할 권한이 있어야 한다.

과학적 연구는 다음과 같이 정의된다.¹⁵⁾

본 규정의 취지를 위해, 과학적 연구 목적의 개인정보 처리는 기술의 발전과 실증, 기초연구, 응용연구 및 민간 투자 연구 등을 포괄하는 광범위한 방식으로 해석되어야 한다. 또한, 유럽연합 기능에 관한 조약(TFEU) 제179조에 따라 European Research Area(ERA)를 유지보존하려는 유럽연합의 목적이 고려되어야 한다. 과학적 연구목적에는 공중보건 분야에서 공익을 위해 시행된 연구도 포함되어야 한다(편집자 강조).

역사적 연구는 “역사 연구 및 계보학 목적의 연구도 포함되어야 하되 망자에는 적용되지 않는다는 점을 유념해야 한다” 고 간략하게 정의되어 있다.¹⁶⁾

통계 목적은 다음과 같이 정의되어 있다.¹⁷⁾

통계목적은 통계 조사나 통계 결과를 작성하는데 필요한 개인정보의 수집 및 처리의 작업일체를 의미한다. 그 통계 결과는 과학적 연구 목적 등 다른 목적을 위해 추가적으로 활용될 수 있다. 통계 목적에는 통계 목적으로의 정보처리 결과가 개인정보가 아닌 집단적 데이터 (aggregate data)이며 이 결과나 개인정보가 다른 특정 개인에 관한 조치나 결정을 지지하는데 활용되지

public interest, scientific or historical research purposes or statistical purposes 1. Processing for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes, shall be subject to appropriate safeguards, in accordance with this Regulation, for the rights and freedoms of the data subject. Those safeguards shall ensure that technical and organisational measures are in place in particular in order to ensure respect for the principle of data minimisation. Those measures may include pseudonymisation provided that those purposes can be fulfilled in that manner. Where those purposes can be fulfilled by further processing which does not permit or no longer permits the identification of data subjects, those purposes shall be fulfilled in that manner.

14) GDPR Recital 158

15) GDPR Recital 159

16) GDPR Recital 160

17) GDPR Recital 162

않는다는 점이 내포되어 있다.

위의 조문들을 살펴보면 다음과 같은 통찰을 얻을 수 있다.

첫째, 과학연구 및 역사연구에는 “민간투자(privately funded)” 연구가 포함되어 있으며 특히 “공익목적의 기록”에는 “공익목적”이라는 제한이 붙지만 나머지 연구목적과 통계목적에는 공익목적의 요건이 부과되지 않는다.

둘째 통계목적의 정보처리에만 집단적 정보(aggregate data) 요건이 부과되어 있음은 과학적 연구나 역사적 연구는 집단적 정보가 아닌 개인정보를 대상으로 이루어질 수 있고 개인정보를 결과물로 남길 수 있음을 의미한다.

셋째, 연구의 목적을 “새로운 지식의 추구”로 정의한다면 통계는 데이터처리방식의 하나로서 연구목적의 행동에 한정되지 않는다. 그렇다면 과학적 연구나 역사적 연구가 아닌 다른 목적을 위해 통계적 방식을 이용할 수도 있다. 주목할 점은 빅데이터를 위한 데이터베이스결합은 주로 개인정보가 아닌 집단적 정보를 생성하여 일반화된 명제를 도출하는 것에 있으므로 상당히 넓게 이용될 수 있을 것으로 보인다. 예를 들어, 위에서 도서관기록과 병원진료기록을 연계하여 “톨스토이의 ‘전쟁과 평화’를 읽은 사람은 심장병 유병율이 10% 낮다”라는 통찰을 얻는다면 그와 같은 통찰이 과학적 의미를 가지고 있지 않다고 할지라도 집단적 정보를 중국적으로 도출하는 것을 목표로 하고 있는 한 데이터연계는 자유롭게 이루어질 수 있는 것이다.

넷째, 공익적기록목적, 연구목적과 통계목적 (Archiving, Research, Statistics 줄여서 ARS)으로 추가처리를 하기 위해서는 89조1항이 명시하는 최소수집원칙을 위한 안전조치를 취해야 하는데 GDPR이 안전조치의 예로 들고 있는 것은 유일하게 ‘가명화’이다. GDPR의 핵심조항인 목적제한성 조항에서 양립가능한 목적의 추가처리가 가능하다면서 ‘양립가능한 목적’의 예로서 공익적 기록, 과학 또는 역사적 연구, 통계를 들고 있어서 우선 ‘공익적 기록, 과학 또는 역사적 연구, 통계’의 범주에 포함되는 경우에는 가명화 여부가 추가처리 허용 여부에서 중요한 의미를 가진다고 볼 수 있다.

3. 가명화

GDPR은 95년 EU디렉티브에는 없었던 “가명화”라는 절차를 새롭게 언급한다. 가명화는 정보에서 직접적인 식별자(이름, 주소 등)를 제거하여 추가정보가 없이는 식별화가 불가능한 상태로 만드는 것을 말한다. 즉 정보를 익명화할 필요는 없지만 그 스스로 개인식별이 가능하지도 않아야 한다. 이때 추가정보는 반드시 개인의 식별이 불가능하도록 기술적 조직적 (technical and organizational measure) 조치를 통해 격리되어 있어야 한다. 이렇게 되면 개인식별의 위험이 낮으니 프라이버시 침해 위험은 줄어들지만 그 정보의 효용은 살아있게 된다. 이와 같은 이유로 GDPR은

개인정보처리자들이 기본적으로 개인정보를 가명화할 것을 장려하고 있다. 그러나 GDPR상의 개인정보의 정의는 “다른 정보와 용이하게 결합하여 개인을 식별할 수 있는 정보”를 포함하고 있기 때문에 가명화된 정보도 계속 개인정보로 간주되어 관련 규제를 받게 된다. 이에 대해 GDPR은 다음과 같은 혜택을 줌으로써 가명화를 장려하고 있다.

첫째 위에서 언급했던 추가처리의 양립가능성 판단에 있어서의 혜택이다. GDPR은 구체적이고 명시적이고 합법적인 목적으로 개인정보를 수집하고 그 목적을 위해서만 그 정보를 이용할 것을 의무화하고 있다. 그러나 제5조에서 원래 수집 목적과 “양립가능한 방식”으로 추가처리를 할 수 있다고 하였다. 제6조4항은 “추가처리 “의 양립가능성을 판단할 때 처리활동 사이의 연계성, 수집의 맥락, 정보의 성격, 정보주체에게 발생할 수 있는 영향 등을 고려하라고 하면서 ” 암호화나 가명화와 같은 안전조치의 실행 여부 “도 고려하라고 규정하였다. 즉 가명화가 된 정보는 더욱 폭넓게 ” 추가처리 “의 범위를 허용받게 된다는 것이다. 그렇다면 이를 빅데이터 상황에 접목해보자면 데이터베이스를 가명화할 경우 기존에 성립된 데이터베이스를 새로운 연구목적으로 다른 데이터베이스와 연계하는 행위도 ” 추가처리 “로 인정될 가능성도 높아지게 된다.

단, 가명화는 추가처리 허용여부의 하나의 고려사항일 뿐 충분조건이 아니며 주된 분석은 “추가이용”의 양립가능성을 중심으로 이루어져야 한다. Article 29 Working Party는 빅데이터를 위한 목적 변경과 관련하여 다음의 2가지 “추가이용”을 분류하고 있다.¹⁸⁾ 첫째 일반적인 흐름이나 상관관계를 읽어내기 위한 분석 또는 둘째 개인에 대한 평가나 판단을 위한 분석이다. 이 중에서 후자의 경우에는 “자유로운, 구체적인, 충분한 제공된 상태에서, 명확한 참여동의의사(free, specific, informed, and unambiguous opt-in consent)”가 필요하다고 하여 결국 개인식별이 이루어지는 상태에서의 추가이용은 양립가능하지 않음을 밝히고 있다.

둘째, 위에서 언급했던 연구목적 또는 통계목적을 위한 추가처리의 요건으로 가명화가 안전조치로 언급되고 있다. 가명화가 양립가능한 목적을 위한 추가처리에서는 하나의 긍정적인 고려요소였다면 기록/연구/통계목적을 위한 추가처리가 양립가능한 목적으로 인정되기 위해서는 하나의 의무사항이다. 왜냐하면 기록/연구/통계 목적을 위한 추가처리의 요건을 규정한 89조1항이 명시적으로 가명화를 요구하고 있기 때문이다.

정리하자면, 가명화는 기록/연구/통계목적을 위한 추가처리를 곧바로 활성화할 수 있는 필요충분조건인 반면 기록/연구/통계 목적이 아닌 양립가능목적에 위한 추가처리에 있어서는 필수조건의 하나라고 볼 수 있다.

18) 전게서, Article 29 WP, 46쪽

양립가능한 목적 + 가명화 + 6조4항의 각종 고려사항 => 동의없는 추가처리 가능성¹⁹⁾

공익기록, 과학연구, 역사연구, 또는 통계의 목적 + 가명화 => 동의없는 추가처리 가능성

III. 우리나라의 개인정보보호법 개정 - 사단법인 오픈넷의 2020년 4월 요구사항

2020년 2월 4일의 개인정보보호법 개정은 공익적 기록 과학연구 및 통계 목적의 “추가처리(further processing)” 조항들을 도입하기 위해 이루어졌다.²⁰⁾ 이는 개인정보 이용의 활성화를 위해 GDPR이 정보주체의 동의 없이 새로운 목적으로 정보를 처리(소위 “추가처리”) 하도록 허용하는 조항들 중에서 가장 활용가능성이 명확한 부분이다. 그러나 GDPR 기준을 구현하기 위해서는 다음과 같은 면에서 추가입법 또는 하위법령 제정작업이 필요해보인다.

첫째, 가명화를 전제로 하여 이루어지는 과학연구의 연구결과물이 사회 전반에 공유되도록 의무화하기 위한 추가입법이 필요하다. 특히 현재 해석상 동의 없는 추가처리가 ‘상업적 연구’도 포함하게 되는데 이 경우 공익성의 확보를 위해서 연구결과의 공유가 필요하다. 가명화된 정보는 다른 정보와 용이하게 결합하여 식별성을 갖추게 되므로 당연히 개인정보이고, 이와 같은 개인정보를 정보주체의 동의 없이 새로운 목적으로 이용하도록 허용하는 “특례”가 인정되기 위해서는 공익적인 성격이 명백해야 한다. 즉 GDPR 전문이 유럽연구공역(European Research Area)을 언급하며 암시하고 있듯이 연구의 혜택이 사회에 환원되는 경우에만 동의 없는 추가처리가 허용되도록 하여 공익성을 보장하는 방향으로 법개정 또는 시행령 제정을 할 필요가 있다. 아래 영국의 개인정보보호법은 제19조에서 의료정보의 경우 기관윤리심의위원회의 심의를 거치도록 하고 있는데 학술적 방법론에 대한 동종계열 학자들의 검증도 거치게 된다는 점을 참조할 필요가 있다.

둘째, GDPR 및 유럽의 기타 개인정보보호법들이 과학연구 목적을 동의요건 면제의 근거로 삼는 반면, 우리나라 개인정보보호법 개정안은 가명화를 동의요건 면제

19) 이 동의없는 추가처리 가능성은 우리나라 개인정보보호법에는 존재하지 않는다.

20) 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.

의 근거로 삼으면서 입법불비가 발생했다. 즉 가명화만 되면 과학연구 목적이 없음에도 불구하고 열람권, 정정권, 삭제권, 처리거부권 등의 정보주체의 권리들이 제한될 가능성이 열린 것이다.²¹⁾ 이 조항은 각종 기업들이 연구 등의 공익적 목표와 무관하게 정보를 가명화하여 정보주체들의 권리를 제한할 위험을 발생시킨다.

물론 개인정보보호위원회가 발행한 개인정보해설서에 따르면 이와 같은 조항은 가명정보의 재식별화를 법으로 금지하여 놓았기 때문에 어쩔 수 없는 것이라고 한다.²²⁾ 그러나 개인정보보호법은 개인정보자기결정권을 보장하기 위해 만드는 법이다. 정보주체가 자신의 권리인 열람권, 정정권 등을 행사하기 위해 재식별화를 요구할 경우 정보처리자는 재식별화를 할 수 있어야 한다. 사실 ‘가명화’는 재식별화를 전제로 행해지는 것이다. 어차피 어떤 상황에서도 재식별화를 하지 못하게 할 거라면 완전익명화를 할 일이지 가명화라는 개념을 도입할 의미가 없다. 예를 들어, 환자가 자신의 입원기록을 열람하길 원한다고 하자. 병원은 보안을 위해 즉 유출시 위험을 최소화하기 위해 가명화하여 보관하고 있다고 하는 경우, 현행법은 병원이 환자에게 입원기록을 열람시켜줄 수 없는 상황이 발생한다.

셋째, 우리나라 개정법은 2개 이상의 데이터베이스의 결합을 국가기관이 지정한 전문기관이 하도록 하고 있는 반면, 결합의 절차에 있어서 재식별키와 연구대상 데이터를 하나의 기관이 보유하지 못 하도록 하는 유럽의 실무를 조문에 반영하고 있지 못하고 있다. 하나의 전문기관이 재식별키와 연구대상 데이터를 보관하게 될 경우 프라이버시 침해 위험은 훨씬 높아진다.

이 요구사항은 결합관리기관과 결합기관의 분리는 <가명정보의 결합 및 반출 등에 관한 고시[시행 2020. 9. 1.] [개인정보보호위원회고시 제2020-9호, 2020. 9. 1., 제정]>를 통해서 어느 정도 해결이 된 반면, 신용정보보호법 및 관련 법령에서는 해결되지 아니하였다.

여기서는 1번째와 2번째 사안에 대해서만 다루기로 한다.

IV. 해법

21) 제28조의7(적용범위) 가명정보는 제20조, 제21조, 제27조, 제34조제1항, 제35조부터 제37조까지, 제39조의3, 제39조의4, 제39조의6부터 제39조의8까지의 규정을 적용하지 아니한다.

22) 제28조의5(가명정보 처리 시 금지의무 등) ① 누구든지 특정 개인을 알아보기 위한 목적으로 가명정보를 처리해서는 아니 된다.

사단법인 오픈넷은 올해 2월 제정된 소위 “데이터3법” 중 아무런 이유 없이 정보주체의 권리를 제한하는 개인정보보호법 제28조의7을 재개정할 것을 요구한다. “데이터3법”의 핵심취지는 GDPR을 벤치마킹하여 ‘통계작성, 과학적 연구, 공익적 기록보존의 목적(이하, “공공목적”)’으로는 개인정보를 정보주체의 동의 없이 이용할 수 있도록 한 개정법 제28조의2에 담겨져 있다. GDPR은 정보주체들이 열람권, 정정권, 처리제한권, 처리거부권을 너무 많이 행사하는 경우 공공목적이 무산되는 것을 방지하기 위해 공공목적의 이용에 한하여 이들 권리를 제한했다. 그런데 우리나라는 데이터3법을 졸속으로 통과시키면서, 개인정보보호법 제28조의7에서 단순히 가명처리만 하면 정보주체의 권리가 제한되도록 하여 개인정보처리자들이 공공목적 없이도 정보주체들의 권리를 제한할 수 있게 하였다.

즉, GDPR은 통계작성, 과학적 연구, 공익적 기록보존의 목적을 위해서는 정보최소화원칙에 부합하는 안전조치(예를 들어, 가명처리)를 적용하면 정보주체의 동의 없이 개인정보를 이용할 수 있으며(GDPR 제89조 1항), 공공목적으로 처리될 때는 제15조(열람권), 제16조(정정권), 제18조(처리제한권) 및 제21조(처리거부권)에 규정된 권리의 적용을 일부 제외할 수 있다(89조 2항)고 하였다. 이에 비해 우리나라 개인정보보호법 **제28조의7은** “가명정보는 [고지권, 파기권, 통지권, 정정권, 삭제권 등]의 규정을 적용하지 아니한다고 되어 있을 뿐이다. 자신에 대한 정보에 대한 열람권, 정정권 등 중요한 권리들이 GDPR 하에서는 공공목적 이용에 한해서 가명처리까지 이루어져야 제한되지만 우리나라 법은 공공목적과 무관하게 가명처리만 되면 정보주체의 권리들이 모두 제한되는 것이다.

이 차이는 형식적 차이 이상의 심각한 혼란을 초래하고 있고 정보인권을 심대하게 침해할 것이다. 정보처리자들은 과학적 연구, 통계작성 등의 목표도 없이 가명처리를 하는 것만으로 정보주체들의 권리를 제한할 수 있게 되었다. 예를 들어 통신사들은 이용자에게 대해 가지고 있는 개인정보를 가명처리하고 재식별키를 제3자에게 보관시키게 되면 이용자들이 자신들에 대해 통신사가 가지고 있는 정보를 열람하겠다고 해도 보여주지 않아도 된다. 정보처리자들이 정보주체 제한을 위해서 조항을 남용하는 것이 아니라 실제로 28조의5가 가명정보의 재식별화를 아무런 예외없이 금지하기 때문에 선의의 정보처리자들도 어쩔 수 없이 정보주체권리 보장을 해주지 못하는 것이다.

더 아이러니한 것은 정부는 가명처리가 정보주체에게 미치는 위험을 감지했음에도 입법불비를 인정하고 개선하려 하지 않고 정보처리자에게 가명처리를 절차적으로 매우 하기 어려운 일로 만들어버렸다. 이에 따라 최근 8월에 개인정보보호위원회가 발표한 가명정보 가이드라인(가명처리편)은 전 세계에서 유일무이하게 가명처리에 엄격한 절차적 요건을 부과하고 있다. 하지만 가명처리는 전 세계적으로 개

인정보보호를 위해 장려되는 조치로서 당연히 정보주체의 동의 없이 할 수 있어야 한다. GDPR도 제32조와 제40조에서 가명처리는 모든 개인정보처리자가 기본적으로 해야 하는 보호조치로 명시하고 있다.²³⁾ 심지어 우리나라의 경우에도 법으로 주민등록번호는 반드시 암호화하여 보관하도록 하여 유출되더라도 식별화 피해를 최소화하도록 하고 있는데(개인정보의 안전성 확보조치 기준 제7조) 여기서 암호화란 정보보호 상으로는 가명처리의 스펙트럼 속의 한 방식일 뿐이다. 그런데 이렇게 가명처리를 어렵게 만들어 놓으면 개인정보처리자들은 프라이버시 보호를 위한 자발적인 가명처리를 하지 않게 되어 유출시 위험이 더 높아질 수밖에 없다.

결국, 가명처리 이전에는 개인정보보호를 위해 장려되고 활발하게 이루어져야 할 가명처리를 어렵게 만들어서 개인정보보호가 약화되고, 가명처리 이후에는 열람권, 삭제권 등 정보주체의 권리가 제한되어 더욱더 개인정보보호가 약화되는 최악의 상황이 만들어져버렸다. 지금이라도 GDPR을 벤치마킹하겠다는 취지를 살려서 제28조의7을 개정하여 ‘과학적 연구, 통계작성, 공익적 기록보존’의 목적을 위해 가명처리된 정보에 대해서만 권리제한이 이루어지도록 하고 가명처리 자체는 모든 개인정보처리자가 활발하게 하도록 장려하는 보완조치들이 이루어져야 할 것이다.

이와 관련하여 가명정보의 재식별화가 정보주체의 요청이 있는 경우 허용되도록 해야 하는데 가명정보의 재식별화 관련해서는 GDPR에 대응조항이 없다. 아래 영국의 개인정보보호법 제171조는 가명정보의 재식별화를 형사별로 금지하되 정보주체의 요청이 있을 경우 허용하는 조항을 참조할 수 있다.

23) 독일 개인정보보호법 64조와 71조도 각각 안전조치와 프라이버시친화적 설계와 관련하여 가명화를 항상 고려할 것을 요구하고 있다. 특히 71조는 목적에 부합하게 모든 정보는 최대한 빨리 ‘가명화 내지 익명화’할 것을 요구하고 있다.

열람권, 정정권, 처리거부권을 보장하기 위한 개정법

	현행	개정
과학적 연구의 정의	제2조 정의 8. "과학적 연구"란 기술의 개발과 실증, 기초연구, 응용연구 및 민간 투자 연구 등 과학적 방법을 적용하는 연구를 말한다.	제2조 정의 8. "과학적 연구"란 기술의 개발과 실증, 기초연구, 응용연구 및 민간 투자 연구 등 과학적 방법을 적용하는 연구를 말한다. 단, 연구결과가 학술지 및 기타 학술적인 통로를 통해서 발표될 것을 목표로 함이 명백한 연구에 한한다.
열람권, 정정권 등의 보장	제28조의7(적용범위) 가명정보는 제20조, 제21조, 제27조, 제34조 제1항, 제35조부터 제37조까지, 제39조의3, 제39조의4, 제39조의6부터 제39조의8까지의 규정을 적용하지 아니한다.	제28조의7(적용범위) 통계작성, 과학적 연구, 공익적 기록보존 등을 위하여 이용된 가명정보는 제20조, 제21조, 제27조, 제34조 제1항, 제35조부터 제37조까지, 제39조의3, 제39조의4, 제39조의6부터 제39조의8까지의 규정을 적용하지 아니한다.
열람권, 정정권 보장을 위한 재식별화	제28조의5(가명정보 처리 시 금지의무 등) ① 누구든지 특정 개인을 알아보기 위한 목적으로 가명정보를 처리해서는 아니 된다.	제28조의5(가명정보 처리 시 금지의무 등) ① 누구든지 특정 개인을 알아보기 위한 목적으로 가명정보를 처리해서는 아니 된다. 단, 제20조, 제21조, 제27조, 제34조 제1항, 제35조부터 제37조까지, 제39조의3, 제39조의4, 제39조의6부터 제39조의8까지의 정보주체의 권리 또는 정보처리자의 의무를 행사하기 위한 경우는 적용되지 아니한다.

<참고: 영국 개인정보보호법>

Data Protection Act 2018

19 Processing for archiving, research and statistical purposes: safeguards

(1) This section makes provision about—

(a) processing of personal data that is necessary for archiving purposes in the public interest,

(b) processing of personal data that is necessary for scientific or historical research purposes, and

(c) processing of personal data that is necessary for statistical purposes.

(2) Such processing does not satisfy the requirement in Article 89(1) of the GDPR for the processing to be subject to appropriate safeguards for the

rights and freedoms of the data subject if it is likely to cause substantial damage or substantial distress to a data subject.

(3) Such processing does not satisfy that requirement if the processing is carried out for the purposes of measures or decisions with respect to a particular data subject, unless the purposes for which the processing is necessary include the purposes of approved medical research.

(4) In this section—

“approved medical research” means medical research carried out by a person who has approval to carry out that research from—

(a) a research ethics committee recognised or established by the Health Research Authority under Chapter 2 of Part 3 of the Care Act 2014, or

(b) a body appointed by any of the following for the purpose of assessing the ethics of research involving individuals—

(i) the Secretary of State, the Scottish Ministers, the Welsh Ministers, or a Northern Ireland department;

(ii) a relevant NHS body;

(iii) United Kingdom Research and Innovation or a body that is a Research Council for the purposes of the Science and Technology Act 1965;

(iv) an institution that is a research institution for the purposes of Chapter 4A of Part 7 of the Income Tax (Earnings and Pensions) Act 2003 (see section 457 of that Act);

“relevant NHS body” means—

(a) an NHS trust or NHS foundation trust in England,

(b) an NHS trust or Local Health Board in Wales, (c) a Health Board or Special Health Board constituted under section 2 of the National Health Service (Scotland) Act 1978,

(d) the Common Services Agency for the Scottish Health Service, or

(e) any of the health and social care bodies in Northern Ireland falling within paragraphs (a) to (e) of section 1(5) of the [Health and Social Care \(Reform\) Act \(Northern Ireland\) 2009 \(c. 1 \(N.I.\)\)](#).

(5)The Secretary of State may by regulations change the meaning of “approved medical research” for the purposes of this section, including by amending subsection (4).

(6)Regulations under subsection (5) are subject to the affirmative resolution procedure.

171 Re-identification of de-identified personal data

(1)It is an offence for a person knowingly or recklessly to re-identify information that is de-identified personal data without the consent of the controller responsible for de-identifying the personal data. (가명정보 재식별화 금지 조항)

(2)For the purposes of this section and section 172-

(a)personal data is “de-identified” if it has been processed in such a manner that it can no longer be attributed, without more, to a specific data subject;

(b)a person “re-identifies” information if the person takes steps which result in the information no longer being de-identified within the meaning of paragraph (a).

(3)It is a defence for a person charged with an offence under subsection (1) to prove that the re-identification-

(a)was necessary for the purposes of preventing or detecting crime,

(b)was required or authorised by an enactment, by a rule of law or by the order of a court or tribunal, or

(c)in the particular circumstances, was justified as being in the public interest.

(4)It is also a defence for a person charged with an offence under subsection (1) to prove that-

(재식별화 항변)

(a)the person acted in the reasonable belief that the person- (정보주체의 동의 또는 추정적 동의)

(i)is the data subject to whom the information relates,

(ii)had the consent of that data subject, or

(iii)would have had such consent if the data subject had known about the re-identification and the circumstances of it,

· ·

(c)the person acted-

(언론, 학술, 예술, 학문 자료의 출간과 관련하여 재식별화가 공익에 부합하는 경우)

(i)for the special purposes,

(ii)with a view to the publication by a person of any journalistic, academic, artistic or literary material, and

(iii)in the reasonable belief that in the particular circumstances the re-identification was justified as being in the public interest, or

<참고: 독일 개인정보보호법>

Section 27 Data processing for purposes of scientific or historical research and for statistical purposes

(1) By derogation from Article 9 (1) of Regulation (EU) 2016/679, the processing of special categories of personal data as referred to in Article 9 (1) of Regulation (EU) 2016/679 shall be permitted also without consent for scientific or historical research purposes or statistical purposes, if such processing is necessary for these purposes and the interests of the controller in processing substantially outweigh those of the data subject in not processing the data. The controller shall take appropriate and specific measures to safeguard the interests of the data subject in accordance with Section 22 (2), second sentence.

(2) The rights of data subjects provided in Articles 15, 16, 18 and 21 of Regulation (EU) 2016/679 shall be limited to the extent that these rights are

likely to render impossible or seriously impair the achievement of the research or statistical purposes, and such limits are necessary for the fulfilment of the research or statistical purposes. Further, the right of access according to Article 15 of Regulation (EU) 2016/679 shall not apply if the data are necessary for purposes of scientific research and the provision of information would involve disproportionate effort.

토론문

가명정보의 세계에 정보주체의 권리는 없다

김선희 변호사

법무법인 이공

참여연대 공익법센터 운영위원

이번에 개정된 개인정보보호법 및 신용정보법의 핵심은 일정한 목적하에 가명정보를 정보주체의 동의 없이 수집 목적 외로 이용하거나 제3자에 제공할 수 있도록 특례를 마련한 것입니다.

전반적으로 GDPR을 벤치마킹한 듯한 모양새를 취하고 있으나, 가명처리나 가명정보를 규정한 맥락이 GDPR과 다릅니다. 가명정보인지 여부가 동의 없는 개인정보 활용을 가능하게 하는 요건으로 이해되다보니, 가명정보를 만들기 위한 가명처리나 정보주체의 권리를 제한 내지 박탈하는 관문이 되고 있고, 그에 더하여 불충분하거나 섬세하지 않은 입법으로 인해 정보주체의 권리는 가명정보의 세계에서 사실상 추방당하였다고 해도 과언이 아닐 정도입니다.

개정된 개인정보보호법(및 신용정보법)²⁴⁾의 가명정보의 처리에 대한 특례규정들이 지닌 문제점에 대해 발제자께서 지적한 점들에 대체적으로 동의하면서, 토론자는 이에 덧붙여 1) ‘가명정보의 처리’에 대해 특례를 신설하였으나 ‘가명처리’에 대해서는 명확한 규정을 두지 않음으로 인해 발생하는 해석상의 혼란 및 정보주체의 권리 침해 가능성, 그리고 2) 가명정보에 대해 정보주체의 권리를 일률적으로 배제하는 개인정보보호법 제28조의7이 가진 위헌성에 대해 조금 더 부연설명하고자 합니다.

1. ‘가명정보의 처리’와 ‘가명처리’의 구별에 대하여

주지하다시피 개정된 개인정보보호법은 ‘가명처리’와 ‘가명정보’의 개념을 새롭게 도입하고 가명처리를 완료한 정보인 가명정보를 개인정보의 한 유형으로 규정하고 있습니다. 개인정보보호법 제3절에는 “가명정보의 처리에 관한 특례”를

24) 신용정보법의 문제가 개인정보보호법보다 좀 더 심각하다고 여겨지나, 이하에서는 주로 개인정보보호법을 위주로 다루고자 합니다.

신설하였는데 제28조의2부터 제28조의7까지 모두 ‘가명정보’와 ‘가명정보의 처리’를 대상으로 할 뿐 ‘가명처리’에 대한 규율내용은 포함되어 있지 않습니다. 제3절뿐 아니라 사실 개인정보보호법 전체에 걸쳐 ‘가명처리’에 대해서는 정의규정(제2조 제1호의2) 외에 별도로 규율하는 조항이 없습니다.²⁵⁾

토론자는 제3절은 ‘가명정보’의 ‘처리’, 즉 이미 가명처리를 완료한 정보를 이용하거나 결합, 제3자 제공하는 등으로 ‘처리’하는 경우에 관한 특례로서 ‘가명처리’에 대해서는 적용되지 않으며 원칙으로 돌아가 개인정보 일반에 대해 적용되는 제반조항들이 모두 적용되는 것으로 해석할 수밖에 없다는 입장이지만,²⁶⁾ 현재 개인정보보호위원회나 개인정보를 처리하는 기업 실무의 해석은 이와 다른 것 같습니다.

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.

[2020 개인정보 보호 법령 및 지침·고시 해설 221쪽]

최근 발행된 개인정보보호위원회의 해설서에서는 개인정보보호법 제28조의2를 ‘통계작성, 과학적 연구, 공익적 기록보존 등’의 목적으로 정보주체 동의 없이 가명정보를 처리하는 경우뿐 아니라 동의 없이 ‘가명처리’하는 것도 허용하는 근거규정으로 제시하고 있는데 법문언의 가능한 해석범위를 넘어 이와 같이 해석하는 근거를 제시하고 있지 않습니다.

한편 제28조의7을 적용할 때는 ‘양자를 구분하여야 한다’고 기재한 것은 제28조의7은 ‘가명정보’에만 적용되고 ‘가명처리’에는 적용되지 않는다는 점을 지적하는 것으로 보이는데, 제28조의2와 제28조의7 모두 ‘가명정보’를 그 대상으로

25) 개인정보보호법 제3조 제7항(개인정보처리자는 개인정보를 익명 또는 가명으로 처리하여도 개인정보 수집목적 달성을 위한 경우 익명처리가 가능한 경우에는 익명에 의하여, 익명처리로 목적을 달성할 수 없는 경우에는 가명에 의하여 처리될 수 있도록 하여야 한다.)에서 ‘가명에 의하여 처리될 수 있도록 하여야 한다’는 해석상 가명정보의 형태로 처리될 수 있도록 하여야 한다는 것으로 이해됩니다.

26) 원칙대로 일반적인 개인정보보호법 규정들이 적용되고, 동의권, 열람요구권도 적용될 수 있어야 할 것입니다. (가명‘처리’ 자체에 대해서는 처리에 대한 삭제나 정정요구는 개념적으로 성립하기 어렵다고 보이고, 향후 나의 개인정보를 가명처리하지 말라는 요구가 가명처리에 대한 동의권 행사인지 가명처리에 대한 처리정지인지는 해석의 여지가 있다고 생각합니다)

함에도 그 적용범위를 달리하는 해석론에도 의문이 있습니다.

개인정보보호법이 ‘가명처리’ 라는 새로운 개념을 도입하였고 가명처리의 결과물인 가명정보에 대해서 정보주체의 권리를 제한하는 특례를 도입했다면 가명처리에 대해서도 조금 더 명확히 규율했어야 하는데, 가명처리에 대한 규율이 불명확하거나 미비하기 때문에 해석상의 혼선이 발생하고 있으며, 개인정보를 처리하는 실무에서는 정보주체에게 불리한, 개인정보처리자에게 유리한 방식으로 운용될 가능성이 매우 높습니다.

실제로 실무에서는 제28조의2와 제28조의7의 적용범위를 모두 가명정보의 처리뿐 아니라 가명처리까지 포함하여 해석하는 경향이 나타나고 있습니다. 예를 들어 개정법 시행 이후 첫 가명정보의 결합 사례는 신한카드의 카드결제정보와 에스케이텔레콤의 기지국 접속정보 등을 금융보안원을 통해 결합한 사례로 알려져 있는데²⁷⁾ 신한카드와 에스케이텔레콤이 위 결합을 위해 자신들이 보유한 이용자들의 개인정보를 가명처리하면서 가명처리에 대해 이용자들의 동의를 받은 적은 없는 것으로 보입니다.²⁸⁾

또 에스케이텔레콤 이용자가 위 가명정보 결합 사례 이후 자신의 개인정보를 가명처리하였는지 여부에 대해 열람을 구하였으나, 가명처리가 완료된 정보를 재식별하는 것이 법에서 금지되어 있고 가명정보에 대해서는 개인정보보호법에서 개인정보의 열람에 관한 제35조 등의 적용을 배제하는 제28조의7을 근거로 제시하며 열람요구에 대해 거부한 사례도 있습니다. 위 열람요구는 가명정보의 처리에 대한 열람을 구한 것이 아니라, 가명처리에 대한 열람을 구한 것이었음에도 그 열람요구를 거부하는 근거로 제28조의7이 활용된 것입니다.

이처럼 가명정보의 처리에 관한 특례규정들은 가명정보의 처리뿐 아니라 가명처리에 대한 정보주체의 권리까지 축소, 배제하는 방향으로 해석, 운용되고 있으며, 가명처리에 대한 입법미비로 인한 불이익이 정보주체에게 전가되고 있음을 보여줍니다.

27) 위 데이터는 금융데이터 거래소(www.findatamall.or.kr)를 통해 현재 판매되고 있으며, 샘플데이터에 따르면 통신사가 보유한 기지국 접속정보와 카드결제정보를 개인단위로 결합하여 “시군구 단위의 주거지, 연령대, 성별, 카드소비등급, 취미코드, 통신소비등급, 19년 해외여행여부, 관심분야, 부산여행일자, 시간대 별로 방문한 관광지, 방문시간대, 체류시간, 해당 방문지에서 소비한 업종, 카드승인 시간대, 숙박지 유형, 숙박지 체류시간대 등”의 정보가 가명정보의 형태로 결합되었음을 추정할 수 있습니다.

28) 신한카드와 에스케이텔레콤은 대신 개인정보처리방침에 가명처리와 관련된 내용을 반영하였습니다. 에스케이텔레콤은 『개인정보 처리방침』을 개정하면서 “SK텔레콤은 수집한 개인정보를 특정 개인을 알아볼 수 없도록 가명 처리하여 통계작성, 과학적 연구, 공익적 기록보존 등을 위하여 처리할 수 있습니다”라는 규정을 추가하였는데, 이와 같은 추상적이고 포괄적인 개인정보처리방침의 형태로 향후 가명처리에 대한 동의를 갈음할 수는 없을 것입니다.

니다.

2. 가명정보에 대해 정보주체 권리를 일률적으로 배제하는 개인정보 보호법 제28조의7, 신용정보법 제40조의3의 문제점

위 조항의 문제점을 지적하며 발제자는 개정방향으로 1) 통계작성, 과학적 연구, 공익적 기록보존을 위하여 이용된 가명정보에 대해서만 열람권 등 정보주체의 권리가 일부 제한되도록 하고 2) 정보주체의 권리 행사 요청에 따른 경우 가명정보를 재식별하는 것은 가명정보에 대한 재식별 금지의무에도 불구하고 허용되도록 하라고 제안하였습니다.

토론자도 발제자의 지적에 동의하면서, 위 조항은 위헌성이 매우 높고 이를 개정할 경우 좀 더 섬세한 접근이 필요하다는 의견을 부연설명하고자 합니다.

위 조항은 ‘가명정보’ 라는 점을 기본권이 제한되기 위한 유일한 요건으로 정하고 있습니다. 개인정보는 그 개념상 살아있는 개인에 ‘관한’ 정보일 것을 요건으로 하는데 개인 관련성 요건이 그 범위에 특별한 제한이 없다 보니 개인정보의 범위는 특정되기 어렵고 확장성, 개방성을 가지고 있습니다. 가명정보를 생성하는 가명처리의 대상이 개인정보이고, 가명처리의 기술이나 방식에도 특별한 제한이 없다 보니 결국 가명정보도 그 범위를 한정할 수 없을 만큼 무궁무진합니다. 결국 가명정보는 개인정보의 하나의 형태 내지 영역으로 볼 수 있습니다.

그리고 위 조항이 규정하고 있는 법률효과로서 기본권 제한은, 개인정보보호법에서 개인정보자기결정권을 구체화한 정보주체의 권리와 그 권리를 보장하기 위해 정보처리자에게 부과되는 의무들을 일률적으로 배제하는 형식을 취하고 있습니다. 법에서 개인정보의 하나로 정한 ‘가명정보’ 의 개념정의에 포함된다는 점 외에 정보주체의 기본권 제한이 발생하기 위한 어떤 부가적인 요건도 없고 **판단의 여지 없이 일의적으로 적용을 배제함**으로써 기본권의 박탈과 같은 효과를 가져오는 것입니다.

위 조항의 의미는 간단히 말하면, ‘가명정보에 대해서는 정보주체의 개인정보자기결정권이 보장되지 않는다’ 입니다.

그런데 이처럼 광범위한 기본권 제한 내지 박탈을 정당화하는 입법목적이 대체 무엇인지부터 생각해볼 필요가 있습니다. 개인정보보호위원회의 해설서에서는 법 제28조의5에서 누구든지 가명정보를 개인을 알아볼 목적으로 처리하는 것을 금지하고 있기 때문에 개인을 알아보아야만 가능한 사항에 대해서는 적용을 배제하는 것

이라고 그 취지를 설명하고 있습니다.

가명정보에 대한 재식별금지의무는 가명정보가 여전히 식별가능한 개인정보임에도 동의 없이 목적 외 이용, 제3자 제공 및 결합할 수 있게 하는 것에서 오는 위험성을 낮추고 재식별에 따른 정보주체 권리침해를 방지하기 위해 부과된 것으로 볼 수 있는데, **정보주체가 자신의 정보를 식별할 것을 전제로 권리행사를 하는 데 대해서까지 재식별 금지의무를 이유로 권리행사를 거부하는 것이 정당화되는**는 의문이 있습니다.²⁹⁾

한편 가명정보에 대해 적용이 배제되는 **제반조항들의 실현을 위해 반드시 가명정보에 대한 재식별이 필요한가**라는 의문도 제기될 수 있습니다. 열람요구권의 예를 들면 자신의 가명정보가 처리되었는지, 어떤 목적으로 어떤 항목이 처리되었는지에 대해 열람을 요구할 때 반드시 가명처리가 완료된 가명정보를 재식별해야만 열람요구한 정보주체의 가명정보가 처리되었는지를 확인할 수 있는 것은 아니라고 생각합니다. 어떤 목적 및 어떤 조건으로 가명처리 대상이 되는 정보주체와 정보항목을 정하여 추출하였는지에 대한 기록 보관을 통해서 가명정보 자체를 재식별하지 않고도 정보주체의 열람요구에 응할 수 있는 가능성은 충분히 상정할 수 있습니다.³⁰⁾

또 가명정보가 유출되었을 때도, 그 유출된 가명정보가 누구를 대상으로 가명처리한 데이터셋이었는지, 가명처리의 대상 및 항목을 선정한 기준에 대한 정보를 통해 유출여부를 확인하여 가명정보에 대한 재식별 없이 유출에 대한 통지를 할 수 있는 가능성도 고려해볼 수 있습니다.

발제자가 제안한 개정방향은 “제28조의2에서 정한 목적으로 처리되는 가명정보에 대해서만” 정보주체의 권리 적용을 배제하자는 제안으로 읽히는데, 제28조의7의 적용범위를 ‘과학적 연구, 통계, 공익적 기록목적’으로 처리한 가명정보에 대해서 한정하더라도 이로서는 정보주체의 권리 제한을 정당화하기에 충분하지는 않다고 생각합니다.

29) 이에 대해서는 가명정보의 재식별을 위해서는 추가정보가 필요한데 개인정보처리자가 정보주체의 요구에 따라 추가정보를 입수 내지 접근하게 하는 것이 가명정보 데이터셋 전체에 포함된 정보주체의 재식별 위험성을 높이는 측면을 생각해볼 수도 있습니다. 그러나 가명정보를 생성하고 추가정보를 별도로 분리하여 보관하는 것은 추가정보를 활용한 재식별의 가능성이나 필요성을 염두에 둔 것이고, 만약 어떤 경우에도, 이처럼 정보주체의 요구가 있는 경우까지만 재식별이 금지된다면 추가정보를 항상 삭제하여 재식별이 불가능하도록 해야지 별도로 보관할 이유도 없습니다.

30) 또 가명정보의 처리 내용에 대해서는 개인정보보호법 제28조의4 제2항에서 “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”고 규정하여 관련 기록의 작성, 보관 의무를 부과하고 있는바, 가명처리에 관한 기록과 가명정보의 처리에 관한 기록을 통해

제28조의2에서 정한 목적으로 가명정보를 처리하는 경우에 대해서라도 그에 대한 정보주체의 권리 제한이 정당화되려면, 가명정보를 처리하는 목적의 공익성, 공공성이 보다 확실히 담보되어야 함은 물론이고, 정보주체의 열람요구권 등 조항을 배제하는 것이 그 가명정보 처리의 목적 달성을 위해서 필요한 수단이어야 하며, 제한되는 권리의 종류나 범위가 가능한 최소화되어야 하고, 가명정보 처리를 통해 달성하고자 하는 목적과 제한되는 기본권 사이의 이익형량이 균형을 이루어야 합니다.

GDPR에서도 가명정보에 대해 정보주체의 권리를 일부 제한하는 규정을 두고 있지만, 그 경우에도 해당 정보가 ‘과학이나 역사적 연구 목적 또는 통계 목적으로 처리되는 경우’ 인지 ‘공익을 위한 기록보존의 목적으로 처리되는 경우’ 인지 **목적**을 구분하여 각각의 경우에 **제한대상이 될 수 있는 권리의 종류를 나누어 규정**하고 있고 어떤 목적으로 가명정보를 처리하더라도 제한되지 않는 권리도 있습니다. 더 중요한 것은 권리 제한이 아무런 조건 없이 일률적으로 적용되는 것이 아니라 “권리로 인해 **특정목적의 달성이 불가능하거나 심각하게 저해될 가능성이 있고 해당 규정의 적용배제가 그 목적의 충족을 위해 필요한 경우**”³¹⁾에 한해서 제한될 수 있다고 하여 가명정보 처리 목적과 정보주체의 권리 사이에 **이익형량의 가능성**을 열어두고 있습니다.

이에 반해 가명정보 처리 목적을 제한하거나 구분하지도 않은 채, 적용이 제한될 필요가 있는 권리의 종류나 제한 조건, 또 권리제한에 따른 기본권 침해를 완화할 수 있는 다른 수단의 도입 등을 전혀 고려하지 않은 채 모든 가명정보에 대해 사실상 개인정보보호법에서 구체화한 정보주체의 모든 권리를 일률적으로 배제한 현행 개인정보보호법 제28조의7은 위헌적이라는 비판을 피할 수 없을 것입니다.

이런 문제점들을 지적하며 지난 11월 초 참여연대 공익법센터에서는 개인정보보호법 제28조의7 및 신용정보법 제40조의3에 대해 개인정보자기결정권 침해를 이유로 헌법소원을 제기한 바 있습니다. 그러나 가능하다면 이미 현실적으로 발생하고 있는 정보주체의 권리 침해상황을 방치하지 말고 입법적인 해결이 신속히 모색되기를 바라는 바입니다.

31) GDPR 제89조 제2항 및 제3항의 후단의 “... such rights are likely to render impossible or seriously impair the achievement of the specific purposes, and such derogations are necessary for the fulfilment of those purposes.”를 참조.

토론문

오병일 대표
진보네트워크센터

1. 과학적 연구의 범위

과학적 연구와 관련하여 “가명화를 전제로 하여 이루어지는 과학연구의 연구결과물이 사회 전반에 공유되도록 의무화하기 위한 추가입법이 필요” 하며, “현재 해석상 동의 없는 추가처리가 ‘상업적 연구’도 포함하게 되는데 이 경우 공익성의 확보를 위해서 연구결과의 공유가 필요” 하다는 것에 동의함. 가명정보 역시 개인정보이고 정보주체의 동의없이 과학적 연구 목적으로 개인정보를 제공하는 것은 일정하게 정보주체의 권리를 제한하는 것이므로, 그에 상응하는 ‘공익적 가치’를 가져야 함.

개인정보보호법은 '과학적 연구'를 ‘과학적 방법을 적용하는 연구’로 동어반복적으로 정의하고 있으며, 과학적 방법을 적용하지 않는 연구가 거의 없다는 점에서 사실상 ‘연구’를 표방하는 모든 연구로 열어두고 있음.

GDPR에서는 ‘과학적 연구’를 정의하고 있지 않고 ‘과학적 연구’에 대한 유럽 개인정보보호이사회(EDPB)의 의견도 아직 발표되지 않은 상황이라, 현재로서는 과학적 연구에 대한 관행적인 인식에 의존할 수 밖에 없는 상황임. 다만, 유럽개인정보보호감독관(European Data Protection Supervisor, EDPS)이 2020년 1월에 발표한 <과학적 연구와 개인정보 보호에 관한 예비 의견서>³²⁾는 유럽연합에서도 과학적 연구의 개념과 범위와 관련된 고민과 논의가 진행되고 있음을 보여줌.

EDPS는 과학적 연구의 개념을 검토하면서 “개인정보처리자가 단지 과학적 연구 목적이라고 주장하는 것으로는 충분하지 않”으며, 학술 연구자(academic researcher)나 비영리 단체 및 정부 기관, 영리 기업도 과학적 연구를 수행할 수 있지만, “과학적 연구가 전체 사회에 유용하며 과학적 지식이 촉진되고 지원해야 할 공공재라는 점을 공통된 전제로 한다”고 보고 있음. 이어 과학적 연구를 위한 개인정보 보호체계는 다음과 같은 세 가지의 기준이 충족될 경우 적용된다고 규정

32) EDPS, A Preliminary Opinion on data protection and scientific research, 2020.1.6

하고 있음. 첫째 개인정보가 처리될 것, 둘째 정보에 기반한 동의(informed consent), 책임성, 감독의 개념을 포함하여, 관련 분야의 방법론이나 윤리가 적용될 것, 셋째 연구가 주로 사적인 이익이 아니라 사회 전체적인 지식 및 복리의 향상을 목적으로 수행될 것 등임. 또한, GDPR 제5조의 규정이 통계작성이나 역사적, 과학적 연구는 애초 수집 목적과 다르더라도 무조건 양립 가능한 것으로 전제되는지에 대해, 그러한 목적으로 처리하는 것을 무조건 허용하는 것은 아니며, 과학적 연구 목적 등으로 활용하기 전에 6(4)조에 따른 양립가능성 조건을 검토할 필요가 있다고 함.

개선 방향과 관련하여 발제자가 제안한 바와 같이 “단, 연구결과가 학술지 및 기타 학술적인 통로를 통해서 발표될 것을 목표로 함이 명백한 연구에 한한다.”는 규정을 ‘과학적 연구’의 개념에 포함시키는 것도 하나의 방법이 될 것임. 그러나 앞의 ‘과학적’이라는 개념과 다른 ‘학술적’이라는 용어를 사용함으로써 ‘과학적’과 ‘학술적’의 의미가 다른지, 공공성 요건을 발표 여부만을 갖고 판단할 것인지 등의 논란을 야기할 수도 있음. 사실 과학적 연구는 제28조의2에서 전제하듯, 정보주체의 동의없이 수행하는 연구만 있는 것은 아니며, 동의에 기반한 연구도 있을 수 있고, 어떤 연구는 공익적 가치를 가지고 있음에도 불구하고 공개되지 못하는 경우도 있을 수 있음. ‘과학적 연구’를 정의하는 것이 쉽지 않다면, 법에서는 과학적 연구의 정의를 삭제하고 과학적 연구의 공익적 가치 요소와 사례들에 대한 의견서(마치 EDPB의 의견서와 같이 개인정보보호위원회가 의견서를 통해 개념에 대한 해석을 제공할 수 있을 것임)를 통해 해석의 지침을 제공하는 것도 하나의 방법임.

2. 정보주체의 권리 제한 요건

개인정보보호법 제28조의7에서 ‘통계작성, 과학적 연구, 공익적 기록보존 등’에 한정되지 않고 ‘가명정보’ 일반에 대해 정보주체의 권리를 제한하는 것의 문체에 대한 발제자의 지적에 동의함.

제28조의5는 가명정보의 재식별을 금지하고 있는데 정보주체의 권리를 보장하기 위해서는 재식별이 필요하다는 것이 그 이유임. 그러나 가명정보를 처리하더라도 항상 정보주체의 권리 보장이 불가능한 것은 아님. 예를 들어 가명정보의 일부가 아니라 전부가 유출되었을 경우, 가명처리를 했던 개인정보처리자는 별도로 보관된 추가정보를 통해 누구의 개인정보가 가명처리되었는지 확인할 수 있음. 비록 가명처리되었다고 하더라도 유출된 가명정보가 개인정보 침해 위험이 큰 정보들이라면 해당 정보주체에게 통지를 할 필요도 있으며, 이것이 정보주체에게 해를 입히는 것

도 아님. 이 경우 가명정보를 재식별하지 않고 애초의 개인정보를 통해 정보주체에게 통지해줄 수 있을 것임. 제21조(개인정보의 파기)의 경우에도 특정한 가명정보를 재식별하지 않고 특정 과학적 연구나 통계 목적이 완료된 후 가명정보 자체를 파기하는 방법으로 보장할 수 있음. (반대로 제21조의 적용을 배제하는 것은 가명처리만 하면 영구적으로 보관할 수 있는 것으로 해석될 위험이 있음. 이와 관련하여 EDPS는 “연구 기관들이 GDPR의 특별 조항을 개인정보를 무한정 보관할 수 있도록 허용하는 것으로 해석하거나 정보주체에게 정보를 제공할 권리를 부인하는 것은 개인정보의 남용으로 간주될 수 있다” 고 지적함.)

제28조의5 및 제28조의7이 오히려 정보주체의 권리를 제한한다면, 해당 조항을 두는 이유가 무엇인지 의문임.

제28조의7은 가명정보에만 적용되고 ‘개인정보의 가명처리’에는 적용되지 않는다는 점도 인식할 필요가 있음. 예를 들어, 정보주체는 자신의 개인정보를 가명처리하여 연구나 통계 목적으로 사용하는 것을 원하지 않을 수 있으며, 이 때 제37조 개인정보 처리정지권을 행사하여 자신의 개인정보를 가명처리하지 말 것을 요구할 수 있음.

이런 측면에서 발제자가 “예를 들어 통신사들은 이용자들이 대해 가지고 있는 개인정보를 가명처리하고 재식별키를 제3자에게 보관시키게 되면 이용자들이 자신들에 대해 통신사가 가지고 있는 정보를 열람하겠다고 해도 보여주지 않아도 된다.” 고 해석하는 것은 그 의미가 모호할 수 있음. 왜냐하면, 통신사들은 서비스 제공을 위해 이용자 개인정보 원본을 가지고 있으며, 자사의 과학적 연구나 타사의 과학적 연구를 위해 가명처리하여 활용할 수 있을텐데, 이때 가명처리에도 불구하고 정보주체는 여전히 자신의 개인정보에 대한 열람권을 행사할 수 있으며, 단지 통신사는 이미 가명처리한 개인정보, 즉 가명정보를 어떻게 처리했는지에 대한 열람권만 제한할 수 있을 뿐임. 또한 정보주체는 자신의 개인정보를 어떠한 목적으로, 언제 어떻게 가명처리 했는지에 대해서도 열람권을 행사할 수 있을 것임.

제28조의7에 ‘통계작성, 과학적 연구, 공익적 기록보존 등을 위하여 이용된’이라는 표현을 덧붙이는 발제자의 대안에 동의하면서도 더 보완이 될 필요가 있음. 즉, 이러한 요건에 더하여, 통계작성, 과학적 연구, 공익적 기록보존 등의 경우에는 무조건 정보주체의 권리가 제한되는 것이 아니라, 정보주체의 권리를 제한할 경우 해당 과학적 연구 등 특정 목적을 달성하기 힘든 경우에만 정보주체의 권리가 제한되도록 해야 함. 예를 들어, 수백만명의 정보주체에게 통지하는 것이 사실상 불가능하거나, 정보주체의 권리를 보장하면 연구의 타당성이 위협받는 경우 등이 이에 해당할 것임. GDPR 제89조의 경우에도 이러한 경우에만 정보주체의 권리를 제

한할 수 있도록 하고 있음.

3. 기타 발제문의 일부 표현에 대한 의견

“가명화가 양립가능한 목적을 위한 추가처리에서는 하나의 긍정적인 고려요소였다면 기록/연구/통계목적에 위한 추가처리가 양립가능한 목적으로 인정되기 위해서는 하나의 의무사항이다.” → 가명화는 안전조치의 하나일 뿐 의무사항은 아님. 오히려 가능하다면 익명처리를 하도록 하고 있음.

“가명화는 기록/연구/통계목적에 위한 추가처리를 곧바로 활성화할 수 있는 필요충분조건” → 마찬가지로 가명화는 가능한 안전조치의 하나이며, 사례에 따라 익명조치 혹은 다른 추가적인 안전조치가 필요할 수 있음.

토론문

최경진 교수
가천대학교 법과대학

“가명정보에 대한 정보주체의 권리 보장을 위한 개인정보보호법 개정 제안”을 발표해주신 발제자에게 감사의 말씀 드립니다. 우리 개인정보보호법 상의 가명정보 및 권리주체의 권리에 대한 검토와 GDPR 상 관련규정에 대한 분석까지 심도 있게 발표해주셔서 많은 것을 알 수 있었습니다.

많은 사람들이 기대하고 바래왔던 개인정보보호 관련법제의 개선을 위한 ‘데이터 3법’ 개정이 드디어 이루어졌고, 그에 따른 결실 중의 하나가 가명처리를 통한 가명정보의 활용과 결합 근거가 마련되었다는 점입니다. 가명처리는 개인 식별성을 저감하고 안전한 개인정보의 활용을 위한 기반으로 도입되었기 때문에 무한정 확장하여 허용되는 것은 아니고, “통계작성, 과학적 연구, 공익적 기록보존 등” (개인정보 보호법 제28조의2 제1항) 혹은 “통계작성, 연구, 공익적 기록보존 등”의 목적인 경우에 한하여 정보주체의 가명정보를 처리할 수 있다. 또한 가명처리는 그 정도에 따라서 원래의 특정개인이 식별될 수 있도록 복원되거나 재식별될 수 있는 가능성을 완전히 제거한 것은 아니기 때문에 가명처리하고 가명정보를 처리하는 과정에서 정보주체를 보호할 수 있는 조치들을 함께 규정하였습니다. 예를 들면, 가명정보의 결합을 제한하여 보호위원회 또는 관계 중앙행정기관의 장이 지정하는 전문기관이 결합을 수행하도록 하였으며, 가명정보에 대한 안전조치의무로서 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 합니다(개인정보보호법 제28조의4 제1항). 아울러 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 합니다(개인정보보호법 제28조의4 제2항). 뿐만 아니라 가명정보처리 시에 누구든지 특정 개인을 알아보기 위한 목적으로 가명정보를 처리해서는 안되는 재식별금지의무가 부과됩니다(개인정보보호법 제28조의5 제1항). 가명정보를 처리하는 과정에서 특정 개인을 알아볼 수 있는 정보가 생성된 경우에는 즉시 해당 정보의 처리를 중지하고, 지체 없이 회수·파기하여야 합니다(개인정보보호법 제28조의5 제2항).

가명정보도 여전히 개인정보의 영역에 포함되기는 하지만, 법에 의하여 재식별 금지 의무를 부과함으로써 가능한 안전한 상태로 유지하려는 것이 입법자의 의도라고 생각합니다. 이러한 취지를 살리기 위하여 개인정보보호법은 가명처리 관련 기록의 보존의무를 부여하되 정보주체의 권리에 관한 규정은 적용하지 않도록 한 것이라고 생각합니다. 이러한 점에서 발제자께서 발제하신 내용 중에서 몇 가지 궁금한 점을 질문하는 것으로 바람직한 법해석 혹은 법제 개선 방향이 무엇인지에 대한 논의를 구체화하는데 보탬이 되고자 합니다.

1. 발제자께서는 “우리나라 개인정보보호법도 보안목적의 가명처리는 자유롭게 하되 동의없는 이용은 ‘과학적 연구, 통계 작성, 공익적 기록보관’의 공공성 등이 확보되는지 엄격하게 관리하고, 가명화된 정보에 대해서도 정보주체의 의사에 따라 재식별화할 수 있는 길을 열어 정보주체의 권리보장을 할 필요가 있다.”고 주장하셨는데,

(1) ‘보안목적의 가명처리’를 자유롭게 한다는 것이 현행 개인정보보호법 하에서 어떠한 의미를 가지는 것인지 보다 구체적으로 말씀 해주시길 부탁드립니다.

(2) 개인정보보호법 제2조제8호는 과학적 연구에 대하여 “기술의 개발과 실증, 기초연구, 응용연구 및 민간 투자 연구 등 과학적 방법을 적용하는 연구”로 규정하고 있고, 신용정보법도 제2조 제9의2에서 연구에 산업적 연구가 포함되는 것으로 규정하고 있습니다. 아울러 신용정보법은 통계작성에 “시장조사 등 상업적 목적의 통계작성을 포함”하는 것으로 규정합니다. 이러한 규정 하에서도 기록보존과 같은 “공익성” 혹은 “공공성”을 요구하는 것이 타당한 것인지 궁금하고, 더 나아가 가명처리가 가능한 “등”의 구체적인 사례나 “등”을 해석함에 있어서도 “공익성”을 요구해야 할 것인지 의견을 부탁드립니다.

2. 발제자께서는 “GDPR 및 유럽의 기타 개인정보보호법들이 과학연구 목적을 동의요건 면제의 근거로 삼는 반면, 우리나라 개인정보보호법 개정안은 가명화를 동의요건 면제의 근거로 삼으면서 입법불비가 발생했다. 즉 가명화만 되면 과학연구 목적이 없음에도 불구하고 열람권, 정정권, 삭제권, 처리거부권 등의 정보주체의 권리들이 제한될 가능성이 열린 것이다.”고 말씀하셨는데, 지적하신 적용범위에 관한 제28조의7의 규정은 가명정보의 처리에 관한 특례를 규정한 제3장 제3절에 위치해있고, 가명정보 처리의 합법적 처리근거가 제28조의2 이하에 규정되어 이를 준수하는 것이 필수적인 것으로 보이는데, GDPR과 다르다고 볼 수 있는지 여쭙고 싶습니다.

3. GDPR에 따르더라도 가명처리가 된 경우에는 사실상 접근권을 포함한 정보주체

의 권리가 실질적으로 작동되기 어려운 것으로 이해하고 있습니다. 가명처리를 통하여 식별성을 저감시켜서 가능한 안전한 상태로 개인정보를 처리하도록 하려는 목적으로 보이는데, 발제자께서는 GDPR의 명확한 입장이 가명정보에 대하여도 정보주체의 권리를 보장해야 한다고 생각하시는지 궁금합니다.

4. 가명정보에 대하여 정보주체의 권리를 보장해야 할 실질적인 실익이 어떠한 것이 있는지, 혹시 사례를 말씀해주실 수 있다면 함께 소개 부탁드립니다.

5. 정보주체의 권리를 보장하기 위해서 가명정보를 재식별할 수 있도록 여지를 만들어놓고, 실제 재식별이 필요하게 되는 경우에 재식별을 허용하는 것이 바람직한가에 대하여도 여쭙보고 싶습니다. 이럴 경우에 현재의 처벌 규정은 “누구든지” 재식별을 금지하고 있는데, 이에 대한 예외 규정을 두어야 하는 것인지도 궁금합니다.

감사합니다.

