

개인정보 데이터 비식별화 정책방향



경인교육대학교 사회과교육과
심우민(조교수, 법학박사)
legislation21@gmail.com
<http://legislation.kr>

C contents

01 개인정보 비식별화 논란

02 입법적 대응방식

03 비식별 조치 입법정책 방향

01

개인정보 비식별화 논란

개인정보 비식별화 논란

01 개인정보 비식별화 논란(1)

➔ 개인정보 보호법제의 체계변화 요청

- 국내외적으로 개인 식별 가능성을 중심으로 한 개인정보 보호법 제 및 체계의 변화에 관한 지속적인 논의가 이루어지고 있음
 - 최근 빅데이터(Bid Data) 분석 등을 통해 다양한 사회적 유용성과 가치를 가지는 정보 산출에 관심이 높아지고 관련 산업이 비약적으로 성장하면서, 이에 대해 개인정보 보호규제가 장애요인으로 등장하고 있다는 평가로 인하여, 개인정보의 비식별화 또는 익명화를 통한 활용이 논의되고 있음
 - EU, 미국, 일본 등 주요 국가들도 빅데이터 등의 산업적 분석 및 활용 과정에서 발생하고 있는 문제점에 착안하여 개인정보 보호법제 개선에 관한 논의를 진지하게 진행하고 있음
- 국내외적으로 개인정보 비식별화(가명화) 또는 익명화, 그리고 그 법적 효과와 관련해서는 아직까지 확고한 개념정의 및 규정 등이 존재하지 않는 임

01 개인정보 비식별화 논란(2)

➔ 비식별화 또는 익명화 개념 논쟁

- 국내의 최근 연구는 우리나라를 비롯한 미국, EU, 일본 등지의 용례를 검토하여, 비식별화와 익명화가 명확하게 구분되지 않는다고 보는 견해도 제시되고 있음
 - 이와 유사하게, 비식별화에 관한 미국 NIST의 보고서는 익명화된 정보도 또한 재식별화할 수 있다는 견지에서, 혼돈을 줄 수 있는 익명화라는 단어를 당해 보고서에서는 사용하지 않는다고 설명하고 있음(NIST, 2015)
- 결과적으로 비식별화든 익명화든 결국에는 특정 조치를 기반으로 개인정보 보호원칙 적용의 예외를 허용하는 것은 재식별화의 위험성을 수반할 수 밖에 없다는 점은 분명함
 - 기술적 발전에 따라 식별 가능성 또는 위험성은 불가피하게 증대될 수 밖에 없는 상황이기 때문에, 향후 개인정보 보호법제의 쟁점은 용어 선택과 사용의 문제가 아니라 실질적으로 정보주체의 권리를 보호할 수 있는지 여부라고 할 것임

01 개인정보 비식별화 논란(3)

➔ 개인정보 비식별 조치 가이드라인

- 정부는 2016년 6월 30일 정부부처 합동으로(국무조정실, 행정자치부, 방송통신위원회, 금융위원회, 미래창조과학부, 보건복지부) 「개인정보 비식별 조치 가이드라인」을 공표하였음
 - 이 가이드라인 이전에는 방송통신위원회의 「빅데이터 개인정보보호 가이드라인」이 공표된 바 있었는데, 이는 다분히 방송통신위원회 소관 영역에 한정하고 있는 성격을 가짐
 - 부처합동 「개인정보 비식별 조치 가이드라인」은 개인정보 관련 부처들이 공동으로 제정 및 공표하였다는 점에서, 향후 우리나라의 개인정보 보호정책에 있어 중요한 의미를 가진다고 평가할 수 있음
- 「개인정보 비식별 조치 가이드라인」은 개인정보자기결정권 및 영업수행의 자유와 같은 헌법적 기본권 제한에 관한 문제이기 때문에 법률로써 규정할 필요가 있다는 주장이 있음(cf. 규범력)

01 개인정보 비식별화 논란(4)

➔ 개인정보 보호입법에 관한 영향

- 「개인정보 비식별 조치 가이드라인」은 현재로서는 행정지도로서의 성격을 가지는 것에 불과하지만, 입법의 필요성은 존재하지 때문에, 그 내용은 향후 입법에 반영될 가능성이 높음
 - 제19대 및 제20대 국회에서는 빅데이터 또는 디지털 신산업 육성의 차원에서 비식별 조치에 관한 법안들이 다수 발의되고 있음
 - 실제 발의된 법률안들은 대부분 정부의 가이드라인 내용을 그대로 답습하고 있는 경우가 많음(cf. 방송통신위원회, 부처합동)
- 최근에는 이 가이드라인의 절차와 유사한 내용을 반영하여, 법률상 가명정보 개념 신설 논의가 입법적으로 이루어지고 있는 상황임(cf. 4차산업혁명위원회 해커톤)

02

입법적 대응방식
이러저 대응차기

02 입법적 대응방식(1)

➔ 입법적 대응방식 개관

➤ 가이드라인을 통한 대응방식

- 영국 ICO(Information Commissioner's Office)의 「익명화 실천규약」(Anonymisation: managing data protection code of practice)은 세계적으로 비식별 조치 등에 관한 최초의 지침 또는 가이드라인 형태의 기준을 제시하고 있음

➤ 입법조치(실정법)를 통한 대응방식

- 최근 제정 및 개정된 EU의 「개인정보 보호규칙」(General Data Protection Regulation, 이하 GDPR)과 일본의 (신)「개인정보 보호법」(個人情報の保護に関する法律)은 비식별 조치를 입법적으로 반영하고 있음

* 참고: 미국의 경우 특별법적 성격의 법률로 Family Educational Rights and Privacy Act, Health Information Technology for Economic and Clinical Health Act)이 있으며, 가장 많이 언급되고 있는 법률로 Health Information Portability and Accountability Act에 따른 'HIPAA 프라이버시 규칙' 도 있음

02 입법적 대응방식(2)

➔ 영국의 익명화 실천규약(1)

➤ 익명화 실천규약의 제정 근거

- EU 「개인정보보호지침」 자체 내에서는 익명화 방식에 대해 좀 더 구체적인 기준들을 규정하지 않고 있지만, 더 자세한 내용들은 EU 회원국들에게 실천규약 (code of conduct)이라는 형식으로 위임하고 있음(동 지침 제27조)

➤ 익명화 실천규약의 의의 및 주요 내용

- 「익명화 실천규약」은 일종의 안내서이기 때문에, 그 자체가 법적인 강제력을 가지는 것은 아니지만, 이 실천규약에서 규정한 사항들을 준수했다는 사실을 ICO가 확인할 경우 이는 추후 ICO가 개인정보 보호와 관련한 법 위반 사실에 대한 조사나 법집행을 할 경우 적극적으로 고려하게 된다는 점에서, 이 규약은 간접적인 영향력을 지니는 가이드라인의 특성을 지니고 있다고 평가할 수 있음
- 이 실천규약은 개인정보의 이용에 있어 보호업무를 충실히 수행하는 과정에서 유발될 수 있는 위험을 관리하는 방식의 일환으로 익명화를 소개하고 있음

02 입법적 대응방식(3)

→ 영국의 익명화 실천규약(2)

➤ 익명화 실천규약의 구성

- 실천규약의 법적지위와 배경(제1장), 익명화와 개인정보 개념정의와의 연관성(제2장), 익명화의 개인정보에의 기여(제3장), 익명화 과정에서의 정보주체의 동의 문제(제4장), 공간(위치)정보(제5장), 타 법령상 공개제한(제6장), 개인정보의 유형별 취급방식(제7장), 개인정보보호 거버넌스(제8장), 연구목적 개인정보 활용(제9장)

➤ 익명화 실천규약의 특징

- 특정 개인에게 손해, 고통 또는 금전적 피해 등과 같이 재식별 결과의 위험성이 있는 경우에는, 익명화 정보를 활용하고자 하는 기관은 그러한 정보 공개로 발생할 수 있는 결과를 설명하고 정보주체의 동의를 구해야 한다고 명시하고 있음
- 정보주체는 자신의 정보가 익명화될 것인지 여부에 대해 구체적으로 통보 받을 수 없기 때문에, 익명화를 실시하고자 하는 기관들은 이 사실을 프라이버시 정책(privacy policies) 및 다른 수단들을 통해 제시해야 한다고 설명함

02 입법적 대응방식(4)

→ EU GDPR의 가명처리(1)

➤ GDPR의 가명처리 규정

- 당초 EU의 「개인정보 보호규칙」(GDPR) 입법 과정에 있어서는 가명정보(pseudonymous data)에 대한 개념정의 규정을 두는 것에 대한 논의가 있었지만, 최종적으로는 가명처리(pseudonymisation)에 관해서만 개념정의 하는 것으로 변경되었음

<GDPR 입법이유>

(26) 정보 보호의 원칙은 식별되었거나 식별 가능한 자연인에 관한 모든 정보에 적용되어야 한다. 가명화를 거친 개인정보는, 추가 정보를 사용하여 해당 자연인을 확인할 수 있는 경우 식별 가능한 자연인에 관한 정보로 간주되어야 한다.... 정보 보호의 원칙은 익명 정보, 즉 식별되었거나 식별 가능한 자연인에 관한 것이 아닌 정보나 정보 주체가 더 이상 식별 가능하지 않은 방식으로 익명 처리된 개인정보에는 적용되지 않는다. 따라서 본 규칙은 통계 또는 연구 목적을 포함한 그러한 익명 정보의 처리와는 관련이 없다.

02 입법적 대응방식(5)

→ EU GDPR의 가명처리(2)

<GDPR 본문>

제4조(정의) (5) '가명화'는 추가 정보를 사용하지 않으면 개인정보가 더는 특정 정보 주체와 연결되지 않도록 개인정보를 처리하는 것을 의미한다. 단, 그러한 추가 정보는 별도로 관리되어야 하며, 개인정보가 식별되었거나 식별 가능한 자연인과 연결되지 않도록 하기 위한 기술적, 조직적 조치가 이루어져야 한다.

제11조(식별을 필요로 하지 않는 처리) 1. 정보 관리자가 개인정보를 처리하는 목적이 정보 관리자에 의한 정보 주체 식별을 필요로 하지 않거나 더 이상 필요로 하지 않게 된 경우, 정보 관리자는 본 규정 준수라는 목적만으로 정보 주체를 식별하기 위해 추가 정보를 유지, 취득, 처리할 의무를 지지 않는다.

2. 본 조 제1항에 언급된 상황에서, 정보 관리자가 정보 주체를 식별할 수 있는 위치에 있지 않다는 사실을 입증할 수 있는 경우, 정보 관리자는 가능하면 이를 정보 주체에게 고지해야 한다. 그러한 경우 제15조~제20조는 적용되지 않으나, 정보 주체가 해당 조항에 따른 자신의 권리를 행사하기 위해 식별을 가능하게 하는 추가 정보를 제공한 경우는 제외된다.

* 참고: 제15조(정보주체의 접근권) / 제16조(정보주체의 수정권) / 제17조(정보주체의 삭제권) / 제18조(정보주체의 처리제한권) / 제19조(개인정보 수정 또는 삭제나 처리제한 통지 의무) / 제20조(정보주체의 정보 이동성에 대한 권리)

02 입법적 대응방식(6)

→ EU GDPR의 가명처리(3)

제6조(처리의 적법성) 4. 개인정보를 수집한 목적 외로 처리하는 것이 정보주체의 동의 또는 제23조(1)의 목적을 보장하기 위한 민주사회의 필요하고 비례적인 조치를 구성하는 유럽연합 또는 회원국 법률에 근거하지 않는 경우, 컨트롤러는 개인정보의 목적 외 처리가 해당 개인정보를 수집한 당초 목적과 양립될 수 있는지 확인하기 위해서 특히 다음 각 호를 고려해야 한다.

- (a) 수집 목적과 의도된 추가처리 목적 간의 연관성
- (b) 특히 정보주체와 컨트롤러 간의 관계와 관해서 등의 개인정보가 수집된 상황
- (c) 특히 제9조에 따른 특정 범주의 개인정보가 처리되는지 여부 또는 제10조에 따른 범죄경력 및 범죄 행위와 관련한 개인정보가 처리되는지 여부 등 개인정보의 성격
- (d) 의도된 추가처리가 정보주체에 초래할 수 있는 결과
- (e) 암호처리나 가명처리 등 적절한 안전조치의 존재

제25조(설계 및 기본설정에 의한 개인정보 보호) 1. 컨트롤러는 개인정보의 처리가 자연인의 권리 및 자유에 미치는 위험의 다양한 가능성 및 정도와 함께 최신 기술, 실행 비용, 그리고 처리의 성격, 범위, 상황 및 목적을 고려하여, 가명처리 등의 기술 및 관리적 조치를 개인정보의 처리 방법을 결정한 시점 및 그 처리가 이루어지는 해당 시점에 이행해야 한다. (이하생략)

02 입법적 대응방식(7)

→ EU GDPR의 가명처리(4)

제32조(처리의 보안) 1. 컨트롤러와 프로세서는 개인정보의 처리가 자연인의 권리 및 자유에 미치는 위험의 다양한 가능성 및 정도와 함께 최신 기술, 실행 비용, 그리고 처리의 성격, 범위, 상황 및 목적을 고려하여, 해당 위험에 적절한 보안 수준을 보장하기 위해 특히 다음 각 호 등을 포함하여 적절한 기술 및 관리적 조치를 이행해야 한다.

(a) 개인정보의 가명처리 및 암호처리; (b) 처리 시스템 및 서비스의 지속적인 기밀성과 무결성, 가용성, 복원력을 보장할 수 있는 역량; (c) 물리적 또는 기술적 사고가 발생하는 경우 개인정보에 대한 가용성 및 열람을 시의 적절하게 복원 할 수 있는 역량; (d) 처리의 보안을 보장하는 기술 또는 관리적 조치의 효율성을 정기적으로 테스트 및 평가하기 위한 절차

제89조(공익적 기록보존 목적 등을 위한 처리와 관련한 안전조치 및 적용의 일부 제외) 1. 공익적 기록 보존 목적, 과학적 또는 역사적 연구 목적, 또는 통계적 목적을 위한 처리는 정보주체의 권리 및 자유를 위해 본 규정에 따라 적절한 안전조치가 적용되어야 한다. 그러한 안전조치는 특히 데이터 최소화 원칙이 준수되도록 기술 및 관리적 조치를 이행해야 한다. 그러한 조치에는 가명처리 방식으로 그러한 목적들을 달성할 수 있다면 가명처리가 포함될 수 있다. 정보주체의 식별을 허용하지 않거나 더 이상 허용하지 않는 추가 처리를 통해 그러한 목적들을 달성될 수 있는 경우에는 그러한 방식으로 달성되어야 한다.

02 입법적 대응방식(8)

➔ 일본의 (신)「개인정보 보호법」상 익명가공정보(1)

➤ (신)「개인정보 보호법」상 익명가공정보 규정

- 일본의 (신)「개인정보 보호법」은 익명가공정보에 관한 개념정의와 아울러, 이에 수반되어야 하는 제반 조치의무 등에 관해서도 규정하고 있음
- EU에서는 관련 정보의 활용 맥락에 따라 그 정보의 속성이 결정되는 반면, 일본의 경우에는 특정 방식(형식)의 가공 처리를 거친 경우에는 익명가공정보가 됨

<일본 (신)「개인정보 보호법」>

제2조(정의) ⑨ 이 법률에서 “익명가공정보”라 함은 다음 각 호에 열거된 개인정보의 구분에 따라 당해 각 호에서 정하는 조치를 취하여 특정 개인을 식별할 수 없도록 개인정보를 가공하여 얻어지는 개인에 관한 정보로서, 당해 개인정보를 복원할 수 없도록 한 것을 말한다.

1. 제1항 제1호에 해당하는 개인정보 - 당해 개인정보에 포함되는 기술 등의 일부를 삭제하는 것 (당해 일부의 기술 등을 복원할 수 있는 규칙성을 갖지 않는 방법에 의해 다른 기술 등으로 치환하는 것을 포함한다)
 2. 제1항 제2호에 해당하는 개인정보 - 당해 개인정보에 포함되는 개인식별부호의 전부를 삭제하는 것 (당해 개인식별부호를 복원할 수 있는 규칙성을 갖지 않는 방법에 의해 다른 기술 등으로 치환하는 것을 포함한다)
- ⑩ 이 법률에서 “익명가공정보취급사업자”라 함은 익명가공정보를 포함하는 정보의 집합물이면서 특정한 익명가공정보를 전자계산기를 이용하여 검색할 수 있도록 체계적으로 구성한 것으로서 정령으로 정하는 것(제36조 제1항에서 “익명가공정보데이터베이스 등”이라고 한다)을 사업용으로 이용하는 자를 말한다. 다만, 제5항 각 호에 열거된 자를 제외한다.

02 입법적 대응방식(9)

➔ 일본의 (신)「개인정보 보호법」상 익명가공정보(2)

제36조(익명가공정보의 작성 등) ① 개인정보취급사업자는, 익명가공정보(익명가공정보데이터베이스 등을 구성하는 것에 한정한다. 이하 같다)를 작성하는 때에는, 특정의 개인을 식별할 수 없도록 그리고 그 작성에 사용되는 개인정보를 복원할 수 없도록 하기 위하여 필요한 것으로서 개인정보보호위원회규칙으로 정하는 기준에 따라, 당해 개인정보를 가공하여야 한다.

③ 개인정보취급사업자는, 익명가공정보를 작성한 때에는, 개인정보보호위원회규칙으로 정하는 바에 따라, 당해 익명가공정보에 포함되는 개인에 관한 정보의 항목을 공표하여야 한다.

⑤ 개인정보취급사업자는, 익명가공정보를 작성하여 스스로 당해 익명가공정보를 취급함에 있어서는, 당해 익명가공정보의 작성에 사용된 개인정보와 관계된 본인을 식별하기 위하여 당해 익명가공정보를 다른 정보와 조합해서는 아니된다.

⑥ 개인정보취급사업자는, 익명가공정보를 작성한 때에는, 당해 익명가공정보의 안전관리를 위하여 필요하고 적절한 조치, 당해 익명가공정보의 작성 및 그 밖의 취급에 관한 고충의 처리 및 그밖에 당해 익명가공정보의 적절한 취급을 확보하기 위하여 필요한 조치를 스스로 강구하고 또한 당해 조치의 내용을 공표하도록 노력하여야 한다.

제37조(익명가공정보의 제공) 익명가공정보취급사업자는, 익명가공정보(스스로 개인정보를 가공하여 작성한 것을 제외한다. 이하 이 절에서 동일하다)를 제3자에게 제공하는 때에는, 개인정보보호위원회규칙으로 정하는 바에 따라, 미리 제3자에게 제공되는 익명가공정보에 포함되는 개인에 관한 정보의 항목 및 그 제공의 방법에 대하여 공표함과 더불어, 당해 제3자에 대해 당해 제공과 관련된 정보가 익명가공정보라는 취지를 명시하여야 한다.

제39조(안전관리조치 등) 익명가공정보취급사업자는, 익명가공정보의 안전관리를 위하여 필요하고 적절한 조치, 익명가공정보의 취급에 관한 고충의 처리 및 그밖에 익명가공정보의 적절한 취급을 확보하기 위하여 필요한 조치를 스스로 강구하고 또한 당해 조치의 내용을 공표하도록 노력하여야 한다.

03
03

비식별 조치 입법정책 방향
비식별 조치 입법정책 방향

03 비식별 조치 입법정책 방향(1)

→ 현행 가이드라인 관련

➤ 가이드라인을 통한 대응방식

- 영국 등의 가이드라인 방식을 통한 대응은 명백히 법령 등의 위임이 있는 경우라고 할 수 있음
- 우리나라 가이드라인의 경우에는 현행 개인정보 보호법제의 해석 및 적용상의 문제점을 해소하기 위한 목적을 가지는 것이라고는 하지만, 이러한 방식이 의회 및 법률 유보의 원칙을 준수한 것인지에 대해서는 별도로 논의가 필요함

➤ 가이드라인에서 규정하고 있는 법적효과

- 현행 가이드라인은 비식별 조치가 이루어진 정보를 개인정보가 아닌 것으로 추정한다는 내용을 명시하고 있음
- 이러한 비식별 조치의 법적 효과(부여)가 타당한 것인지에 대해서는 원론적 측면에서 재검토가 필요할 것으로 판단됨

03 비식별 조치 입법정책 방향(2)

→ 입법형식 관련

- 가이드라인 또는 법률(입법)을 통한 대응
 - 가이드라인을 통한 대응이 적절한 것인지, 아니면 법률 개정을 통한 대응이 적절한 것인지에 대해서는 논의가 필요할 것으로 보임
 - 기본권 제한의 문제가 결부되어 있기 때문에 법률 개정을 통한 대응이 필요하다고 볼 수 있지만, 빅데이터 분석 등 데이터 활용 기술이 급격하게 진보하고 있는 상황에서 오히려 법률을 근거로 한 대응은 다소 경직성을 가질 수 있는 측면이 충분히 있음
- 새로운 법률 규정방식(입법기술) 모색
 - 가이드라인을 통해 기술적 변화에 신속하게 대응하는 체계를 구상한다고 치더라도, 기본적인 사항(용어설정 및 법적효과) 등에 대해서는 법률에 명시적으로 규정할 필요성이 있을 것임
 - EU 및 영국의 실천규약과 관련한 법령상 규정과 같이, 민간의 적극적인 의견수렴을 전제로 한 기준설정 작업도 현재의 기술 환경에서 유효한 방식일 수 있음

03 비식별 조치 입법정책 방향(3)

➔ 개인정보 자기결정권 관련

➤ 정보주체의 개인정보자기결정권

- 개인정보 보호사안에 있어 궁극적으로 중요한 것은 개인정보자기결정권의 실현 방식이라고 할 수 있음
- 개인정보자기결정권의 실현방식 중 가장 대표적인 것이 정보주체의 동의권이라고 할 수 있는데, 이것이 아니더라도 정보주체 스스로가 자기의 정보를 통제할 수 있는 방식은 다양하게 모색이 가능함

➤ 정보주체의 관리 및 통제 가능성 확보

- 정보주체의 관리가능성을 확보하기 위해서는 자신의 정보가 어느 단계에서 어떻게 처리되고 있는지를 정보주체가 명확하게 파악할 수 있어야 함
- 현행 우리나라의 가이드라인은 정보주체는 자신의 정보에 비식별 조치가 취해 지는지 여부에 대한 사실조차 파악할 수 없음(cf. 개인정보가 아닌 것으로 추정)
- 영국, EU, 일본 등에서는 비식별 등의 조치가 이루어지는 정보의 항목들을 정보주체가 파악할 수 있도록 공지하는 규정을 두고 있어 참조할 필요가 있음

03 비식별 조치 입법정책 방향(4)

➔ 최근 입법개선 쟁점 사례 – 정책 편의성(?)

➤ 물건의 위치정보 동의권 면제(?)

- 개인 식별 가능성 여부 관계 없이 위치정보의 수집을 위하여 정보주체(소유자)의 동의를 받도록 중첩적으로 규정되어 있던 위치정보법 제15조가 최근 개정되어, 물건의 위치정보인 경우에는 소유자의 동의를 면제함
- 그러나 물건의 위치정보 여부 판단이 개념적으로 어려울 뿐만 아니라, 물건의 위치정보인 경우에도 프라이버시 위협이 존재하는 경우가 있음

➤ 가명정보 개념 신설(?)

- 가명정보 개념 신설을 통하여 개인정보보호법상 동의요건 및 관련 규제를 면제하는 방식으로 개인정보의 활용을 촉진하는 방안이 추진중임(cf. 4차위 해커톤)
- 가명정보라는 법적 개념을 신설하는 것의 타당성은 차치하고라도, 새로운 정보 개념을 창출하는 경우에는 이에 해당하는지 여부에 대한 논란이 또 다시 발생할 수 밖에 없음(cf. 전통적 개념법학적 사고)

03 비식별 조치 입법정책 방향(5)

➔ 개인정보 입법패러다임 전개방향

➤ 실질적이고 새로운 프라이버시 관념 정립

- 향후 개인정보 개념 논란보다는 실질적인 프라이버시 보호 확대에 주안점을 둘 필요가 있으며(보호영역 확대), 특히 일률적 요건 규제(ex. 획일적 동의요건)보다는 실질적인 위험이 있는 곳에 규제가 이루어질 수 있는 것이 바람직함(risk-based approach)

구분	프라이버시 →	개인정보자기결정권 →	新프라이버시
보호대상	식별성 비전제 (사생활 영역)	식별성 전제 (개인정보)	식별성 + 비식별성 (포괄성)
권리주장	소극적/사후적	적극적/사전적	소극적 + 적극적
규제 및 집행	맥락적 형량	개인정보 (확정)개념 전제 (해석적 형량 불가피)	실효적 보호 (구체성 → 이용 활성화)

**들어 주셔서
감사합니다**