



국회토론회

정보주체의 관점에서 본 개인정보보호법 개정 방향

일시

2021. 12. 16.(목) 오후 2시



참여연대 채널

주최

더불어민주당 민병덕 국회의원
정의당 배진교 국회의원
경제정의실천시민연합
민변 디지털정보위원회
사단법인 정보인권연구소
진보네트워크센터
참여연대

국회 토론회

정보주체 관점에서 본 개인정보보호법 개정 방향

순서

2:00-2:10	인사말	국회의원 민병덕 (더불어민주당) 국회의원 배진교 (정의당)
	사회	한상희 (참여연대 정책자문위원장, 건국대법전원 교수)
2:10-2:40	발제	정보주체의 권리 강화를 위한 개선방안 김보라미 (경실련 소비자정의센터 운영위원, 변호사)
	지정토론	권건보 (아주대학교 법학전문대학원 교수)
2:40-3:10	발제	개인정보처리자의 책임성 강화 방안 서채완 (민변 디지털정보위원회 간사, 변호사)
	지정토론	최경진 (가천대학교 법학과 교수)
3:10-3:15	휴식	
3:15-5:00	종합토론	이진규 (네이버 CPO) 오병일 (진보네트워크센터 대표) 이병남 (개인정보보호위원회 개인정보보호정책과 과장) 김보라미 (경실련 소비자정의센터 운영위원) 권건보 (아주대학교 법학전문대학원 교수) 서채완 (민변 디지털정보위원회 간사) 최경진 (가천대학교 법학과 교수)

C/O/N/T/E/N/T/S

인사말

국회의원 민병덕 (더불어민주당)	1
국회의원 배진교 (정의당)	2

발제 및 지정토론

발제 : 정보주체의 권리 강화를 위한 개선방안 / 김보라미 (경실련 소비자정의센터위원)	4
토론 / 권건보 (아주대 법학전문대학원 교수)	22
발제 : ‘개인정보처리자의 책임성 강화’를 위한 개인정보 보호법 개정과제 / 서채완 (민주사회를 위한 변호사모임 디지털정보위원회 간사)	26
토론 / 최경진 (가천대학교 법학과 교수)	58

종합 토론

1. 이진규 (네이버 CPO)	61
2. 오병일 (진보네트워크센터 대표)	69
3. 이병남 (개인정보보호위원회 개인정보보호정책과 과장)	75



인사말



국회의원 민병덕 (더불어민주당)

새로운 산업의 발전 이후에, 입법이 따라가는 것이 관행이고 현실입니다.

그럴 때 우리 국회는 신기술의 적용을 독려하고, 새로운 산업의 발전 및 신규 일자리와 먹거리를 확보하는 것에 주목합니다. 그 신기술이라는 것은 세계 경쟁 환경 속에서는 어찌면 그리 새로운 것이 아니고 한참 따라가야 하는 기술일 수도 있기 때문에, 우리 기업들은 최대한 규제를 철폐해 달라는 요청하십니다.

이러한 변화에 따라 개인의 인권과 자유와 공동체의 안전에 대한 고민에 소홀할 우려가 있는데, 이러한 간극을 메꿔 주는 목소리가 있습니다.

수많은 IoT 디바이스를 통한 무분별한 개인정보의 수집,
언제 해킹당할지 모르는 수준 낮은 보안 카메라,
출입문부터 결제까지 자연스럽게 수집되는 개인의 생체인식 정보와 민감정보,
이렇게 수집되는 데이터가 대규모로 가공되고 거래되고 유통되고, 해외로 다시 국내로 돌아다니는 현실입니다.

산업의 발전을 위해서는 좀 풀어주어야 할 것 같고,
개인의 인권을 위해서는 좀 묶어두어야 할 것 같고,
고민입니다.

오늘 다양한 의견과 고민을 하는 시간을 갖겠습니다. 고맙습니다.

인사말



국회의원 배진교 (정의당)

안녕하십니까, 정의당 원내대표 배진교입니다.

먼저, 오늘 토론회를 공동으로 주최하는 더불어민주당 민병덕 의원님과, 경실련, 민변 디지털정보위원회, 정보인권연구소, 진보네트워크센터, 참여연대 대표님과 회원들에게 감사드리며, 아울러 발제자와 토론자에게도 감사의 인사를 드립니다.

디지털 시대가 현실화 되면서 하루에도 수많은 데이터를 생산하고 소비합니다. 이렇게 생성된 데이터에는 많은 개인정보가 포함되어있는 만큼, 정보 보호 중요성은 아무리 강조해도 지나치지 않습니다.

2020년 8월 개인정보보호법이 시행되었으나, 당시 개인정보의 목적 외 활용 제공의 범위를 확대하고 정보주체의 동의 없이 개인정보를 활용할 수 있도록 하는 데 치우쳐 있을 뿐 빅데이터 시대에 개인정보를 보호할 수 있는 장치는 없었다는 한계를 갖고 있었습니다.

이에 올해 9월 개인정보보호위원회는 2차 개정안을 제출했습니다. 정보주체의 권리강화를 강조하며 전송요구권 도입, 자동화된 결정에 대한 대응권 도입을 골자로 하고 있습니다. 그러나 정보주체의 고지받을 권리 확대, 수사 명분으로한 개인정보 제3자 제공 문제, 민감정보의 경우 과학적 연구 목적이란 이름으로 제한없이 활용되는 문제 등에 대한 내용은 빠져있습니다.

또한, 개인정보를 처리하는 처리자에 대한 책임성도 모호합니다. 현실적으로 정보주체가 개인정보처리자가 되어 자신의 개인정보를 통제하는 것은 불가능한 만큼 개인정보처리자가 적법하게 개인정보를 처리할 수 있도록 책임성을 부여하는 문제는 굉장히 중요합니다.

따라서, 개인정보처리자의 책임성 강화와 개인정보 영향평가 제도 강화, 개인정보 중심설계 및 기본설정 제도 도입, 개인정보 보호감독관 제도 도입 등을 통해 개인정보 보호체계를 강화하는 내용을 담아 법안 발의 중임을 아울러 말씀드립니다.

오늘 토론회는 데이터 경제의 발전과 개인정보 보호의 균형점을 찾기 위한 자리가 될 것이라 기대합니다. 다양하고 깊이 있는 전문가분들의 의견을 경청하겠습니다.

감사합니다.

...

발 제

정보주체의 권리 강화를 위한 개선방안

김보라미 (경실련 소비자정의센터위원,
법률사무소 디케 변호사)



I. 들어가면서

2020년 1월 9일, 국회본회의에서 202개의 법률안들이 거의 토론이 이루어지지 아니한 채 19시 5분부터 21시 48분까지 총 2시간 43분 동안 통과되었습니다. 이 법률안들 중에는 소위 ‘데이터 3법’이라 불렀던 「개인정보보호법」, 「신용정보의 이용 및 보호에 관한 법률(이하 “신용정보법”）」, 「정보통신망 이용촉진 및 정보보호 등에 관한 법률(이하 “정보통신망법”）」이 포함되어 있었습니다. 비록 본회의에서 위 법률안들은 통과되었지만 「개인정보보호법」은 반대 14인, 기권 21인, 신용정보법은 반대 15인, 기권 23인으로 반대토론에 공감하여 당론에 반대하는 표결도 이루어진 바 있었습니다.

본회의에 위 법률안들이 올라오기 전, 채이배 의원은 법사위에서 「개인정보보호법」의 법체계 정합성의 문제를 제기한 바 있었습니다. 채이배 의원은 “법사위가 과방위 부대의견¹⁾을 무시하고 있다”며 법정합성의 문제를 체계적으로 제기하였으나, 더불어민주당 송기현 법사위 간사는 “이 법이 완전할 수는 없지만 여야가 합의를 해서”라는 우선 통과시켜야 한다고 여당의 입장을 설명하여 해당 법률안은 법정합성도 제대로 검토하지 못하였습니다. 이 날, 「개인정보보호법」의 안타까운 운명은 결정된 것이었습니다.

II. 2020. 1. 9. 개정된 「개인정보 보호법」 입법과정에서 활용규정만 입법화된 채, 정보주체의 권리보장은 전혀 포함되지 못하였습니다.

문재인 대통령은 2018년 8월 31일 ‘데이터경제 활성화 규제혁신 행사’에 참석해 “4차 산업혁명시대, 미래 사업의 원유가 바로 데이터”라고 칭하며 “데이터를 잘 가공·활용하면 생산성이 높아지고 새로운 서비스와 일자리가 생겨난다”고 선언하고 데이터 규제 혁신이 혁신성장과 직결된다고 강조한 바 있습니다. 그러나 문대통령은 데이터규제혁신만을 강조한 것이 아니었습니다. “개인정보 보호의 중요성 등을 감안해 개인과 관련한 정보를 개인정보, 가명정보, 익명정보로 구분해 개인정보는 철저히 보호하고, 가명정보는 확실한 안전장치 담보 후 활용하며, 익명정보는 규제 대상에서 제외해 자유롭게 활용하게 하자”고도 제안하였습니다. 문대통령의 개인과 관련한 정보를 개인정보, 가명정보, 익명정보로 구분한 제안은 2018년 4월 5일자 4차 산업혁명위원회 제3차 규제·제도 혁신

1) 과방위는 법사위에서 법정합성을 맞추어달라는 취지로 부대의견을 의결하기도 하였다.

해커톤의 토론결과²⁾에 기반한 것이기도 했습니다. 이에 따라, 2018년 11월 15일 같은 날 인재근의원의 발의하여 「개인정보 보호법 일부개정법률안」 이, 김병욱 의원이 발의하여 「신용정보법 개정법률안」 이 발의되었습니다. 정부·여당은 위와 같이 법안을 발의한 직후인 2018년 11월 21일 「개인정보보호 관련 법안 개정 당정청 회의」 를 열고 “데이터완화와 관련한 정보주체(개인)의 권리에 대한 입법은 내년으로 미루면서 개인정보보호위원회권한 강화와 가명정보 활용허용을 연내 추진하겠다”라는 결론에 이르렀다. 그러나 2020년 1월 9일 본회의에서 법이 통과되기까지 개인정보주체의 권리보장은 전혀 추가 논의되지 못하였습니다.

즉, 현 개인정보보호법에는 GDPR에서 활용규정만을 들여왔을 뿐, 그에 비례적인 정보주체의 권리보장규정은 전혀 도입되지 못하였습니다.

III. 정보주체의 권리 보장을 위한 논의와 입법례들

1. UN 인권이사회의 권고안(2017. 3. 22.)에서의 우려

UN 인권인사회는 2017. 3. 22. ① 개인을 프로파일링하기 위한 개인정보의 자동화된 처리가 차별을 낳거나 경제적, 사회적, 문화적 권리 등 인권의 향유에 달리 잠재적으로 영향을 미칠 수 있고, ② 디지털 시대 민감정보 등 개인정보의 수집, 처리, 공유가 상당히 증가하여 자신의 개인정보를 재사용, 판매, 다목적 재판매하는데 대해 자유롭고 명시적이며 충분한 설명을 들은 후 동의하고 있지 못하며, ③ 기술 발달의 급속한 속도가 정부 기업, 개인이 감시, 감청, 정보수집을 실시할 수 있는 역량을 강화하여 프라이버시권 등 인권을 침해하거나 유린할 수 있고, ④ 이는 결국 표현의 자유와 간섭 없이 의견을 가질 자유, 평화적인 집회결사의 권리 등 다른 인권을 간섭하여 특히 영토 밖에서 대량으로 이루어질 때 민주사회 원리와 충돌할 수 있다는 우려를 표명한 바 있습니다. 3)

2. UN 인권이사회의 권고안의 구체적 내용

2) 4차 산업혁명위원회, 2018. 4. 5. 「보도자료 “가명정보의 활용 범위와 목적 등에 대한 합의(이하 ”중략“), 4차 산업혁명위, 제3차 규제·제도 혁신 해커톤 개최」 참조

3) UN Human rights Council , 「The rights to privacy n the digital age」, 2017. 3. 22., <https://documents-dds-ny.un.org/doc/UNDOC/LTD/G17/073/06/PDF/G1707306.pdf?OpenElement>

국가들에 대한 권고

- (a) 디지털 통신의 맥락을 포함하여, 프라이버시권을 존중하고 보호할 것.
- (b) 관련 국가 입법이 국제인권법상 의무를 준수하는 등 프라이버시권 침해를 종결시키고 침해 방지 여건을 창출하는 조치를 취할 것.
- (c) 국제인권법상 의무를 완전하고 효과적으로 이행하여 프라이버시권을 옹호하기 위하여, 대량의 감시·감청·수집 등 통신 감시, 감청, 개인정보 수집에 관한 절차, 관행, 입법을 검토할 것.
- (d) 국가의 통신 감시, 감청, 개인정보 수집에 대해 투명성과 책임성을 적절하게 보장하기 위한, 독립적이고 효과적이며 적정하게 자원이 할당되고 불편부당한 사법적, 행정적, 혹은 의회의 국내 감독 체제를 수립하거나 유지할 것.
- (e) 불법적이거나 자의적인 감시에 의해 프라이버시권이 침해된 개인들에게 국제인권 의무에 상응하는 효과적인 구제대책을 제공할 것.
- (f) 효과적인 제재 및 구제대책을 포함하는 적정한 규제를 개발·유지·시행하여, 개인·정부·기업·민간단체들의 불법적이거나 자의적인 개인정보 수집·처리·보관·이용으로 인한 프라이버시권 침해와 유린으로부터 개인을 보호할 것.
- (g) 이러한 측면에서 모든 개인, 특히 여성은 물론, 아동, 취약 계층과 소수자들에 영향을 미칠 수 있는 디지털시대 프라이버시 침해와 유린에 대해, 예방 조치와 구제대책을 추가적으로 개발하고 유지할 것.
- (h) 자신의 프라이버시를 효과적으로 보호하는 데 필요한 디지털 리터러시와 기술적인 능력을 함양하기 위해 모든 이에게 양질의 교육 및 평생 교육 기회를 장려할 것.
- (i) 기업들에 대하여 프라이버시권을 자의적이고 불법적인 방식으로 간섭하는 조치를 취하도록 요구하는 것을 삼갈 것.
- (j) 국가 기관이 사적인 이용자 데이터나 정보에 대한 제공을 요청할 때 기업들이 적정하고 자발적인 투명성 조치를 도입할 수 있게끔 적절한 조치를 고려할 것.
- (k) 개인의 자유롭고, 명시적이고, 충분한 설명에 따른 동의 없이 개인정보가 판매되고, 다목적으로 재판매되며 타 기업에 공유되는 피해에 대응하는 규제, 예방 조치와 구제대책을 개발하고 유지할 것.

기업들에 대한 권고

(a) 디지털시대 프라이버시권을 비롯하여 유엔기업과 인권이행원칙(보호, 존중, 구제 프레임워크)에 상응하는 인권존중의 책임을 다할 것과 프라이버시에 영향을 미칠 수 있는 개인정보의 수집, 이용, 공유, 보관에 대한 정보를 이용자에게 제공할 것과 이용자에게 충분한 설명에 따른 동의를 적절히 허용하는 투명성과 정책 수립

(b) 자유롭고, 명시적이고, 충분한 설명에 따른 동의 없이 개인정보가 판매되고, 다목
적으로 재판매되며 타 기업에 공유되는 피해에 대응하는 규제, 예방 조치와 구제대책
을 개발하고 유지할 것.

(c) 암호화와 익명화 조치 등 디지털 시대에 디지털 통신의 기밀성을 안전하게 지키고 보호하는 기술적 해법을 가능케 하기 위해 노력할 것을 독려하며 국가는 그 사용을 간섭하지 않을 것을 요청

3. 유럽 「일반개인정보보호법(GDPR)」 과 미국 각 주법들을 통한 개인정보 보호법의 입법화

유럽에서도 프로파일링을 포함한 신기술 및 거대 글로벌 기업들에 의한 개인정보보호 분야에서 발생한 새로운 이슈들을 해결하기 위한 새로운 법률 도입의 필요성이 강조되어⁴⁾, 「일반개인정보보호법(GDPR)」이 2012년 1월 25일 처음으로 제안되었고⁵⁾, 이후 수년간의 논의 끝에 2016년 4월 14일 유럽의회에서 의결되어 2018년 5월 25일 시행되었습니다.

「일반개인정보보호법(GDPR)」은 프로파일링 시대에 개인정보처리 원칙과 개인정보주체의 권리, 보호조치 등을 과거 지침(directive)에서보다 구체화하고, 이를 위반할 경우 직전 회계연도의 연간 전 세계 총 매출액을 기반으로 과징금을 정하여 그 금액도 상향 조정하였습니다.⁶⁾

4) 유럽 일반개인정보보호법 전문 (6)

5) https://edps.europa.eu/data-protection/data-protection/legislation/history-general-data-protection-regulation_en

6) 유럽 개인정보 보호법 제83조 제5항

실제 최근 「일반개인정보보호법(GDPR)」에 따라 이루어진 대략적인 과징금 부과 현황(정확한 통계가 제시되지 않아 관련 정보를 제공하고 있는 법률사무소의 통계를 인용하였으므로 정확하지 아니할 수 있습니다)을 보면, 2019. 1.경 구글을 상대로 프랑스에서 부과한 5천만 유로의 과징금을 포함하여 상당히 적극적인 조치들이 이루어지고 있음을 확인할 수 있습니다.

「일반개인정보보호법(GDPR)」에 의한 2018. 5. 25. - 2021. 3. 1.까지 과징금 부과 현황 ⁷⁾			
순 번	위반유형	위반건 수	과징금
1	데이터 처리를 위한 법적 근거 부족	202건	평균 820,000유로
2	정보보안을 위한 기술적, 관리적 조치의 부족	114건	평균 560,000유로
3	일반 데이터처리 원칙 미준수	86건	평균 220,000유로
4	정보주체 권리의 보장 미비	50건	평균 150,000유로

미국에서도 시민들의 정보주체의 개인정보에 대한 권리강화에 대한 요구에 따라, 캘리포니아주에서 「소비자 개인정보 보호법(California Consumer Privacy Act)」이 2020. 1. 1. 부터 시행되었고, 이외에도 여러 주에서도 개인정보 보호법 개정안들이 발의되어 해당 주의회에서 논의되고 있습니다.⁸⁾

미국의 캘리포니아주 개인정보 보호법은 유럽연합의 개인정보 보호법에 비교될 만큼 엄격한 규정들을 규정하고 있는바, 소비자에게 알 권리(Notice/Transparency Requirement), 삭제권(Right of Deletion), 접근권(Right of Access), 거부권(Right of Opt-Out), 차별금지권(Prohibition on Discrimination) 등을 부여하고, 사업자에게 관련

7) CMS, 「GDPR Enforcement Tracker Report, 2nd Edition 2021, <https://cms.law/en/deu/publication/gdpr-enforcement-tracker-report>

8) http://leginfo.legislature.ca.gov/faces/codes_displayText.xhtml?lawCode=CIV&division=3.&title=1.81.5.&part=4.&chapter=&article=

<https://www.technologylawdispatch.com/2020/02/privacy-data-protection/wisconsin-representative-proposes-groundbreaking-data-privacy-law-modeled-after-gdpr-including-statutory-penalties-up-to-20-million-or-4-percent-of-total-annual-revenue/?fbclid=IwAR2au33-A3Vlg0xbgAUzEsXSUnaXXRD0e76oLk4WFNTwM-cE0s9HPWP1e28>

규정 위반의 경우 의도적 위반에 대하여는 민사벌의 처벌을 규정하고, 소비자에게는 법정손해배상액 또는 실손해액의 배상을 해야 할 책임 등을 규정하고 있습니다.

유럽 「일반개인정보보호법(GDPR)」이나 캘리포니아 「소비자 개인정보 보호법(California Consumer Privacy Act)」 등 개인정보주체의 권리를 강화하며 권리 내용과 그 절차를 구체화하고 있는 흐름 역시, 우리나라의 프라이버시 체계에서 함께 고려하여야 할 점이라 평가되어야 하겠습니다.

IV. 현 「개인정보보호법」 통과시 과방위에서 의결된 부대의견

개인정보보호법」이 통과되면서, 「정보통신망법」상 개인정보 보호조항들이 모두 삭제되어 「개인정보보호법」으로 이관되었는데, 이 과정에서 법 체계정합성 및 과방위의 우려사항이 부대의견으로 의결된 바 있었습니다. 실제로 현 「개인정보보호법」은 「정보통신망법」 조항을 조화롭게 흡수하기보다는 해당 조항들을 특례로 정하는 비정상적인 체계를 채택하여 통과되었습니다. 국회 과방위는 2019년 12월 4일 다음과 같은 부대의견을 의결하고 이를 법사위에 「정보통신망법」 개정안과 함께 제시하고 이를 포함하여 법정합성과 체계를 맞추어 「개인정보보호법」을 의결해 달라고 요구한 바 있으나 이러한 의결은 전혀 반영되지 않았습니다.

2020. 12. 23. 과방위 임시회 회의에서 박선숙 의원은 “부대의견 여섯 가지에 관해 방송통신위원회가 여섯 가지 항목 전체에 불수용 의견을 표명하고 있다”라고 지적하면서 방송통신위원회가 「개인정보보호법」의 개정과정에서 법사위에서의 심도 깊은 논의에 협조하지 않고 있음을 지적하였습니다.

이후 2020년 1월 9일 국회 법사위 회의에서, 채이배 의원도 “법사위가 과방위 부대의견까지 무시하면서 정말 터무니없는 짓을 지금 하고 있다. 정보통신망법에서 누락된 내용들을 다시 답아야 한다”고 법사위에서 위 부대의견이 전혀 논의되지 않고 있음을 지적한바 있습니다. 하지만 방송통신위원회 한상혁 위원장은 “(과방위에서 부대의견으로 올라왔으나 개인정보보호법에서) 누락된 내용이 지금 법사위에서 수정이 안 되어 있지요”라는 채이배 의원의 질의에, “법사위에서 논의하시는 결과에 따라서 저희들은 수용하겠다는 말씀을 드리겠다”고 답변을 회피하였습니다.

과방위에서 의결된 부대의견에서도, 현 「개인정보보호법」이 정보주체에 대한 보호조치가 미흡하므로 이를 추가하여야 한다는 점이 언급되어 있습니다.

이렇듯 무시된 과방위의 부대의견은, 향후 보호조치의 검토에 있어서 고려되어야 할 필요가 있습니다.

<과방위에서 의결된 부대의견 - 「개인정보 보호법 일부개정법률안(대안)」에 대한 의견>
1. 법 적용대상자인 개인정보처리자와 정보통신서비스 제공자의 용어 개념에 대한 혼선이 야기될 가능성이 있으므로 향후 정합성 제고 차원에서 재검토 및 이에 대한 개선이 필요함
2. 개정안 제28조의2 제1항에 “정보주체 또는 제3자의 이익을 부당하게 침해할 우려가 없는 경우에 한하여”라는 조건을 추가하여 가명정보 처리 시에 정보주체의 권리가 보호될 수 있도록 하는 것이 바람직함
3. 가명정보의 목적 외 이용 또는 제3자의 제공 처리 시에 이를 공표하도록 하는 조항, 개인정보 프로파일링(profiling)의 정의 신설 및 개인정보 프로파일링으로 인한 정보주체 권리 침해 방지에 대한 조항을 추가로 반영하는 것이 바람직함
4. 제28조의4 제1항 위반의 경우, 동일한 위반 행위에 대하여 형사처벌(징역형·벌금)과 행정처분(과태료)을 동시에 부과하고 있으므로 법리적 차원에서 개선이 필요함
5. 제28조의4 제2항을 위반할 경우 형사처벌 대신 과태료 부과만 가능하게 되는데 기록을 작성·보관하지 않은 가명정보처리자에게 과태료를 부과하는 것은 ‘정보제공자 본인의 동의 없이’ 처리할 수 있는 가명처리의 특성상 매우 낮은 수준의 처분이므로 이에 대한 개선이 필요함

6. 제28조의5 제1항의 경우 “누구든지 특정 개인을 알아보기 위한 목적으로 가명정보를 처리하여서는 아니된다”고 규정하여 특정 개인을 알아보기 위한 목적만 없다면 특정 개인을 알아볼 수 있는 정보를 생성해도 과태료 부과에 그치므로 이에 대한 개선이 필요함

V. 「개인정보 보호법」 상 정보주체들을 위한 조건들

현 「개인정보보호법」은 안전조치없이 활용과 관련된 조항들만 입법화된 상황입니다. 즉, 가명정보 및 양립가능성 제도를 도입하여 정보주체의 통제권이 약화되어 있는 반면, 생체인식정보 등 민감정보 수집의 증가, 데이터의 대규모화, 개인정보 처리의 복잡화 등 신기술 발전에 따라 개인정보 침해 위험이 증가하는 점에 대한 보호조치가 전혀 고려되어 있지 않습니다. 새로운 기술 환경에서의 정보주체의 권리 보호를 위한 규정은 미흡한 실정인바, 이에 정보주체의 고지받을 권리, 정보주체에게 중대한 영향을 미치는 자동화된 의사결정에 대한 배제등의 권리 등 권리를 신설하여 빅데이터, 인공지능 환경에서 정보주체의 개인정보에 대한 통제권을 강화되어야 할 필요가 있습니다.

1. 개인정보의 적법한 처리 근거의 정비(안 제15조 제1항 제7호 및 안 제17조 제1항 제2호)

종전에는 공중위생 등 공공의 안전과 안녕을 위하여 긴급히 필요한 경우로서 일시적으로 처리되는 경우 개인정보보호법의 적용이 일부 배제되었던 것을, 개인정보의 적법한 처리 근거로 추가하여 개인정보 보호조치 등을 준수하도록 정비할 필요가 있습니다.

개인정보의 적법한 처리 근거의 정비 (안 제15조 제1항 제7호 및 안 제17조 제1항 제2호)	
제15조(개인정보의 수집·이용) ① 개인정보처리자는 다음 각 호의 어느 하나에 해당하는 경우에는 개인정보를 수집할 수 있으며 그 수집 목적	제15조(개인정보의 수집·이용) ① -- ----- ----- -----

의 범위에서 이용할 수 있다.

1. ~ 6. (생략)

<신설>

-----.

1 ~ 6. (현행과 같음)

7. 공중위생 등 공공의 안전과 안녕을 위하여 긴급히 필요한 경우로서 일시적으로 개인정보가 처리되는 경우

2. 정보주체의 고지받을 권리 확대(안 제15조 제2항·제4항, 제17조 제2항·제5항, 제18조 제3항·제6항)

종전에는 동의를 받을 때에만 개인정보 처리와 관련한 정보를 고지하도록 하던 것을, 동의 외의 다른 근거에 따라 처리할 경우에도 개인정보 처리와 관련한 정보를 정보주체에게 고지하도록 하는 등 정보주체의 고지받을 권리를 확대하여 개선할 필요가 있습니다. 다만, 이 경우 정보주체에게 통지하는 것이 가능하지 아니하는 경우에는 그러하지 아니합니다.

정보주체의 고지받을 권리 확대안

(안 제15조 제2항·제4항, 제17조 제2항·제5항, 제18조 제3항·제6항)

제15조

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.

제15조

② ----- 제1항 제1호 내지 제4호 및 제6호에 따라 정보주체로부터 개인정보를 수집하는 경우 -----사항을 사전에 -----

-- 이를 알려야 한다.

<p>② 개인정보처리자는 제1항제1호에 따른 동의를 받을 때에는 다음 각 호의 사항을 정보주체에게 알려야 한다. 다음 각 호의 어느 하나의 사항을 변경하는 경우에도 이를 알리고 <u>동의를 받아야 한다.</u></p> <ol style="list-style-type: none"> 1. 개인정보를 제공받는 <u>자</u> 2. 개인정보를 제공받는 자의 개인정보 이용 <u>목적</u> 3. 4. (생략) 5. <u>동의를 거부할 권리가 있다는 사실</u> 및 동의 거부에 따른 불이익이 있는 경우에는 그 불이익의 내용 <p>③·④ (생략)</p> <p><신설></p>	<p>-----</p> <p>② ----- ----- 받은 경우, 제15조 제1항 제2호·3호에 따라 개인정보를 수집한 목적 범위에서 개인정보를 제3자에게 제공하는 경우, ----- ----- <u>사항을 사전에</u> ----- ----- ----- <u>제공해</u> <u>야 한다.</u></p> <ol style="list-style-type: none"> 1. ----- <u>자 및 그</u> <u>의 상세 연락처</u> 2. ----- ----- <u>목적 및 법적</u> <u>근거</u> 3. 4. (현행과 같음) 5. <u>제1항 제1호에 따라 동의를 받아 개인정보를 제3자에게 제공하는 때에는, 동의를</u> ----- ----- ----- <p>③·④ (현행과 같음)</p> <p>⑤ <u>개인정보처리자가 연락처 등 정보주체에게 통지할 수 있는 개인정보를 수집하지 아니한 경우에는 제2항을 적용하지 아니한다</u></p>
-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------	---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------

다만, 위와 같이 제15조와 제17조의 수집·이용을 처리로 통합한다면, 위 규정은 다음과 같이 변경할 수 있겠습니다.

개인정보의 처리의 적법요건으로 통합할 경우, 통지의 예시

제00조(개인정보의 제공) ① 개인정보처리자는 다음 각 호의 어느 하나에 해당되는 경우에는 그 처리의 목적 범위내에서 정보주체의 개인정보를 처리할 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.
7. 공중위생 등 공공의 안전과 안녕을 위하여 긴급히 필요한 경우로서 일시적으로 개인정보가 처리되는 경우

② 개인정보처리자는 제1항 제1호 내지 제4호 및 제6호에 따라 개인정보를 처리하는 경우 다음 각 호의 사항을 사전에 정보주체에게 알려야 한다. 다음 각 호의 어느 하나의 사항을 변경하여 처리하는 경우에도 이를 알려야 한다.

1. 개인정보처리자 및 제공받는 자에 대한 상세 연락처
2. 개인정보처리의 목적 및 법적 근거
3. 개인정보의 보유 및 이용기간
4. 처리하려는 개인정보의 항목
5. 제1항 제1호에 따라 동의를 받아 개인정보를 처리할 때에는, 동의를 거부할 권리가 있다는 사실 및 동의 거부에 따른 불이익이 있는 경우에는 그 불이익의

내용

③ 개인정보처리자가 연락처 등 정보주체에게 통지할 수 있는 개인정보를 수집하지 아니한 경우에는 제2항을 적용하지 아니한다

3. 범죄수사목적의 제3자 제공의 예외조항 정비 (안 제18조 제2항 제7호)

종전에는 범죄의 수사목적에 대하여 제3자 제공이 가능하였던 것을, 제3자 제공의 예외조항에서 삭제하여 수사절차에서도 형사소송법 등이 정한 적법절차 원칙을 지키고 개인정보보호원칙을 강화할 필요가 있습니다.

범죄수사 목적의 제3자 제공의 예외조항정비

7. <u>범죄의 수사</u> 와 공소의 제기 및 유지를 위하여 필요한 경우	7. <u>공소의 제기</u> 및 유지를 위하여 필요한 경우
--------------------------------------------	-----------------------------------

4. 정보주체 이외로부터 수집한 경우 고지받을 권리 확대(안 제20조)

종전에는 정보주체 이외로부터 개인정보를 수집한 개인정보를 처리하는 때에 정보주체의 요구가 있는 경우에만 개인정보 처리와 관련한 정보를 고지하던 것을, 정보주체의 요구가 없는 경우에도 고지받을 권리를 확대할 필요가 있습니다.

정보주체 이외로부터 수집한 경우 고지받을 권리 확대

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

<p>경우에 한한다.</p> <p><신설></p> <p><신설></p> <p>1. 2. (생략)</p>	<p>-----</p> <p>-----.</p> <p>1. 정보주체가 제1항 각 호 정보를 알고 있는 경우. 이때 정보주체가 각 호의 정보를 알고 있다는 점은 개인정보처리자가 입증하여야 한다.</p> <p>2. 개인정보처리자가 수집한 정보에 연락처 등 정보주체에게 알릴 수 있는 개인정보가 없는 경우</p> <p>3. 4. (현행 제1호 및 제2호와 같음)</p>
--------------------------------------------------------------------------	-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------

5. 개인정보의 전송 요구의 신설(안 제35조의2)과 감독규정(안 35조의3)

개인정보의 전송요구권이 현실에서 정보주체의 통제권 보장보다는, 산업적 활용촉진만 강조되고 있어 「개인정보보호법」에 신설되는 것에 대하여는 찬성하기 어려운 부분이 큼니다. 다만, 정부안에 대하여 부득이 다음과 같은 정보주체의 보호조치조건을 검토하였습니다.

정부안과 관련하여서는, 정보주체가 개인정보처리자에게 그가 처리하는 자신의 개인정보를 정보주체 본인, 다른 개인정보처리자에게 전송할 것을 요구할 수 있도록 하고, 개인정보 전송요구의 요건 및 금지행위를 정하고, 개인정보의 전송요구와 관련된 개인정보관리전문기관에 대한 개인정보영향평가의 의무화 및 보호위원회의 감독근거규정 신설하는 것이 필요합니다.

제35조의2 (개인정보의 전송요구) ① 정보주체는 매출액, 개인정보의 규모 등을 고려하여 대통령령으로 정하는 개인정보처리자에 대하여 다음 각 호의 요건을 모두 충족하는 경우에 개인정보처리자가 처리하는 자신의 개인정보를 자신, 다른 개인정보처리자에게 전송할 것을 요구할 수 있다.

1. 개인정보가 제15조제1항제1호에 따른 동의나 제15조제1항제4호에 따른 계약에 따라 처리되는 경우
2. 개인정보가 컴퓨터 등 정보처리장치에 의하여 자동화된 방법으로 처리되는 경우

② 제1항에 따라 정보주체가 전송을 요구하는 경우에 개인정보보호위원회가 고시하는 컴퓨터 등 정보처리장치로 처리가능하고 통상적으로 이용되는 구조화된 형식으로 전송하여야 한다. 다만, 개인정보처리자는 시간, 비용, 기술 등의 사정 등을 고려하여 합리적인 범위내에서 정보전송요구를 거절할 수 있다.

③ 제1항에 따른 전송 요구는 다음 각 호에는 적용하지 아니한다.

1. 개인정보처리자가 개인정보를 기반으로 생성한 정보
2. 제3자의 개인정보나, 영업비밀 등을 포함한 정당한 권리나 이익과 관련되는 정보

④ 정보주체에게 기만적이거나, 위계나 위력 등의 부당한 방법으로 전송요구권 행사를 유인하여서는 아니된다.

⑤ 보호위원회는 제1항 내지 제5항에 따른 전송 요구와 전송의 방법 및 절차, 거절사유, 금지행위 등에 관하여 필요한 사항을 고시로 정하여야 한다.

제35조의3 (개인정보관리 전문기관) ① 다른 법령에서 개인정보의 전송요구권 행사와 관련되어 인가, 허가, 지정받은 개인정보처리자(이하 “개인정보관리 전문기관”)는 제33조에서 정한 개인정보영향평가를 받아야 한다.

② 보호위원회는 개인정보관리 전문기관에 대하여 이 법 또는 이 법에 따른 명령의 준수 여부를 감독한다.

③ 보호위원회는 제2항의 감독을 위하여 그 소속 직원으로 하여금 업무에 대하여 검사하도록 할 수 있으며, 필요한 경우 자료의 제출, 관계자의 출석 및 의견의 진술을 요구할 수 있다.

④ 보호위원회는 이 법에 따른 명령을 위반한 경우 개인정보관리 전문기관에 대하여 다음 각호의 조치를 할 수 있으며, 그 위반정도가 큰 경우 인가, 허가, 지정권자에게 해당 인가, 허가, 지정의 취소를 요구하여야 한다.

1. 주의 또는 경고
2. 임직원에게 대한 해임권고, 직무정지 또는 면직요구
3. 위반행위에 대한 법 제64조에 따른 시정명령

⑤ 보호위원회는 개인정보관리 전문기관의 행위 중 정보주체의 권리침해의 우려가 있는 경우에는 고시로 금지사항을 정할 수 있다.

⑥ 보호위원회는 제2항 내지 제4항에 따른 감독절차에 대하여는 고시로 정하여야 한다.

6. 자동화된 의사결정에 대한 배제 등의 권리 규정 신설(안 제37조의2)

정보주체는 인공지능을 포함한 신기술의 적용에 따라 생명·신체·재산 등에 중대한 영향을 미치는 자동화 의사결정 등에 대하여 일정한 경우를 제외하고는 그 대상이 되지 않아야 하며, 그 대상이 될 경우라도 이의제기 및 설명을 요구할 수 있도록 할 필요가 있습니다.

제37조의2(자동화된 의사결정에 대한 배제등의 권리) ① 정보주체는 자동화된 개인정보처리에만 의존하여 정보주체에게 개별적으로 법적 효력 또는 생명·신체·재산에 중대한 영향을 미치는 결정의 적용은 금지된다. 다만 다음 각 호의 경우에는 그러하지 아니하다.

1. 정보주체가 자동화 의사결정에 대하여 설명을 듣고 명백하게 동의의 의사표시를 한 경우
2. 법률에 특별한 규정이 있거나 법령상 의무를 준수하기 위하여 불가피한 경우
3. 계약의 체결 및 이행을 위하여 불가피하게 필요한 경우

② 정보주체는 제1항 제1호 또는 제3호의 경우에는 그 결정에 대하여 이의제기 또는 설명 등을 요구할 수 있다.

③ 제2항에 따른 요구를 받은 개인정보처리자는 특별한 사정이 없는 한 그 요구에 따라 위 결정의 적용배제, 재처리, 설명 등 필요한 조치를 하여야 한다.

④ 개인정보처리자는 아동에 대하여 마케팅 목적으로 자동화된 개인정보처리에만 의존한 의사결정을 하여서는 아니된다.

⑤ 개인정보처리자는 제1항에서 정한 자동화된 의사결정에 대하여 대통령령이 정하는 바에 따라 정보주체가 사전에 쉽게 인식할 수 있도록 알려야 한다.

1. 자동화된 의사결정의 유무
2. 자동화된 의사결정에 활용된 개인정보
3. 자동화된 의사결정의 알고리즘 혹은 결정에 영향을 미치는 주요 요소
4. 자동화된 의사결정이 정보주체에게 미치는 위험성 및 예상되는 결과

⑥ 보호위원회는 제1항에서 정한 자동화된 의사결정에 대한 기준에 대하여 필요한 사항을 고시로 정할 수 있다.

...

토론

권건보 (아주대 법학전문대학원 교수)



“정보주체의 권리 강화를 위한 개선방안”에 대한 토론문

김보라미 변호사님의 발제문을 통해 소위 데이터3법 처리 당시 졸속적인 입법 과정, 정보통신망법과 개인정보보호법 사이의 체계적 정합성의 문제, 국제사회와 국내에서의 입법동향 등에 대해 자세히 알 수 있었습니다.

특히 당시 정보주체의 권리 보장 강화 필요성이 제기되었고 그에 대한 후속적 입법을 과제로 남겨두었다는 점을 상기해준 것은 현 시점에서 매우 중요한 의미가 있다고 생각합니다.

발제자의 여러 지적과 문제의식에 대해 깊이 공감하며, 법률 개정의 방향에 대해서도 대체로 동의합니다.

다만 지정토론자로서 구체적인 개정사항에 대해 궁금한 점이 몇 가지 있어서 질문을 드리고자 합니다.

가. 정보주체의 고지받을 권리 확대와 관련하여 (안 제15조 및 안 제17조 관련)

- 개정안 제15조 제2항 제2문에 의하면 변경 사항이 있을 때는 알리기만 하면 되고, 그에 대한 별도의 동의는 없어도 되는 것처럼 읽힐 수 있음

- 만약 취지가 그런 것이 아니라면, 제2문에서도 동의(제1항 제1호에 따른 경우)를 요구할 필요가 있는 것은 아닌지?

- 동조 제2항 제2호에서 “개인정보의 수집·이용에 대한 법적 근거”를 알리도록 하고 있는데, 이는 제1항 제1호 내지 제4호 및 제6호에 따른 수집의 모든 경우에 적용되는 것인지? 아니면 제2호 내지 제3호에 국한되는 것인지?

- 개정안 제17조 제1항 제2호의 “제6호·제7호”는 제15조 제1항의 제6호 및 제7호를 가리키는 것으로 보임

- 밑줄 친 것만 주목해서 보면 마치 “제39조의3 제2항의 제2호·제3호”를 대체하는 내용으로 읽힐 수 있는데, 그러한 오해의 여지는 없겠는지?

- 개정안 제17조 제2항에서 “받을 때에는”를 “받은 경우”로 수정할 것을 제안하고

있는데, 이는 뒤에 나오는 “사전에”라는 문구와 어울리기 어려운 것은 아닌지?

- 굳이 동조 제1항 제1호의 문구와 통일하기 위해 “받은 때에는”이라는 문구를 포기해야 할 이유가 있는지?

- 개정안 제17조 제2항 제2문에서도 마찬가지로 변경사항에 대한 별도의 동의(제1항 제1호에 따른 경우)가 필요한 것이 아닌지?

다. 정보주체 이외로부터 수집한 경우 고지받을 권리 확대(안 제20조) 관련

- 개정안 제20조 제1항에서 “정보주체의 요구가 있으면”이라는 문구를 삭제한 것은 정보주체의 권리를 실질적으로 보장한다는 측면에서 바람직한 방향이라고 생각함

- 다만 개인정보를 처리하는 즉시 고지의무를 부과하는 것에 대해 개인정보처리자의 부담 증가를 이유로 관련 업계에서 강력히 반발할 가능성이 있어 보임

- 개정안의 고지사항은 EU의 GDPR을 참고한 것으로 보이는데, GDPR 제14조 제3항에서는 개인정보 입수 후 합리적 범위 내에서 1개월 이내 등의 말미를 주고 있음

- 개정안에서 개인정보를 처리하는 때에는 즉시 정보주체에게 알리도록 하고 있는데, 여기서 처리 즉시 고지의무는 합리적 기대가능성을 전제하는 개념인지?

- 개정안 동조 제4항에 따른 적용 배제 사유로 제1호 및 제2호를 추가한 것으로 그러한 경직성의 문제를 충분히 대처할 수 있다고 보는지?

- 개정안 제1항 제6호에서 “~동의 철회를 요구할 권리”라는 문구는 어색해 보이는데, “~처리 정지를 요구할 권리 및 ~동의를 철회할 권리가 있다는 사실”로 수정함이 어떨지?

마. 자동화된 의사결정에 대한 배제 등의 권리 규정 신설 (안 제37조의2) 관련

- 개정안 제37조의2 제1항은 정보주체가 자동화된 의사결정의 대상이 되지 않을 권리를 규정하고자 한 것으로 보임

- 그런데 “정보주체는” 부분과 “결정의 적용은 금지된다.”라는 부분의 조응이 자연스럽게 보이지 않음

- 이것이 정보주체의 동의가 없는 자동화된 의사결정의 원칙적 금지를 규정하고자 하는 것인지? (사전통제권?)

- 아니면 개인정보보호위원회 법안처침 자동화된 의사결정이 있는 경우 그 결정의 적용을 거부할 권리를 부여하는 것인지? (사후저지권?)

- 동조 제5항에서 “다음 각 호의 사항을”이라는 문구가 들어가야 할 것으로 보임

정보주체의 권리 강화를 위한 법률개정의 방향을 구체적으로 제시해주신 김보라미 변호사님의 심도 있는 발제에 감사드리며, 이것으로 지정토론에 갈음하고자 합니다.

...

발제

‘개인정보처리자의 책임성 강화’를 위한 개인정보 보호법 개정과제

서채완 (변호사, 민주사회를 위한 변호사모임 디지털정보위원회 간사)



1. 입법과제로서 개인정보처리자의 책임성 강화

□ 개인정보 보호법은 그 제정 취지가¹⁾ 데이터 활용의 활성화 등을 목적으로 하는 것이 아니라 개인의 자유와 권리를 보호하고, 나아가 개인의 존엄과 가치를 구현함을 목적으로 하는 법률임(개인정보 보호법 제1조)

○ 구체적으로는 정보주체가 가지는 사생활의 비밀과 자유²⁾ 및 개인정보자기결정권³⁾ 등의 헌법상 기본권과,

○ 헌법 제6조 제1항⁴⁾ 제10조⁵⁾ 및 제37조 제1항⁶⁾ 에 따라 국내적 효력을 가지는 국제인권법상 프라이버시권⁷⁾을 구체적으로 보장하는 법률에 해당함

□ 그럼에도 불구하고 2020. 8. 5. 시행된 현행 개인정보 보호법은 빅데이터 등 신기술 및 신사업 활성화에 치중하여,⁸⁾ 정보 주체의 동의 없는 개인정보(가명정보를 포함)의 처리를 폭넓게 허용하고 있는 상황임

-
- 1) 개인정보 보호법의 제정 취지는 다음과 같음: “정보사회의 고도화와 개인정보의 경제적 가치 증대로 사회 모든 영역에 걸쳐 개인정보의 수집과 이용이 보편화되고 있으나, 국가사회 전반을 규율하는 개인정보 보호원칙과 개인정보 처리기준이 마련되지 못해 개인정보 보호의 사각지대가 발생할 뿐만 아니라, 최근 개인정보의 유출·오용·남용 등 개인정보 침해 사례가 지속적으로 발생함에 따라 국민의 프라이버시 침해는 물론 명의도용, 전화사기 등 정신적·금전적 피해를 초래하고 있는 바, 공공부문과 민간부문을 망라하여 국제 수준에 부합하는 개인정보 처리원칙 등을 규정하고, 개인정보 침해로 인한 국민의 피해 구제를 강화하여 국민의 사생활의 비밀을 보호하며, 개인정보에 대한 권리와 이익을 보장하려는 것임.”
 - 2) 「대한민국 헌법」 제17조 모든 국민은 사생활의 비밀과 자유를 침해받지 아니한다.
 - 3) 헌법재판소 2005. 7. 21. 선고 2003헌마282 결정
 - 4) 「대한민국 헌법」 제6조 ① 헌법에 의하여 체결·공포된 조약과 일반적으로 승인된 국제법규는 국내법과 같은 효력을 가진다.
②외국인은 국제법과 조약이 정하는 바에 의하여 그 지위가 보장된다.
 - 5) 「대한민국 헌법」 제10조 모든 국민은 인간으로서의 존엄과 가치를 가지며, 행복을 추구할 권리를 가진다. 국가는 개인이 가지는 불가침의 기본적 인권을 확인하고 이를 보장할 의무를 진다.
 - 6) 「대한민국 헌법」 제37조 ①국민의 자유와 권리는 헌법에 열거되지 아니한 이유로 경시되지 아니한다.
 - 7) 「시민적 및 정치적 권리에 관한 국제규약 (B규약)」 제17조 1. 어느 누구도 그의 사생활, 가정, 주거 또는 통신에 대하여 자의적이거나 불법적인 간섭을 받거나 또는 그의 명예와 신용에 대한 불법적인 비난을 받지 아니한다.
2. 모든 사람은 그러한 간섭 또는 비난에 대하여 법의 보호를 받을 권리를 가진다.
 - 8) 현행 개인정보 보호법(2020. 2. 4. 법률 제16930호로 개정된 것)의 개정취지는 다음과 같음: “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 상황임. 그러나, 현행법상 개인정보 보호 감독기능은 행정안전부·방송통신위원회·개인정보보호위원회 등으로, 개인정보 보호 관련 법령은 이 법과 「정보통신망 이용촉진 및 정보보호 등에 관한 법률」 등으로 각각 분산되어 있어 신산업 육성을 위한 데이터 이용 활성화를 지원하는 데 한계가 있어 왔음.이에 따라, 정보주체의 동의 없이 과학적 연구, 통계작성, 공익적 기록보존 등의 목적으로 가명정보를 이용할 수 있는 근거를 마련하되, 개인정보처리자의 책임성 강화 등 개인정보를 안전하게 보호하기 위한 제도적 장치를 마련하는 한편, 개인정보의 오용·남용 및 유출 등을 감독할 감독기구는 개인정보 보호위원회로, 관련 법률의 유사·중복 규정은 이 법으로 일원화함으로써 개인정보의 보호와 관련 산업의 발전이 조화될 수 있도록 개인정보 보호 관련 법령을 체계적으로 정비하려는 것임.”

○ 개인정보 보호법의 개정은 애초에 해당 법률이 제정된 취지에 부합하도록 ‘신사업의 육성과 데이터의 이용 활성화’가 아닌 4차 산업혁명 내지 디지털 시대에 필요한 ‘프라이버시권 등 정보주체의 권리의 적극적인 보호’가 그 목적이 되는 것이 타당함

○ 현재 개인정보 보호법 개정에는 있어 국제적인 기준으로서 참고되는 유럽연합 일반개인정보보호법(General Data Protection Regulation, “GDPR”) 또한, 그 제정 취지가 정보주체의 권리를 확대하고, 공적인 개인정보의 보호를 강화하며, 기업의 책임성 강화 등을 목적으로 제정되었음⁹⁾

□ 한편 국제인권법을 관장하는 유엔인권최고대표사무소(Office of High Commissioner for Human Rights, “OHCHR”)와 유엔 인권이사회(United Nations Human Rights Council) 및 산하 프라이버시 특별보고관(Special Rapporteur on the right to privacy)은,

○ 디지털시대에서 광범위하게 제약될 수 있는 정보주체의 권리를 적극적으로 보장할 것과 동시에 기업 등의 책임성을 강화하라는 취지의 기준을 권고하고 있음

○ 유엔인권이사회 등은 디지털시대의 프라이버시권 보고서를 통해 국가에게 프라이버시권을 간섭하지 않을 의무뿐만 아니라, 프라이버시권을 적극 보장·보호할 의무가 있음을 확인하며,¹⁰⁾

○ 인권을 존중해야 할 사적 주체(Private actor)의 책임성을 명확히 하는 것을 목적으로 하고 있으며, 프라이버시권의 침해에 대한 실효성 있는 구제의 권리를 실질적으로 보장할 것을 강조하고 있음¹¹⁾

9) 유럽연합 일반개인정보보호법 전문 (6) “격한 기술발전과 세계화에 따라 개인정보보호 분야에 새로운 도전이 제기되었다. 개인정보의 수집 및 공유 규모가 상당한 수준으로 확대되었다. 기술을 통해 민간기업과 공공기관이 업무수행을 위해 전례 없는 규모로 개인정보를 활용하게 되었다. 개인은 개인정보를 공적으로 세계적으로 활용할 수 있다. 기술은 경제와 사회생활을 변화시켜왔다. 앞으로는 기술을 통해 유럽 역내의 자유로운 정보 이동과 제 3국 및 국제기구로의 개인정보 이전을 용이하게 하고, 개인정보를 높은 수준으로 보호해야 한다”

10) UN Human Rights Committee (HRC), “CCPR General Comment No. 16: Article 17 (Right to Privacy), The Right to Respect of Privacy, Family, Home and Correspondence, and Protection of Honour and Reputation”, 8 April 1988, para. 9; United Nations High Commissioner for Human Rights, “The right to privacy in the digital age”, A/HRC/39/29, 3 August 2018, para. 23-25 등 참조

11) United Nations High Commissioner for Human Rights, 위의 글, para. 42.-49., para. 50.- 57.; Special Rapporteur on the right to privacy, “Purpose of the mandate”, <https://www.ohchr.org/en/issues/privacy/sr/pages/srprivacyindex.aspx> 등 참조

<p>용촉진 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.</p> <p>1. ~ 6. (생략)</p> <p>7. 범죄의 수사와 공소의 제기 및 유지를 위하여 필요한 경우</p>	<p>우는 공공기관의 경우로 한정한다.</p> <p>1. ~ 6. (현행과 같음)</p> <p>7. 공소의 제기 및 유지를 위하여 필요한 경우</p>
----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------	-------------------------------------------------------------------------------------

□ 현행 개인정보 보호법은 범죄 수사에 필요한 경우 공공기관이 보유한 개인정보를 목적 외로 이용·제공하는 것을 폭넓게 허용하고 있고(제18조 제1항 제7호), 이에 따라 영장 없이 개인정보가 수사기관에 빈번하게 제공되었음

□ 정보주체의 입장에서는 공공기관이 보유하는 개인정보는 법률이 규정하는 구체적인 목적 범위 내에서만 활용되는 것을 전제로 개인정보를 제공하고, 민간 영역보다 강화된 보호를 기대할 수밖에 없음

○ 따라서 수사기관에게 공공기관이 보유한 개인정보의 목적 외 이용을 전면적으로 허용하는 것은 정보주체에 대한 보호수준을 약화시키는 것이고,

○ 수사기관은 필요한 경우 영장 및 허가를 통해 개인정보에 접근할 수 있다는 점에서, 영장 및 허가 없는 개인정보의 이용을 허용하는 위 조항은 헌법 및 국제인권법이 요청하는 적법절차의 원칙¹⁴⁾ 및 좋은 행정의 권리 보장 원칙에 부합하지 않음

□ 이에 개인정보 보호법 제18조 제1항 제7호가 규정하는“범죄의 수사와 공소의 제기

14) 적법절차의 원칙은 공권력에 의한 국민의 생명·자유·재산의 침해는 반드시 합리적이고 정당한 법률에 의거해서 정당한 절차를 밟은 경우에만 유효하다는 원리로서

및 유지를 위하여 필요한 경우”에서 “범죄의 수사”를 삭제하는 개정안을 제안하고자 함

다. 민간정보의 법률에 따른 보호 및 범위 확대

□ 개정안

현 행	개 정 안
<p>제23조(민감정보의 처리 제한) ① 개인정보처리자는 <u>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.</u></p> <p>1. <u>정보주체에게 제15조제2항 각 호 또는 제17조제2항 각 호의 사항을 알리고 다른 개인정보의 처리에 대한 동의와 별도로 동의를 받은 경우</u></p> <p>2. <u>법령에서 민감정보의 처리를 요구하거나 허용하는 경우</u></p> <p><u><신 설></u></p>	<p>제23조(민감정보의 처리 제한) ① ----- -----<u>다음 각 호의 개인정보</u>----- ----- -----<u>. <단서 삭제></u>-----</p> <p>1. <u>사상·신념, 노동조합·정당의 가입·탈퇴, 정치적 견해에 대한 정보</u></p> <p>2. <u>건강, 성생활 등에 관한 정보</u></p> <p>3. <u>인종·민족 등에 관한 정보</u></p> <p>4. <u>생체인식정보(지문, 홍채, 음성, 필적 등 개인의 신체적·행동적 특성에 관한 정보로서 개인을 인증하거나 식별하기 위하여 기술적으로 처리되는 개인정보를 말한다)</u></p> <p>5. <u>유전자검사 등의 결과로 얻어진 유전 정보</u></p> <p>6. 「형의 실효 등에 관한 법률」 제2조 제5호에 따른 범죄경력자료에 해당하는 정보</p> <p>7. <u>그 밖에 정보주체의 사생활을 현저히 침해할 우려가 있는 개인정보로서 대통령령에서 규정하는 정보</u></p> <p>② 제1항에도 불구하고 개인정보처리자</p>

는 다음 각 호의 어느 하나에 해당하는 경우 민감정보를 처리할 수 있다. 다만, 제1항제6호에 따른 범죄경력자료에 대하여는 제3호와 제4호를 적용하지 아니한다.

1. 정보주체에게 제15조제2항 각 호 또는 제17조제2항 각 호의 사항을 알리고 다른 개인정보의 처리에 대한 동의와 별도로 제1항 각 호의 개인정보 처리에 대한 동의를 받은 경우
 2. 다른 법령에서 제1항 각 호의 개인정보의 처리를 요구하거나 허용하는 경우
 3. 정보주체 또는 그 법정대리인이 의사 표시를 할 수 없는 상태에 있거나 주소불명 등으로 사전 동의를 받을 수 없는 경우로서 정보주체 또는 제3자의 급박한 생명, 신체, 재산의 이익을 위하여 명백히 필요하다고 인정되는 경우
 4. 공중위생, 방역 등 공공의 안전과 안녕을 위하여 긴급히 일시적으로 처리되는 경우
- ③ 제1항 및 제2항의 규정은 제28조의2 제1항에 우선하여 적용한다.

<신 설>

□ 현행 개인정보 보호법은 민감정보를 ‘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’라고 정의하고, 동의 또는 법령상의 명시적인 근거를 민감정보 처리의 요건으로 규정하고 있음(제23조 제1항)

○ 그러나 같은 법 시행령 제18조는 민감정보를 유전정보, 범죄경력자료, 인종이나 민족에 관한 정보 등을 열거하면서, 정부가 시행령의 개정을 통해 민감정보의 보호범위

를 언제든지 약화시킬 수 있도록 하고 있으며,

○ 이와 더불어 공공기관이 민감정보를 처리하는 경우 처리되는 민감정보를 민감정보로서 보호하지 않도록 하고 있음¹⁵⁾

□ 민감정보의 보호는 정보주체의 인격과 존엄에 밀접한 관련성이 있는 개인정보를 보호하는 것으로서 헌법 및 국제인권법상 프라이버시권 보호의 핵심적인 내용에 해당함

○ 위와 같은 핵심적인 사항을 개인정보 보호법 시행령에 규정하는 것은 결국 행정기관에 입법권을 백지상태로 위임하는 것으로 헌법상 포괄위임금지원칙에 위배될 여지가 있음¹⁶⁾

○ 참고로 헌법재판소도 민감정보가 “개인의 인격 및 사생활의 핵심”에 해당한다며, 일반적인 개인정보보다 더 높은 수준의 보호가 필요하다고 실시하였는데,¹⁷⁾

○ 위 헌법재판소의 판시는 민감정보에 대한 세밀한 보호가 법률적으로 이루어져야 한다는 점을 시사함

○ 관련하여 GDPR 또한, 민감정보의 처리가 기본적으로 합법성을 획득하거나, 정보주체의 명백한 동의라는 기초 아래 이루어져야 한다는 점을 강조하고 있음¹⁸⁾

□ 이에 GDPR과 현행 개인정보보호법 시행령이 규정하는 민감정보를 법률에 명시하

15) 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.

1. 유전자검사 등의 결과로 얻어진 유전정보
2. 「형의 실효 등에 관한 법률」 제2조제5호에 따른 범죄경력자료에 해당하는 정보
3. 개인의 신체적, 생리적, 행동적 특징에 관한 정보로서 특정 개인을 알아볼 목적으로 일정한 기술적 수단을 통해 생성한 정보
4. 인종이나 민족에 관한 정보

16) “법률의 위임은 반드시 구체적이고 개별적으로 한정된 사항에 대하여 행해져야 한다. 그렇지 아니하고 일반적이고 포괄적인 위임을 한다면 이는 사실상 입법권을 백지위임하는 것이나 다름없어 의회입법의 원칙이나 법치주의를 부인하는 것이 되고 행정권의 부당한 자의와 기본권 행사에 대한 무제한적 침해를 초래할 위험이 있기 때문이다.”(헌법재판소 1991. 7. 8. 선고 91헌가4 결정 등 참조)

17) 헌법재판소 2018. 8. 30. 선고 2014헌마368 결정

18) GDPR 전문 51-53문단; 제9조(특정 범주의 개인정보의 처리) 참조

여 그 규범력과 정보주체의 권리에 대한 보호 수준을 강화하고, 개인정보처리자가 민감 정보를 예외적으로 처리할 수 있는 경우를 세부적으로 명시하고자 함

○ 이와 더불어, 현행 개인정보 보호법의 해석상 논란¹⁹⁾이 되고 있는 민감정보에 대한 가명정보의 처리 특례규정의 장 적용 가부에 관하여, 민감정보에 관한 규정이 우선 적용된다고 명시하여, 민감정보의 처리에 있어서는 가명처리 특례규정이 적용될 수 없다는 점을 명확히 하고자 함

라. 통계작성 등을 위한 동의 없는 개인정보 처리에 관한 안전장치 마련

□ 개정안

현 행	개 정 안
<p>제3절 <u>가명정보의 처리에 관한 특례</u></p> <p>제28조의2(<u>가명정보의 처리 등</u>) ① 개인정보처리자는 통계작성, 과학적 연구, 공익적 기록보존 등을 위하여 <u>정보주체의 동의 없이 가명정보를 처리할 수 있다.</u></p> <p><신 설></p> <p><신 설></p> <p><신 설></p> <p><신 설></p>	<p>제3절 <u>통계작성, 과학적 연구, 공익적 기록보존 목적 처리를 위한 안전조치</u></p> <p>제28조의2(<u>통계작성 등을 위한 개인정보의 처리</u>) ① ----- -----<u>다음 각 호의 요건을 모두 갖추는 경우 정보주체의</u>----- -----<u>개인정보를</u>-----.</p> <ol style="list-style-type: none"> 1. <u>정보주체의 동의를 받는 것이 불가능하거나, 동의를 받으면 그 목적을 달성할 수 없는 경우</u> 2. <u>처리의 목적이 정보주체의 권리보다 우선하는 경우</u> 3. <u>가명처리를 포함한 기술적·관리적 및 물리적 조치를 취한 경우</u> <p>② <u>개인정보처리자는 제1항에 따라 개인정보를 처리하는 경우에는 목적에 필요한 최소한의 개인정보만 처리하여야 하며 익명처리로 목적을 달성할 수 있는 때에는 이에 의하여야 한다.</u></p>

19) 민감정보에 대해서 가명처리특례규정이 적용될 수 있다는 취지의 해석이 있지만, 민감정보에 대한 정보주체의 권리와 법률에 의한 특별한 보호를 전면적으로 배제한다는 점에서, 위와 같은 취지의 해석은 기본권 보호의 관점에서 타당하지 않음

<신 설>

<신 설>

<신 설>

② (생 략)

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.

② 결합을 수행한 기관 외부로 결합된 정보를 반출하려는 개인정보처리자는 가명정보 또는 제58조의2에 해당하는 정보로 처리한 뒤 전문기관의 장의 승인을 받아야 한다.

③ 제1항에 따른 결합 절차와 방법, 전

③ 개인정보처리자는 제1항제3호에 따라 가명처리를 하는 경우에는 정보주체가 식별되지 않도록 추가 정보를 파기하거나, 필요한 경우 별도로 분리하여 보관·관리하여야 한다.

④ 개인정보처리자는 제1항제3호에 따라 가명처리를 한 개인정보를 보관·관리하는 경우에는 해당하는 정보가 분실·도난·유출·위조·변조 또는 훼손되지 않도록 대통령령이 정하는 바에 따라 안전성 확보에 필요한 조치를 취하여야 한다.

⑤ 개인정보처리자는 제1항에 따른 처리를 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.

<삭 제>

<삭 제>

문기관의 지정과 지정 취소 기준·절차, 관리·감독, 제2항에 따른 반출 및 승인 기준·절차 등 필요한 사항은 대통령령으로 정한다.

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.

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.

제28조의5(가명정보 처리 시 금지의무 등)

① (생략)

<신설>

② (생략)

제28조의6(가명정보 처리에 대한 과징금

부과 등) ① 보호위원회는 개인정보처

<삭제>

제28조의5(가명정보 처리 시 금지의무 등)

① (현행과 같음)

② 제1항에 불구하고 정보주체는 이 법에서 정한 권리를 행사하기 위한 목적으로 본인임을 식별할 수 있는 정보를 개인정보처리자에게 제공하는 방법 또는 제28조의2제3항에 따라 정보를 별도로 분리하여 보관하고 있는 개인정보처리자에게 요청하는 방법으로 가명정보의 식별을 요청할 수 있다.

③ (현행 제2항과 같음)

<삭제>

리자가 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.

② 과징금의 부과·징수 등에 필요한 사항은 제34조의2제3항부터 제5항까지의 규정을 준용한다.

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

<신 설>

<신 설>

제28조의7(적용범위) -----다음 각 호의 경우 제20조--제20조의2-----
-----제35조--제35조의2--제36조 및 제37조의-----아니 할 수 있다.

1. 시간·비용·기술 등을 고려할 때 위 각 규정의 적용이 가능하지 아니한 경우
2. 제28조의2제1항 본문에서 정한 처리 목적달성을 명백하게 저해하는 경우

□ 현행 개인정보 보호법이 규정하는 가명정보의 처리 특례의 장이 가진 가장 큰 문제점은 가명처리의 본질이 안전조치임에도 불구하고,²⁰⁾ 이를 활용의 관점에서 도입되는 조치와 같이 접근한다는 지점임

○ 과학적 연구 등 정보주체의 동의 없는 가명정보의 처리를 폭넓게 허용하고 있다는 점(제28조의2)

○ 광범위한 식별과 무분별한 영리목적의 개인정보 활용을 야기할 수 있는 정보의

20) GDPR 제32조 (a)항은 개인정보의 가명처리와 암호처리를 보안 수준을 보장하기 위한 기술 및 관리적 조치라고 규정하고 있음

결합을 전면적으로 허용하고 있다는 점(제28조의3)

○ 헌법 및 국제인권법에 의해 정보주체가 보장받는 처리정지권 등 기본적 인권을 전면적으로 박탈하고 있다는 점(제28조의7) 등이 대표적인 문제점으로 지적될 수 있음²¹⁾

□ 이에 시민사회단체가 제안하고자 하는 개정안에서는 가명정보의 처리 특례의 장의 명칭을 “통계작성, 과학적 연구, 공익적 기록보존 목적 처리를 위한 안전조치”로 명시하여 가명처리의 본질이 안전조치임을 명확히 하고,

○ 가명정보의 처리에 있어 목적 제한 외에 준수되어야 할 엄격한 요건을 구체적으로 규정하였으며,

○ 현재 가명정보의 결합을 허용하는 방식으로 사용되는 조항들을 삭제한 뒤 가명정보의 처리에 관한 일반적인 규율을 받게 하였음,

○ 더불어 가명정보의 처리에 있어 정보주체의 권리를 제한할 수 있는 경우도 보다 구체적으로 규정하여, 정보주체의 권리가 전면 박탈되지 않도록 하였음

마. 개인정보 보호 설계 및 기본설정 도입

□ 개정안

현 행	개 정 안
제29조(안전조치의무) <u>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</u>	제29조(안전조치의무) <u>개인정보처리자는 개인정보가 이 법을 위반하여 처리되거나, 분실·도난·유출·위조·변조· 훼손되지 아니하도록, 가명처리, 암호화, 내부 관리계획 수립, 정기적 평가, 접속기록 보</u> 관-----

21) 참고로 헌법 제37조 제2항은 자유와 권리의 본질적인 내용을 침해할 수 없다고 규정하며 기본권의 본질내용 침해금지를 강조하고 있음. 현재 특례조항은 가명정보의 처리에 있어 정보주체의 기본권을 제한하는 것이 아니라 전면적으로 박탈한다는 점에서 개인정보자기결정권 등 정보주체가 가진 기본권의 본질내용을 침해하고 있다고 보아야 함

하여야 한다.

<신 설>

-----.

제29조의2(설계 및 기본설정에 의한 개인정보보호) ① 개인정보처리자는 개인정보의 처리 방법을 결정하거나 그 처리가 이루어지는 시점에 다음 각 호의 사항을 종합적으로 고려하여 개인정보를 안전하게 보호할 수 있는 적절한 기술적·관리적 조치를 이행하고 설계해야 한다.

1. 정보주체의 권리 및 자유에 미치는 위험성
2. 개인정보 침해적 기술을 새롭게 도입하는지 여부
3. 비용
4. 개인정보 처리의 성격, 범위, 맥락 및 목적
5. 그 밖에 개인정보보호위원회가 제3조에 따른 개인정보보호 원칙의 준수 및 이를 위한 보호조치를 위하여 필요하다고 정하는 사항

② 개인정보처리자는 개인정보가 불특정 다수에게 열람되지 않는 것을 포함한 기본설정을 통해 처리 목적에 필요한 최소한의 개인정보만 처리되도록 기술적·관리적 조치를 이행해야 한다. 다만, 정보주체가 기본설정에 대하여 설명을 듣고 명백한 의사로 다른 선택을 할 경우에는 그러하지 아니하다.

③ 제32조의2에 의거한 인증은 제1항에서 정한 설계기준 및 제2항에 규정된 기본설정의 준수를 입증하기 위해 사용될 수 있다.

④ 개인정보보호위원회는 제1항에 따른

	<p>설계기준 및 제2항에 따른 기본설정에 대하여 고시로 정할 수 있다.</p>
--	----------------------------------------------

□ 현행 개인정보 보호법은 개인정보처리자가 부담하는 안전조치의무를 기술적 안전 조치로서만 이해하고 있고, 안전조치 의무가 이행되어야 할 상황을 “분실·도난·유출·위조·변조 또는 훼손”으로 한정하고 있는 문제점이 있음(제29조)

□ 반면 GDPR은 제24조²²⁾에서 개인정보의 처리가 정보주체의 권리 및 자유에 미칠 위험의 다양성을 고려하여 적절한 기술 및 관리적 조치가 취해져야 할 것을 강조하고 있는데,

○ 즉 ‘안전조치의무’는 단순히 분실·도난·유출·위조·변조 또는 훼손 상황에 한정하여 개인정보처리자가 물리적 조치를 취할 의무로서 이해되는 것이 아니라,

○ 정보주체가 가지는 권리에 대해 위험성을 초래할 수 있는 개인정보 처리 전반에 필요한 보호조치를 취할 의무로서 이해되어야 할 것임

□ 한편 유엔인권최고대표사무소는 상품의 제공 및 서비스 등 개인정보처리가 수반되는 행위에 있어 프라이버시 설계(Privacy by design)²³⁾와 프라이버시 기본설정(Privacy by default)²⁴⁾을 대표적 안전조치로서 도입되어야 할 것을 강조하고 있음²⁵⁾

○ GDPR과 다른 유럽의 개인정보 보호 법제 역시 프라이버시 설계와 기본설정에 관한 규정을 구체적으로 명시하고 있음²⁶⁾

22) GDPR 제24조 1. 개인정보처리자는 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, 그 처리가 본 규정에 따라 이루어졌음을 보장하고 입증할 수 있도록 적절한 기술 및 관리적 조치를 취해야 한다.

23) 개인정보의 처리 방법을 결정하거나 그 처리가 이루어지는 시점에 시스템의 설계에 있어 프라이버시의 보호를 위한 조치를 고려할 것을 의미함

24) 개인정보의 처리 방법을 결정하거나 그 처리가 이루어지는 시점에 프라이버시의 보호를 기본으로 설정할 것을 필수적으로 요구하는 것을 의미함

25) United Nations High Commissioner for Human Rights, “The right to privacy in the digital age”, A/HRC/39/29, 3 August 2018, para. 31.

26) GDPR 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. 그러한 기술 및 관리적 조치는 본 규정의 요건을 충족시키고 개인정보주체의 권리를 보호하기 위해 데이터 최소화 등 개인정보보호 원칙을 효율적으로 이행하고 필요한 안전조치를

□ 이에 개정안은 안전조치 의무가 이행되어야 할 상황에 개인정보보호법을 위반한 경우를 포괄적으로 포함하고, 가명처리 등 필요한 안전조치를 구체적으로 명시하였음

○ 이와 더불어 GDPR 규정 등의 내용을 구체적으로 반영하여 개인정보 보호를 위한 설계 및 기본설정에 관한 조항을 신설하였음

바. 개인정보 처리방침에 관한 심사제도 및 개인정보처리감독관 제도의 도입

□ 개정안

현 행	개 정 안
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 개인정보 파일에 대하여 개인정보 처리방침을 정한다.	제30조(개인정보 처리방침의 수립 및 공개) ① ----- ----- ----- ----- ----- ----- -----
1. 개인정보의 처리 목적	1. -----목적 및 그 처리의 법적 근거
2. ~ 6. (생략)	2. ~ 6. (현행과 같음)
<신설>	6의2. 제31조의3에 따른 개인정보 보호 감독관의 성명 및 연락처(해당하는 경우에만 정한다)
7.·8. (생략)	7.·8. (현행과 같음)
② ~ ④ (생략)	② ~ ④ (현행과 같음)
<신설>	제30조의2(개인정보 처리방침의 심사) ① 누구든지 보호위원회에 개인정보 처리

개인정보처리에 통합할 수 있도록 설계되어야 한다.
 2. 컨트롤러는 기본설정을 통해 각 특정 처리 목적에 필요한 개인정보만 처리되도록 적절한 기술 및 관리적 조치를 이행해야 한다. 그 의무는 수집되는 개인정보의 양, 그 처리 정도, 보관기관 및 이용가능성에 적용된다. 특히, 그러한 조치는 기본설정을 통해 개인정보가 관련 개인의 개입 없이 불특정 다수에게 열람되지 않도록 한다.
 3. 제42조에 의거한 승인된 인증 메커니즘은 본 조 제1항 및 제2항에 규정된 요건의 준수를 입증하는 요소로 사용될 수 있다

방침이 이 법에 위반되는지에 대한 심사를 청구할 수 있다.

② 보호위원회는 직권으로 개인정보 처리방침이 이 법에 위반되는지의 여부를 심사할 수 있다.

③ 보호위원회는 심사대상인 개인정보 처리방침이 변경된 때에는 제1항에 따라 심사를 청구한 자의 신청 또는 직권으로 심사대상을 변경할 수 있다.

④ 제1항에 따른 개인정보 처리방침의 심사청구 또는 제3항에 따른 심사대상의 변경신청은 보호위원회에 서면이나 전자문서로 제출하여야 한다.

⑤ 보호위원회는 제1항의 심사청구에 따라 심사하는 경우 30일 이내에 그 결과를 청구인에게 통지하여야 한다. 다만, 그 기간 내에 심사를 마치지 못하였을 때에는 14일의 범위에서 한 차례 심사기간의 연장할 수 있다.

⑥ 보호위원회는 제1항 내지 제3항에 따라 개인정보 처리방침을 심사하는 경우 개인정보 처리방침이 이 법에 위반된 사실을 확인한 때에는 개인정보처리자에게 제64조제1항에 따른 시정조치를 명할 수 있다.

⑦ 제1항부터 제4항까지에 따른 개인정보 처리방침의 심사 청구 방법 및 절차 등에 필요한 사항은 대통령령으로 정한다.

제31조의2(개인정보 보호감독관의 임명)

① 개인정보처리자는 처리하는 개인정보의 종류, 규모, 처리의 성격 등을 고려하여 대통령령이 정하는 경우에 개인

<신 설>

정보 보호에 관한 전문지식을 갖춘 사람을 개인정보 보호감독관으로 임명하여야 한다.

② 개인정보 보호감독관은 다음 각 호의 업무를 수행한다.

1. 개인정보처리자와 개인정보취급자에게 개인정보 보호와 관련된 법규 준수에 대한 의견제시 및 이행권고

2. 개인정보처리자의 법규 준수 현황과 개인정보 관리 실태에 관한 감독

3. 제33조에 따른 개인정보 영향평가에 관한 의견제시 및 감독

4. 보호위원회와의 협력

5. 그 밖에 개인정보처리에 대한 독립적 감독을 위하여 대통령령으로 정한 업무

③ 개인정보처리자는 대통령령으로 정하는 기준에 따라 개인정보 보호감독관을 다른 개인정보처리자와 공동으로 임명할 수 있다.

④ 개인정보처리자는 개인정보 보호감독관의 임명 여부를 개인정보보호위원회에 보고하여야 한다.

⑤ 개인정보 보호감독관의 임명요건, 업무, 자격요건, 그 밖에 필요한 사항은 대통령령으로 정한다.

제31조의3(개인정보 보호감독관의 지위)

① 개인정보 보호감독관은 제31조의2제3항에 따른 업무를 수행함에 있어서 독립성을 보장받으며 위 업무수행을 이유로 해임 또는 징계받지 아니한다.

② 개인정보처리자는 개인정보 보호감독관이 개인정보 보호에 관한 모든 업

<신 설>

<p><신 설></p>	<p>무에 적시에 관여할 수 있도록 하여야 한다.</p> <p>③ 개인정보 보호감독관은 개인정보처리자를 대표하는 자에게 직접 보고해야 한다.</p> <p>④ 정보주체는 자신의 개인정보 처리 및 이 법에 따른 권리행사와 관련된 모든 사항에 대해 개인정보 보호감독관에게 상담 및 조사 등을 요청할 수 있다.</p> <p>⑤ 개인정보처리자는 개인정보 보호감독관이 업무를 효율적으로 수행할 수 있도록 보호위원회가 고시로 정하는 행정·재정적 지원을 하여야 한다.</p> <p>⑥ 개인정보 보호감독관은 공정하고 독립적인 직무수행이 곤란하다고 판단하는 경우에는 직무수행을 회피하여야 한다.</p> <p>제31조의4(개인정보 보호감독관과 개인정보 보호책임자와의 관계) 개인정보처리자가 개인정보 보호감독관을 임명한 경우 제25조제4항제3호에 따른 “관리책임자” 및 제30조제1항제6호에 따른 “개인정보 보호책임자”의 표기는 “개인정보 보호감독관”으로 할 수 있다.</p>
--------------------	------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------

□ 현행 개인정보 보호법에 따르면 개인정보처리자는 개인정보 처리방침을 수립할 의무를 부담하지만(제30조).

○ 정보주체의 권리를 과도하게 제약하는 방식으로 개인정보 처리방침을 제정, 개정하더라도 이에 대한 적절한 보호조치가 이루어질 수가 없다는 문제점이 있음

□ 한편 GDPR에 따라 유럽에서는 독립적 지위에서 개인정보처리자의 업무를 감독하는 개인정보 보호감독관(Data Protection Officer) 제도를 도입·시행하고 있음

○ 관련하여 현행 개인정보 보호법은 개인정보처리자에게 개인정보처리책임자를 지정할 것을 규정하고 있지만(제31조),

○ GDPR 제37조 내지 제39조가 규정하고 있는 개인정보 보호감독관과는 그 독립성과 수행업무에 있어 본질적인 차이가 있음

□ 정보주체의 권리를 적극적으로 보호하기 위해서는 정보주체의 권리를 과도하게 제한할 수 있는 개인정보처리방침에 대한 적극적인 보호조치가 필요하고, 개인정보처리자의 일반적인 개인정보 처리에 대한 적극적인 감독과 개선이 필요하다고 할 것임

□ 이에 개정안은 개인정보보호위원회에게 개인정보처리방침에 대한 시정조치를 할 수 있는 권한을 부여하고, 그 실효성 확보를 위해 시민들에게 개인정보처리방침에 대해 심사를 신청할 수 있는 권리를 보장하도록 하였음

○ 더불어 시민사회단체는 개정안을 통해 GDPR이 규정하고 있는 개인정보 보호감독관 제도를 도입할 것을 제안하고자 함

○ 모든 개인정보처리자로 하여금 개인정보 보호감독관을 두도록 하는 것이 현실적으로 어려울 수 있다는 지점을 고려하여, 개정안에서는 개인정보보호 감독관을 임명해야 하는 개인정보처리자의 범위를 대통령령으로 제한할 수 있도록 하였고,

○ 개인정보보호감독관이 수행하는 업무도 GDPR의 수준에는 미치지 못하는 정도로 규정하였음

○ 그러나 위와 같은 지점은 추후 제도가 확립되어 감에 따라 추가 개정이 필수적이라 할 것임

사. 개인정보파일의 등록 예외 축소

□ 개정안

현 행	개 정 안
제32조(개인정보파일의 등록 및 공개) ①	제32조(개인정보파일의 등록 및 공개) ①

<p>(생략)</p> <p>② 다음 각 호의 어느 하나에 해당하는 개인정보파일에 대하여는 제1항을 적용하지 아니한다.</p> <p>1. (생략)</p> <p>2. <u>범죄의 수사, 공소의 제기 및 유지, 형 및 감호의 집행, 교정처분, 보호처분, 보안관찰처분과 출입국관리에 관한 사항을 기록한 개인정보파일</u></p> <p>3. 「<u>조세범처벌법</u>」에 따른 <u>범칙행위 조사</u> 및 「<u>관세법</u>」에 따른 <u>범칙행위 조사에 관한 사항을 기록한 개인정보파일</u></p> <p>4. 5. (생략)</p> <p>③ ~ ⑥ (생략)</p>	<p>(현행과 같음)</p> <p>② ----- ----- -----.</p> <p>1. (현행과 같음)</p> <p><삭제></p> <p><삭제></p> <p>4. 5. (현행과 같음)</p> <p>③ ~ ⑥ (현행과 같음)</p>
---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------	--------------------------------------------------------------------------------------------------------------------------------------------------------------

□ 현행 개인정보 보호법은 범죄의 수사 등과 관련한 개인정보파일 및 조세범 관련 개인정보파일을 등록 예외로서 규정하고 있음(제32조 제2항 제2호 및 제3호)

□ 개인정보파일의 등록은 개인정보 자체를 공개하라는 것이 아니라, 개인정보파일의 명칭, 운영 근거 및 목적, 기록되는 개인정보의 항목 등을 개인정보보호위원회에 등록하여 보호위원회의 감독 권한을 강화하려는 것임

□ 수사기관의 개인정보 처리 역시 개인정보보호위원회의 감독을 받아야 하는 대상이기 때문에 특별한 이유 없이 등록을 면제하는 것은 타당하지 않음

□ 이에 개정안은 현재 등록 예외로 규정된 범죄의 수사 등과 관련한 개인정보파일 및 조세범 관련 개인정보파일을 등록대상 개인정보파일의 예외에서 제외하여 범죄의 수사 등에 대한 개인정보보호위원회의 감독 권한을 강화하고자 함

자. 개인정보 영향평가 제도 강화 및 보완

□ 개정안

현 행	개 정 안
<p>제33조(개인정보 영향평가) ① <u>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.</u></p> <p><u><신 설></u></p> <p><u><신 설></u></p> <p><u><신 설></u></p> <p><u><신 설></u></p> <p>② 영향평가를 하는 경우에는 다음 각 호의 사항을 <u>고려하여야</u> 한다.</p> <p>1. <u>처리하는 개인정보의 수</u></p> <p>2. <u>개인정보의 제3자 제공 여부</u></p>	<p>제33조(개인정보 영향평가) ① <u>개인정보처리자는 다음 각 호의 경우</u>-----</p> <p>-----</p> <p>-----<u>때에는</u>-----</p> <p>-----<u>개인정보처리자는</u>-----</p> <p>-----.</p> <p>1. <u>자동화된 처리에 근거하여 개인을 체계적이고 광범위하게 평가하여 해당 평가에 근거한 결정이 해당 개인에게 법적 효력을 미치거나 이와 유사하게 개인에게 중대한 영향을 미치는 경우</u></p> <p>2. <u>제23조제1항 각호의 정보를 대규모로 처리하는 경우</u></p> <p>3. <u>공개된 장소에 대한 대규모의 체계적 모니터링을 하는 경우</u></p> <p>4. <u>기타 처리의 성격과 범위, 상황, 목적을 참작하여 정보주체의 권리에 중대한 위험을 초래할 것이 예상되는 경우로서 대통령령으로 정하는 경우</u></p> <p>② -----</p> <p>-----<u>종합적으로 고려하여야</u>-----</p> <p>-----.</p> <p>1. <u>개인정보 처리의 성격과 범위, 맥락, 목적</u></p> <p>2. <u>개인정보를 침해할 우려가 있는 기술</u></p>

3. (생략)

4. 그 밖에 대통령령으로 정한 사항

③ (생략)

④ 공공기관의 장은 제1항에 따라 영향 평가를 한 개인정보파일을 제32조제1항에 따라 등록할 때에는 영향평가 결과를 함께 첨부하여야 한다.

⑤ ~ ⑦ (생략)

⑧ 공공기관 외의 개인정보처리자는 개인정보파일 운용으로 인하여 정보주체의 개인정보 침해가 우려되는 경우에는 영향평가를 하기 위하여 적극 노력하여야 한다.

<신설>

<신설>

<신설>

의 도입

3. (현행과 같음)

4. -----정보주체의 개인정보 침해에 관한 사항으로 대통령령으로-----

③ (현행과 같음)

④ 개인정보처리자는 제1항에 따른-----
-----등록하여야 할 때에는 영향평가의-----.

⑤ ~ ⑦ (현행과 같음)

⑧ 개인정보처리자는 제1항 각 호에 해당하지 아니하는 경우에도-----
-----실시하기-----.

⑨ 개인정보처리자는 영향평가와 관련된 정보를 인터넷 홈페이지 등에 게재하여 공개하여야 한다.

⑩ 보호위원회는 제1항제2호 내지 제5호에서 정한 영향평가가 요구되는 처리 작업, 제2항에서 정한 영향평가의 고려 사항, 제9항에서 정한 영향평가와 관련한 공개의무자 및 공개대상정보 등에 대한 구체적 사항을 고시로 정할 수 있다.

제33조의2(사전자문) ① 개인정보처리자는 제33조에 따른 영향평가를 통해 개인정보의 처리가 중대한 위협을 초래할 수 있음에도 불구하고 그 위협을 완화하기 위한 일련의 조치를 하지 않고 있는 것으로 평가되는 경우에는 해당 개인정보의 처리 이전에 보호위원회에 자문을

신청해야 한다.

② 보호위원회는 개인정보처리자로부터 제1항에 따른 자문을 신청받은 경우 신청일로부터 8주 이내에 해당 개인정보처리자에게 문서로 개인정보 처리에 대한 권고 의견을 회신하여야 한다.

③ 보호위원회는 처리되는 개인정보의 성격을 고려하여 제2항에 따른 회신기간을 6주의 범위에서 한 차례 연장할 수 있다. 이 경우 회신기간 연장 사유를 해당 개인정보처리자에게 통지하여야 한다.

④ 개인정보처리자는 제1항에 따라 보호위원회에 자문을 신청할 때에는 다음 각 호에 해당하는 자료를 제출하여야 한다.

1. 제1항에 따른 자문의 대상인 개인정보처리(이하 '자문대상 개인정보처리'라 한다)에 관여하는 자들의 개별적 책임을 확인할 수 있는 경우 개별적인 책임에 관한 자료
2. 자문대상 개인정보처리의 목적 및 방법
3. 자문대상 개인정보처리로부터 정보주체의 권리를 보호하기 위해 제공되는 조치
4. 개인정보보호감독관을 임명한 경우 개인정보보호감독관의 연락처
5. 제33조제1항에 따른 영향평가결과
6. 기타 보호위원회가 제출을 요청하는 자료

⑤ 제1항에 따른 자문의 신청 절차 및 방법 등에 필요한 사항은 대통령령으로 정한다.

□ 현행 개인정보 보호법은 영향평가를 시행해야할 의무를 부담하는 주체가 공공기관으로 한정되고 있고, 같은법 시행령이 정하는 기준을 요건으로 하고 있음. 또한, 영향평가 결과보고서를 단순히 개인정보보호위원회에 제출하도록 규정하고 있음(제33조 제1항)

○ 한편 개인정보영향평가는 제도의 본질이 정보주체의 권리에 미치는 개인정보 처리의 영향을 평가하는 제도인데,

○ 오늘날 대두되고 있는 프로파일링을 포함한 자동화된 결정에 의한 개인정보 처리, 새로운 기술의 도입에 대한 영향평가 등이 실질적으로 공백의 영역이 되고 있음

○ 이처럼 현행 개인정보 보호법이 규정하는 개인정보 영향평가는 민간에 의해 발생할 수 있는, 다양한 형식으로 이루어지는 개인정보처리에 있어 정보주체의 권리 침해 등을 평가할 수 없다는 대상의 문제, 영향평가 결과가 공개되지 않는다는 투명성의 문제가 있음

□ 국제인권규범 및 GDPR 등은 프라이버시권 등의 보호를 위한 필수적 안전장치인 영향평가를 실시해야 할 의무를 공공기관 등 국가 등 공공기관의 의무일 뿐만 아니라, 사적 주체도 부담해야 할 의무임을 명확히 하고 있음

○ 유엔인권최고대표사무소는 기업에게 ‘인권영향평가’를 실시해야할 의무를 부과하도록 하고 있고,²⁷⁾ GDPR 역시 영향평가 의무를 공공기관으로 한정하여 부과하고 있지 않음

○ 나아가 영향평가 기준에 자동화된 결정, 새로운 기술적 또는 조직적 솔루션의 적용 등을 포함할 것을 권고하고 있기도 함²⁸⁾

□ 투명성과 관련하여서는 미국, 유럽연합, 캐나다 등 다른 국가들은 영향평가 결과보

27) United Nations High Commissioner for Human Rights, “The right to privacy in the digital age”, A/HRC/39/29, 3 August 2018, para. 45.-46.

28) 제29조 정보 보호 실무반의 ‘정보보호영향평가(Data Protection Impact Assessment, DPIA) 및 규정 2016/679의 목적 상 "심각한 위험을 발생시킬 수 있는"정보 처리 판단 지침, 2017 참조

고서 제출과 함께 영향평가의 결과를 전부 혹은 부분적으로나마 공개하도록 하고 있음²⁹⁾30)

□ 이에 현행 개인정보 영향평가제도 시행의 의무주체를 공공기관에서 개인정보처리자로 확대하고,

○ 새로운 기술의 도입, 개인에게 중대한 영향을 미치는 자동화된 의사결정, 민감정보의 대규모 처리, 공개된 장소에 대한 대규모의 체계적 모니터링의 경우 등을 영향평가의 대상으로 규정하는 개정안을 제안하고자 함

○ 개정안은 투명성의 확보를 위해 공공기관의 경우 개인정보파일을 등록할 때 영향평가 결과도 등록하도록 하였고, 대통령령이 정하는 기준으로 그 결과를 공개할 수 있도록 하였음

○ 한편 영향평가의 실효성 확보를 위해 개정안은 개인정보 보호위원회의 ‘사전 자문 제도’를 신설하였는데, 해당 제도는 중대한 위험이 있는 개인정보처리 이전 개인정보 보호위원회의 자문을 거치도록 하는 제도로서 GDPR이 정보주체의 권리 침해를 사전적으로 예방하기 위해 중요하게 규정하고 있는 제도임³¹⁾

차. 과징금 규정 정비

□ 개정안

현 행	개 정 안
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, 주민등록	제34조의2(과징금의 부과 등) ① ----- ----- ----- ----- -----100억원-

29) 장시영, “개인정보 영향평가 (Privacy Impact Assessment) 제도의 국내·외 현황 비교 및 시사점 분석”, 2018, 11쪽

30) “관리자들은 정보보호영향평가(DPIA)의 요약 또는 결론 등 적어도 일부에 대한 공개를 고려해야 한다”(제29조 정보 보호 실무반의 ‘정보보호영향평가(Data Protection Impact Assessment, DPIA) 및 규정 2016/679의 목적 상 “심각한 위험을 발생시킬 수 있는”정보 처리 판단 지침, 2017 참조)

31) GDPR 제36조 참조

<p>번호가 분실·도난·유출·위조·변조 또는 훼손되지 아니하도록 개인정보처리자가 제24조제3항에 따른 안전성 확보에 필요한 조치를 다한 경우에는 그러하지 아니하다.</p> <p>② ~ ⑤ (생략)</p>	<p>----- ----- ----- ----- ----- ----- ----- ----- ----- ----- ----- -----</p> <p>② ~ ⑤ (현행과 같음)</p>
<p><신설></p>	<p>제64조의2(과징금의 부과) ① 보호위원회는 다음 각 호의 어느 하나에 해당하는 행위가 있는 경우에는 해당 개인정보처리자 또는 정보통신서비스 제공자에게 전체 매출액의 100분의 4 이하에 해당하는 금액을 과징금으로 부과할 수 있다. 다만, 매출액이 없거나 매출액의 산정이 곤란한 경우로서 대통령령으로 정하는 경우에는 100억원 또는 자본금의 100분의 4 중 큰 금액 이하로 과징금을 부과할 수 있다.</p> <ol style="list-style-type: none"> 1. 제15조제1항, 제17조제1항·제2항, 제18조제1항·제2항 및 제19조(제26조제7항에 따라 준용되는 경우를 포함한다)를 위반하여 개인정보를 이용·제공한 경우 2. 제15조제2항, 제17조제2항, 제18조제3항 또는 제26조제3항을 위반하여 정보주체에게 알려야 할 사항을 알리지 아니한 경우 3. 제22조제6항(제26조제7항에 따라 준용되는 경우를 포함한다)을 위반하여 법정대리인의 동의를 받지 아니하고

만 14세 미만인 아동의 개인정보를 수집한 경우

4. 제23조제1항제1호(제26조제7항에 따라 준용되는 경우를 포함한다)를 위반하여 이용자의 동의를 받지 아니하고 민감정보를 처리한 경우
5. 제24조제1항 및 제24조의2제1항(제26조제7항에 따라 준용되는 경우를 포함한다)을 위반하여 고유식별정보를 처리한 경우
6. 제26조제4항에 따른 관리·감독 또는 교육을 소홀히 하여 특례 수탁자가 이 법의 규정을 위반한 경우
7. 제28조의5조제1항(제26조제7항에 따라 준용되는 경우를 포함한다)을 위반하여 특정 개인을 알아보기 위한 목적으로 정보를 처리한 경우
8. 이용자의 개인정보를 분실·도난·유출·위조·변조 또는 훼손한 경우로서 제29조의 조치(내부 관리계획 수립에 관한 사항은 제외한다)를 하지 아니한 경우(제26조제7항에 따라 준용되는 경우를 포함한다)
9. 제36조제2항(제26조제7항에 따라 준용되는 경우를 포함한다)을 위반하여 정정·삭제 등 필요한 조치를 하지 아니하고 개인정보를 계속 이용하거나 이를 제3자에게 제공한 경우
10. 제37조제2항(제26조제7항에 따라 준용되는 경우를 포함한다)을 위반하여 개인정보의 처리를 정지하지 아니하고 계속 이용하거나 제3자에게 제공한 경우
11. 제39조의3제1항(제26조제7항에 따라

준용되는 경우를 포함한다)을 위반하여 이용자의 동의를 받지 아니하고 개인정보를 수집한 경우

12. 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 해당 개인정보처리자 또는 정보통신서비스 제공자등이 매출액 산정자료의 제출을 거부하거나 거짓의 자료를 제출한 경우에는 해당 개인정보처리자 또는 정보통신서비스 제공자등과 비슷한 규모의 개인정보처리자 또는 정보통신서비스 제공자등의 재무제표 등 회계자료와 가입자 수 및 이용요금 등 영업현황 자료에 근거하여 매출액을 추정할 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.

□ 현행 개인정보 보호법은 가명정보의 처리 및 정보통신서비스제공자 등에 대한 과징금의 부과기준을 전체 매출액 또는 위반행위 관련 매출액의 100분의 3 이하 또는 4억원 이하로 기준을 세우고 있고(제28조의6, 제39조의 15), 주민등록번호 분실의 경우 5억원 이하를 기준으로 세우고 있음(제34조의2)

○ 위와 같이 현행 개인정보 보호법이 규정하고 있는 과징금 부과 기준은 국제적 추세에 비교했을 때 다소 완화된 기준에 해당함

□ 관련하여 GDPR은 제83조에서 행정 과태료의 부과기준을 세부적으로 정하고 있는데, 그 기준은 아래와 같음

○ 일반적 위반 사항의 경우 전 세계 매출액의 2%, 혹은 1천만 유로(약 125억원) 중 높은 금액

○ 중요한 위반 사항³²⁾의 경우 전 세계 매출액의 4%, 혹은 2천만 유로(약 250억원) 중 높은 금액

□ 참고로, 유엔 프라이버시 특별보고관 역시 한국의 방문조사 결과보고서를 통해 프라이버시권 침해에 대해 가해자에게 전 세계매출액의 4-5% 수준의 과징금을 부과할 것을 권고한 바 있음³³⁾

□ 개정안은 이상과 같이 국제사회에서는 과징금의 기준을 전 세계 매출액 최대 100분의 4이하, 약 125~250억까지 규정하고 있는 추세를 고려하여,

○ 관련 매출액이 아닌 전체 매출액을 기준으로,

○ 100분의 4 이하, 100억원 수준으로 과징금의 기준을 정비하였음

○ 현재 산재되어 있는 과징금 조항을 통합하여 일률적인 기준을 적용하도록 하였음

○ 참고로 고유식별번호 처리에 관한 과징금 조항의 경우 현재 5억원의 기준을 100억으로 상향하여 개정하거나, 신설될 과징금 조항의 각호로 규정하여 통합할 것을 제안함

32) 개인정보 처리 기본원칙 위반, 정보주체의 권리 보장 의무 위반, 제3국이나 국제조직의 수령인에게 개인정보 이전 시 준수 의무 위반, 감독기구가 내린 명령 또는 정보 처리의 제한 불복, 개인정보 이동 중지 미준수 및 열람 기회 제공 의무 위반 등

33) Joseph Cannataci, "Report of the Special Rapporteur on the right to privacy—Visit to the Republic of Korea", 25 June 2021, para. 65.

...

토론

최경진 (가천대학교 법학과 교수)



...

종합 토론

이진규 (네이버 CPO)



○ [정보주체의 권리 강화를 위한 개선방안 (김보라미 변호사님 발제)]은 우선 데이터 3법 개정 법률안이 국회 본회의를 통과하던 배경을 상세히 설명하면서, ‘법정합성에 대한 검토 미흡’이 있었던 점을 다시 상기해 주셨습니다. 또한, 개인정보주체의 권리보장에 관한 입법이 데이터3법 개정 이후 추진하는 것은 사전에 예정되었던 것이므로 이에 대한 본격적인 논의를 해야 한다는 당위성에 대해서도 말씀해 주셨습니다. 이어서, UN 인권이사회의 권고안의 구체적 내용에 대한 설명과 더불어, GDPR 및 미국 각 주에서의 개인정보보호법 입법화에 대해서도 전반적으로 잘 짚어 주셨습니다. 오늘 토론회의 배경 및 필요성을 파악하는데 이보다 더 적절한 수준의 정보 제공은 어려울 것으로 생각합니다.

○ 우선 “개인정보의 적법한 처리근거의 정비(제15조, 제17조)”와 관련하여 현실에서 가장 문제가 되는 것은 동의를 받을 때, 법에서 정보주체에게 알리도록 하는 내용을 어떻게 알리도록 하는지에 관하여 해외 사업자와 차별적으로 적용되고 있는 법 집행 관행이라 할 것입니다. 정보주체의 개인정보 처리에 관한 사항을 자세하고 효과적으로 정보주체에게 알리고, “충분히 알고하는 동의”가 이뤄질 수 있도록 **제도를 정비하는 것에 반대할 개인정보처리자는 없을 것이라** 생각합니다. 다만, 글로벌 개인정보 처리환경에서 절대 다수의 개인정보처리자가 Privacy Policy or Notice에 개인정보 처리에 관한 내용을 기재하고, 이를 정보주체가 확인하고 동의할 수 있도록 안내하는 것이 일반적이지만 우리나라는 그렇지 않습니다. 한마디로 “개인정보처리방침 따로, 개인정보 수집 및 이용에 대한 동의 따로, 개인정보 제3자 제공 동의 따로, 개인정보 위수탁 동의 따로” 등 복잡한 구조를 현실에서 강제하고 있습니다. 이로 인해 개인정보처리와 관련하여 어떠한 문제가 생겼을 때, 개인정보처리방침은 처분을 하기 위해 규제당국에서 살펴보는 ‘증거자료’로서의 기능 외에 실질적 기능을 하지 못하고 있습니다. 정보주체가 자신의 개인정보 처리에 관한 정보를 적절하게 고지 받을 권리를 확대하는 것에 반대할 이유가 전혀 없습니다. 다만, 이를구현하는방식에있어기존에별다른기능을하지못했던 ‘개인정보처리방침’이 실질적인 기능을 할 수 있게 해주어야 한다고 생각하며, 이에 대해서도 관심을 기울여 주시기를 바랍니다.

○ “정보주체 이외로부터 수집한 경우 고지받을 권리 확대(제20조)”와 관련하여 정보주체 이외로부터 개인정보를 수집한 경우, 정보주체의 자기정보 통제권 확립

을 위해 고지받을 권리가 필요하다는 점과 취지 등에 대해서는 원칙적으로 동의합니다. 다만, 현행과 같이 A라는 오픈마켓에 상품을 올려놓은 B라는 판매자에게 물건을 구매하자마자, 카카오톡으로 “A로부터 상품 구매 및 배송과 관련한 고객 개인정보를 제공받았다.”라는 개인정보 수집출처 고지가 전달되는 것과 같이 이미 정보주체가 알고 있는 사실에 대해 다시 고지를 하는 배제할 필요가 있을 것으로 생각됩니다. 물품 구매 과정에서 ‘개인정보 제3자 제공’에 대한 동의가 별도로 진행되고, 그 과정에서 정보주체가 자신의 개인정보가 누구에게, 어떤 목적으로 제공되는지 등에 관한 내용을 확인하게 되는데 재차고지를하도록하는것은정보주체에게직관적이지않으며, 개인정보처리자에게 불필요한 부담을안길것입니다. 이 역시, 개인정보처리방침의 실질화를 위해 개인정보 제3자 제공에 관한 사항을 처리방침 내에 담고, 이를 정보주체에게 다시 확인하게끔 제시하는 방안이 현실에서 작동해야 할 것입니다. 다만, 제3자를 개별적으로 특정하는 방안이 현실적으로 작동하기 어려울 수 있으므로 ‘범주화’ 하여 안내하는 방안에 대해서도 검토를 부탁드립니다. 기존의 구매내역을 볼 수 있는 웹페이지가 존재한다면, 해당 웹페이지로 연결되는 URL을 안내하는 방안과 같이 현실에서 잘 동작할 수 있는 방안에 대해서도 적극 고려를 부탁드립니다.

○ “개인정보 전송요구권의 도입(제35조의2, 제35조의3)”에 대해 4차산업혁명위원회가 주관한 ‘해커톤’의 논의를 거쳐 합의에 이른 것은 전적으로 ‘정보주체의 권리를 보장’하고 ‘개인정보보호법이 개인정보에 관한 기본법으로서 기능할 수 있도록’하기 위한 것이었지, 개인정보보호법을 기반으로 하여 데이터 산업의 활성화를 꾀하거나 하는 것은 전혀 아니다는 점을 꼭 강조하고 싶습니다. 우선, 정보주체의 기본적 권리를 매출액, 개인정보 규모 등을 기준으로 재단하여 특정 개인정보처리자에게만 전송요구권을 행사할 수 있도록 하는 것이 이와 같은 해커톤의 합의 정신을 제대로 반영한 것인지에 대해 매우 강한 의문이 있습니다. 또한, 해커톤 합의 당시에는 ‘기술적 지원’을 위하여 개인정보보호 전담 지원기관(한국인터넷진흥원 등)을 활용하여 기술 등 지원체계를 구축하고, 상시적인 개인정보 이동, 관리현황 모니터링을 하도록 한다고 하였지, 별도의 개인정보관리전문기관을 만들고 해당 기관으로 하여금 정보주체의 권리행사를 지원하도록 한다는 내용은 논의 되지도 않았습니니다. 개인정보관리전문기관이 수행하는 역할도 불분명하거나와, 해당 기관이 개인정보를 활용할 수 있는 규정이 향후 도입된다거나 하는 경우 현재 신용정보법의 마이데이터 제도와 같이 특정 사업자에 대한 허가제를 기반으

로 한 ‘데이터 몰아주기’가 제도적으로 형성되는 문제도 있습니다. 개인정보보호법의 개인정보 전송요구권은 정보주체에게 portable data를 돌려줄 수 있는 구조를 만들면 족하지, 그 외에 산업발전 등을 고려하여 무리하게 정부가 개입할 여지를 만드는 것은 보호법이 ‘<보호법>으로서의 역할’을 스스로 포기하는 것에 다름 없습니다. 다시 해커톤 합의의 정신으로 돌아가 정보주체가 자신의 개인정보에 대한 실질적 통제권을 행사할 수 있는 기반을 만드는 것이 중요할 것입니다. 아울러, GDPR에도 도입된 여러 권리가운데 이동권이 왜 ‘잊혀진 권리(forgotten right)’로 불려지고 있는 것인지에 대한 배경도 다시 조사하여 해당 권리의 도입에 대해 근본적으로 재검토해보기를 바랍니다. 전송요구권이 현실에서 동작하기 위해서는 많은 사회적 리소스가 투입되어야 하며, 시간도 적잖게 필요합니다. 서둘러 도입하였다가 되돌리기 어려운 ‘정보주체 통제권의 상실’로 이어지지 않아야 할 것입니다.¹⁾

※참고: 제9차 해커톤의 <개인정보 이동권제도 도입> 합의사항

- ◆ 디지털 시대의 정보주체를 위한 새로운 권리인 개인정보 이동권은 「개인정보 보호법」에 원칙적으로 규정
- ◆ 개인정보 이동권 행사를 위한 합리적이고 구체적인 기준 마련 필요
- ◆ 개인정보 이동권 행사와 관련한 정보주체의 실질적 보장방안 마련
- ◆ 법제도 정비 뿐 아니라 기술적 지원 등을 위한 정부 노력 필요

○ “자동화된 의사결정에 대한 배제 등의 권리 규정(제37조의2)”은 GDPR의 내용을 거의 그대로 가져온 것인데, 도입 자체에 대한 반대보다는 ‘디테일에 있는 악마에 있다.’는 점에 항상 유의해야 한다는 생각입니다. 우리개인정보보호법에 ‘명백하게’, ‘불가피하게’라는 문구로 인해 지나치게 제한적인 법해석으로 인하여 현실에서 발생하는 여러 문제점이 있다는 점을 언급해봅니다. 또한, 제4항에서 “아동에 대하여 마케팅 목적으로 자동화된 개인정보 처리에만 의존한 의사결정을 하여서는 아니된다.”라고 규정하고 있는데, ‘마케팅 목적’이 구체적으로 무엇인지, ‘법적 효력, 생명/신체/재산에 중대한 영향을 미치는 (중요한) 결정’이 아니라 “모든 자동화 처리에 의한 의사결정”을 해서는 아니되는 것인지, ‘의사결정’은 또한 무엇을 의미하는 것인지 등 다양한 의문을 제기하지 않을 수 없습니다. 그럼에도, 특별한 보호를 요하는 대상인 아동 보호에 대한 취지에는 공감합니다.

1) ALIAS, “Research Report-GDPR Data Portability: The Forgotten Right”, p. 22, URL: https://cellar-c2.services.clever-cloud.com/alias-code-is-law-assets/static/report/gdpr_data_portability_the_forgotten_right_report_full.pdf

○ 서채완 변호사님께서도 입법과제로서 [개인정보처리자의 책임성 강화를 위한 개인정보보호법 개정과제]에 대한 배경을 잘 말씀해주신 것으로 생각합니다. 말씀해주신 배경과 취지에 전적으로 동의합니다.

○ “과학적 연구의 개념을 구체화(제2조 제8호)”할 필요가 있다는 점에 대해서는 이견이 없습니다. 오히려 산업계에서도 ‘과학적 연구’가 구체적으로 무엇을 의미하는지, 그 범위는 어디까지 인지, 어떤 연구가 과학적 연구에 해당하는지에 대한 객관적 요건이 마련될 수 있는 것인지 등에 대한 의문이 있었던 것이 사실입니다. 다만, 제안해주신 ‘공인된 연구윤리’에 대한 사회적 합의를 어디에서 찾아야 할 것인지는 앞으로도 지난한 논의가 필요할 것으로 생각되며, 그로 인해 자칫 과학적 연구 목적의 개인정보 처리가 일시적으로 연옥(limbo)에 빠지게 되는 것은 아닌지 우려가 있습니다. 물론, 법에서는 이 정도로 반영하고, 차후 하위 법령 내지 가이드라인 등에서 이를 풀어나가는 것도 가능하다고 생각합니다.

○ “개인정보 보호 설계 및 기본설정 도입(제29조 제29조의2)”은 소위 ‘privacy by design and default’를 법문으로 구체화한 의미가 있다고 판단되며, 그 취지에 동감합니다. 다만, 이를 위해서는 개인정보를 설계에 의하여, 또한 기본으로 보호하기 위한 원칙을 언급하고, 이를 달성하기 위한 다양한 ‘기술 중립적 수단’에 대해 제시를 해야 할 것인데, 법 제29조의 안전조치 의무를 통해 ‘대통령령’에 구체적으로 기술적, 관리적, 물리적 보호조치를 정하도록 하고, 실질적으로는 관련 고시에 세부 내용을 위임하게 하는 경우 지나치게 복잡한 구조가 될 것으로 보입니다. GDPR은 보호조치를 세세하게 가이드하지 않으며, 위험 수준에 따라 가용한 효과적 수단을 개인정보처리자의 판단에 따라 선택할 수 있도록 하고 있다는 점에 주목할 필요가 있습니다. 제29조의2를 신설하여 ‘privacy by design and default’를 구현하는 것은 원칙적으로 찬성하나, 그에 상응하여 구체적인 보호조치를 강제하는 관련 시행령 및 고시 폐지에 대한 논의도 함께 진행되지 않는 경우 기존의 국가 후견주의적 ‘특정 개인정보보호 방식의 강제’가 절대로 해결되지 않을 것이며, 오히려 더 악화될 우려가 있다고 생각합니다.

○ “개인정보처리감독관제의 도입(31조의3)”에 대해서는 찬성 의견입니다. 다만, 기존의 개인정보보호책임자(CPO) 제도와의 조화를 어떻게 해야 할 것인지는 매

우 어려운 문제라고 판단됩니다. 실무에서 역할과 책임을 어떻게 나누어서 수행해야 할 것인지에 대해선 더 많은 논의가 필요할 것으로 생각됩니다. 여기에 더하여, 개인정보처리방침에 대한 심사제도가 자칫 불만을 품은 고객(들)에 의해 악용되는 상황에서의 개인정보처리자 보호에 대한 내용도 함께 고민이 필요한 지점으로 생각이 됩니다. 현재도 보호위원회가 처리방침의 법 위반 여부를 직권조사 하는 것이 불가능하지 않은 상황이라는 점도 고려가 필요합니다. 또한, 약관법에 따라 공정거래위원회가 수행하는 심사와의 관계도 정비가 필요할 것입니다.

○ “개인정보 영향평가 제도 강화 및 보완(제33조, 제33조의2)”와 관련하여 GDPR의 경우 리스크를 판단하여 그 크기에 따라 개인정보영향평가 수행여부를 개인정보처리자가 자체적으로 판단할 수 있는 여지가 있습니다. 영향평가를 모든 개인정보처리자에게 확대하면서, 이를 수행해야 하는 기준을 법에 이렇게 규정하는 방식이 적절한 것인지 의문이 듭니다. 현재 공공부문에서만 수행하는 “매우 형식적인” 개인정보 영향평가가 자칫 민간에도 도입되거나, 그러한 방식이 마치 표준처럼 자리잡는 경우 민간에서의 개인정보 처리 행태에 미치는 부정적 영향이 매우 클 것으로 생각됩니다. 일부 문구는 수정의 여지도 있는 것으로 보입니다(예: 자동화된 처리 à 전적으로 자동화된 처리 등). GDPR의 자구를 가져오다 보니 일부는 모호한 지점도 있습니다. 공공에 대해서는 현재와 같이 강화된 개인정보 영향평가를, 민간에서는 자율적이고 유연한 방식의 영향평가가 자리잡을 수 있도록 유도하는 방안이 검토되어야 할 것으로 생각됩니다. 게다가 민간에서의 개인정보 영향평가 내용을 등록하도록 하는 것은 과도하다 하지 않을 수 없습니다. 민간의 개인정보 처리에 관한 내용이 공개됨으로써 발생하는 영업기밀의 유출이나 경쟁사에 경쟁정보(competitive edge)가 전달되어 발생하는 문제 등에 대해서도 고려를 해야 할 필요가 있습니다.

○ “과징금 규정 정비(제34조의2, 제64조의2)”와 관련하여, 김보라미 변호사님의 발제에서 확인할 수 있는 바와 같이 실제 유럽연합이 부과한 과징금의 평균 금액 수위는 그다지 높지 않습니다. 소위 ‘high-profile case’의 경우에만 보여주기 식의 높은 과징금이 부과되는 것을 확인할 수 있습니다. UK ICO의 British Airways, Marriott Hotel 과징금 부과 사례에서 보듯 경제적 상황을 고려한 과징금 경감(기존 예고 대비 1/10 수준으로 감액)하는 유연성도 갖추어져 있습니다. 그런데, 우리나라는 기계적 산식에 의해 계산한 결과를 법에 따라 감경하는 경우

에도 사전에 정해진 ‘산식’에 의하여 과징금을 부과하게 됩니다. 유연성이 없는 상황에서 과징금 상단을 전체매출의 4%로 하게 되면 기계적, 산술적 계산식에 의한 과도한 과징금 부과를 피할 방법이 없으며 결국 국내 개인정보 관련 산업에 엄청난 위축효과가 발생할 것으로 예상됩니다. 악마는 디테일에 있습니다. GDPR의 내용을 그대로 가져온다고 해서, 우리가 유럽연합과 같은 수준으로 과징금 부과가 가능할 것인지에 대해 매우 큰 의문이 있습니다. 개인정보 유출통지, 신고제도에서 우리나라와 같이 ‘중요한 개인정보’가 아니라 그냥 ‘일반 개인정보’ 유출의 경우에도 신고, 통지를 무조건 하도록 하는 주요 국가는 없습니다. 대부분 위험 기반이거나, 재무 정보 유출의 경우에만 통지 신고를 하도록 되어 있습니다(유럽, 미국, 일본 등). 우리나라에서의 개인정보 유출이나 침해 위험이 과도하게 인식되고 있는 것은 이와 같은 ‘무조건 반사적’ 유출 통지, 신고제도의 구조에 기인한 것임에도 이런 제도의 불합리성이나든지 개선 필요성에 대해서는 그 어떤 법률 개정안에도 나와있지 않습니다. 매번 규제와 통제만 강화되는 방향으로 논의되는 것이 과연 응보적 보복 외에 어떤 의미를 갖을 것인지 쉽사리 이해하기 어렵습니다. 과징금 부과와 관련한 논의는 정부안, 시민사회안, 개인정보처리자안 등을 모두 테이블에 올려놓고 전면적인 재검토를 해야 합니다. 전 세계 모든 규제의 최상단만 모아놓는 슈퍼규제를 만들어 낼 가능성도 배제할 수 없습니다.

○ 현장에서 실제 정보주체가 자신의 권리를 행사하지 않는 이유는 열람권이나 정정권을 직접 행사할 수 있을 만한 ‘시스템(메뉴, 기능)’이 갖추어져 있고, 권리를 행사할 필요가 크지 않으며, 별도의 권리행사에 대한 인식 없이도 고객센터 문의 등을 통해 충분히 사안이 해결되고 있기 때문으로 파악됩니다. 권리를 행사하는 경우가 많지 않다고 하여 권리 행사의 필요성이 부정되는 것은 절대로 아닐 것입니다. 다만, 이동권과 같이 제대로 활용되지 않는 권리의 도입에 있어서는 ‘현실에서 어떤 문제가 있기 때문에’ 그런 것인지 충분히 사회적인 논의를 거쳐야 할 것으로 생각합니다. 개인정보처리자에 대한 책임성을 강화하는 지점에 있어서도 현실에서 ‘workable solution’인지에 대한 고민이 선행될 필요가 있습니다. 만들어 놓고, 나중에 고쳐가며 대응한다고 하기엔 현장에서의 개인정보 처리 환경이나 상황이 매우 어렵습니다. 데이터3법으로 제시된 장미빛 미래는 아무것도 현실화된 것 없는 상황에서, 책임성만 강화되는 상황이 현재 개인정보처리자들이 맞닥뜨린 암울한 상황이라 하지 않을 수 없습니다. 차라리 GDPR을 그대로 수용하거나, 과거의 정보통신망법으로 되돌리는 것이 낫다는 푸념도 들립니다. 시민사회에

서 제안해주신 발제의 내용이 보다 더 넓은 사회구성원들과 공유되어 논의될 수 있는 기회가 더욱 더 많이 생겨서 부디 합리적인 법률안이 마련되기를 진심으로 희망합니다. 감사합니다.

...

종합 토론

오병일 (진보네트워크센터 대표)



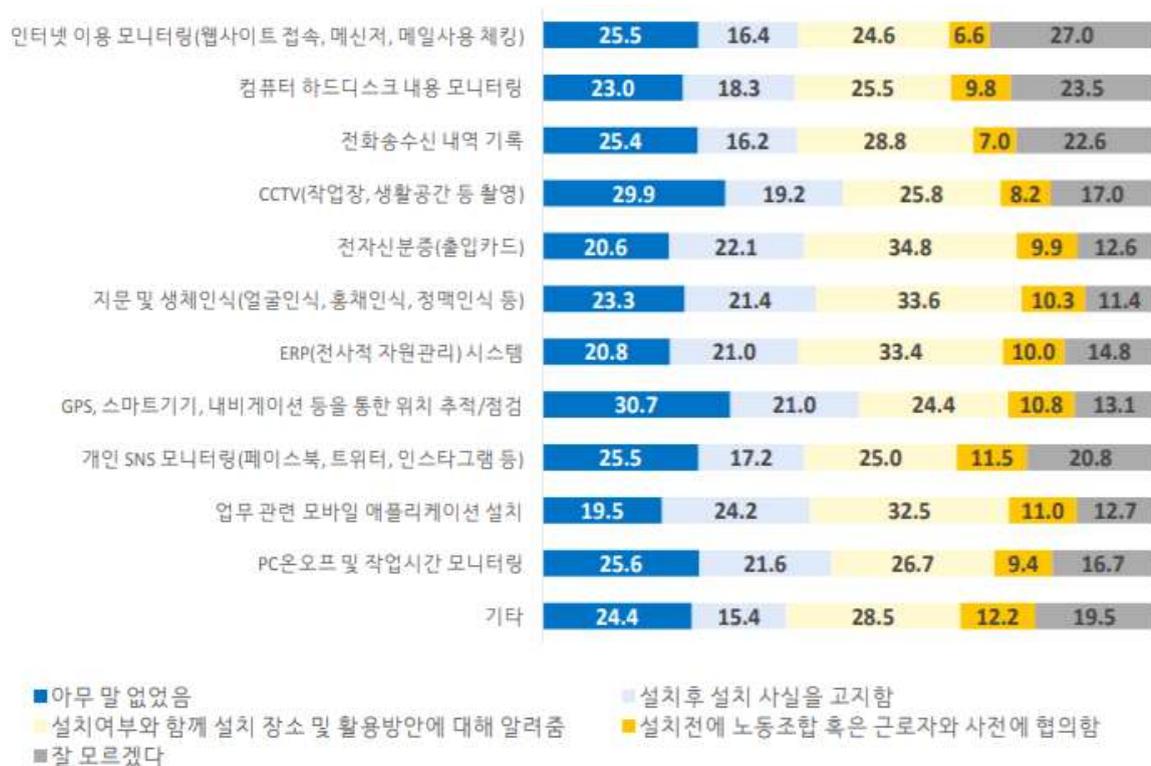
발제자와 함께 시민사회의 개인정보 보호법 개정 대안을 함께 논의한 입장이므로, 발제를 보완하는 방향에서 토론하고자 함.

1. 정보주체의 고지받을 권리

- 정보주체의 권리 보호를 위해 ‘투명성’은 매우 중요한 원칙임. 투명성이 보장되지 않아 개인정보의 처리 목적이 무엇인지, 자신의 개인정보가 어떻게 처리되고 있는지 인지하지 못할 경우, 개인정보 처리가 위법하게 이루어지는지 혹은 자신의 권리가 침해되는지 역시 인지하기 힘들 것임.

- 특히 취약한 정보주체라고 할 수 있는 노동자의 경우, 사내에서 다양한 전자기술을 통해 어떠한 개인정보가 수집되어 활용되는지 제대로 고지받지 못하고 있고, 노동자 개인정보 처리방침 역시 존재하지 않는 경우가 많은 것으로 나타났음.

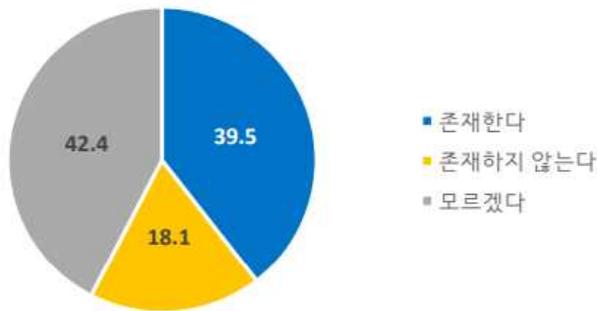
<디지털 전자기술 도입시 고지 및 협의 여부>



<디지털 전자기술 관련 노동자의 인지 정도>



<개인정보 처리방침 존재 여부>



- 개인정보 처리방침을 통해 개인정보 처리에 관한 정보를 제공하지 않는 것은 위법이지만, 현행 법률 역시 동의를 받을 때에만 개인정보 처리에 관한 정보를 고지하도록 하고 있는 한계가 있음. 따라서 투명성 강화를 위해서는 어떠한 법적 근거에 따라 개인정보를 수집하더라도 정보주체에게 고지하도록 할 필요가 있음.

2. 개인정보파일 등록의 예외 축소

- 제32조는 공공기관의 개인정보 파일을 보호위원회에 등록하도록 하고 있음. 그런데 제2항에서 일부 개인정보파일의 경우에는 그 등록을 면제하고 있음.

제32조(개인정보파일의 등록 및 공개) ① (생략)

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

- 국가 기밀의 경우 등록의 예외를 인정하더라도 제2호 및 제3호의 개인정보파일의 경우 등록을 면제하는 근거가 무엇인지 의문임.

- 이는 단지 해당 개인정보파일에 대한 국민의 알권리를 제한할 뿐만 아니라, 정보주체의 열람권도 제한할 수 있음. <개인정보보호 포털>에서 공공기관에 대한 열람등요구를 할 때 우선 개인정보파일 목록을 검색하도록 하고 있는데 검색 결과가 나오지 않기 때문임. 물론 해당 공공기관의 홈페이지에서 개인정보 열람신청을 할 수는 있으나 다른 공공기관에 비해 접근성이 떨어지는 것은 사실이며, 또한 어떠한 개인정보파일을 가지고 있는지 파악이 되지 않을 경우 열람을 신청하는 개인정보의 항목을 특정하는데 어려움을 겪을 수 있음.

- 최근 법무부-과기정통부의 출입국 심사 고도화를 명분으로 한 안면인식정보의 무단 제3자 제공과 관련하여 토론자의 피해 여부 확인을 위해 개인정보 열람신청을 하고자 하였으나, 개인정보 열람이 원활하게 이루어지고 있지 않음.

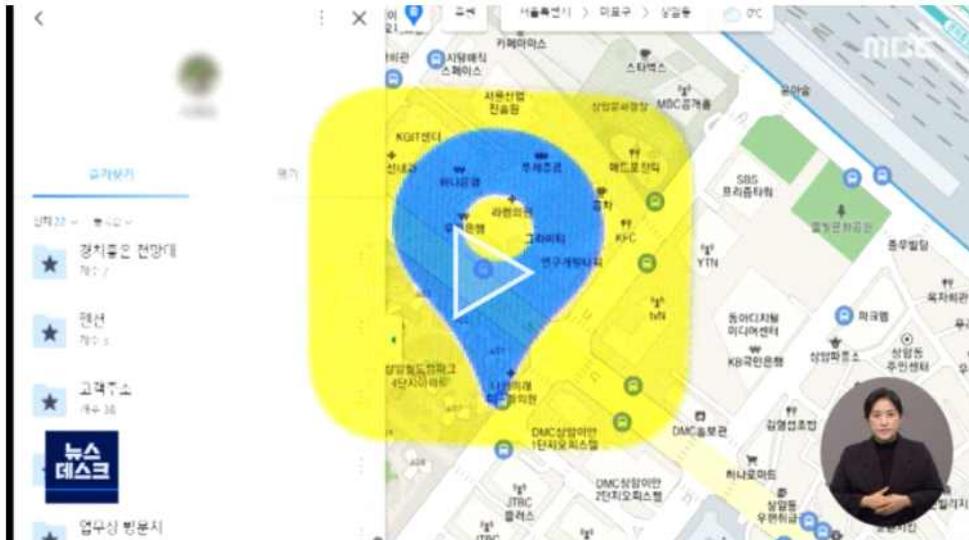
3. 개인정보보호 중심설계 및 기본설정

- 카카오맵 리뷰, 폴더 내용을 '공개'로 기본 설정 - 정보주체의 인식없이 민감한 개인정보 노출. 개인정보보호 기본설정이 고려되었다면 피할 수 있었던 문제임.

[단독] 군사 기밀·외도 사실까지...개인정보 '줄줄' 카카오프렌드 오맴

입력 2021-01-14 20:21 | 수정 2021-01-14 21:45

12 가 뒤 < >



출처 : MBC 뉴스, 2021.1.14.

https://imnews.imbc.com/replay/2021/nwdesk/article/6058233_34936.html

- 개인정보보호 중심설계 및 기본설정은 개인정보 보호원칙으로부터 자연스럽게 도출될 수 있는 원칙으로 개인정보 처리자에 추가적인 부담을 야기할 이유는 없음. 법에서 명확하게 이를 규정한다면 오히려 수범자들에게 명확한 지침을 제공해줄 수 있음.

- 개인정보보호위원회는 <인공지능(AI) 개인정보보호 자율점검표>(2021.5.31)에서 현행 법에 명시적인 규정이 없음에도 불구하고 '개인정보보호 중심설계(Privacy by Design)'를 기본원칙으로 제시하고 있음. 또한 이 원칙의 정착을 위해 한국디자인진흥원과 업무협약을 체결하기도 하였음.(2021.10.15) 2021-2023 개인정보보호 기본계획의 수립 원칙으로 개인정보보호 중심설계를 강조하기도 하였음. 개인정보보호법 2차 개정에서 이를 명확하게 반영하여 개인정보보호위원회의 여러 사업 및 지침의 원칙으로 수립할 필요가 있음.

4. 민감정보의 보호

- 현행 개인정보보호법은 시행령에서 규정하고 있는 민감정보에 대해서만 공공기관이 처리하는 경우 민감정보로 간주하지 않고 있음. 법에서 규정한 민감정보와 시행령에서 규정한 민감정보에 대해 이처럼 차이를 둘 합리적인 이유가 없음. 따라서 시행령의 단서 조항을 삭제하는 것도 하나의 방법이지만, 법 개정을 계기로 시행령에 규정된 민감정보를 법에 규정하는 것이 합리적일 것임.

시행령

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.

1. 유전자검사 등의 결과로 얻어진 유전정보
2. 「형의 실효 등에 관한 법률」 제2조제5호에 따른 범죄경력자료에 해당하는 정보
3. 개인의 신체적, 생리적, 행동적 특징에 관한 정보로서 특정 개인을 알아볼 목적으로 일정한 기술적 수단을 통해 생성한 정보
4. 인종이나 민족에 관한 정보

- 민감정보에 대해서도 ‘가명정보의 처리에 관한 특례’가 적용된다고 해석하는 것은 특별한 보호를 필요로 하는 민감정보의 특성을 무시하는 것임. 민감정보 역시 과학적 연구 목적 등으로 처리하는 것을 인정하더라도 (‘과학적 연구’의 개념을 어떻게 볼 것인가는 별론으로) 과학적 연구 목적의 처리 과정에서 보다 엄격한 보호가 이루어지도록 할 필요가 있음. 시민사회안에서는 제23조 개정에서 이를 별도로 규정하고 있지 않은데, 이는 민감정보의 과학적 연구 목적의 처리는 법률에 근거해서 처리해야 한다는 취지임.

...

종합 토론

이병남 (개인정보보호위원회 개인정보보호정책과 과장)



정보주체 관점의 개인정보 보호법 개정 방향

□ 개정안(정부안) 주요내용

- 정보주체가 디지털 시대로의 전환에 대응할 수 있도록 전송요구권 등 새로운 권리를 신설하고, 피해구제를 위한 분쟁조정제도를 실질화
- 개인정보 보호에 대한 실질적인 책임성 확보를 위해 형벌을 경제적 제재 중심으로 전환하고 시정명령 등 제도를 개선

< 개인정보보호법 개정안(정부안) 개정방향 >



□ 디지털 시대 정보주체의 권리 보장

- ① 개인정보 전송요구권(이동권) 도입
 - (필요성) 데이터 경제 활성화로 개인정보가 대량 수집·유통되고 있으나, 정보주체는 본인정보를 자기주도적으로 통제하는데 한계
 - (개정안) 본인정보를 본인 또는 제3자에게 전송 요구할 수 있도록 일반적 권리로서 개인정보 전송요구권(이동권) 신설
- ② 자동화된 결정에 대한 대응권 신설
 - (필요성) AI기술 발전 등에 따라 자동화된 결정이 광범위하게 활용되면서 특정인에 대한 편견 등 새로운 프라이버시 이슈 제기
 - (개정안) 인공지능 등을 이용한 자동화된 결정이 정보주체의 권리 또는 의무에 중대한 영향을 미치는 경우, 해당 결정을 거부하거나 설명 등을 요구할 수 있는 권리를 도입
- ③ 개인정보 분쟁조정제도 개선
 - (필요성) 조정신청 시 의무적으로 용해야 하는 기관은 공공기관에 한하며, 분쟁조정위에 사실 확인을 위한 조사권이 없어 적극적 조정에는 한계
 - (개정안) 분쟁조정 요청 시, 의무적으로 용해야 하는 대상을 공공기관에서 모든 개인정보처리자로 확대하고, 개인정보 분쟁조정위에 사실조사권 도입

□ 개인정보처리자의 책임성 강화

- ① 책임성 확보 방식 전환 : 형벌 중심에서 경제제재 중심으로
 - (필요성) 경미한 위반사항까지 형벌을 규정하고 개인정보 업무담당자 중심의 형벌 적용으로 기업 등 개인정보처리자 차원의 책임성 확보에 한계
 - (개정안) 정보통신서비스 제공자에게만 적용되던 형벌규정을 삭제하고, 개인정보 유출 시 형벌은 삭제하는 대신 과징금을 강화
 - 정보통신서비스제공자 대상 과징금을 개인정보처리자로 확대하고, 과징금 상한액 기준을 '위반행위 관련'에서 '전체 매출액'으로 전환

※ 다만, 과징금이 책임의 범위를 벗어나 과도하게 부과되지 않도록 '위반행위에 상응하는 비례성'과 '침해 예방에 대한 효과성'을 확보하도록 함

② 개인정보 침해 조사 및 제재 기능 강화

- (필요성) 시정명령 부과 요건이 지나치게 경직적이고 조사 거부 등에 대한 제재수준이 미흡
 - 개인정보취급자의 사적 이용 및 수탁자에 대한 제재근거 또한 부재
- (개정안) 시정명령 부과 요건을 합리화하고 조사 거부 등에 대한 과태료 상향
 - 개인정보취급자가 '업무상 알게 된 개인정보를 사적 목적으로 이용 시 처벌근거 마련, 수탁자도 과태료·과징금·형벌 등 제재대상에 포함'

③ 형식적인 동의제도 개선과 개인정보처리방침 평가제 도입

- (필요성) 복잡하고 경직적인 동의제도 운용으로 기업·기관 등 개인정보처리자는 합리적인 개인정보 처리 및 활용에 제약을 받고,
 - 정보주체 또한 복잡한 고지사항·절차 등으로 '동의의 형식화' 만연
- (개정안) 사전동의만을 강제하는 '동의 만능주의' 관행을 개선하고, '개인정보 처리방침 평가제'를 통한 보호수준 제고 및 사후 감독 강화
 - 계약 체결·이행의 개인정보 수집·이용 적법요건을 합리적으로 정비

④ 온-오프라인 이원화된 규제 일원화

- (필요성) 데이터 3법 개정 시, 정보통신망법의 정보통신서비스 제공자 대상 규정을 특례(제6장)로 단순 이전·병합
- (개정안) 정보통신서비스 특례규정을 폐지하고, 일반규정으로 일원화하여 모든 개인정보처리자에게 동일규범 적용 및 책임성 확보

- | |
|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <ul style="list-style-type: none">▶ (규정통합) 일반규정과 유사 중복되는 특례규정은 일반규정으로 통합·정비<ul style="list-style-type: none">▪ 수집·이용 동의, 만14세 미만 아동 개인정보수집, 유출 통지·신고제도 등▶ (적용확대) 특례에만 규정된 제도는 일반규정에 신설하여 전 분야로 확대<ul style="list-style-type: none">▪ 해외사업자의 국내대리인 지정, 이용내역 통지, 손해배상책임의 보장 등 |
|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|