개인정보보호법 시행령 개정안에 대한

BSA | The Software Alliance 의견서

2020년 5월 11일

BSA 소개 및 의견서 개요

BSA [1]는 먼저 개인정보보호법 시행령 개정안에 대한 협회의 의견을 전달할 수 있는 기회를 주신점에 대해 행정안전부에 감사의 말씀을 전합니다. BSA의 의견서는 정보 제공자(데이터 제공자)의 개인정보 및 기타 권리를 보호하면서 데이터의 유연성과 유용성을 향상시키는 수단으로 가명화된 개인 데이터의 활용을 향상시키기 위해 고안된 조치에 중점을 두고 있습니다.

BSA 회원사들은 타 사업체들을 지원하는 기술 기반 제품 및 서비스를 만드는 비즈니스 솔루션 제공 회사들입니다. 현재 협회의 회원사들은 클라우드 스토리지 서비스, 고객 관계 관리 소프트웨어, 인적 자원 관리 프로그램, 자격 증명 관리 서비스 및 협업 소프트웨어 등과 같이 비즈니스에 필수적인 기술들을 제공하고 있습니다. 이러한 소프트웨어 기업들은 개인정보를 보호하는 기술 및 제품을 제공하고 있으며, 이용자 데이터를 이용한 수익 창출에 의존하지 않는 비즈니스 모델들을 채택하고 있습니다. BSA 회원사들은 기업이 소비자의 신뢰를 얻고, 개인의 데이터를 책임감 있게 다루어야 한다는 것을 인식하고 있습니다.

따라서, BSA는 한국의 개인정보보호법 및 관련 법안의 개정을 포함하여 한국이 4차 산업 혁명을 선도할 수 있도록 지원하는 정부의 노력을 지지하고 환영합니다. BSA는 전 세계 여러 정부와 활발한 교류를 통해 쌓은 풍부한 경험을 토대로 데이터 기반의 기술이 책임 있게 활용될 수 있도록 협회와 회원사 차원의 지원을 제공하고 소비자의 개인정보에 따른 사생활을 보호하며 소비자에게 강력한 권리를 제공할 수 있도록 효과적이고 국제적으로 상호 운용 가능한 법률 시스템을 장려하고 있습니다.[2] BSA 회원사는 기업

[1] BSA | Software Alliance(www.bsa.org)는 각국 정부를 대상으로 세계 시장에서 전 세계 소프트웨어 업계를 대변하는 협회입니다. 세계의 가장 혁신적인 기업들이 회원사로 참여하여 경제에 활기를 불어넣고 현대 생활을 향상시키는 소프트웨어 솔루션을 만들어 내고 있습니다. 현재 워싱턴 DC에 본사를 두고 총 30개가 넘는 국가에서 활동하고 있는 BSA는 합법적 소프트웨어 사용을 증진하는 프로그램을 지지하는 활동을 선도적으로 진행중에 있으며, 기술 혁신을 촉진하고 디지털 경제의 성장을 추진하는 공공 정책을 지지합니다.

BSA의 회원사는 다음과 같습니다: Adobe, Amazon Web Services, Atlassian, Autodesk, AVEVA, Bentley Systems, Box, Cadence, Cisco, CNC/Mastercam, IBM, Informatica, Intel, MathWorks, Microsoft, Okta, Oracle, PTC, Salesforce, ServiceNow, Siemens, Industry Software Inc., Sitecore, Slack, Splunk, Synopsys, Trend Micro, Trimble Solutions Corporation, Twilio, Workday

[2] https://www.bsa.org/files/policy-filings/A4_2018_BSA_Global_Privacy_Best_Practices.pdf에서 BSA의 글로벌 개인정보

의 역량 강화에서부터 원격 근무로의 전환에 이르는 사회적, 경제적 목표를 발전시킬 수 있는 기술을 제공하고, COVID-19 연구원 및 대응 이해관계자들이 전염병 확산에 대처할 수 있도록 운영의 연속성을 보장하고 있습니다. 행정안전부가 목표를 달성하는 데 있어 BSA의 의견이 도움이 되기를 희망합니다.

부록

- 부록 1: 행정안전부 요청한 형식에 따른 각 조항 별 의견.
- 부록 2: 국제 표준: 개인정보 보호법에서 데이터 관리자와 처리자의 차이점.[3] 영문과 국문 버전.

권고사항

전반적 논평

전 세계적으로 국가들이 개인정보 보호법 및 규정을 개발하거나 현대화함에 있어, 이러한 규정들이 국제적으로 상호운용 가능한 방식으로 소비자에게 효과적인 개인정보 보호 기능을 제공하도록 설계되고, 빠르게 발전하는 기술 및 비즈니스 모델들을 포용할 수 있는 유연성을 갖추어 고급 데이터 분석 및 인공지능(**AI**)과 같은 유망한 신기술 분야에서 혁신과 발전을 촉진하는 것이 중요합니다.

BSA는 개인 데이터 수집 및 데이터 이용의 투명성을 제고하는 정책을 지원하고, 소비자가 자신의 데이터를 제어할 수 있도록 하며, 기업이 강력한 보안적 의무를 가져야 한다는 의견에 동감하며, 합법적인 비즈니스 목적에 따른 데이터 이용을 장려합니다.[4]

이와 관련하여 개인정보보호법 시행령 개정안은 개인정보보호위원회(보호위원회)를 격상하고, 개인 데이터, 특히 가명화 된 데이터를 보다 유연하게 이용할 수 있도록 장려하고 있습니다. BSA는 행정안전부가 개인정보보호법 시행령을 마무리할 때, 위와 같은 목표를 강화하고 지원할 것을 요청 드립니다.

데이터 관리자 및 데이터 처리자의 구분

먼저, 한국의 개인정보보호법은 국제적으로 합의된 방식인 법의 적용을 받는 주체의 유형을 구분하여 정의하는 방식의 법률과 동떨어져 있습니다. 특히, 개인정보보호법 제2조 5항에 정의된 "개인정보 관리자(**데이터 관리자**)"와 "개인정보 처리자(**데이터 처리자**)" 사이에 명확한 구분이 없습니다. 세계의 여러 개인정보보호법에 있어서 이러한 근본적인 차이점을 구분하는 것은 개인에 대한 데이터를 언제와 어떻게 수집하고 이용하기로 결정한 기업(데이터 관리자)과 다른 회사를 대신하여 데이터를 처리하는 기업(데이터 처리자)을 구별하는 중요한 역할을 합니다.

데이터 관리자와 데이터 처리자를 구분해야 하는 이유는 두 주체 모두 개인정보를 보호하는 데 중요한 역할을 하기 때문입니다. 이에 따라 개인정보보호법은 두 유형의 개체를 모두 정의하고 이들의 의무가 소비자 데이터를 보호하는 역할을 반영하도록 해야 합니다. 예를 들어, 데이터 관리자는 일반적으로 소비자와 상호 작용하고 소비자의 데이터를 수집할 시기와 이유를 결정합니다. 따라서 개인정보보호법은 일반적으로 데이터 처리에 대한 동의를 얻기 위한 요구 사항 및 소비자의 권리 요청을 존중할 의무를 포함하여 소비자 관련 의무를 데이터 관리자에게 부과합니다.

반대로, 데이터 처리자는 일반적으로 개별 데이터 제공자와 직접적인 관계가 없고, 대부분 기본 데이터를 보지 않은 채 데이터 관리자를 대신하여 데이터를 처리합니다. 실제로, 데이터 처리자는 관리자를 위해 저장하거나 처리하는 데이터에 액세스하는 것이 계약상 금지될 수 있습니다. 그러므로 데이터 처리자는 합리적인 보안 조치를 제정하는 등 보유한 데이터를 보호하는 중요한 의무를 져야 합니다. 그러나

보호 모범 실천사례를 참조할 수 있다.
한국어: https://www.bsa.org/files/policy-filings/A4_2018_BSA_Global_Privacy_Best_Practices_ko.pdf

[3] https://www.bsa.org/files/policy-filings/03032020controllerprocessor.pdf
한국어: https://www.bsa.org/files/policy-filings/kr05042020controllerprocessor.pdf

[4] *BSA 글로벌 개인정보 보호 모범 실천사례. 전게서. cit.*

데이터 처리자에게 소비자 대상 의무를 부과하게 되면, 궁극적으로 소비자의 개인정보를 침해할 수 있습니다. 그 이유는 처리자가 자신이 모르는 개개인을 식별하기 위해 검토하지 않아도 되었을 (대부분의 경우 검토할 수 없는) 많은 양의 데이터를 검토하고, 법적 요구 사항을 충족하기 위해 데이터에 접근해야 할 수도 있기 때문입니다.

개인정보보호법은 데이터 관리자와 데이터 처리자를 명확하게 구분하지 않기 때문에, 현 상태에서는 행정안전부가 개인정보보호법 시행령에서 데이터 관리자에게 부과된 광범위한 의무에 대해 신중하게 검토해야만 합니다. 따라서 BSA는 행정안전부가 개인정보보호법 시행령을 데이터 제공자 및 관련된 데이터를 인지하고 그러한 데이터의 처리 방법에 대해 의사 결정을 내리는 데이터 관리자에만 광범위한 의무를 적용하도록 하고, 데이터 처리자에게는 해당 의무를 면제하는 방향으로 작성하시기를 권고 드립니다. 위에서 언급한 바와 같이, 데이터 관리자에 대한 의무를 데이터 처리자에게 확장하는 경우 개인정보의 보안을 강화하기보다 약화시킬 우려가 있습니다. 애초에 데이터 제공자가 누구인지 또한 이러한 데이터가 무엇을 수반하는지 알 수 없도록 설계된 데이터 처리자는 관리자 수준의 법적 요구 사항을 준수하기위해 불가피하게 데이터 제공자의 정보에 접근해야 할 것입니다.

행정안전부가 개인정보보호법의 의무에서 데이터 처리자를 배제해야 하는 사례는 개인정보보호법 5장, 제35-37조 및 개인정보보호법 시행령 개정안(제48조 4항, 제48조 5항, 제48조 7항 등)에 명시된 소비자 권리, 그리고 데이터 침해와 관련하여 데이터 제공자에게 통지할 의무(개인정보보호법 제34조, 개인정보보호법 법령 제48조 3항)등 입니다. 이와 같이 권고하는 이유는 위에서 언급했듯이 데이터 처리자(예: 클라우드 컴퓨팅 서비스 제공 업체)가 특정 데이터 주체에 관한 정보를 가지고 있지 않을 수도 있고, 어떤 데이터가 개인 데이터이며 이들 법률에 적용되는지조차 모를 수 있기 때문입니다. 실제로, 다수의 데이터 처리자는 고객을 대신하여 처리하는 데이터의 세부 사항을 인식하지 않아야 하는 계약상의 의무를 지고 있습니다. 따라서 소비자 권리를 보호할 의무는 데이터 관리자에 부과되어야 하며, 데이터 관리자는 제3자인 데이터 처리자가 이러한 데이터를 어떻게 관리하는 지에 대한 책임을 지는 것이 바람직한 구조입니다.

바람직한 거버넌스 및 이해관계자 자문

개정된 개인정보보호법은 개인정보보호위원회에 구속력 있는 규칙, 요구 사항 및 표준을 개발할 수 있는 무수한 기회와 권한을 부여하고 있습니다.[5]

개인정보보호법 법령상으로 보호위원회가 확립할 표준과 지침은 국제적으로 인정된 표준 및 새로운 모범 사례와 일치하는 방식으로 개발되어야 한다는 점을 명확하게 명시하는 것이 중요합니다. 새로운 기술 및 비즈니스 프로세스와 일치하지 않는 지나치게 규범적인 요구 사항을 방지하기 위해 규제는 성과 지향적이고 리스크에 기반이 되어 만들어져야 합니다.

새로 일원화되는 보호위원회가 목표를 달성하도록 지원하기 위해서는 개인정보보호법 시행령에 따라 보호위원회가 공개적이고 투명한 자문을 수행하고 국내외 기업을 포함한 민간 부문 이해관계자와 긴밀히 협력하도록 해야 합니다. 이런 협력을 통해 보호위원회가 최신 기술 개발 및 국제 모범 사례를 인지하는데 큰 도움이 될 것이며, 혁신을 조성하고 지능 정보 사회를 창조하는 동시에 한국인의 사생활과 개인정보 모두를 효과적으로 보호할 수 있게 될 것입니다.

국경 간 데이터 전송

국경 간 데이터를 전송할 수 있는 능력은 현대 디지털 경제의 원동력이기 때문에 개인정보보호법과 해

[5] 예를 들어, 제12조는 보호위원회에 개인정보 처리 표준, 개인정보 유출 유형, 예방 조치에 관한 표준 개인정보보호 지침을 수립할 권한을 부여한다. 제13조는 보호위원회가 개인정보 보호 마크의 도입 및 촉진을 포함한 자기 규제 활동을 촉진하고 지원하기 위한 정책을 수립할 것을 요구한다. 보호위원회는 가명화된 정보의 조합(제28조 3항), 가명화된 정보에 대한 정보를 저장, 관리 및 기록하는 절차 및 방법에 관한 규칙을 규정할 것이다(제28조 4항). 보호위원회는 개인정보 관리자의 데이터 처리 및 기타 데이터 보호 관련 조치가 법률을 준수하는지 여부를 인증하고 해당 인증을 관리하도록 설계된 개인 및 기관의 자격을 결정할 수 있다(제32조 2항). 또한 보호위원회는 개인정보 영향평가(PIA)를 수행할 기관을 지정하고 전문가를 육성하며 개인정보 영향평가에 대한 기준을 개발 및 보급할 책임이 있다(제33조).

당 법의 시행을 통해 기업이 책임감 있게 데이터를 국제적으로 전송할 수 있도록 해야 한다는 점을 강조드리고 싶습니다.

개인 데이터의 국경 간 전송이 규제적 요구 사항에 의해 제한되는 경우, 이는 데이터 보호 목표의 발전을 제한할 뿐만 아니라 의도하지 않은 결과를 유발하게 됩니다. 이로 인해 기업의 운영이 방해되고 한국에 서비스를 제공하는 비용이 의도치 않게 상승함으로써 한국에서 사업 기회를 크게 박탈하여 다른 국가와 비교해 사업 경쟁적 열위에 놓이게 할 것입니다.

구체적 권고사항

다음 섹션에서는 개인정보보호법 시행령 개정안의 특정 조항을 조정하기 위한 구체적 권고사항에 대해 설명 드리겠습니다. 이들 권고사항은 부록 1의 표에 요약되어 있습니다.

다른 개인정보 관리자 등이 보유한 가명화 된 정보의 조합

개인정보보호법 제28조 3항 1호에 따르면, 다른 개인정보처리자가 처리한 가명화 된 정보의 조합은 보호위원회 또는 다른 정부 기관이 지정한 ***전문기관이 수행할 것을*** 요구한다. 이는 법률상 매우 유감스러운 요구사항으로 판단됩니다. 개정안에서 명시된 목표 중 하나는 가명화 된 개인정보를 이용하여 데이터 분석을 더욱 향상시키고 촉진하여 중요한 발견과 성과를 도모하는 것이었습니다.

이 요구사항의 목적은 조합 및 분석 과정에서 가명화된 데이터를 재식별하는 가능성을 최소화하는 것으로 보입니다. 그러나, 이는 별도의 "전문가 데이터 조합 기관"(**EDCA**)이 가명화 데이터 조합 프로세스를 수행할 것을 요하고 있으므로, 기업의 효과적인 데이터 분석 및 기업 간 협력에 중대한 장애가 될 수 있습니다.

BSA는 행정안전부가 개인정보보호법에 따라 개인정보보호법 시행령의 개정안을 가능한 유연한 방식으로 작성해 주실 것을 권고 드립니다. 이는 각 당사자가 법에 준거하여 데이터를 보호하도록 위탁하는 계약 약정에 따라 연구 및 과학적 목적뿐만 아니라 상업적 목적으로도 가명화된 데이터 세트를 공유 및 결합할 수 있도록 하기 위함입니다. 개인정보보호법에서 인식한 바와 같이, 가명화된 데이터에 포함된 개인을 식별하지 않고 가명화된 데이터를 처리하고 조합하는 데에는 여러 가지 목적이 있습니다. 여기에는 통계 목적, 과학 연구 및 공익을 위한 보관 목적이 포함됩니다.

예를 들어, COVID-19 전염병에 효과적으로 대응하려는 노력은 기업과 정부가 민감한 개인정보를 사생활을 보호하는 방식으로 활용해서 효율성을 극대화하는 것이 중요하다는 점을 가장 뚜렷하게 보여주었습니다. 이러한 관점에서, 전문 정부 기관을 통해 이러한 분석을 수행하기 위한 추가 요구사항은 잘못된 방향으로 나아가는 것으로 사료됩니다.

더욱 우려되는 부분은 개인정보보호법 시행령 개정안 제29조 2항에서 특정 상황을 제외하고는 EDCA의 승인에 따라, 보호위원회가 지정한 대로 EDCA가 제공한 지정된 물리적 공간(**분석 공간**)에서만 데이터 관리자가 이러한 데이터 조합의 결과를 볼 것을 요구하고 있다는 점입니다. BSA는 행정안전부가 분석 공간을 관리자가 순전히 자발적인 목적으로 활용할 수 있도록 제29조 2항 3호를 개정할 것을 촉구합니다.

BSA는 또한, 개인정보보호법 시행령에서 한정한 물리적 분석 공간 대신 클라우드 컴퓨팅 인프라에 기반한 별도 논리적 분리 및 "가상" 공간에서 분석을 할 수 있게 시행령을 개정해 주실 것을 요청 드립니다.

BSA는 해당 의견서를 통해 대한민국 지능 정보 사회 육성이라는 목표를 달성하고 고급 데이터 분석의 혁명으로부터 혜택을 얻도록 지원하고자 합니다. 고급 데이터 분석, 데이터 공유 및 데이터 조합은 개인정보를 보호하는 방식으로 수행 가능합니다. **이 문제의 해결방안은 복잡한 방식에서 벗어나, 데이터 관리자가 누구이며, 어디서, 어떤 방식으로 개인의 데이터를 처리하건 간에 개인 데이터의 보호에 대한 책임을 데이터 관리자가 지도록 하는 것입니다.**

개인정보의 추가 이용/제공 등에 관한 기준

개인정보보호법은 "개인정보처리자는 당초 수집 목적과 합리적으로 관련된 범위에서" 데이터 주체의 동의 없이 추가 용도를 위해 데이터 관리자가 개인정보를 이용(개인정보보호법 제15조 3항)하거나 개인정보를 제공(개인정보보호법 제17조 4항)할 수 있도록 허용하고 있습니다.

개인정보보호법 시행령 개정안 제14조 2항은 데이터 관리자가 "합리적으로 관련된 범위에서 "에 한에서 데이터를 이용하거나 제공하는 조건에 맞도록 충족되어야 하는 4가지 조건을 명시하고 있습니다. 그 조건은 다음과 같습니다.

1) 개인정보를 추가적으로 이용하려는 목적이 당초 수집 목 적과 상당한 관련성이 있을 것
2) 개인정보를 수집한 정황과 처리 관행에 비추어 볼 때 추 가적으로 이용할 수 있을 것으로 예측 가능할 것
3) 개인정보의 추가적 이용이 정보주체 또는 제3자의 이익을 부당하게 침해하지 아니할 것
4) 가명처리를 하여도 추가적 이용 목적을 달성할 수 있는 경우에는 가명 처리하여 이용할 것.

BSA는 데이터 관리자가 개인정보를 수집하는 목적을 데이터 주체에게 알리고 해당 설명, 거래 상황 또는 데이터 주체의 합리적인 기대와 일치하는 방식, 또는 데이터가 수집된 원래 목적과 양립하는 방식으로 데이터를 이용해야 한다는 데 동의합니다. 그러나 개인정보보호법 시행령 개정안에 현재 사용된 언어는 상당히 제한적인 것으로 보여집니다.

"합리적으로 관련된" 이라는 개념이 데이터가 처음 수집된 상황에 따라 다르다는 것을 명확히 하기 위해, 제14조 2항의 첫 부분을 아래와 같이 수정하실 것을 제안 드립니다.

> *개인정보보호법 제15조 3항 및 제17조 4항에 따른 대통령령으로 정하는 경우는* ***데이터가 수집된 원래 목적과 이용이 양립한다는 것에 기반해 데이터 주체의 합리적인 기대를 고려하여*** *다음의 모든 조건을 만족하는 경우를 말한다. 이 경우 개인정보보호법의 제17조 4항의 목적상 "이용"은 "제공"으로 간주해야 한다.*

처음 두 가지 조건 중 추가적 이용이 원래 수집 목적과 "합리적으로 관련"되어 있다는 첫 번째 조건은 개인정보보호법에 명시된 의무와 가장 일치하는 것으로 보입니다. 추가적 이용이 "예측 가능"하다는 두 번째 조건은 수집 당시 예측 가능한 이용이 이러한 수집에 대한 규제와 합리적으로 관련될 수 있기 때문에 이도 마찬가지로 "합리적으로 관련된" 예로 간주될 수 있습니다. 그러나 데이터의 추가적 이용이 초기 수집과 명백하게 "합리적으로 관련되어" 있지만, 상황이 바뀌는 경우 "예측할 수 있는" 상황이 아닌 경우가 발생할 수 있습니다.

또한, 세번째 조건은 데이터 처리자가 추가적 이용을 위해 충족시켜야 하는 사항이 명시되어 있습니다. "... 데이터 주체 **또는 제3자의** 이익을 부당하게 침해하지 않을 것", "제3자"의 이익을 추가 사용에 대한 의무조건으로 포함시키는 것은, 데이터 관리자가 「…데이터 주체에 불이익이 발생했는가를…」(제15조 제3항 및 제17조 제4항)만 고려해야 한다는 조문의 범위를 넘어 서게 됩니다. 또한, 제3자의 "넓은" 범위로 인해 이익이 침해되지 않도록 데이터 관리를 요구하는 것은 일일이 확인하기가 어려우며 따라서 개인정보보호법 개정 취지에 합법적인 추가 사용을 더욱 제한할 수 있는 매우 광범위하고 정의되지 않은 표준이 될 것으로 사료됩니다.

따라서 다음과 같이 조건 1)과 2)를 결합할 것을 권고 드리며, 3)의 "제 3자"를 삭제해 주실 것을 제언 드립니다.

1) *개인정보를 추가로 이용하는 목적은* ***개인정보가 수집된 상황과 관행을 고려하여 개인정보가 수집된 원래 목적과 합리적으로 관련되거나 데이터 주체가 이를 예측 가능한 경우여야 한다.***

~~2) *개인정보의 추가 이용은 개인정보가 수집된 상황과 관행에 비추어 예측할 수 있다.***

3) *개인정보의 추가적 이용이 정보주체* ~~***또는 제3자의***~~ *이익을 부당하게 침해하지 아니할 것*

또한 BSA는 14조 4항에 명시된 "가명화된 데이터가 이용될 수 있다면 데이터는 가명화되어야 한다"는 조항에 우려가 있습니다. 이 조건은 개인정보보호법의 의도와 일치하지 않을 수 있으며 실제로 해석하거나 구현하기 어려울 수 있습니다. BSA 역시 가명화된 정보의 이용을 장려하는 것이 중요하다는 점을 인식하고 있습니다. 하지만, 이러한 조항은 데이터를 처리하는 것에 기반해 결과의 정확성에 부정적인 영향을 미치거나 데이터의 가치를 데이터 주체 또는 데이터 관리자에게 감소시키는 상황이 발생할 수 있다.

따라서 가명화된 데이터가 이용될 수 있는 경우에는 이를 요구하는 대신 개인정보보호법 법령 제14조 2항의 초안을 수정하여 데이터 관리자가 데이터 가명화를 고려하도록 할 것을 권고 드립니다. 이 경우 데이터 관리자는 가명화된 데이터를 이용하여 개인정보 보호를 강화하거나, 차선의 처리 결과가 데이터 주체 또는 데이터 관리자에게 요하는 비용 사이에서 가능한 비용 또는 절충안을 고려해야 할 것입니다. 따라서 14조 4항을 다음과 같이 수정할 것을 권고 드립니다.

> ***4. 개인정보 관리자는 가명화된 개인정보로*** *추가 이용의 목적을 달성할 수 있는지 고려해야 한다.* ***그리고 만약에 목적에 부합할 시*** *가명화된* ***개인정보에 의존할 것****.*

민감한 정보의 범위

개인정보보호법 시행령 개정안 제18조 3항은 개인정보보호법 제23조에 따라 "민감한 개인정보"로 지정된 정보 목록에 "개인의 신체적, 생리적, 행동 적 특징에 관한 정보로서 특정 개인을 알아볼 목적으로 일정한 기술적 수단을 통해 생성한 정보" 정의하였습니다. BSA는 이들 범주가 실질적으로 너무 광범위하므로 행정안전부가 이 규정의 범위를 자연인을 고유하게 식별할 목적으로 이용되는 특정 생체 정보로 크게 좁히는 방안을 고려할 것을 권고 드립니다.

처벌

개인정보보호법 제28조 6항은 가명화된 데이터를 개인을 식별하는 방식으로 처리하여 개인정보보호법을 위반하는 데이터 관리자에 대해 최대 총 판매액의 3%의 벌금을 부과하고 있습니다. 마찬가지로 개인정보보호법 제39조 15항은 개인정보보호법의 특정 금지 사항을 위반하는 정보 통신 서비스 제공 업체에 대해 최대 총 수익의 3%의 벌금을 부과합니다.

개인정보보호법 시행령 개정안 제29조 6항 4호 및 제48조 10항 4호는 개인정보보호법 시행령 개정안의 표 1-3 및 표 1-5를 참조하여 이들 벌금을 계산하는 방법을 명시하고 있습니다.

법을 고의 또는 과실로 위반하는 사례를 효과적으로 억제해야 합니다. 그러나 개인정보보호법 위반에 대한 구제 및 처벌은 그 위반으로 인한 피해에 비례하여 효과적으로 이루어져야 한다는 점을 강조하는 것이 중요합니다.

대부분의 경우 자신의 행동이 개인정보보호법을 위반할 수 있다는 통지나 경고를 받은 기업은 자신의 행동을 자발적으로 시정할 것입니다. 결과적으로, 개인정보보호법 시행령 개정안은 벌금을 부과하기 전에 데이터 관리자 및 정보 및 통신 서비스 제공 업체가 보호위원회의 지침, 권고 또는 명령에 따라 조치를 이행할 수 있는 적절한 기간을 제공해야 합니다. 벌금은 비즈니스 운영자가 적시에 적절한 조치를 취하지 않는 경우에만 적용해야 하도록 해야 합니다.

벌금이 부과되는 경우, 적절한 수단으로는 개인이 겪는 경제적 피해를 보상하기 위한 금전적 구제책 제공, 향후 위반을 방지하기 위해 맞춤형 행동 기반 구제책을 부과하는 등 방안이 도입할 수 있을 것입니다.

결론

BSA는 해당 의견서를 행정안전부에 제공할 수 있는 기회를 얻어 기쁘게 생각합니다. BSA는 한국의 개인정보보호법 및 데이터 관련 사항을 현대화하려는 정부의 노력을 지지하며, 개인정보보호법 및 개인정

보보호법 시행령에 따라 새로운 책임을 맡은 보호위원회와 협력할 것을 기대하고 있습니다. BSA에서 드리는 의견이 한국의 4차 산업 혁명으로의 전환 과정과 지능 정보 사회를 구축하기 위한 목표를 달성하려는 노력에 도움이 되길 바랍니다.

의견서 관련 대한 질문이나 별도의 의견이 있으실 경우 언제든지 문의주기 바랍니다. 추가 논의도 가능하며, 추후 다른 정부 관련 업무도 지원할 기회가 있기를 고대하고 있겠습니다.

BSA | 소프트웨어 연합

부록 1 : 행정안전부 요청한 형식에 따른 각 조항 별 의견

개정안	동의 여부	이유
제29조의2(개인정보처리자 간 가 명정보의 결합 등) 1. 법 제28 조의3제1항에 따른 전문기관(이 하 “결합전문기관”이라 한다)에 가명정보의 결합을 신청하려는 개인정보처리자(이하 “결합신청자”라 한다)는 보호위원회가 정하여 고시하는 결합신청서를 해당 결합전문기관에 제출하여야 한다. 2. 결합전문기관은 특정 개인을 알아볼 수 없도록 보호위원회가 정하여 고시하는 절차와 방법에 따라 가명정보를 결합하여야 한다. 이 경우 보호위원회는 결합전문기관이 특정 개인을 알아볼 수 없도록 하는데 필요한 지원 업무를 한국인터넷진흥원이 수 행하도록 할 수 있다. 3. 결합신청자는 보호위원회가 정하여 고시하는 바에 따라 결 합전문기관에 설치된 안전성 확 보에 필요한 기술적 · 관리적 · 물 리적 조치가 된 공간(이하 “분석공간”이라 한다)에서 제2항에 따라 결합된 정보를 분석할 수 있다. 4. 제3항에도 불구하고 분석공간에서는 결합 목적을 달성하기 어렵거나 분석공간의 이용이 어려운 경우로서 결합신청자가 제2항에 따라 결합된 정보의 반출을 신청하는 경우, 결합전문기관은 개인을 다시 알아볼 가능성 등을 고려하여 보호위원회가 정하여 고시하는 바에 따라 평가한 후 반출을 승인할 수 있다.	동의하지 않음	BSA는 가명화된 데이터의 조합과 이용을 위한 정책 입안을 지지합니다. 그러나 행정안전부가 개인정보보호법 시행령을 개정을 통해 제3자 전문가 데이터 결합 기관을 통해 데이터를 결합시키도록 요구하는 것이 아니라 당사자들 간의 계약상 약정에 따라 상업적으로 관련되는 가명성 및 관련 데이터의 결합을 허용할 것을 촉구합니다. 또한 제29조의2 3항과 4항에 명시된 데이터 분석을 위한 물리적 공간은 지극히 자발적인 의지로 활용 가능하도록 분명히 명시하는 개정을 해주 실 것을 촉구합니다. BSA는 또한, 개인정보보호법 시행령에서 한정한 물리적 분석 공간 대신 클라우드 컴퓨팅 인프라에 기반한 별도 논리적 분리 및 “가상” 공간에서 분석을 할 수 있게 시행령을 개정해 주실 것을 요청 드립니다. 아울러 결합된 데이터 세트를 반출하기 위해 EDCA의 승인을 받아야 하는 요건이 남아 있는 경우, 개인정보보호법 시행령에 a) 특별한 사유가 없는 한 EDCA가 반출 요청을 승인한다, b) EDCA가 그러한 요청을 거부할 경우의 근거를 명시한다, c) 신청자에게 거부권을 행사할 법적 근거를 추가 명시해 주실 것을 요청 드립니다. 이러한 권고안의 목적은 서로 다른 데이터 관리자를 통해 결합된 가명 데이터 세트를 분석할 때를 포함하여, 일반적으로 데이터 분석을 수행하는 개인정보 보호 수단을 용이하게 하기 위함입니다.

제14조의2(개인정보의 추가적인 이용·제공 기준 등) 법 제15조 제3항 및 법 제17조제4항에서 “대통령령으로 정하는 바”란 다 음 각 호의 사항을 모두 충족하는 경우를 말한다. 이 경우 법 제17조제4항에 관하여는 ‘이용을 ‘제공으로 본다. 1. 개인정보를 추가적으로 이용하려는 목적이 당초 수집 목 적과 상당한 관련성이 있을 것 2. 개인정보를 수집한 정황과 처리 관행에 비추어 볼 때 추 가적으로 이용할 수 있을 것으로 예측 가능할 것 3. 개인정보의 추가적 이용이 정보주체 또는 제3자의 이익을 부당하게 침해하지 아니할 것 4. 가명처리를 하여도 추가적 이용 목적을 달성할 수 있는 경우에는 가명처리하여 이용할 것	동의하지 않음	개인정보법 시행령 개정안은 "합리적으로 관련된" 이란 개념을 데이터 제공자와 데이터 관리자의 관계에 따라 조건화됨을 명확히 구분해야 합니다. 아래 제14조의 2에 대한 권고사항을 참고 부탁드립니다. 더욱이, "예측 가능한"과 "합리적으로 관련된"이라는 용어는 유사하며, "예측 가능한"은 별도의 추가 조건이 아닌 "합리적으로 관련됨"을 결정하기 위한 하위 요인 집합으로 간주될 수 있으므로, 아래 기술한 바와 같이 제 1)항과 2)항을 결합하는 것을 권고 드립니다. 또한, “제3자”를 삭제해 시켜 주시어 개념이 너무 넓고, 불명확 한 점을 해소해 개인정보보호법의 범위내에서 추가적 활용을 활성화 시켜 주시길 요청드립니다. 마지막으로, 데이터 관리자들은 이용 가능할 때 가명화된 정보를 이용하도록 권장할 수 있지만, 개인 데이터의 가명을 수시로 **요구**할 경우 개인정보보호법 제15조 제3항 및 제17조 제4항과 일관되지 않으며, 이는 데이터 이용에 도움이 되지 않습니다. 그러므로, 개인정보보호법 시행령을 개정하여 데이터 관리자가 이용 가능한 경우 가명 데이터를 이용하도록 권장하도록 하고, 가명정보의 이용으로 발생하는 단점이 개인 정보보호 강화의 이익을 초과하지 않을 시에도 가명화된 데이터를 이용하도록 권장할 것을 제안드립니다. 개인정보보호법 시행령 개정안 제14조 2항의 첫 부분을 아래와 같이 수정하실 것을 권고 드립니다. 개인정보보호법 제15조 3항 및 제17조 4항에 따른 대통령령으로 정하는 경우는 **데이터가 수집된 원래 목적과 이용이 양립한다는 것에 기반해 데이터 주체의 합**

		리적인 기대를 고려하여 다음의 모든 조건을 만족하는 경우를 말한다. 이 경우 개인정보보호법의 제17조 4항의 목적상 "이용"은 "제공"으로 간주해야 한다. 1) 개인정보를 추가로 이용하는 목적은 **개인정보가 수집된 상황과 관행을 고려하여 개인정보가 수집된 원래 목적과 합리적으로 관련되거나 데이터 주체가 이를 예측 가능한 경우여야 한다.** ~~**2) 개인정보의 추가 이용은 개인정보가 수집된 상황과 관행에 비추어 예측할 수 있다.**~~ 3) 개인정보의 추가적 이용이 정보주체 ~~**또는 제3자의**~~ 이익을 부당하게 침해하지 아니할 것 4) **개인정보 관리자는** 가명화된 개인정보로 추가 이용의 목적을 달성할 수 있는지 **고려해야 한다. 그리고 만약에 목적에 부합할 시** 가명화된 **개인정보에 의존할 것.**
제18조(민감정보의 범위) 1. ~ 2. (현행과 같음) 3. 개인의 신체적, 생리적, 행동 적 특징에 관한 정보로서 특정 개인을 알아볼 목적으로 일정한 기술적 수단을 통해 생성한 정보 4. 인종이나 민족에 관한 정보 로서 해당 정보의 처리 목적이나 상황에 비추어 개인을 부당하게 차별할 우려가 있는 정보	동의하지 않음	개인정보보호법 시행령 개정안 제18조 3항은 개인정보보호법 제23조에 따라 "민감한 개인정보"로 지정된 정보 목록에" 개인의 신체적, 생리적, 행동 적 특징에 관한 정보로서 특정 개인을 알아볼 목적으로 일정한 기술적 수단을 통해 생성한 정보" 정의하였습니다. BSA는 이들 범주가 실질적으로 너무 광범위하므로 행정안전부가 이 규정의 범위를 자연인을 고유하게 식별할 목적으로 이용되는 특정 생체 정보로 크게 좁히는 방안을 고려할 것을 권고 드립니다.
Articles 29 (6)-4, 48 (10)-4 and Annexes 1 and 3: 제29조의6(가명정보 처리에 대한 과징금의 부과기준 등) ④ 법 제28조의6에 따른 과징금의 산정	동의하지 않음	개인정보보호법 시행령 개정안은 벌금을 부과하기 전에 데이터 관리자 및 정보 및 통신 서비스 제공 업체가 보호위원회의 지침, 권고 또는 명령에 따라 조치를 이행할 수 있는 적절한 기간을 제공해야 합니다. 벌금은 비즈니스 운영자가 적시에 적절한 조치를 취하지 않는 경우에만 적용해야 하도록 해

기준과 산정절차는 별표 1의3과 같다 제48조의10(과징금의 산정기준 등에 대한 특례) ④ 법 제39조의15제4항에 따른 과징금의 산정기준과 산정절차는 별표 1의5와 같다 **[별표 1의 3] 과징금 산정기준과 산정절차(제29조의6제4항 관련)** 가. 기준금액의 산정 1. 과징금의 산정단계 과징금은 법 제28조의6제1항에 따른 위반행위와 이에 영향을 미치는 행위를 종합적으로 고려하여 기준금액에 필수적 가중·감경, 추가적 가중·감경을 거쳐 과징금을 산 정한다. 2. 과징금의 산정단계에 따른 산정방식과 고려사유 가. 기준금액의 산정 1) 기준금액은 제29조의6제1항에 따른 전체 매출액에 위반행위의 중대성에 따라 다 음과 같이 구분된 과징금의 산정비율(부과기준율)을 곱하여 산출한 금액으로 한다. 위반행위의 중대성 / 부과기준율 매우 중대한 위반행위 / 1천분의 27 중대한 위반행위 / 1천분의 21 보통 위반행위 / 1천분의 15 2) 제29조의6제2항 각 호의 어느 하나에 해당하는 경우에는 1)에도 불구하고 위반행 위의 중대성에 따라 기준금액을 다음과 같이 한다. 위반행위의 중대성 / 기준금액		야 합니다. 벌금이 부과되는 경우, 적절한 수단으로는 개인이 겪는 경제적 피해를 보상하기 위한 금전적 구제책 제공, 향후 위반을 방지하기 위해 맞춤형 행동 기반 구제책을 부과하는 등 방안이 도입할 수 있을 것입니다.

매우 중대한 위반행위	3억 6천만원
중대한 위반행위	2억 8천만원
보통 위반행위	2억원

3) 위반행위의 중대성은 고의·중과실 여부, 영리 목적의 유무, 위반행위로 인한 개 인정보의 피해규모, 개인정보의 공중에 노출 여부 및 위반행위로 인하여 취득한 이익의 규모 등을 종합적으로 고려하여 판단한다.

나. 필수적 가중·감경
위반행위의 기간과 횟수 등에 관하여 다음의 사항을 고려하여 기준금액의 100분의 50의 범위에서 가중하거나 감경해야 한다.

다. 추가적 가중·감경
개인정보 보호를 위한 노력 정도, 위반행위에 대한 조사의 협조 여부, 위반행위의 주 도 여부 등을 종합적으로 고려하여 필수적 가중·감경을 거친 금액의 100분의 50의 범위에서 가중하거나 감경할 수 있다

[별표 1의 5] 과징금의 산정기준과 산정절차(제 48 조의 10 제 4 항 관련

1. 과징금의 산정단계
과징금은 법 제39조의15제3항 각 호에 따른 고려 사항과 이에 영향을 미치는 행위를 종합적으로 고려하여 기준금액에 필수적 가중、감경, 추가적 가중 、감경을 거쳐 과징금을 산정한다.

2. 과징금의 산정단계에 따른 산정방식과 고려 사유

가. 기준금액의 산정

1)기준금액은 제48조의10제1항에 따른 위반행위와 관련한 매출액에 위반 행위

의 중대성에 따라 다음과 같이 구분된 과징금의 산정비율(부과기준 율)을 곱하여 산출한 금액으로 한다

위반행위의 중대성	부과기준율
매우 중대한 위반행위	1천분의 27
중대한 위반행위	1천분의 21
보통 위반행위	1천분의 15

2) 제48조의10제2항 각 호의 어느 하나에 해당하는 경우에는 1)에도 불구하고, 위반행위의 중대성에 따라 기준금액을 다음과 같이 한다

위반행위의 중대성	부과기준율
매우 중대한 위반행위	3억 6천만원
중대한 위반행위	2억 8천만원
보통 위반행위	2억원

3) 위반행위의 중대성은 고의·중과실 여부, 영리 목적의 유무, 위반행위로 인한 개인정보의 피해규모, 개인정보의 공중에 노출 여부 및 위반행위로 인하여 취득한 이익의 규모 등을 종합적으로 고려하여 판단한다.

나) 필수적 가중·감경
위반행위의 기간과 횟수 등을 고려하여 기준금액의 100분의 50의 범위에서 가중하거나 감경해야 한다.

다. 추가적 가중·감경
개인정보 보호를 위한 노력 정도, 위반행위에 대한 조사의 협조 여부, 위반행위의 주도 여부 등을 종합적으로 고려하여 필수적 가중·감경을 거친 금액의 100분의 50의 범위에서 가중하거나 감경할 수 있다.

3. 세부 기준
위반행위와 관련한 매출액의 산정에 관한 세부 기준, 위반행위의 중대성 판 단

기준, 필수적 가중、감경 및 추가적 가중、감경을 위한 세부 기준과 그 밖에 과징금의 부과에 필요한 사항은 보호위원회가 정하여 고시한다.		

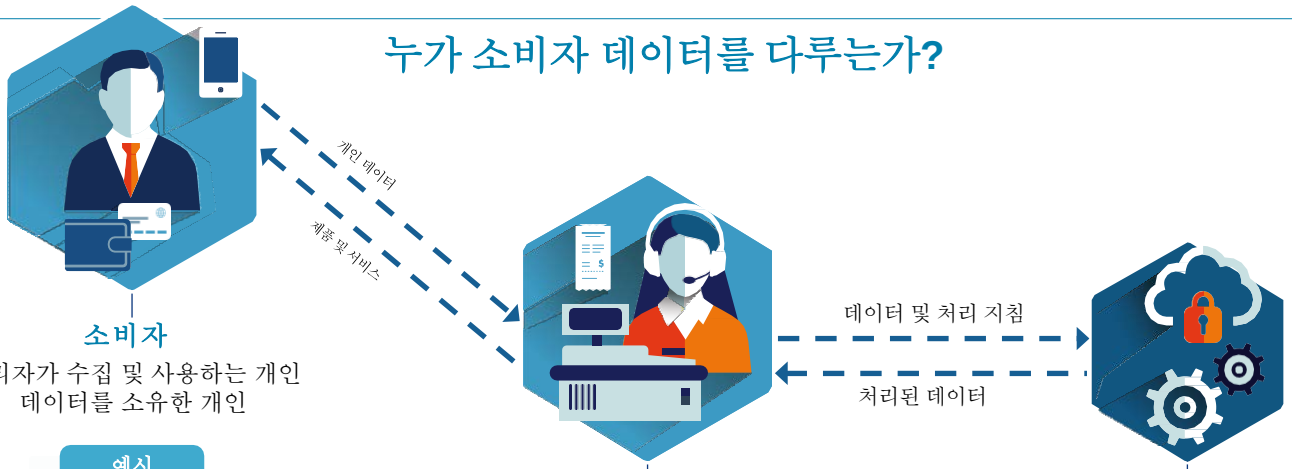
국제 표준: 개인정보보호법 내 관리자와 처리자의 차이점

포괄적인 개인정보보호법은 소비자 데이터를 다루는 모든 기업에 강력한 의무를 부여해야 합니다. 이러한 의무는 기업이 소비자 데이터와 상호 작용하는 방식을 반영할 때 소비자 개인정보를 보호하고 신뢰를 심어주기에 충분할만큼 엄격해야 합니다.

전 세계 개인정보보호법은 두 가지 형태의 기업 즉, (1)소비자 데이터를 수집하는 방법과 이유를 결정하고, 해당 데이터의 **관리자** 역할을 하는 기업과 (2)다른 기업을 대신하여 데이터를 처리하는 데이터 **처리자** 역할을 하는 기업을 구분하고 있습니다.

이러한 기본적인 구별은 유럽 연합의 일반 데이터 보호 규정("GDPR" - European Union's General Data Protection Regulation) 및 캘리포니아 소비자 개인정보보호법("CCPA" - California Consumer Privacy Act)을 포함한 다수의 글로벌 개인정보보호법에 중요한 요소로 작용하고 있습니다. 두 가지 유형의 비즈니스 모두 중요한 책임과 의무를 지니고 있으며, 이는 모든 법률에서 제시되어야 합니다.

누가 소비자 데이터를 다루는가?



소비자

관리자가 수집 및 사용하는 개인 데이터를 소유한 개인

예시

소매점에서 쇼핑하거나, 온라인으로 제품을 구매하거나, 소셜 미디어 플랫폼에서 정보를 공유하는 소비자.

소비자가 가지는 권리:

- 관리자가 어떤 유형의 데이터를 수집하는지와 그 이유를 **파악할 수 있는 권리**
- No라고 말하고, 판매 뿐만 아니라 광범위한 유형의 사용을 **거부할 수 있는 권리**
- 자신에 대한 정보에 **접근할 수 있는 권리**
- 그 정보를 **수정할 수 있는 권리**
- 그 정보를 **삭제할 수 있는 권리**
- 자신의 데이터를 **안전하게 보호할 수 있는 권리**
- 자신의 데이터가 **기대에 맞게 사용되도록 할 수 있는 권리**

관리자

소비자로부터 데이터를 수집할지 여부 및 그 방법과 해당 데이터의 사용 목적을 결정한다.

예시

호텔, 은행, 소매점, 여행사 및 소비자 대상 기술 제공업체와 같이 소비자와 직접 상호작용하는 기업.

관리자의 의무:

소비자 데이터를 처리하는 데 필요한 동의 얻기

접근, 수정, 또는 삭제에 대한 소비자 요구에 응답

소비자의 기대와 일치하는 데이터 사용

처리자

관리자의 지시에 따라 관리자를 대신하여 데이터를 처리한다.

예시

클라우드 컴퓨팅과 같은 B2B(Business-to-Business) 제품을 제공하는 기업, 다른 기업의 지시에 따라 데이터를 처리하는 인쇄 업체, 택배 및 기타 업체와 같은 공급 업체.

처리자의 의무:

관리자의 지시에 일치하는 데이터 처리

데이터 보안을 보호하도록 설계된 적절한 보안 장치 채택

관리자와 처리자는 소비자의 개인정보와 보안을 보호할 수 있도록 각 역할에 따른 책임을 져야 합니다.

전 세계 개인정보보호법은 관리자와 처리자를 구분하고 있습니다.

전 세계 개인정보보호법은 개인의 데이터를 수집하고 사용하는 바를 결정하는 기업과 해당 데이터를 처리하기만 하는 기업을 기본적으로 구분하고 있습니다.

소비자 데이터를 수집하는 방법과 이유를 결정하는 기업.	다른 기업의 지시에 따라 소비자 데이터를 처리하는 기업.
GDPR: 관리자 처리의 "목적과 방법"을 결정한다.	**GDPR: 처리자** 관리자를 "대신하여" 개인 데이터를 다룬다.
CCPA: 기업 처리의 "목적과 방법"을 결정한다.	**CCPA: 서비스 제공자** 기업을 "대신하여" 개인정보를 처리한다.

관리자와 처리자를 구별하는 것은 GDPR 및 CCPA뿐만 아니라 여러 개인정보보호법에 중요합니다. 또한 ISO 27701을 포함한 선도적인 국제 개인정보보호 표준, 그리고 APEC 국가 간 개인정보보호 규칙과 같이 국경을 넘어 데이터를 전송할 수 있도록 보장하는 자발적 프레임워크 역시 관리자와 처리자를 구분하고 있습니다.

예

한 조직이 행사 초대장을 만들기 위해 인쇄 회사와 계약한다. 이 조직은 연락처 데이터베이스에서 초대할 사람의 이름과 주소를 인쇄 회사에 제공하고, 인쇄 업자는 이 정보를 사용하여 초대장과 봉투에 정보를 기입한다. 그런 다음 이 조직은 초대장을 발송한다.

이 조직은 초대장과 관련된 개인 데이터의 관리자다. 조직은 개인 데이터가 처리되는 목적(개별 주소가 지정된 행사 초대장을 보냄) 및 처리 수단(초대된 사람의 주소 세부 사항을 사용하여 우편물에 개인 데이터를 적용함)을 결정한다. 인쇄 회사는 이 조직의 지시에 의해서만 개인 데이터를 다루는 처리자다. 인쇄 회사는 데이터를 판매하거나 마케팅과 같은 다른 용도로 사용할 수 없다. 인쇄 업체가 이러한 제한을 무시하고 자체 목적으로 데이터를 사용하는 경우 관리자가 되며, 관리자에 부과된 모든 의무가 적용된다.

소비자 개인정보를 보호하기 위해 관리자와 처리자를 구분하는 것이 왜 중요한가?

관리자와 처리자를 구분하면 소비자 데이터를 다루는 기업의 역할을 반영한 의무를 개인정보보호법에 부여할 수 있습니다. 이를 통해 부주의하게 새로운 개인정보 침해나 보안 위험을 만들지 않고 소비자의 개인정보를 보호할 수 있습니다.

데이터 보안. 관리자와 처리자 모두 소비자 데이터를 보호해야 하는 엄중한 의무를 지어야 합니다.

» 두 유형의 기업 모두에 이 의무를 적용하면 소비자 데이터를 확실히 보호할 수 있습니다.

» 관리자와 처리자 모두 데이터의 양과 민감도, 규모, 비즈니스의 성격, 사용 가능한 도구의 비용과 관련하여 합리적이고 적절한 보안 조치를 취해야 합니다.

소비자 권리 요구. 개인 데이터에 대한 접근, 수정 또는 삭제 요구와 같은 중요한 소비자 권리 요구에 응답하려면 해당 데이터의 내용에 대해 알아야 합니다.

» 관리자는 소비자와 상호 작용하고 데이터 수집 시기와 그 이유를 결정합니다. 따라서 GDPR 및 CCPA와 같은 법률은 관리자가 소비자 권리 요구에 응답하도록 요구하고 있습니다. 나아가 관리자는 소비자가 법적 보류 대상 정보를 삭제하도록 요청할 시, 그러한 소비자의 요구를 거부할 이유가 있는지도 결정해야 합니다.

» 반대로 처리자는 자신이 처리하는 데이터의 내용을 모르는 경우가 종종 있고, 계약상 데이터를 보지 못하게 될 수 있습니다. 처리자가 소비자의 요구에 직접 응답하는 것은 적절하지 않고, 이 경우 보안 위험(알지 못하는 소비자에게 데이터를 제공함)과 개인정보 위험(자신이 보지 말아야 할 데이터를 봄)이 발생하게 됩니다. 대신 처리자는 관리자가 소비자의 요구에 응답하는 데 필요한 데이터를 수집하기 위해 사용할 도구를 관리자에게 제공해야 합니다.