백서

GDPR과 CCPA를 넘어서:

ID 거버넌스가 고객과의 신뢰 구축과 컴플라이언스 준수를 지원하는 방법

Executive Summary

비즈니스에 영향을 주는 개인정보 보호 규제는 세계적으로 점차 확산되는 추세입니다. 2018년 많은 논의를 거쳐 유럽 연합의 개인정보보호법(General Data Protection Regulation, GDPR)이 발효되었습니다. 또한 2020년 1월에는 캘리포니아 소비자 개인정보 보호법(California Consumer Privacy Act, CCPA)이 제정되어 세계에서 다섯 번째로 큰 캘리포니아주에서 사업을 하는 기업들에게 영향을 미칠 예정입니다.

하지만 이는 시작에 불과합니다. 데이터 유출, ID 도용 및 관련 스캔들이 널리 알려짐에 따라 전 세계적으로 개인정보 보호 및 컴플라이언스 법률이 급속히 제정되고 있습니다. 미국에서만 9개의 주에서 기업에 상당한 영향을 미칠 규제 법안이 제출되거나 통과됐습니다. 이 법안에 따라 기업은 소비자에게 더욱 높아진 투명성과 개인 식별 정보(PII)에 대한 통제력을 제공해야 합니다.

기업은 새로운 개인정보 보호 법안과 규제를 무시할 수 없습니다. 경제적인 관점으로만 살펴보자면, GDPR 시행 후 첫 12개월 동안에는 적정 수준의 벌금이 부과되다가 현재는 2억 달러를 초과하는 수준으로 크게 증가했습니다. 하지만 이는 법에서 명시한 한도인 글로벌 연매출의 4% 보다 훨씬 낮은 수준입니다. 하지만 글로벌 기업의 부담은 경제적인 측면에서 끝나지 않습니다. 소비자의 신뢰를 잃을 수 있기 때문입니다.

개인 정보 보호 측면에서 소비자가 기업을 신뢰하지 않으면 영업 및 마케팅을 효과적으로 전개해 나갈 수 없습니다. 현재 기업이 개인 정보를 처리하려면 명시적 동의가 필요합니다. 그리고 동의에는 신뢰가 필요합니다. 신뢰가 없다면 동의를 얻을 수 없습니다. 동의 없이는 데이터를 얻을 수 없습니다. 결국 영업과 마케팅 캠페인의 효과도 떨어집니다.

개인정보 보호는 컴플라이언스 뿐만 아니라 핵심 비즈니스 장점을 확보하는 측면에서 중요합니다. 개인정보 보호 및 ID 거버넌스는 기업이 소비자와 신뢰할 수 있는 관계를 구축하게 도움으로써 고객 충성도를 제고하고 궁극적으로 매출을 증대합니다.

이 백서는 GDPR, CCPA 및 관련된 전 세계의 개인정보 보호 규제를 간략하게 다룹니다. 규제 준수, ID 거버넌스 데이터 보호를 통해 소비자 신뢰를 구축한 사례를 확인하고 적절한 ID 관리 솔루션의 필요성에 대해 설명합니다. 또한 대표적인 기업 2곳이 개인정보 보호 컴플라이언스 목표를 달성한 방법을 사례로 언급합니다.

개인정보 보호법(GDPR)

2018년 5월 25일, GDPR은 전 세계적으로 피할 수 없는 현실이 되었습니다. 이 포괄적인 데이터 보호 법안의 명시적 목적은 유럽 전역의 국가별 데이터 보호법을 통합하는 것입니다. 이 법안은 유럽 기반의 기업 뿐만 아니라 유럽 내에서 사업을 하는 모든 기업에 적용됩니다.

GDPR은 PII(개인식별정보)의 수집, 저장, 사용 방법 및 무단 접속으로부터 데이터를 보호하는 방법에 대해 다양하고 상세한 요건을 제시합니다.[1] 개인 정보를 식별하고 보호하는 방법뿐만 아니라 새로운 투명성 요구사항에 부합하는 방법, 개인 정보 유출 식별 및 보고 방법, 개인정보 보호 담당자 훈련 방법 등이 포함됩니다.

GDPR의 원칙을 준수하지 않는 경우 벌금이 부과되기 때문에 기업에 심각한 경제적 손실을 끼칠 수 있습니다. 초기의 데이터 유출은 적정 수준의 벌금으로 끝났지만, 최근 매겨진 벌금 액수가 전 세계 뉴스의 헤드라인을 장식하자 업계에서도 이제 주의를 기울이고 있습니다. 2건의 벌금 사례 중 하나는 50만 명에게 영향을 미친 데이터 유출이 발생한 대표적인 항공사[2](2억3천만 달러)이며 다른 한 곳은 호텔 투숙객 3억8천3백만 명의 개인 정보를 해킹당한 대표적인 서비스 기업[3](1억2천3백만 달러)입니다. 많은 글로벌 기업들이 이 사건에 촉각을 곤두세웠습니다.

캘리포니아 소비자 개인정보 보호법(CCPA)

개인정보 보호에 대해 기업에 추가적인 압박을 가하는 캘리포니아 소비자 개인정보 보호법(CCPA)도 초읽기에 들어갔습니다.[4] 2020년 1월 1일부터 캘리포니아주에서 사업을 하는 대부분의 대기업들은 엄격한 신규 주 개인정보 보호법을 준수해야 합니다. 이 법은 모든 캘리포니아 주민에 대한 합법적이며 강제적인 개인정보 보호 권리를 부여합니다. GDPR과 마찬가지로 CCPA는 캘리포니아주에 기반을 둔 기업에만 적용되는 것이 아니라 캘리포니아주에서 사업하는 모든 기업에 적용됩니다.

CCPA는 캘리포니아주 소비자에게 다음과 같은 개인정보 보호를 제공합니다.[5]

- **소유 권한:** 소비자가 기업에게 개인 정보를 공유 및 판매하지 말라고 통지할 권리가 보장됩니다.
- **컨트롤:** 소비자와 관련하여 수집된 개인 정보에 대한 통제권을 소비자에게 제공합니다.
- **보안:** 기업이 개인정보 보호에 대한 책임을 집니다.
- 다음 기준을 하나 이상 충족하는 모든 기업은 CCPA를 준수해야 합니다.
  - 매출이 2천500만 달러를 초과하는 경우
  - 상업적인 목적으로 5만 명 이상의 소비자, 가정, 디바이스에 대한 개인정보를 구매, 취득, 판매, 공유하는 경우
  - 연 매출의 50% 이상이 소비자의 개인 정보 판매로 발생하는 경우

작년 많은 기업들이 GDPR을 준수하는 과정에서 상당한 어려움을 겪었는데 이제는 CCPA도 준수해야 합니다. 시간은 계속 흘러가고 데드라인이 다가오고 있습니다. 맞춤형 마케팅 캠페인 목적으로 캘리포니아주에서 소비자 ID 데이터를 수집하고 소비자 프로파일을 구축하는 기업은 당장 조치를 취해야 과중한 벌금을 피할 수 있습니다.

GDPR과 CCPA의 차이점은 무엇인가요?

CCPA는 GDPR과 범위 측면에서 다소 차이를 보입니다. CCPA는 소비자에게 자신의 데이터를 통제하고 사용을 거부할 수 있는 권리를 부여합니다. 두 규제 모두 기업이 데이터를 안전하게 저장하고 수집된 개인 정보 종류를 투명하게 공개하며 주로 '잊혀질 권리'라고 부르는 소비자 정보 삭제에 대한 요청을 관리할 것을 요구합니다. 이는 기업 전체의 모든 시스템에서 개인 정보를 삭제할 수 있게 된다는 뜻입니다.

CCPA는 데이터를 처리할 때 법적으로 동의가 있어야 합니다. 또한, PII를 수집하기 전에 명시적 동의를 요청하는 GDPR과 달리 CCPA는 사용자에게 취소할 수 있는 권한을 부여합니다.

추가적인 글로벌 규제

GDPR 및 CCPA도 중요하지만 이 2가지 규제는 세계적인 추세의 시작일 뿐입니다. 전 세계적으로 이미 다양한 개인정보 보호 및 컴플라이언스 법안이 고려되고 있거나 시행 중입니다. 미국에서만 9개 주 의회가 기업이 소비자에게 PII에 대한 투명성과 통제권을 강화해야 한다는 광범위한 의무를 부과하는 법안을 제출했습니다.[6]

국제적인 측면에서 개인정보 보호 규제는 더욱 엄격해지며 비즈니스에 끼치는 영향도 커지고 있습니다. 이는 기업이 무시할 수 없는 전 세계적 현상입니다. 다음 표는 캐나다의 개인정보 보호 및 전자문서에 관한 법률(Personal Information Protection and Electronic Documents Act, PIPEDA) 등 계류 중인 규제의 일부입니다.

현재 실행 중이거나 예정 또는 제안된 데이터 보호 및 개인정보 보호 규제 예시

미주 지역	EMEA(유럽, 중동 및 아프리카) 지역	아시아 태평양 지역
아르헨티나: PDPL/Bill No. MEN-2018-147-APN-PTE[7] 미국: 캘리포니아: CCPA(AB 375) 캐나다: PIPEDA[8] 하와이: SB 418[9] 메릴랜드: SB 0613[10] 매사추세츠: SD 341[11] 미시시피: HB 2153[12] 뉴멕시코: SB 176[13] 뉴욕: S00224[14] 노스다코타: HB 1485[15] 로드아일랜드: S0234[16] 텍사스: HB 4518[17]	유럽 연합: GDPR 러시아: 연방법 No. 152-FZ[18]	호주: 1988년 개인정보 보호법 / 정보 프라이버시 원칙(IPPs)[19] 중국: 개인정보 보안서[20] 인도: 개인정보 보호 법안[21] 일본: APPI[22]

규제 준수 및 신뢰 구축

이러한 규제로 인해 소비자의 신뢰를 구축하는 것은 전 세계적으로 기업들에게 더욱 중요한 일이 되었습니다. GDPR, CCPA, 관련 법안은 기업이 소비자의 정보를 수입 및 사용하기 전에 소비자에게 동의를 구하고, 그 동의를 기록으로 남겨둘 것을 요구합니다.

또한 규제 준수 뿐만 아니라 소비자와 깊고 신뢰할 수 있는 디지털 관계를 구축하고자 하는 기업에게 개인정보 보호는 아주 중요합니다. 자신의 개인 정보가 비공개로 안전하게 보관되기를 기대하는 소비자들이 점차 증가하고 있습니다. 공개적으로 알려진 수많은 데이터 악용, 유출, 신원 도용 사례는 개인 정보를 안전하게 관리하는 믿을 만한 기업으로 인정받을 수 있는 기준을 높였습니다. 소비자가 기업에 데이터를 저장하면 신뢰 계약이 시작됩니다. 신뢰가 한 번 무너지면, 다시 회복하기 어렵습니다.

소비자는 기업이 가치로 보답하고 본인이 브랜드를 신뢰하는 경우에만 데이터 처리에 동의할 것입니다. 신뢰가 없다면 동의도 없습니다. 동의가 없다면 데이터도 없습니다. 결국 영업과 마케팅 캠페인의 효과도 떨어집니다. 신뢰는 소비자 데이터를 획득하려는 기업에게 '새로운 화폐'가 되었습니다.

동의의 중요성: 사용자 경험 재고

GDPR과 CCPA에 따라 소비자는 언제든 동의를 확인 및 수정하고 심지어 취소할 수 있습니다. 다른 말로 하면 기업이 사용하기 편한 웹 양식을 제공하여 동의를 획득하고 사람들에게 복잡한 절차를 요구하여 의도적으로 동의를 취소하는 것을 어렵게 만드는 것은 준수에 해당하지 않습니다. 더구나 기업은 데이터를 수집하는 이유와 어떤 목적으로 사용할 것인지 명료하게 밝혀야 합니다.

이는 마케팅 기업에 상당한 영향을 미치게 됩니다. 예를 들어 기업은 이제 GDPR에 따라 동의를 얻기 위해 게이티드 리드 생성 콘텐츠의 랜딩 페이지에 미리 확인 표시가 된 상자를 사용할 수 없습니다. 동의는 거부가 아닌 참여로 표현되어야 합니다. 즉, 소비자가 동의하려면 상자에 표시해야 합니다. 하지만 CCPA는 암묵적 동의를 허용하기 때문에 미리 확인 표시가 된 상자도 규제에 준수하는 것으로 간주됩니다. 이러한 차이로 인해 글로벌 기업은 두 주요 시장의 웹사이트와 앱에 서로 다른 등록 양식을 표시해야 하는 문제를 해결해야 합니다. 지역 문제를 해결하기 위해 전혀 다른 웹사이트와 앱을 배포할 수도 있지만, 이를 위해서는 코드 개발 및 유지 노력을 몇 배로 늘려야 합니다.

또한 새로운 규제는 과도한 데이터 수집을 금지합니다. 기업은 제공하는 서비스 또는 제품에 필요한 개인정보만을 수집할 수 있습니다. 이메일 뉴스레터를 제공하거나 백서를 다운로드하는 사람에게 휴대폰 번호나 성별을 묻는 것은 이제 허용되지 않습니다. 이는 기업이 사용자 경험을 재고하고 다시 설계하여 등록 페이지 및 기타 양식에서 과도한 데이터 수집으로 여겨질 수 있는 모든 데이터 필드를 제거해야 한다는 뜻입니다.

글로벌 리테일 기업, 현재와 미래의 개인정보 보호법 준수를 간소화하기 위해 중앙 집중식 솔루션 구현

한 글로벌 리테일 기업은 최근 Akamai Identity Cloud를 구축해 개인정보 보호 컴플라이언스 요구사항에 대응했습니다. 이를 통해 소비자에게 투명성과 본인의 개인 정보에 대한 통제권을 제공할 수 있었습니다. 등록 중 수집되는 PII를 최소화하고 모든 데이터를 처리하기 전에 동의를 요청했습니다.

Identity Cloud는 등록 및 로그인에 대해 맞춤형 사용자 경험과 목적에 따라 점진적으로 적용되는 동의 양식을 제공합니다. 이를 통해 기업의 소비자는 자신이 동의하거나 동의하지 않은 데이터의 목적을 쉽게 이해할 수 있습니다. 소비자는 언제든지 동의 설정을 검토, 변경, 취소할 수 있습니다.

Identity Cloud의 범위 지정 접속 기능을 통해 ID 데이터에 접속하는 직원의 업무에 따라 데이터 기록 및 기록 내 특정 필드에 대한 접속을 제한할 수 있습니다. 예를 들어, 고객 서비스 담당자는 마케팅 담당자 또는 개발자와 다른 접속 권한을 갖고 있습니다. 이 특별한 기능은 소비자 데이터 노출의 위험을 줄이고 높은 수준의 데이터 보안을 제공합니다.

또한, 고객 데이터에 대한 세분화된 접속 제어 기능을 갖춘 단일 중앙 저장소를 제공하여 '유해한' ID 데이터의 확산을 줄일 수 있습니다. 유해한 데이터에는 고객이 동의를 취소하거나 삭제를 요청한 후에도 여전히 데이터베이스에 저장된 데이터 등이 포함됩니다. 또한 중앙 저장소는 '잊혀질 권리'와 관련된 데이터 삭제 요청을 간소화합니다.

마지막으로 모든 동의 설정은 누가 언제 어떤 리소스에 접속했는지에 대한 변경 로그와 감사 내역, 감사 전용 형식의 고객 프로필과 함께 저장됩니다.

데이터 보안 보장

컴플라이언스는 개인 정보 보호 문제에 국한되지 않습니다. 악의적인 공격자로부터 소비자의 데이터를 안전하게 보호하는 것은 개인정보 보호를 보장하는 것과 밀접한 관련이 있습니다. 개인 ID 데이터는 쉽게 악용될 수 있기 때문에 해킹 공격의 주요 표적이 되어 왔습니다. IBM Security가 후원하고 Ponemon Institute에서 진행한 2018년 데이터 유출로 인한 비용 연구[23]에 따르면 조사 대상 기업의 거의 절반(48%)이 데이터 유출의 근본 원인을 악성 또는 범죄 공격이라고 파악하고 있으며 유출 ID 기록당 평균 약 157달러의 비용이 든 것으로 확인되었습니다.

데이터 유출은 수십만 건(또는 수백만 건)의 기록이 포함되기 경우가 많기 때문에 기업에 심각한 재정적 피해를 끼칠 수 있습니다. 뿐만 아니라 이후에는 기업 평판 하락, 소비자 신뢰 상실, GDPR 및 CCPA의 벌금과 관련된 매출 손실도 발생합니다.

ID 거버넌스의 필요성

PII를 수집하고 컴파일하는 기업에게 개인 ID는 귀중한 자산입니다. 하지만 더욱 중요한 것은 ID 소유자이자 자신의 ID가 보호하고 남용되지 않기를 바라는 소비자에게는 개인 ID는 더욱 중요한 자산이라는 점입니다.

소비자의 개인적 삶의 영역이 점차 디지털로 이동하면서 이름, 주소, 휴대폰, 성별, 결제 정보, 개인 선호도부터 쇼핑 탐색 이력과 기타 행동 데이터에 이르는 개인 정보는 기업의 프로파일 데이터가 됩니다. 기업이 주요 데이터를 안전하게 지키고 보호해야 할 필요성이 상당히 증가했으며 전 세계 규제 기관은 규제를 크게 강화하면서 이에 대응하고 있습니다.

규제 준수 및 보안은 ID 관리의 복잡성과 중요도를 크게 높이는 핵심 요인입니다. 하지만 기업 수준의 ID 관리 솔루션은 등록 중 수집되는 데이터를 최소화하고 데이터를 처리하기 전에 동의를 요청하여 고객에게 투명성과 개인 정보에 대한 통제권을 제공할 수 있습니다.

기업은 적절한 ID 관리를 통해 소비자의 신뢰를 회복할 수 있습니다.

신속하게 GDPR에 대응한 글로벌 음료 브랜드

한 세계적인 음료 회사는 GDPR 기한을 2개월 앞두고 유럽의 모든 소비자들에게 GDPR 개인정보 보호를 준수해야 하는 어려운 과제에 직면해 있었습니다. 이전에 Identity Cloud를 구현한 적이 있었지만, 달라지는 소비자 개인정보 보호 규제에 맞춰 신속히 컴플라이어스를 보장해야 했습니다.

컴플라이언스가 완료되는 데까지 딱 2달이 소요되었습니다. 이 기업이 중점을 둔 것은 GDPR 요구 사항을 준수하면서도 마케팅과 맞춤 기능을 위해 데이터를 사용해도 좋다는 소비자의 명시적인 동의를 획득하는 것이었습니다. Identity Cloud는 웹사이트부터 모바일 앱, IoT 디바이스에 이르는 모든 디지털 자산에 점진적으로 적용되는 사용자 맞춤형의 세분화된 동의 양식을 제공했습니다. 이 강력한 기능은 GDPR을 준수하는 것 뿐만 아니라 소비자가 보다 쉽게 동의 설정을 이해하고 관리할 수 있도록 함으로써 소비자와의 신뢰를 구축할 수 있도록 지원했습니다.

솔루션을 구축하는 과정 중에서 특히 어려운 영역 중 하나는 GDPR의 '잊혀질 권리'를 중시하는 측면과 소비자 프로모션 기간 동안 데이터를 보유할 법적 의무 사이의 균형을 맞추는 일이었습니다. Identity Cloud은 법정 기한 동안 데이터를 보관하고 해당 기한이 끝나는 시점에 삭제하는 기능 및 소비자와 소통하는 기능을 제공합니다.

Akamai Identity Cloud

Identity Cloud는 고객 ID 및 접속 관리를 위한 Akamai 솔루션입니다. 소비자가 개인 계정을 만들고 웹사이트, 모바일 앱, IoT 기반 애플리케이션에 안전하게 로그인하는 데 필요한 모든 것을 기업에게 제공합니다. Identity Cloud는 안전한 고객 프로파일 저장소를 제공하며 고객에 대한 360도 뷰를 확보할 수 있고, 개인정보 보호를 준수하는데 필요한 노력을 크게 절감할 수 있는 유용한 툴을 제공합니다.

Identity Cloud는 기업이 규제 문제를 해결하는 데 도움이 되는 특화된 기능과 사용자 경험을 지원합니다. Identity Cloud 개인정보 보호 기능에는 개인 정보를 수집, 관리, 보호하는 데 필요한 클라이언트 등록, 로그인, 인증, SSO(Single Sign-On), 범위 지정 접속 제어, 선호도 및 동의 관리를 포함한 여러 가지 다른 기능이 있습니다.

Identity Cloud는 기업이 개인정보 보호 관련 규제를 준수하는 데 도움이 되는 다음 기능을 제공합니다.

- 명시적 동의를 위한 확인란 동의 메커니즘
- 접속 제어를 위한 중앙화된 거버넌스
- 점진적 허가, 등록, 프로파일링
- 손쉬운 데이터 기록 접속 메커니즘
- 데이터 수정 및 무결성 메커니즘
- 데이터 이식성
- 데이터 제거/삭제
- 사용자 및 통합을 위한 범위 지정 접속
- 데이터 가명화
- 나이 제한

Identity Cloud를 통해 빠르고 유연한 방식으로 엔터프라이즈급 ID 관리를 구현할 수 있습니다. 클라우드 기반 아키텍처를 기반으로 설계된 솔루션이기 때문에 용량 요구에 따라 지능적으로 확장할 수 있고 트래픽 급증을 원활히 처리하며 수천만의 사용자에게 쾌적한 사용자 경험을 제공합니다. Akamai Identity Cloud는 기업이 국제적인 개인정보 보호 규제를 준수하고 클라이언트 데이터를 관리하며 모든 지역 및 애플리케이션에서 데이터를 안전하게 보관하여 리스크를 감소할 수 있도록 설계되어 있습니다.

Akamai Identity Cloud에 대한 자세한 내용은 akamai.com/identitycloud를 참조하시기 바랍니다.

결론

GDPR, CCPA, 관련 개인정보 보호 규제 준수와 안전 보장은 소비자와의 신뢰 관계를 구축하고 유지하고자 하는 모든 기업에 중요한 요인입니다. 소비자는 투명성 뿐만 아니라 본인의 귀중한 개인 정보가 비공개로 안전하게 보관되기를 요구합니다. 최근 전 세계적으로 발생한 데이터 유출, 신원 도용 관련 사건은 기업이 PII의 믿을 수 있는 수호자가 되어야 한다는 필요성을 강조합니다.

소비자가 기업이 개인 정보를 수집하고 저장하는 것을 허용하면, 이는 본질적으로 신뢰 계약을 시작한 것입니다. 한 번 신뢰가 깨지면 회복하는 것은 매우 어렵습니다. 오늘날 소비자 데이터를 수집 및 저장하고 고객 인증정보와 개인정보를 처리하는 일은 기업이 위반하거나 침해할 수 없는 주의의무입니다. 신뢰가 깨지면 브랜드 평판, 소비자 충성도는 물론 궁극적으로 현재 매출과 비즈니스 성공에 위험을 초래할 수 있습니다.

부록: 개인정보 보호 규제 요건 개요

이 부록은 GDPR, CCPA 및 전 세계의 주요 데이터 보호 및 개인정보 보호 규제에서 확인되는 일반적인 요건 유형을 간략히 보여줍니다. 요건에는 동의, 거절 권한, 접속 권한, 잊혀진 권리, 데이터 이식성, 보안, 유출 알림 등이 있습니다. 이러한 권리 이행은 제정된 여러 개인정보 보호 및 보호법에 따라 달라집니다. 따라서 어떤 법률이 적용되는지 확인하려면 법적 자문을 받기 바랍니다.

Akamai Identity Cloud를 통해 이러한 규제 컴플라이언스 요건을 해결하는 방법을 자세히 알고 싶다면 블로그 게시물을 확인해보세요.

동의	기업은 특정한 목적을 위해 개인 정보를 수집하거나 처리하기 전에 최종 사용자에게 반드시 동의를 받아야 합니다. 유효한 동의 획득 요건 및 동의가 필요한 시점은 적용되는 규제에 따라 달라집니다.
거절 권한	요건에서는 데이터 주체에게 다이렉트 마케팅 또는 통계 분석 등 특정 데이터 처리 유형에 대해 본인의 개인 정보 사용을 거부할 권리를 제공합니다.
접속 권한	여러 법은 데이터 주체에게 처리되는 개인 정보에 접속, 확인, 수정할 권한을 제공하며 일부 경우에는 그러한 데이터의 사용 및 공개에 대한 추가 정보를 요구할 수도 있습니다.

개인 정보 제거 및 삭제 권한	여러 법은 소비자의 '잊혀질 권리'를 포함하고 있습니다. 이는 본인의 개인 정보를 제거하여 써드파티에 공유하거나 써드파티를 통한 처리에 노출되지 않게 하는 것입니다.
데이터 이식성	기업은 데이터 주체에게 일반적으로 사용되며, 시스템이 인식 가능한 양식의 사본을 제공해야 합니다. 이를 통해 사용자는 불편 없이 자신의 데이터를 다른 기업에 전송할 수 있습니다.
보안	기업은 부주의 또는 불법에 의해 데이터가 접속, 수정, 분실, 파괴, 공개될 위험에 대응하는 데이터 보안 안전장치를 구현해야 합니다.
유출 알림	기업은 데이터 유출 상황을 처음 파악한 후 일정한 기간 내로 최종 사용자에게 데이터 유출을 반드시 알려야 합니다.

출처

1) https://ec.europa.eu/commission/priorities/justice-and-fundamental-rights/data-protection/2018-reform-eu-data-protection-rules_en
2) https://www.cnet.com/news/british-airways-faces-record-breaking-230m-gdpr-fine-for-2018-data-breach/
3) https://www.zdnet.com/article/marriott-faces-123-million-gdpr-fine-in-the-uk-for-last-years-data-breach/
4) https://leginfo.legislature.ca.gov/faces/billCompareClient.xhtml?bill_id=201720180AB375
5) https://www.caprivacy.org/
6) https://www.dwt.com/insights/2019/02/copycat-ccpa-bills-introduced-in-states-across-cou
7) https://www.argentina.gob.ar/sites/default/files/mensaje_ndeg_147-2018_datos_personales.pdf
8) https://www.priv.gc.ca/en/privacy-topics/privacy-laws-in-canada/the-personal-information-protection-and-electronic-documents-act-pipeda/
9) https://www.capitol.hawaii.gov/measure_indiv.aspx?billtype=SB&billnumber=418&year=2019
10) http://mgaleg.maryland.gov/webmga/frmMain.aspx?pid=billpage&stab=01&id=sb0613&tab=subject3&ys=2019rs
11) https://malegislature.gov/Bills/191/SD341
12) http://billstatus.ls.state.ms.us/documents/2019/html/HB/1200-1299/HB1253IN.htm
13) https://www.nmlegis.gov/Legislation/Legislation?chamber=S&legType=B&legNo=176&year=19
14) https://assembly.state.ny.us/leg/?default_fld=&bn=S00224&term=2019&Summary=Y&Actions=Y&Text=Y&Committee%26nbspVotes=Y&Floor%26nbspVotes=Y
15) https://www.legis.nd.gov/assembly/66-2019/bill-index/bi1485.html
16) http://webserver.rilin.state.ri.us/billtext19/senatetext19/S0234.htm
17) https://capitol.texas.gov/tlodocs/86R/billtext/html/HB04518I.htm
18) https://pd.rkn.gov.ru/authority/p146/p164/
19) https://pd.rkn.gov.ru/authority/p146/p164/
20) https://www.tc260.org.cn/front/postDetail.html?id=20190201173320
21) https://meity.gov.in/content/personal-data-protection-bill-2018
22) https://www.ppc.go.jp/en/
23) https://www.ibm.com/security/data-breach