



국제 표준: 개인정보보호법 내 관리자과 처리자의 차이점

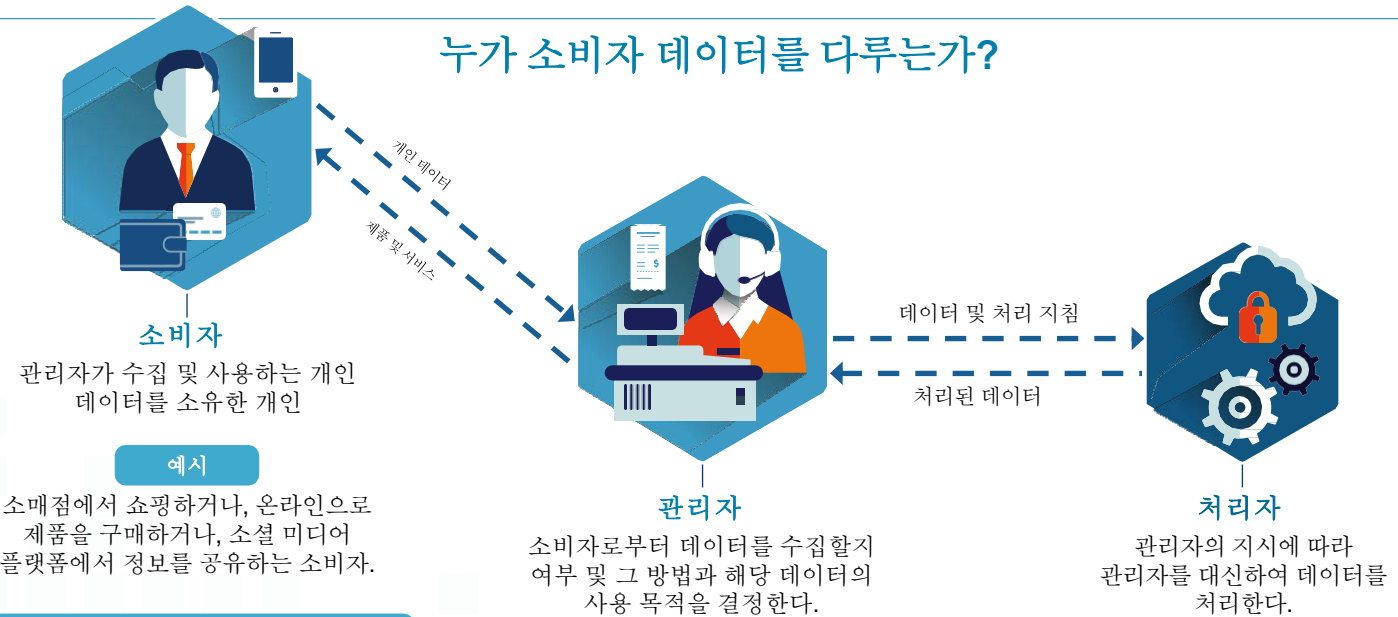
포괄적인 개인정보보호법은 소비자 데이터를 다루는 모든 기업에 강력한 의무를 부여해야 합니다. 이러한 의무는 기업이 소비자 데이터와 상호 작용하는 방식을 반영할 때 소비자 개인정보를 보호하고 신뢰를 심어주기에 충분할만큼 엄격해야 합니다.

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.

관리자

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

예시

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

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.

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**

관리자의 의무:

소비자 데이터를 처리하는 데 필요한 동의 얻기
접근, 수정, 또는 삭제에 대한 소비자 요구에 응답
소비자의 기대와 일치하는 데이터 사용

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 보호 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.