개인정보보호법(GDPR)

개인정보보호법(GDPR)은 유럽연합 시민의 개인정보 처리와 보호에 관한 토대를 새롭게 형성하는 유럽연합의 규정입니다.

GDPR은 개인정보를 처리하는 모든 조직의 의무와 책임, 개인정보의 수집·처리·저장에 관한 개인의 권리를 새롭게 규정하고 있습니다.

GDPR의 영향

조직이 GDPR을 준수해야 하는 경우, 고려해야 할 요소에는 여러 가지가 있습니다. 각 조직이 법률적 자문을 통해 조직의 구체적인 상황에 맞는 방법을 결정하는 것을 강력하게 권고합니다.

1. 데이터 파악

데이터를 보호하려면 먼저 데이터가 어떻게 처리되고, 공유되고, 활용되고, 보관되고, 삭제되는지 그 취급 방식을 알아야 합니다. 조직의 GDPR 전략을 구축함에 있어 데이터의 유형과 데이터의 활용 방식, 저장 방식을 파악하는 것은 필수 요소입니다.

2. 소유권 및 책임 규정

데이터 보호 규정을 준수하는 책임자를 명확히 규정하는 것이 중요합니다. 일부 조직의 경우, 개인정보보호책임자를 임명해야 할 수 있습니다. GDPR에는 조직의 데이터 보호 규정 준수 프로그램 도입을 규정하는 '책임' 원칙도 새롭게 명시되었습니다. 이에 따라 조직은 내부 데이터 보호 정책을 구축하고 직원들에게 교육을 제공해야 합니다.

3. 데이터 처리에 관한 법적 근거 마련

조직이 반드시 따라야 하는 GDPR 규정 중 또 한 가지는 다양한 유형의 개인정보를 처리하는 것에 관한 법적 근거를 문서화해야 한다는 것입니다. 예를 들어, 사용자의 동의를 데이터 처리의 근거로 사용할 경우 사용자 동의를 어떻게 구할 것인지, 그리고 동의를 얻는 방법과 시기를 어떻게 명시할 것인지를 고려해야 합니다.

4. 데이터 주체의 권리 이해

데이터 주체의 권리를 수용하는 데이터 처리 절차를 마련하려면 먼저 개인정보에 관한 이들의 권리를 이해해야 합니다. 예를 들면, 데이터 주체에게는 자신의 개인정보에 액세스하고, 그 개인정보를 전자상으로 수정하고, 삭제하고, 내보낼 권리가 있습니다. 또한, 특정한 상황에서 자동 의사 결정과 정보 수집을 거부할 권리가 있습니다.

5. 확실한 프라이버시 중심 설계

GDPR는 처음으로 프라이버시 중심 설계를 법적 요건으로 명시했습니다. 따라서 조직은 프라이버시 중심 설계를 어떻게 비즈니스 프로세스의 일환으로 구축할 수 있을지 고려해야 합니다. 경우에 따라 개인정보 보호 영향 평가를 시행해야 할 수도 있습니다.

6. 데이터 유출 관리에 대비

강력한 데이터 보호 프로그램을 구축하는 데 있어 데이터 유출 관리에 대한 정책과 절차를 검사하고, 이를 항상 최신으로 유지하는 것은 매우 중요합니다. GDPR에 따르면 조직은 데이터 유출 사실을 적시에 파악해 관련 당국에 보고해야 합니다. 데이터 유출과 보고 불이행에는 벌금이 부과될 수 있습니다.

7. 필수 정보 전달

조직은 온라인 개인정보 보호정책과 기타 공지문을 최신 상태로 유지하고, 이러한 정책과 공지문이 모든 데이터 보호 방침을 포괄하도록 해야 합니다. 새 규정에는 데이터 처리에 관한 법적 근거를 상세히 설명하고, 문제 발생 시 민원을 제기할 수 있는 관련 당국을 사용자들에게 알려주는 것이 포함됩니다.

8. 공급업체와의 협력

조직 내부의 정책만으로는 GDPR 규정을 완벽하게 이행할 수 없습니다. 조직을 대신해 개인정보를 처리하는 모든 외부업체 역시 데이터 보호에 필요한 규정을 충족해야 합니다. 협력 중인 공급업체에 다음과 같은 질문을 해봐야 합니다.

- 네트워크 및 정보 보안, 개인정보 보호, 데이터 보호를 위한 탄탄한 체계를 갖추고 있는가?
- 국제적으로 승인된 표준을 준수하고 있으며, 이를 입증할 수 있는가?
- 강력한 신뢰와 안보 문화를 입증할 수 있는가? 데이터 관리에 필요한 제어 기능은 얼마나 갖추고 있으며, 데이터 관리자로서 조직이 요구하는 의무를 충실히 이행하고 있는가?

Dropbox: 데이터 보호

Dropbox와 전 세계 수백만 명의 개인 고객과 기업 고객 간의 관계에서 가장 근본이 되는 것은 바로 신뢰입니다.

Dropbox는 고객과의 신뢰와 믿음을 소중하게 여기며, 고객 정보를 보호하기 위해 책임을 다합니다. 이러한 신뢰를 깨트리지 않기 위해 Dropbox는 처음부터 보안, 규정 준수 및 개인 정보 보호에 가장 큰 역점을 두었으며, 앞으로도 이를 유지하도록 힘쓰겠습니다.

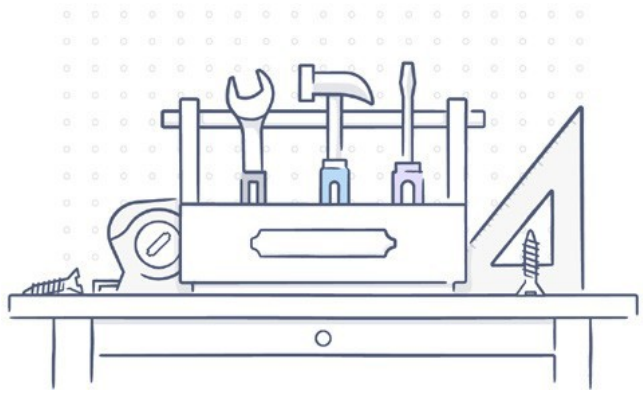
보안: 보호 및 통제

보호: 아키텍처 및 정보 보안

Dropbox는 확장 가능한 보안 인프라스트럭처 전체에 분산되어 있는 보안 데이터 전송, 암호화, 네트워크 구성, 애플리케이션 수준 제어 등의 다중 보안 계층으로 데이터를 보호하는 안전한 분산형 인프라스트럭처로 설계되었습니다. Dropbox의 강력한 정보 보안 관리 체계는 위험성을 평가하고 Dropbox에 보안 문화를 구축할 수 있도록 설계되었습니다. Dropbox는 직원들에게 보안 교육을 제공하고, 모의 해킹 등 애플리케이션과 네트워크에 테스트를 실시하고, 위험성 평가를 시행하고, 보안 정책 준수 현황을 감시하며 정기적으로 보안 정책을 검토하고 업데이트합니다. 자세한 내용은 Dropbox Business 보안 백서에서 확인하실 수 있습니다.

제어: IT 관리자의 강력한 권한

Dropbox는 IT 관리자에게 필요한 제어 기능과 가시성을 제공해 조직이 GDPR을 준수하는 데 필요한 의무를 더 편리하게 관리할 수 있도록 도와줍니다. 관리자는 Dropbox 관리 대시보드를 통해 팀 활동을 모니터링하고, 연결된 장치를 확인하고, 공유 활동을 감시할 수 있습니다. 또한, 그룹을 생성해 특정한 폴더에 대한 팀원들의 액세스를 간편하게 관리하고, 팀 폴더 관리 도구를 통해 동기화 관리 등과 같은 팀 폴더 활동을 한눈에 확인하고 제어할 수 있습니다. 링크 권한 기능으로 공유 링크에 비밀번호나 만료일을 설정해 액세스를 일시적으로만 허용하거나 액세스 권한을 조직 내 사람들로만 제한할 수 있습니다. 또한, 계정 전송 도구를 사용해 직무가 변경됐을 때 파일을 다른 사람에게 간편하게 전송할 수 있고, 원격 삭제 기능을 사용해 장치를 분실하거나 도난당했을 때 파일을 원격으로 삭제할 수 있습니다.



규정 준수: 신뢰 및 검증

규정 준수는 서비스의 신뢰성을 검증할 수 있는 효과적인 방법입니다. Dropbox의 보안 방식이 ISO 27001, 27017, 27018 및 SOC 1, 2, 3 등 가장 널리 통용되는 표준과 규정을 준수하고 있다는 것을 확인해보시기 바랍니다. Dropbox는 독립적인 외부 감사업체로부터 통제 현황에 대한 감사를 받으며 이들이 제공한 보고서와 의견을 가능할 때마다 사용자들과 공유하고 있습니다. Complianceweb 페이지에서 Dropbox가 준수하는 표준과 보안 사례 입증에 대해 더 자세하게 확인하실 수 있습니다.

개인정보 보호: Dropbox의 약속

Dropbox는 개인적인 정보이든 업무에 관한 정보이든 사용자들의 신뢰를 진지하게 받아들이며 시스템에 있는 모든 정보를 보호하는 데 최선을 다합니다. Dropbox의 개인정보 보호정책에는 Dropbox가 사용자 정보를 어떻게 처리하고 보호하는지 명확하게 설명되어 있습니다. Dropbox는 투명성 보고서와 정부의 개인정보 요청에 관한 처리 원칙을 발행해 이러한 요청을 받은 횟수와 이 요청이 어떻게 검토되고 처리되는지 투명하게 공개합니다. 또한, 법이 개인정보 보호를 더욱 강화하는 방향으로 개정될 수 있도록 노력하고 있습니다.

안전한 데이터 보호를 위한 협력

Dropbox의 데이터를 보호하는 데는 비즈니스 고객의 협력도 필요합니다. Dropbox는 직원들에게 보안 및 개인정보 보호 사례에 대한 교육을 제공하고, 신뢰할 만한 가치가 있는 조직이 되는 것을 최우선으로 여기는 조직 문화를 구축하고, 시스템과 운영 현황에 엄격한 외부 감사를 실시하는 등 기업의 인프라스트럭처, 네트워크, 애플리케이션을 보호하기 위해 포괄적인 조치를 취하고 있습니다. Dropbox의 공동 책임 안내서를 통해 Dropbox가 사용자들의 계정을 보호하는 방식과 조직이 팀의 데이터에 대한 가시성과 제어를 유지하는 방법에 대해 더 자세하게 확인하실 수 있습니다.