GDPR 에 대한 준비

Endian 이 당신을 도울 수 있습니다.

General Data Protection Regulation이란 무엇인가?

GDPR은 2018 년 5 월부터 유럽 전역의 데이터 개인 정보 보호법을 준수하여 모든 EU 시민의 데이터 개인 정보를 보호하고 권한을 부여하며 지역의 조직이 데이터 프라이버시에 접근하는 방식을 바꿔 놓을 유럽 규정입니다.

누구에게 해당하는가?

GDPR은 유럽 시민들의 개인 데이터를 수집하는 모든 회사 및 단체를 대상으로합니다.
또한 EU 지역 외부에 위치한 서비스 및 데이터베이스에서도 EU 시민의 데이터 프라이버시와 EU 회원국의 개인 데이터를 다루는 모든 회사 및 단체에 적용됩니다.

개인정보 란 무엇인가?

유럽 집행위원회 (European Commission)에 따르면 "개인 정보 란 개인적, 직업적 또는 공공의 삶과 관련된 개인의 정보를 의미합니다. 이름, 사진, 전자 메일 주소, 은행 세부 정보, 웹 사이트 및 소셜 네트워크 활동, 의료 정보 또는 PC의 IP 주소 등 모든 것에 관한 것입니다. "

GDPR 주요변화

GPDR에 따른 주요 변경 사항의 개요 및 이전 지침과 다른 점은 다음과 같습니다.:

• **동의**

동의 조건이 강화되었습니다. 개인정보 사용 동의는 명확하고 평이한 언어를 사용하여 동의가 명확하고 구별 가능하며 쉽게 접근 할 수 있는 형식이어야 합니다. 또한 동의를 철회하는 것도 쉬워야 합니다.

• **광범위한 데이터 주체 권한 :**

• 데이터에 무료로 액세스 할 수 있는 권리

• 데이터 삭제 권리 라고도 알려진 잊혀질 권리는 데이터 주체가 데이터 보유자에게 자신의 개인 데이터를 지우고 데이터의 추가 수집을 중단하도록 권한을 부여합니다

• 사용자 입장에서의 데이터 편집 권한

• **위반 통지**

위반 통지는 의무 사항이 되며 데이터 소유주는 위반 사실을 알게 된 후 72 시간 이내에 통보해야 합니다.

• **특정 조건이 적용되지 않는 한 명시 적 동의없이 EU 경제 지역 밖으로 데이터를 전송할 수 없습니다.**

• **데이터 보호 담당관**

각 공용 조직은 물론 큰 크기의 데이터베이스를 관리하는 회사에는 데이터 보호를 담당하는 DPO (Data Protection Officer)가 있어야합니다. 내부자 또는 외부 인사가 기용될 수 있습니다.

• **벌칙**

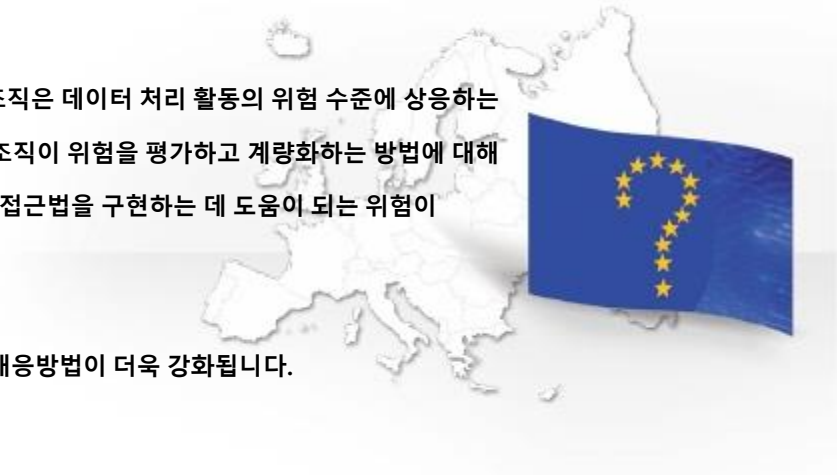
GDPR 하에서 GDPR을 위반하는 조직은 최대 2 천만 유로 (EU)의 제재 또는 전세계 연간 매출의 4 % 에 해당하는 벌금에 처해질 수 있습니다.

• **특정 위험 분석**

GDPR 전체에서 개인 데이터 처리를 통제하는 조직은 데이터 처리 활동의 위험 수준에 상응하는 보호 조치를 구현하도록 권장됩니다. GDPR은 조직이 위험을 평가하고 계량화하는 방법에 대해 침묵하고 있지만, 특정 추세는 조직이 위험 기반 접근법을 구현하는 데 도움이 되는 위험이 나타나는 부분에서 나옵니다.

• **의무의 비례 성.**

이제는 데이터 관리자의 규모와 취급의 위험에 대응방법이 더욱 강화됩니다.

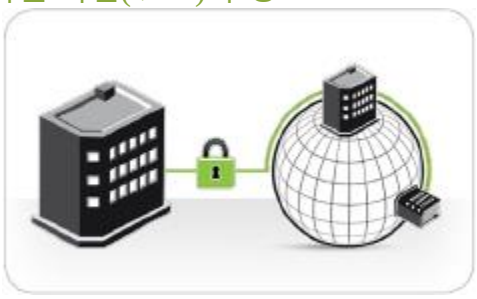


Endian 이 어떻게 귀하의 준비를 도울 수 있을까요? : 예방, 보호, 통제

GDPR의 목적은 점점 더 데이터 중심의 세계에서 모든 EU 시민들을 개인 정보 및 데이터 침해로부터 보호하는 것입니다. 자체 네트워크를 방어하고 보호하기 위해 가능한 최상의 기술을 채택해야 합니다. 따라서 전송 시작부터 데이터를 보호 할 수 있는 솔루션을 채택해야 네트워크 관리자가 잠재적 인 위험을 인지하고 위협에 즉시 대응할 수 있습니다.
Endian 은 예방, 보호 및 제어 할 수 있는 모든 필요한 도구를 포함한 완벽한 솔루션입니다.

민감한 데이터 전송에 안전성을 부여하기 위한 암호화된 터널(VPN) 구성

Endian은 자사의 모든 제품에 전송 데이터 암호화의 고급 시스템을 포함하고 있으며 관리의 단순화가 각기 다르기 때문에 사용자와 개체를 손쉽게 구성하여 사람의 실수를 최소화 할 수 있습니다. GDPR에서 요청한대로 네트워크에서 일어나는 일을 지속적으로 관리하기 위해 첫 번째 규칙은 다른 리소스에 대한 액세스 권한을 가진 사람을 파악하고 해당 리소스를 언제 확인할 수 있는지를 파악하는 것입니다. Endian Connect Platform 응 이용하여 전 세계적으로 확산 된 네트워크에서도 세분화 된 방식으로 사용권한을 인증하고 필요시 제한 할 수 있습니다.



실시간 네트워크 가시화

지금 현재 귀사의 네트워크에서 어떤 일이 일어나고 있는지 알고 있습니까? 귀사의 사용자가 어떤 응용 프로그램을 실행하고 있는지 알고 있습니까? 만일 그렇지 않다면 귀사의 생산성이 저하 될 수 있으며 새로운 GDPR 규칙을 지키지 못하고 있을 수 있습니다.
당사의 솔루션을 적용하면 네트워크 트래픽, 직관적 인 대시 보드 및 실시간 데이터를 즉시 제어하고 데이터를 저장할 수 있습니다.
이 패키지는 또한 광범위한 웹 리포팅, 전자 메일, 보안등을 포함하며 선택한 매개 변수에 따라 다양하게 구성 할 수 있습니다.

제어 및 실시간 대응 (IPS, Web, Mail 보안)

현재 모든 Endian 제품에 기본 기능으로 포함 된 Advanced Content Security Package 를 활용하여 클라우드의 고성능 제로 데이 (zero-day) 엔진을 악용하여 바이러스, 멀웨어, 피싱 및 스팸 등의 방식으로 웹 및 메일 에 대한 위협으로부터 회사를 보호 할 수 있습니다.
Endian 은 능동적 인 보호를 위해 시장에서 제공되는 최고의 기술인 침입 방지 시스템, 딥 패킷 검사 및 컨텐츠 필터링 기능을 제공하며 200 개 이상의 범주가 지속적으로 업데이트 됩니다.

Wi-Fi 와 (BYOD)

GDPR을 준수하기 위해 손님 및 외부 협력자 에게도 보호 및 모니터링을 확대해야 합니다. 방문자와 게스트에게 네트워크 보안을 손상시키지 않으면 서 웹 서핑을 제공하십시오.
Endian UTM 솔루션은 게스트 액세스 관리를 제공하며 전용 및 분리 된 물리적 네트워크에서 게스트 액세스 관리를 제공하고 규칙을 작성하고 필터를 적용 할 수 있습니다.

사용자 및 트래픽 데이터를 안전하게 기록하고 보관하세요.

endian 하드웨어의 다양한 메모리 장치 덕분에 네비게이션로그, 트래픽 및 사용자 데이터베이스를 로컬에 저장할 수 있습니다.
또한 외장 메모리를 사용하면 백업이 암호화로 더욱 안전하게 보호됩니다.
데이터베이스는 인프라 내에서 항상 안전하며 필요나 권한 여부에 따라 제어될 수 있습니다.

Endian UTM 네트워크 보안 솔루션

endian 하드웨어는 사용이 간편한 올인원 제품이므로 네트워크에 최대한의 보호를 보장하기 위해 추가 모듈이 필요하지 않습니다. 고객에게 더 많은 것을 제공하기 위해 모든 기기에 고급 핫스팟 서비스가 기본 포함됩니다. endian 는 하드웨어, 소프트웨어 또는 가상머신 방식으로 제공됩니다.

하드웨어

지사 및 산업 시설에서 대규모 네트워크에 이르기까지 모든 규모의 보안 요구 사항에 맞게 UTM 소프트웨어를 통합하는 특수 설계된 완벽한 하드웨어 입니다.

가상머신

단 몇 초 내에 가상 네트워크 및 인프라를 보호하십시오. 모든 주요 가상화 플랫폼 (VMware, Xen / XenServer, Hyper-V, KVM)을 지원합니다.

소프트웨어

좋아하는 하드웨어 또는 기존 하드웨어가 모든 기능을 갖춘 Endian UTM 장비로 바뀝니다. 비즈니스 리소스에 필요한 하드웨어를 필요에 따라 확장하십시오.