elastic

Elastic을 사용하여 글로벌 개인정보 보호법 준수 지원

개요

현대 디지털 세상에서 비즈니스를 성공적으로 운영하기 위해 조직은 데이터, 특히 AI에서 데이터의 역할에 집중하고 있습니다. 이에 따라 개인정보 보호법과 규제가 폭발적으로 늘어나며 전 세계 비즈니스 환경을 재편하고 있습니다. 이러한 규제 변화의 흐름에 발맞추는 것은 단순히 위험을 줄이고 완화하는 차원을 넘어섭니다. 급변하는 개인정보 보호 법령 및 규제 환경을 준수하는 것은 고객의 신뢰를 높이고, 재무적 성장을 견인하며, 운영 회복력을 강화할 수 있는 핵심적이고 강력한 시장 차별화 요소가 됩니다.

이 백서는 개인정보 보호법의 필수 개념을 소개하고, 조직이 Elastic의 강력한 플랫폼을 활용하여 적용 가능한 개인정보 보호 요건을 충족할 뿐만 아니라, 이를 빠르고 효율적이며 안정감 있게 운영 환경에 적용하는 방법을 제시합니다. 전 세계 개인정보 보호 규정에 공통적으로 적용되는 6가지 개인정보 보호 기본 원칙을 개괄하고, 이를 Elastic의 플랫폼 솔루션과 매핑하여 조직이 개인정보 보호를 단순한 규제 준수 의무에서 시장의 강력한 경쟁 우위로 전환할 수 있도록 지원하고자 합니다.

참고: 이 백서는 정보 제공 목적으로만 제공되며 법률적인 조언을 구성하거나 대체하기 위한 것이 아닙니다. 구체적인 법률 조언은 자신의 법률 고문에게 직접 문의하시기 바랍니다.

배경 및 글로벌 개인정보 보호법 개요

글로벌 개인정보 보호법은 개인 데이터를 수집하는 조직에 점점 더 복잡한 과제를 안겨 주고 있습니다. 개인 데이터가 세계에서 가장 가치 있는 상품 중 하나로 널리 인식됨에 따라, 개인정보 보호법 준수는 기업의 중요한 비즈니스 원동력이 될 수 있습니다. 반면, 이를 준수하지 못할 경우 회사의 성장에 큰 걸림돌이 될 수 있습니다.

조직이 수집하는 개인 데이터가 늘어남에 따라, 데이터를 관리하고 보호할 수 있는 확장 가능한 솔루션을 찾는 것이 매우 중요해졌습니다. 이는 점점 더 개인정보 보호를 중시하는 세상에서 기업의 책임성을 입증하고, 신뢰할 수 있는 공급업체로서 긍정적인 평판을 쌓는 핵심 요소가 됩니다.

여러 개인정보 보호법 간에는 차이점이 있지만, 많은 법률이 몇 가지 핵심적이고 원칙을 공유하고 있습니다.

주요 개인정보 보호 법률에는 다음이 포함됩니다:

- 유럽연합(EU)의 일반 개인정보 보호법(GDPR)과 그에 상응하는 영국의 유사 규정
- 캘리포니아 소비자 개인정보보호법('CCPA')과 같은 미국 주별 개인정보 보호법
- 브라질 일반 개인정보 보호법('LGPD')
- 캐나다 개인정보 보호 및 전자문서법('PIPEDA')
- 일본 개인 정보 보호법('APPI')

Elastic 플랫폼이 제공하는 유연성과 확장성은 조직이 이처럼 다양하고 복잡한 법적 요구 사항을 효율적으로 탐색하고 관리할 수 있도록 지원합니다.

개인 데이터

이제 '개인정보(데이터)'라는 개념이 성명, 이메일 주소, 주민등록번호, 전화번호와 같은 명확한 식별자에만 국한되던 시대는 지났습니다. 오늘날 전 세계의 개인정보 보호 법률들은 특정 기기나 개인과 연관될 수 있는 모든 정보를 포착하기 위해 개인정보의 범위를 매우 광범위하게 정의하고 있습니다.

정보가 개인의 고유 식별자와 연결될 수 있는 경우 개인정보 보호법이 적용될 가능성이 높다고 가정하는 것이 적절한 실무 원칙입니다. 스마트폰, IoT 기기 및 기타 컴퓨팅 기기들이 일상에 널리 보급됨에 따라, 모든 산업 분야의 조직에서 개인정보 수집량이 급증했습니다. 이로 인해 조직이 이러한 데이터 처리를 확실하게 관리할 수 있도록 하는 제품과 서비스에 대한 필요성이 절실하고 분명하게 나타나고 있습니다.

컨트롤러 및 프로세서

전 세계의 개인정보 보호법은 조직이 개인정보의 '컨트롤러'로 행동하는지 또는 '프로세서'로 행동하는지에 따라, 서로 다르면서도 종종 중복되는 의무를 부과합니다.

- **컨트롤러**(CCPA에서는 '비즈니스'라고도 함)는 개인정보 처리의 목적과 수단을 결정합니다. 이들은 어떠한 개인정보를 수집하고 어떻게 처리할지에 대해 독립적인 결정을 내리는 주체입니다.
- **프로세서**(CCPA에서는 '서비스 제공자'라고도 함)는 상위 컨트롤러(또는 때때로 다른 프로세서)에게 서비스를 제공하며, 컨트롤러에 대한 서비스 제공을 목적으로 오직 컨트롤러의 지침에 엄격히 따라서만 개인정보를 처리할 수 있습니다.

컨트롤러와 프로세서에게 부과되는 의무는 서로 다르지만, 각자의 역할에서 법규를 준수하려면 처리 중인 개인정보의 유형을 이해하고, 개인정보를 대상에 맞게 확장 가능하며 효율적인 방식으로 찾아낼 수 있어야 합니다.

전 세계 대부분의 개인정보 보호법은 개인이 자신의 데이터에 대한 액세스, 삭제, 정정 등 특정한 권리를 행사할 수 있도록 보장하고 있습니다. 응답 기한이 비교적 짧기 때문에, Elastic과 같은 플랫폼을 활용해 비정형 및 정형 데이터 세트를 효율적으로 조사하는 것은 규정 준수 절차를 간소화할 뿐만 아니라, 규제 당국의 조사나 민사 소송의 위험을 줄이는 데에도 도움이 됩니다.

기본적인 개인정보 보호 원칙

글로벌 개인정보 보호법은 종종 기본적인 개인정보 보호 원칙을 기반으로 합니다.
이를 대략 살펴보면 다음과 같습니다.

1

고지

개인정보 보호법은 조직이 개인정보 보호 관행에 대한 정확한 최신 정보를 제공하도록 규정하고 있습니다.

2

설계 단계부터 개인정보 보호

개인정보 보호법은 조직이 자신의 관행이 개인의 개인정보 보호 권리와 이익에 어떤 영향을 미칠지 심사숙고하고, 해당 법률을 준수할 수 있도록 제품을 설계하도록 규정하고 있습니다.

3

권리

개인정보 보호법은 개인에게 자신의 개인정보에 대한 특정한 권리를 부여하며, 여기에는 데이터에 대한 액세스, 삭제 및 정정 권한 등이 포함될 수 있습니다.

4

데이터 최소화

개인정보 보호법에 따라 조직은 데이터 최소화(수집 목적에 부합하는 비즈니스 용도에 필요한 개인정보만을 수집 및 처리)를 실천해야 하며, 보유 제한 및 삭제 정책을 시행하여 조직에 필요하지 않은 데이터를 보관하지 않도록 해야 합니다.

5

보안

개인정보 보호법은 개인정보를 보호하기 위해 특정 보안 표준을 규정하고 있습니다.

6

침해 알림

개인정보에 악영향을 미치는 보안 사고나 데이터 유출이 발생할 경우, 개인정보 보호 및 보안 법률은 해당 조직에 수많은 의무를 부과합니다.

규정 미준수로 인한 비용

개인정보 보호법 위반은 막대한 벌금, 법률 비용, 평판 손상으로 이어질 수 있습니다. GDPR이나 CCPA와 같은 프레임워크에 따라 규제 벌금은 회사의 순이익에 실질적인 영향을 미칠 만큼 막대할 수 있습니다. 또한, 민사 소송 당사자들은 데이터 유출에 따른 집단 소송을 포함하여 개인정보 침해에 대한 손해 배상을 청구할 수도 있습니다.

IBM Security 와 Ponemon 연구소의 보고서에 따르면, 2024년 데이터 유출로 인한 평균 비용은 전년 대비 10% 증가한 488만 달러에 달했습니다. 또한 AON의 사이버 위험 보고서는 2024년 세간에 널리 알려진 56건의 사이버 사건이 관련 조직에 평균 27%의 주가 하락을 초래했다는 것을 밝혔습니다. 분명 이러한 종류의 평판 훼손은 조직의 경쟁 우위에 돌이킬 수 없는 타격을 줄 수 있습니다. 이러한 환경에서 규정 준수는 단순한 비용이 아니라 전략적 투자입니다.

데이터 보호와 규정 준수 요구 사항을 위해 Elastic 사용

Elastic은 개방적이고 유연한 엔터프라이즈 솔루션을 통해, 조직이 중요한 관련 답변을 전례 없는 속도로 찾아낼 수 있도록 지원합니다. 전 세계 개인정보 보호법을 준수하기 위해서는 개인정보가 어디에 저장되어 있고 어떻게 이동하며 그 외에 어떤 방식으로 처리되는지 조직의 전체 데이터 생태계에 대한 이해가 반드시 필요합니다. 바로 이러한 과정에서 Elasticsearch Platform의 진정한 가치가 발휘되며, 원활한 규정 준수를 위해 이러한 프로세스들을 단순화하고 자동화합니다. 아래에서는 위에서 설명한 6가지 기본 개인정보 보호 원칙에 부합하는 Elastic의 가치를 간략하게 설명합니다.

고지

Elastic의 데이터 매핑 기능을 통해 조직은 사내 서버뿐만 아니라 그 너머에 존재하는 개인정보의 범위와 유형을 파악할 수 있습니다.

고지는 개인정보 보호법의 핵심적인 기초 원칙입니다. 개인은 조직이 자신에 대해 수집하는 개인정보의 유형, 수집 목적, 그리고 제3자에게 데이터가 공개되는 상황을 이해할 권리가 있습니다. 데이터 개인정보 보호 법률은 대개 조직이 이러한 개념들을 설명하는 포괄적인 개인정보 처리방침을 제공할 것을 요구하며, Elastic 또한 자체적인 개인정보 보호 정책을 통해 이를 실천하고 Elastic Trust Center에서 이러한 개념을 상세히 안내하고 있습니다.

이 고지 원칙을 준수하려면 조직은 수집하는 개인정보의 범위를 이해해야 합니다. 이를 위해서는 조직 내 모든 개인 데이터 흐름을 식별하고 문서화하는 체계적인 프로세스인 강력한 데이터 매핑 작업이 필요합니다.

확장 가능한 솔루션이 없으면 조직은 많은 경우 수집된 개인정보와 그 데이터가 내외부로 이동하는 경로를 식별하기 위해 뒤죽박죽이 된 구식 스프레드시트, 데이터 인벤토리 설문 조사에 대한 응답, 다양한 사업부와의 마구잡이식 인터뷰에 의존해야 할 수밖에 없습니다.

기껏해야 그러한 기록들은 작성된 그 순간에만 정확할 뿐이며, 데이터가 동력이 되는 경제 체제 내의 데이터 수집 및 처리 요구 사항으로 인해 어려움을 겪게 됩니다.

Elastic은 조직이 데이터 매핑 프로세스를 개선하는 데 필요한 핵심적인 인사이트 확보할 수 있도록 지원합니다. 어떠한 유형의 개인정보가 수집되는지, 해당 데이터가 어디에 위치하는지, 그리고 누구에게 공개되는지에 대한 파악 없이는 조직이 개인전보 보호법을 준수하고 있다고 확언할 수 없습니다. 데이터 흐름에 관한 정보를 Elastic에 색인함으로써, Elastic의 강력한 풀텍스트 검색 기능을 통해 개인정보에 의존하는 애플리케이션, 테이블, 쿼리 또는 보고서들을 신속하게 식별할 수 있습니다.

Elastic을 사용하여 데이터 매핑을 효율화하면 조직이 개인정보 보호법의 계약 의무를 준수하는 데에도 도움이 됩니다. 식별된 데이터 흐름을 통해 조직이 데이터 보호 부속 합의서, 데이터 전송 메커니즘 또는 기타 개인정보 보호 관련 특약 체결이 필요한 대상이 누구인지 판단할 수 있기 때문입니다. 마찬가지로, 오늘날의 공급망은 수백 혹은 수천 개의 공급업체와 하위 처리업체로 확장될 수 있습니다. 수천 개의 계약서를 색인하고 즉각적으로 풀텍스트 검색을 수행할 수 있는 능력은 공급업체 상태 보고서 작성을 용이하게 하며, 무엇보다 중요한 것은 선제적인 공급업체 관리 프로그램을 가능하게 한다는 점입니다.

설계 단계부터 개인정보 보호

조직은 Elastic을 사용하여 데이터 최소화 원칙을 구축하는 등 설계 단계부터 개인정보 보호를 강화할 수 있습니다.

조직이 개인정보 저장소로 Elastic을 사용하는 것을 고려하고 있다면, Elastic의 중앙 오케스트레이션 소프트웨어인 Elastic Cloud Enterprise('ECE')의 기능을 통해 시작 단계부터 올바른 방향을 잡을 수 있습니다. 설계 단계부터 데이터 보호 원칙은 액세스 제한, 정확성 유지, 적절한 데이터 보안 제어 적용, 그리고 보관 기간 제한을 통해 개인정보를 가치 있는 자산처럼 취급하는 것을 의미합니다.

하나의 대규모 데이터 저장소와 복잡한 중복 데이터 액세스 제어(다양한 프로젝트에서 특정 데이터에만 액세스를 허용하는 데 필요)가 있는 기존 데이터 아키텍처와 달리, Elastic은 프로젝트별로 새로운 Elasticsearch 클러스터를 실체화하고 해당 프로젝트와 관련된 데이터만 클러스터에 포함할 수 있도록 지원합니다.

이러한 분산 아키텍처는 또 다른 핵심 개인정보 보호 원칙인 개인정보 최소화를 가능하게 합니다. 예를 들어, 고객은 Elastic을 사용하여 데이터를 저장 공간 계층별로 분류할 수 있습니다. 이때 Elastic이 제공하는 액세스 로그 정보를 통해 비즈니스에 사용되지 않는 데이터를 식별해 데이터 보존 정책과 관행을 수립하는 데 근거가 될 수 있습니다.

또한 Elastic은 조직이 언제, 어떻게 개인정보 보호 영향 평가(DPIA)를 실시해야 하는지 파악할 수 있도록 지원합니다. DPIA는 GDPR 및 유사한 개인정보 보호 규정에 따라 개인정보를 책임감 있게 처리하고 개인에게 미칠 수 있는 잠재적 피해를 최소화하기 위해 수행되는 의무적인 평가 절차이기도 합니다. 데이터가 어디에 있는지, 어떻게 처리되는지, 그리고 어디로 흐르는지 파악하면 DPIA 과정을 효율화할 수 있습니다. 이는 전통적으로 DPIA는 개인정보의 사용처를 파악하기 위해 여러 부서 간의 다각적인 협력이 필요했던 작업입니다. DPIA는 기본적인 규정 준수를 입증하는 동시에, 조직이 글로벌 개인정보 보호법에 따라 허용된 범위 내로만 개인정보 처리를 제한할 수 있도록 합니다.

데이터 주체의 권리

조직은 Elastic을 사용하여 관련 개인정보를 식별하고, 정보 주체의 권리 적용 여부를 평가하며, 정보 주체의 요청을 이행할 수 있습니다.

글로벌 개인정보 보호법은 개인이 자신의 개인정보가 처리되는 방식에 대해 특정 선택권을 갖게 합니다. 이러한 권리에는 일반적으로 개인정보에 대한 액세스 권한, 삭제 권한, 정정 권한과 더불어 특정 유형의 개인정보 처리에 반대할 권리가 포함됩니다. Elastic의 데이터 매핑 기능은 조직이 데이터 주체의 요청을 처리할 수 있게 하는 핵심적인 토대를 형성합니다.

- **액세스:** Elasticsearch를 통해 조직은 데이터 저장소를 검색하여 조직 전체에 흩어진 개인정보를 식별할 수 있으며, 여기에는 개인정보에 의존하는 테이블, 쿼리, 보고서 또는 애플리케이션을 파악하는 것이 포함됩니다. 또한 조직은 Elastic을 활용하여 최종 사용자 검색 기능을 구현함으로써, 최종 사용자가 직접 자신의 데이터를 검색하게 할 수 있습니다. 최종 사용자에게 이러한 강력한 검색 기능을 제공하면 최종 사용자가 셀프 서비스 도구를 통해 자신의 데이터를 식별하고 내보낼 수 있으므로 고객 지원 요청이 줄어듭니다. 셀프 서비스 도구만으로 부족한 경우, 조직은 Elastic을 사용해 자체 데이터 저장소를 신속하게 검색하여 데이터 주체의 액세스 요청을 이행할 수 있습니다.

- **삭제:** Elastic을 사용해 개인에 대해 보관 중인 개인정보를 식별한 후, 조직은 해당 데이터를 변형하는 데 Elastic을 추가로 활용할 수 있습니다. 여기에는 삭제 예외 조항에 따른 보존 데이터 태깅, 영구 삭제, 그리고 익명화나 특정 유형의 개인정보 가명화처럼 개인정보 보호법에서 허용하는 기타 삭제 기술의 적용이 포함됩니다. 비용이 많이 드는 엔지니어링 구축 없이 Elastic을 통해 개인정보를 신속하게 변형함으로써, 조직은 규정을 준수하고 감독 기관의 조사를 피하며, 글로벌 개인정보 보호법의 테두리 내에서 데이터의 유용성을 유지할 수 있습니다.

- **수정:** 마찬가지로, 개인정보 보호법은 개인이 자신의 개인정보에 대한 정정을 요청할 수 있도록 허용하는 경우가 많습니다. Elastic은 개인에 대해 보관된 개인정보를 격리할 수 있으므로, 조직은 데이터를 찾는 데 시간을 허비하지 않고 요청을 처리하는 데만 집중할 수 있습니다.

- **처리 제한:** GDPR 및 영국의 유사 법률과 같은 일부 개인정보 보호법은 개인정보 처리에 대한 반대권이나 처리 제한을 요청할 권리도 포함하고 있습니다. 조직은 Elastic의 데이터 매핑 및 데이터 분류 기능을 사용하여 이러한 요청에 어떻게 대응할지 신속하게 확인하고, 그에 맞춰 액세스 및 사용 권한을 제한할 수 있습니다. 이를 통해 귀중한 시간을 절약하고, 규정 준수 팀이 법에서 규정한 짧은 기한 내에 요청에 응답할 수 있도록 지원합니다.

데이터 최소화

설계 단계부터 개인정보 보호 섹션에서 미리 살펴본 바와 같이, Elastic은 기업의 데이터 최소화 역량을 지원합니다. 데이터 최소화 원칙에 따라 조직은 개인정보의 수집과 처리, 보존을 조직이 승인한 처리 목적을 달성하는 데 필요한 정보로만 한정해야 합니다.

예를 들어, 이러한 의무를 충실히 이행하기 위해 개인정보 처리를 최소화하는 한 가지 방법은 **가명화**(정보 내의 개인 식별자를 대체 값으로 교체) 또는 **익명화**(더 이상 개인을 식별할 수 없도록 정보에서 개인 식별자를 완전히 제거)를 통하는 것입니다. 유럽의 한 선도적인 항공사가 저장 전 단계에서 Elastic 수집 파이프라인을 사용하여 민감한 데이터를 어떻게 난독화하는지 확인해 보시기 바랍니다. 이러한 성과는 다양한 소스에서 데이터를 수집하여 익명화 및 가명화를 포함한 데이터 변형을 용이하게 하는 Elastic의 통합 도구인 Logstash를 통해서도 달성할 수 있습니다. 이를 통해 데이터 최소화 목표를 달성하고 데이터 보안 위험을 줄일 수 있습니다.

데이터 매핑과 감사를 위해 Elastic을 사용하면 조직은 보관된 개인정보의 실제 사용 현황을 더욱 면밀히 분석할 수 있으며, 이를 통해 조직은 데이터 보존 기간과 정책을 보다 효과적으로 맞춤 설정할 수 있습니다.

보안 및 침해 알림

Elastic이 조직의 개인정보를 보호하고 데이터 유출 사고 발생 시 신속하게 대응하도록 돕는 방법에 대한 자세한 내용은 Elastic의 보안 백서를 검토해 주시기 바랍니다.

결론

데이터 개인정보 보호는 단순한 규제 요건이 아니라 비즈니스에 필수적인 요소입니다. 막대한 벌금, 비즈니스 중단, 평판 훼손 및 고객 신뢰 상실의 위험에 직면한 상황에서 조직은 데이터를 매핑, 분류, 관리, 변환, 분석 및 삭제할 수 있는 신뢰할 수 있고 확장 가능한 방법이 필요합니다. Elastic은 이 프로세스의 모든 단계를 간소화하여, 조직의 규정 준수와 고객 신뢰 확보에 필요한 확장 가능한 역량을 제공합니다.

