Informatica

백서

GDPR의 'D'에 대처하는 방법에 대한 권고

Informatica 정보

디지털 변혁은 우리의 기대치를 바꿔 놓았습니다. 이제 더 적은 비용으로 더 나은 서비스를 더 빠르게 제공할 수 있어야 합니다. 이러한 상황에 부응하기 위해서는 기업은 변화해야 하며, 데이터가 이에 대한 해답을 쥐고 있습니다.

엔터프라이즈 클라우드 데이터 관리 분야의 세계적인 선도 기업인 Informatica는 모든 부문, 카테고리, 틈새시장에서 지능적인 방식으로 고객을 지원할 준비가 되어 있습니다. Informatica는 더욱 민첩하게 운영하고, 새로운 성장 기회를 발견하거나 새로운 혁신을 이룰 수 있는 통찰력을 기업에 제공합니다. 모든 종류의 데이터에 100% 집중하여 성공에 필요한 다양한 서비스를 제공하고 있습니다.

Informatica가 제공하는 모든 것에 대해 알아보고 다음에 올 지능형 혼란을 타개하기 위해 데이터의 힘을 활용해 보시길 바랍니다.

목차

1. 총괄 요약

2018년 5월부터 유럽 연합 일반 정보 보호 규정(GDPR)이 시행되어 개인 정보 보호가 강화됩니다. GDPR은 EU에서 설립된 모든 조직뿐 아니라 EU 정보 주체의 개인 정보를 보유하고 있는 조직(세계 어느 곳이나 무방)이 EU 정보 주체에게 재화나 용역을 제공할 때 또는 EU 정보 주체의 활동을 모니터링하거나 추적할 때 적용됩니다. 이 규정은 여러 조직은 물론 조직이 고객, 소비자, 파트너, 직원 및 기타 "정보 주체"(여기서 "정보 주체"는 개인)와 관련된 데이터를 관리하는 방식에도 상당한 영향을 미칠 수 있습니다. GDPR은 개인의 데이터 기록의 저장, 처리, 액세스, 전송, 공개에 영향을 주는 데 그치지 않고 위반 시 상당한
처벌이 따를 수 있습니다.

GDPR에 따르면 조직은 현재 및 장래의 정보 자산을 사용하는 방법을 충분히 숙지하여 이러한 새로운 데이터 기밀 보호 요건을 통합하고 시민의 프라이버시 권리를 강화해야 합니다. 많은 조직의 경우, 이에 수반되는 정보 관리 관행의 변화로 인해 현재 및 장래의 데이터 기능에 대한 철저한 평가가 필요할 것입니다. 이 백서에서는 이러한 요구 사항을 나눠 살펴보는 것이 데이터 과제 이해에 어떤 도움이 되며 조직이 GDPR 이니셔티브와 관련하여 어떤 방향을 택해야 하는지 알아봅니다.

이해를 돕기 위해 이 백서에서는 GDPR 여정에 관한 많은 조직의 몇 가지 공통적 질문을 살펴봅니다. 이런 질문을 진입점 질문이라고 합니다. 각각의 진입점 질문에 답하도록 돕기 위해 Informatica는 중요하다고 생각되고, 각 기능에 맞춰져 있으며, 각 기능의 개발 방법에 대한 기술 활용 사례인 일련의 기능 요구 사항을 제시했습니다. 아래 표는 이 항목들이 어떤 관계에 있는지 보여 줍니다.

진입점 질문	기능 요구 사항	기술 활용 사례
우리의 잠재적인 범위 내 데이터는 모두 어디에 있는가?	민감한 데이터 검색 및 위험 분석	탐지 및 보호
우리 개인 정보가 어떻게 사용되고 있는가?	정책 해석	엔터프라이즈 데이터 거버넌스
정보 주체 데이터를 어떻게 관리해야 하는가?	개인 정보 관리	데이터 일치 및 연결 활용 사례
어떻게 데이터를 보호하고 무단 액세스를 방지해야 하는가?	데이터 보안 제어 활성화	탐지 및 보호

동의 획득 및 관리와 같이 요구 사항이 여러 기능 요구 사항 및 기술 활용 사례에 걸치는 예도 있기 때문에 조직들은 관련된 잠재적 복잡성에 대한 명확한 이해가 필요합니다.

GDPR이 던져 주는 과제도 많지만, 데이터 사용과 관련된 많은 기회 또한 제공합니다. 이 백서에서는 잠재적 활용 사례 접근법을 설명하고 Informatica의 깊이 있는 데이터 관리 경험을 바탕으로 조직들이 이러한 과제를 해결하는 동시에 혁신적 데이터 관리, 거버넌스, 보안 기능을 도입하여 규정 준수 프로그램을 극대화하도록 돕습니다. Informatica는 데이터 자동화, 보안, 제어를 위한 통합되고 혁신적인 소프트웨어 솔루션을 제공하며, 이러한 솔루션은 조직의 GDPR 이니셔티브를 신속히 지원할 수 있습니다.

2. 배경

2.1 일반적 배경 및 잠재적 영향

사회가 급속히 디지털화되면서 거의 모든 조직은 데이터의 힘을 활용하여 비즈니스 결정을 개선하고, 고객 및 파트너를 상대하며, 혁신적 비즈니스 프로세스를 추진하고 있습니다. 유럽 연합 집행 위원회는 생성, 수집, 처리, 저장되는 데이터 상당 부분이 사실상 개인 정보이며 EU 정보 주체의 방대한 정보를 노출시킬 수 있음을 인정했습니다.

기존의 데이터 보호 규정은 개인 정보의 보호와 안전에 관한 우려를 효과적으로 불식시키지 못했습니다. EU 회원국의 다양한 데이터 보호 규정은 정보 주체들의 불만의 대상이었으며, 90%는 데이터가 저장 또는 처리되는 곳에 상관없이 EU 전체적으로 동일한 데이터 보호 규정을 원한다고 답했습니다.*

이에 따라 디지털 시대 시민의 기본적인 프라이버시 권리를 보다 잘 보호하고 데이터 보호 법률의 다양성과 관련된 우려를 해결하기 위해 GDPR이 제정되었습니다.

2018년 5월부터 여러 조직은 GDPR에 따라 고객, 시민, 직원 및 그 밖의 사람들에 대한 데이터를 보다 효과적으로 관리하고 보호해야 합니다. 이 규정은 국적 또는 거주지를 불문하고 EU 정보 주체에 적용되어 개인 정보 보호에 대한 원칙과 규칙을 제공합니다.

GDPR이 "원칙" 기반 규정이라는 것은 조직마다 고유한 업무 및 데이터 사용 상황에 따라 이행하거나 하지 말아야 할 의무를 고려해야 함을 뜻합니다. 따라서 많은 조직은 이러한 원칙을 해석해 GDPR 이니셔티브의 길잡이로 삼아야 합니다.

GDPR에 따라 많은 조직은 현재 및 장래의 정보 자산을 활용하는 방법을 보다 잘 이해하여 이러한 새로운 데이터 기밀 보호 원칙을 준수해야 합니다. 이는 여러 조직의 사람, 프로세스, 기술, 데이터 관리 관행 및 정책에 영향을 미칩니다.

이 규정을 위반할 경우, 위반의 종류와 규모에 따라 상당한 벌금에 처해질 수 있습니다. 적용되는 벌금은 최고 2,000만 유로 또는 조직의 전 세계 총 연 매출의 4% 중 더 큰 액수입니다.

2.2 GDPR은 누구와 관련됩니까?

GDPR 준수에는 여러 차원이 있으며 실제 지리적 위치로 국한되지 않습니다. 북미, 아시아 및 기타 지역의 조직도 EU 정보 주체의 데이터를 저장하고 처리하는 경우, GDPR을 준수해야 합니다. 오늘날에는 전문 데이터 처리 기업만이 아니라 소비자와 직접 거래하는 조직(B2C) 및 다른 조직과 거래하는 조직(B2B)에서도 개인 정보를 취급합니다. EU 정보 주체에 대한 데이터를 처리하는 조직은 운영 또는 데이터 센터가 물리적으로 위치한 국가가 어딘지에 상관없이 규정 준수 요구 사항을 완벽히 숙지해야 합니다.

* http://ec.europa.eu/justice/data-protection/reform/index_en.htm

2.3 데이터 관점에서 GDPR이 까다로운 이유는 무엇입니까?

여러 조직에는 GDPR과 관련된 명확한 데이터 과제가 있습니다. GDPR 준수는 개인 정보가 조직 내 어디에 있건 상관없이 이를 제어하고 관리해야 함을 뜻합니다. 하지만 데이터가 조직 전체와 비즈니스 생태계까지 확산됨에 따라 데이터 관리가 어려워질 수 있습니다. 데이터 다양성의 증가와 클라우드 기반 컴퓨팅으로의 전환 같은 유의미한 추세로 인해 고도로 역동적인 IT 지형이 만들어짐으로써 데이터 관리 및 보안의 어려움이 가중됩니다. 이러한 어려움을 보여 주기 위해 Informatica는 여러 조직이 GDPR과 관련하여 답하려 애쓰고 있는 몇 가지 질문을 제기합니다.

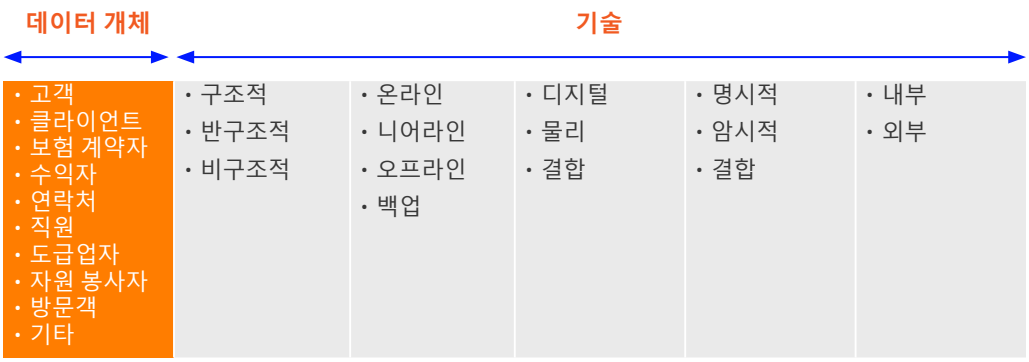
- GDPR 원칙이 적용될 수 있는 관련된 모든 범위 내 데이터는 조직과 조직의 생태계 어디에 있습니까? 이 데이터가 위험에 처해 있습니까?
- 조직들은 운영 생태계에서 데이터를 어떻게 추적 관리하고 있습니까?
- 조직은 필요한 모든 정책과 절차를 적용하고 집행하기 위해 모든 관련 데이터 자산을 어떻게 정의하고 관리합니까?
- GDPR 원칙이 적용되는 모든 관련된 범위 내 데이터 기록은 조직의 어디에 보관되어 있습니까? 이들을 식별하고 연결할 방법은 무엇입니까?
- 조직은 정보 주체가 제공하는 동의를 어떻게 획득하고 관리합니까? 조직은 정보 주체의 동의 여부 선택의 변경이나 동의의 정의를 어떻게 관리할 수 있습니까?
- 조직은 어떻게 하면 필요한 기간 내에 정보 접근 요청, 삭제 권리, 정보 이동 요청에 효율적이고 효과적으로 대응할 수 있습니까?
- 조직은 관련 데이터에 대한 접근을 어떻게 제어합니까? 조직의 기능 또는 활동에 필요하지 않은 개인 정보 데이터는 제거됩니까?

2.4 범위 내에 포함될 수 있는 데이터 유형

또 다른 잠재적 과제는 조직이 보유한 데이터의 유형에 어떻게 대응하느냐입니다. 이 맥락에서 유형은 다음 두 가지로 정의됩니다.

1. 데이터 개체 유형
2. 데이터 개체 유형을 관리하는 기술 유형

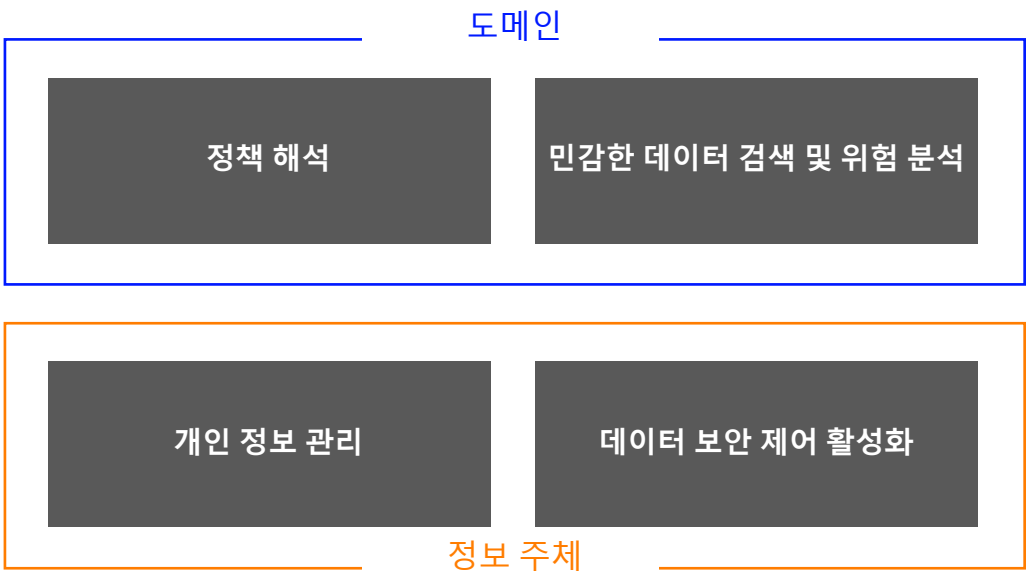
정보 주체 정보의 대부분은 하나 이상의 데이터 개체 유형 및 하나 이상의 기술 유형에 속합니다. 아래 다이어그램은 범위 내 GDPR 데이터에 적용될 수 있는 데이터 및 기술 유형의 몇 가지 예를 보여 줍니다.



이처럼 유형이 다양하기 때문에 조직은 범위 내 GDPR 데이터 자산의 포착과 관리를 위해 아주 다른 접근법, 방법, 기술을 고려해야 할 수도 있습니다.

3. 진입점, 기능 요구 사항, 기술 활용 사례

Informatica는 이해와 인식을 높이고 활동 계획 수립을 돕기 위해 몇몇 일반적인 GDPR 데이터 과제가 부각된 몇 가지 핵심적인 진입점 질문을 파악했습니다. 이러한 진입점은 종종 사람, 프로세스, 기술을 신중히 고려해야 답할 수 있는 간단한 질문에 좌우됩니다. 이러한 질문에 답할 수 있도록 Informatica는 필요한 잠재적 기능과 필요한 기능을 제공하는 일부 기술 활용 사례를 제시했습니다. 필요한 기능은 그룹으로 체계화되어 있습니다. 아래 다이어그램은 이런 그룹화의 원리와 각 그룹의 관련성을 보여 줍니다.



이러한 기능은 도메인과 정보 주체라고 하는 두 가지 영역에 속합니다.

도메인은 정보 주체 데이터의 도메인과 연관됩니다. 도메인은 범위를 정의하고 데이터에 대한 조직적 관점을 제공하는 데 사용되는 도메인 검색 및 관리에 대한 통찰을 제공하도록 돕습니다.

정보 주체는 트랜잭션 수준에서 실제 정보 주체 데이터와 연관됩니다. 정보 주체는 주체 수준 대응 및 주체 수준 통찰을 제공하는 데 사용되는 개인 정보 관리에
대한 통찰을 제공하도록 돕습니다.

3.1 진입점 질문: 우리의 잠재적인 범위 내 데이터는 모두 어디에 있는가?

배경: 일반적으로 데이터는 기업 내의 여러 시스템, 애플리케이션, 출처에 산재해 있습니다. 대규모 조직이나 인수를 통해 규모가 커진 조직에서는 더욱 그렇습니다. EU 정보 주체가 조직에서 할 수 있는 역할(고객, 공급업체, 파트너, 직원 등)로 인해 개인 정보가 한 부서 또는 시스템으로 국한될 가능성은 낮습니다. 다양한 IT 시스템이 있는 조직은 핵심 애플리케이션에 있는 데이터뿐 아니라 스프레드시트, 로컬 데이터베이스, 빅 데이터 솔루션에 있는 데이터도 고려해야 합니다.

필요한 기능: 민감한 데이터 검색 및 위험 분석은 다양한 기술 솔루션에서 데이터를 검색하고 실제 데이터 양 및 데이터 확산 같은 다른 정보 출처와 함께 사용하여 데이터의 위험 점수를 작성할 수 있는 기능입니다. 위험 점수는 조직에서 가장 위험도가 높은 데이터가 저장된 곳을 파악하여 위험에 따라 잠재적인 개선 또는 보안 제어 요구 사항 우선 순위를 정하는 데 도움이 됩니다. 장기적으로 위험 점수를 추적하면 개선 또는 제어 활동으로 데이터 위험 포지션이 개선되었는지 알 수 있습니다. 합법적 목적을 뒷받침하려면 동의가 필요할 수 있으므로 데이터 계보(data lineage) 같은 기능은 조직이 새로운 개인 정보 저장소를 파악해 개인 정보 사용의 잠재적 변화를 이해하는 데 도움이 됩니다.

기술 활용 사례: 민감한 데이터 검색 및 위험 분석은 탐지 및 보호 활용 사례로 특징지을 수 있으며, 탐지에 중점을 둡니다. 이는 범위 내의 민감한 데이터가 어디에 있고 어디로 확산되는지에 대한 통찰과 데이터 위험에 대한 분석적 통찰을 제공하는 핵심 기능입니다. 이 활용 사례에 적용할 수 있는 일반적 기능은 다음과 같습니다.

- **데이터 정책 정의:** 비즈니스 및 IT 정의, 애매한 데이터, 정책 충돌
- **자동화된 데이터 검색:** 관련된 범위 내의 민감한 데이터 찾기, 일차 통과(first pass) 및 지속적 모니터링, 데이터 분류, 지원 시스템 통합
- **데이터 확산:** 데이터가 어디에 있는가? 데이터가 어디로 가는가? 새로운 출처?
- **데이터 위험 점수 결정:** 데이터 이동 + 확산 + 접근 + 용량에 기반, 우선 순위 결정 및 계획, 이력, 시간 경과에 따른 점수 모니터링
- **데이터 보호:** 데이터 접근 제한이 필요한 곳, 익명화해야 하는 데이터, 암호화를 적용해야 하는 곳 파악 및 시간, 위치, 역할에 기반한 데이터 보기

기술 솔루션: Informatica Secure@Source를 사용하여 범위 내 데이터 위치 발견, 데이터 분류, 데이터 확산 모니터링, 위험 점수 할당에 도움을 받을 수 있습니다. 시간 경과에 따른 추적을 통해 변화가 규정 준수 노력에 긍정적 영향을 미치는지 부정적 영향을 미치는지 알 수 있습니다.

이점: 데이터 위치에 대한 통찰을 제공할 뿐 아니라 위험에 따라 데이터 등급을 정합니다.

3.2 진입점 질문: 우리 개인 정보가 어떻게 사용되고 있는가?

배경: 세계는 모든 부문에 영향을 미치는 디지털 변혁을 겪고 있습니다. 생성, 수집, 분석되는 데이터의 증가 추세는 전 세계적으로 뚜렷하며, 이 데이터 중 상당 비율은 개인의 개인 정보로 볼 수 있습니다. 조직에서 데이터가 확산됨에 따라 이 데이터의 소유권, 제어, 관리는 더욱 어려워집니다. 여러 규정 준수 형식처럼 GDPR 준수도 데이터 거버넌스에 기업 차원에서 접근하는 것이 최선입니다.

필요한 기능: 정책 해석이란 정책, 책임, 프로세스, 데이터 용어, 논리적 및 물리적 모델에 대한 비즈니스 및 기술 이해를 획득하는 기능입니다. 중요한 것은 여기서 기술 환경에 대한 이해와 비즈니스 환경에 대한 이해가 연결된다는 점입니다. 이 연결은 범위 내 데이터 도메인 관련 정보에 대한 총체적 관점을 조직에 제공하고, 데이터 자산 관리에 대한 접근법의 불가결한 부분을 형성합니다.

기술 활용 사례: 정책 해석은 기업 데이터 거버넌스 활용 사례로 특징지을 수 있습니다. 이는 조직의 데이터 관리에 대한 하향식 및 상향식 관점을 제공하고 정보에 대한 비즈니스 관점과 IT 관점을 연결하는 핵심 기능입니다. 이 활용 사례에 적용되는 일반적 요구 사항은 다음과 같습니다.

- **정책 정의:** 비즈니스 정의 및 IT 정의, 전체 비즈니스 운영 수준에서의 문서화, 논리적/물리적 데이터 및 프로세스 모델
- **책임:** 누가 데이터를 소유하고, 누가 데이터를 사용하며, 어떤 기능이 품질과 보안을 책임지는가?
- **용어의 정의 및 프로세스:** 비즈니스 프로세스, 주요 데이터 개체, 속성, 시스템, 품질 및 제어, 표준화, 동의의 비즈니스 정의
- **변경 프로세스:** 관리되는 정의 프로세스, 관리되는 변경 프로세스, 프로세스 거버넌스
- **아티팩트와의 연결:** 논리적-물리적 아티팩트 연결, 기술적/비즈니스 데이터 계보, 데이터 품질 통합

기술 솔루션: 비즈니스 및 IT 기능이 데이터 거버넌스의 공통 목표를 위해 협력할 수 있도록 하는 엔터프라이즈 데이터 거버넌스 솔루션 채택. **Informatica Axon Data Governance** 같은 솔루션은 비즈니스와 IT의 데이터 관점을 통합하고 논리적 데이터 자산과 물리적 데이터 자산 간의 연결을 생성하도록 특별히 설계되었습니다.

이점: 조직이 범위 내 데이터를 위한 총체적 데이터 거버넌스 기능을 빠르게 구축해야 하는 프로세스, 정책, 데이터 개체 정의에 모든 주제 전문가가 신속하고 손쉽게 기여.

3.3 진입점 질문: 정보 주체 데이터를 어떻게 관리해야 하는가?

배경: 복잡한 IT 환경에서 데이터가 다양하게 사용되기 때문에 개별 정보 주체들의 모든 정보에 대한 단일한 관점을 형성하기는 어렵습니다. 이 어려움은 시스템마다 데이터 저장 및 인덱싱에 사용하는 메커니즘이 크게 다르다는 점에서 기인합니다. 개별 정보 주체의 데이터와 이 데이터를 조직 내에서 저장, 관리 또는 처리하는 방법에 대한 완전한 관점이 없다면 GDPR 준수는 어려워지며, 개별 정보 주체의 권리와 관련된 어려움은 특히 큽니다.

필요한 기능: 개인 정보 관리는 식별된 모든 출처 내의 정보 주체 기록을 식별하여 각 개별 정보 주체의 기록을 일치 및 연결하며, Entity 360 리포지토리를 생성하는 기능입니다. 이 리포지토리는 범위 내 출처에서 어떤 실제 데이터 기록이 보유되며 각 데이터 조각이 개별 정보 주체에 어떻게 연결되는지에 관한 고품질 데이터 출처를 제공합니다. Entity 360은 조직이 정보 접근 요청, 삭제 권리 또는 정보 이동 요청에 대응할 때 권위 있는 정보 출처 역할을 할 수 있습니다. 비즈니스 관점에서 볼 때 Entity 360은 개인 정보 사용 동의에 대한 조직의 관리를 지원할 수 있고, 그 다음 어떤 채널을 통해 언제 동의했는가/동의를 철회했는가 및 어떤 구체적 약관에 동의했는가 등 이 동의에 대한 관리도 지원할 수 있습니다.

기술 활용 사례: 개인 정보 관리는 데이터 일치 및 연결 활용 사례로 특징지을 수 있습니다. 이는 시스템에서 정보 주체 기록을 식별하고 유사한 기록을 일치시켜 연결을 생성함으로써 데이터에 대한 교차 시스템적 관점을 제공하는 핵심 기능입니다. 이 활용 사례에 적용할 수 있는 일반적 기능은 다음과 같습니다.

- **관련 데이터에 대한 접근:** 정보 주체 데이터 프로파일링, 원본 시스템에서 관련 데이터 추출, 반구조적/비구조적 콘텐츠에 분석 프로세스 적용
- **데이터 품질 처리:** 데이터 품질 수준 평가, 수동/자동 개선 적용, 수동 개선을 위한 프로세스 제어, 지표 보고
- **동의, 동의 획득 방법, 동의 관리 방법 등 정보 주체에 대한 신뢰할 수 있는 단일 데이터 출처:** 동의에 따라 주체에 대한 다양한 관점과 견해를 포함합니다
- **일치 및 연결:** 비즈니스 프로세스를 정의하고, 기록을 일치시키며, 유사한 기록을 점수에 연결하고, 동의와 연결
- **데이터 지속성:** 연결된/연결되지 않은 기록, 분석, 보고서 유지

기술 솔루션: 고급 알고리즘을 사용하여 데이터가 저장된 곳에 상관없이 동일 정보 주체에 관련된 모든 데이터를 일치시킴으로써 모든 데이터 도메인에서 정보 주체 기록 검색에 도움이 되는 솔루션 채택. **Informatica Relate 360**은 고급 알고리즘을 활용하여 동일 정보 주체에 연결된 데이터를 식별하고, 마스터 데이터 관리는 정보 주체 관련 데이터에 대한 공통적 관점을 유지하고 관리할 수 있는 프레임워크를 제공합니다.

이점: 개인들에 대한 단일 관점은 GDPR을 뛰어넘는 비즈니스 효과가 있음을 보여 주었습니다. 이는 해당 개인이 맞춤형 개인 경험에 대한 기대가 커지고 있는 고객인 경우에 특히 그렇습니다. GDPR 관점에서 볼 때 각 개별 정보 주체의 모든 데이터를 연결할 수 있다면 해당 개인의 권리를 행사할 수 있도록 해야 하는 부담을 덜어줍니다. 여기에는 데이터 사용을 이해할 권리, 잊혀질 권리, 동의가 올바르게 활용되도록 하는 것 등이 포함됩니다.

3.4 진입점 질문: 어떻게 데이터를 보호하고 무단 액세스를 방지해야 하는가?

배경: 데이터 보호 제어는 GDPR 동의 요구 사항 규정 및 개인 정보 보호를 위한 접근법입니다. 테스트 목적으로 사용되는 프로덕션 데이터를 제거, 마스킹 또는 익명화하거나 외부 데이터 전송에 사용되는 데이터를 익명화해야 한다는 IT의 요구 사항이 있을 수 있습니다. 규정 준수를 위해 애플리케이션에서 사용자 수준의 개인 정보에 대한 데이터 접근 제어를 검토해야 합니다.

필요한 기능: 탐지 및 보호 역시 정보 주체 관련 정보에 대한 접근 제어와 보호를 제공합니다. 정보 주체 정보는 조직과 조직 생태계의 다양한 개인들에게 종종 노출됩니다. 데이터 보안 제어는 봐서는 안 될 사람들에게서 정보 주체 정보를 제거하거나 숨기고, 봐야 할 사람들은 볼 수 있도록 하는 데 사용됩니다.

기술 활용 사례: 동의 제어 활성화는 탐지 및 보호 활용 사례로 특징지을 수 있습니다. 이는 데이터 접근을 보호하여 마스킹, 암호화, 접근 제어 같은 데이터 중심 제어를 적용하고 데이터와 애플리케이션의 아카이빙 및 삭제 등 데이터 수명 주기를 관리하는 핵심 기능입니다. 이 활용 사례에 적용할 수 있는 일반적 기능은 다음과 같습니다.

- **위험 분석 입력:** 위험 점수를 사용하여 데이터 제어 방법 지시
- **오케스트레이션:** 식별된 위험과 안전하지 않은 접근 또는 조건에 대한 모니터링을 기반으로 데이터 보호 작업을 예약하고 조정하는 기능
- **데이터 보안 제어:** 정적 또는 동적 마스킹, 익명화, 역할 기반 접근, 암호화 또는 토큰화.
- **변경/업데이트 기록:** 원본 시스템 대비 애플리케이션, 동의 기록 대비 기록 마스킹 또는 아카이빙 결과, 증거를 위한 감사 내역 생성
- **아카이빙:** 프로덕션 시스템에서 데이터 아카이빙, 활동을 기록하여 증거 제공, 우발적 사용 또는 접근 방지를 위해 오프라인으로 이동

기술 솔루션: 데이터 자산의 수명 주기 관리에 도움이 될 수 있는 솔루션을 채택하고 이러한 자산에 대한 제어 적용. **Informatica Persistent Data Masking**과 **Informatica Dynamic Data Masking**을 사용하여 개인 정보에 대한 무제한 접근이 가능한 사람 및 시스템 수를 자동으로 제한할 수 있습니다. **Informatica Secure@Source**는 보안 제어 업데이트를 오케스트레이션하여 데이터 보안 개선을 제공합니다.

이점: 데이터 마스킹에 자동화를 도입하여 개인 정보 침해 위험을 줄입니다. 개인 정보의 가시성은 조회 권한이 있는 사람들로 제한되며, 적절한 보호 없이는 개인 정보가 확산되지 않습니다.

4. 파트너

많은 규정과 규정 준수 형식이 그렇듯 기술만으로는 규정 준수를 보장할 수 없습니다. 조직은 기존 서비스 및 기술 솔루션을 제공하는 것 외에 GDPR 여정을 위한 최선의 사고 리더십이 필요합니다. Informatica는 고도로 숙련된 파트너들과 협력하여 광범위한 GDPR 이니셔티브를 지원하고 있습니다. 이 파트너들은 데이터 관리를 깊이 이해하고 GDPR 준수에 주력하고 있기 때문에 특별히 선택되었습니다.

적합한 파트너를 찾거나 요구 및 요건에 따라 최선의 파트너를 찾도록 도와줄 현지 Informatica 담당자에게 문의하십시오.

5. 결론

이 백서에서는 조직이 GDPR이 데이터에 미치는 영향을 고려해야 할 이유를 설명합니다. 이 새 규정은 여러 조직에게 도전이자 기회입니다. 규정 시행까지 남은 시간이 얼마 없기 때문에 많은 조직은 GDPR 원칙에 대한 해석이 현재와 장래의 데이터 관리 프로세스에 어떤 영향을 미칠지 고려해야 합니다.

조직들이 이런 해석을 신속히 실행할 수 있도록 Informatica는 이해 관계자들이 던지는 몇 가지 핵심적 진입점 질문을 제시하고 이러한 질문에 답하는 데 필요한 몇 가지 기능을 제안했습니다. 이러한 질문과 기능은 GDPR 요구 사항의 어느 한 부분만 해결하는 것이 아니라 GDPR이 제기하는 많은 데이터 과제에 대처할 수 있는 종합적 기능을 구축하는 데 도움이 됩니다.

각 기능마다 그에 맞는 기술 활용 사례가 있습니다. 각 활용 사례에는 소프트웨어 솔루션 유형과 이를 제공하는 데 사용할 수 있는 기술이 나와 있습니다.

Informatica는 20년 이상 데이터 관리업계를 선도하면서 전 세계 수많은 조직의 복잡한 데이터 관리 문제를 해결해 왔습니다. GDPR로 많은 조직은 복잡한 데이터 관리 문제를 떠안게 될 것입니다. Informatica와 관련 파트너 생태계는 이러한 조직들의 GDPR 이니셔티브를 도와줄 적임자입니다.

6. 참고

GDPR 준수는 각 조직의 구체적인 비즈니스, 운영 및 데이터 사용에 기반합니다. 이 문서는 조직이 GDPR 준수 노력을 강화할 때 유용한 일련의 논의 사항을 제공하는 것이며, 법률 자문이나 지침 또는 권장 사항을 제공하는 것을 목적으로 하지 않습니다. 조직이 어떤 의무를 이행해야 하는지에 대해서는 자체 법률 고문과 상의해야 합니다.

Informatica

한국인포매티카 06611 서울시 서초구 서초동 강남대로 465 교보타워 B동 13층, 대표 전화: +82 2 6293 5001
informatica.com/kr linkedin.com/company/informatica twitter.com/InformaticaKR

IN09_0218_03337