전자책:

SAP 데이터의 개인정보 보호관련규제준수를 위한 길:

글로벌 데이터 개인정보 보호 프로젝트에서 얻은 교훈을 바탕으로 SAP 시스템 내 데이터 개인정보 보호 준수를 위한 필수 단계에 대한 실용적인 가이드

James Watson | EPI-USE Labs의 Business Owner 데이터 프라이버시, 리스크 및 산업 솔루션 담당

James는 EPI-USE Labs의 데이터 개인정보 보호 및 SAP 산업특화 솔루션에 대한 글로벌 비즈니스 책임을 맡고 있으며, 모든 지역과 주요 계정에서 복잡한 요구사항을 충족하기 위해 Data Sync Manager(DSM)을 운영하고 있습니다. 20년 이상의 기능 및 비즈니스 배경을 가지고 있는 제임스는 개발, 기초, 테스트/능력 센터와 리더십 팀 간의 다리를 제공하여 데이터 개인정보 보호 컴플라이언스를 위한 경로에 대한 안내와 조언을 제공합니다. 그의 경력에는 비운영 데이터 관리 및 익명화, 운영 데이터 제거 또는 수정, 시스템 레이아웃 최적화(SLO) 및 SAP 산업특화 솔루션에 대한 전문성이 포함됩니다.

목차

소개

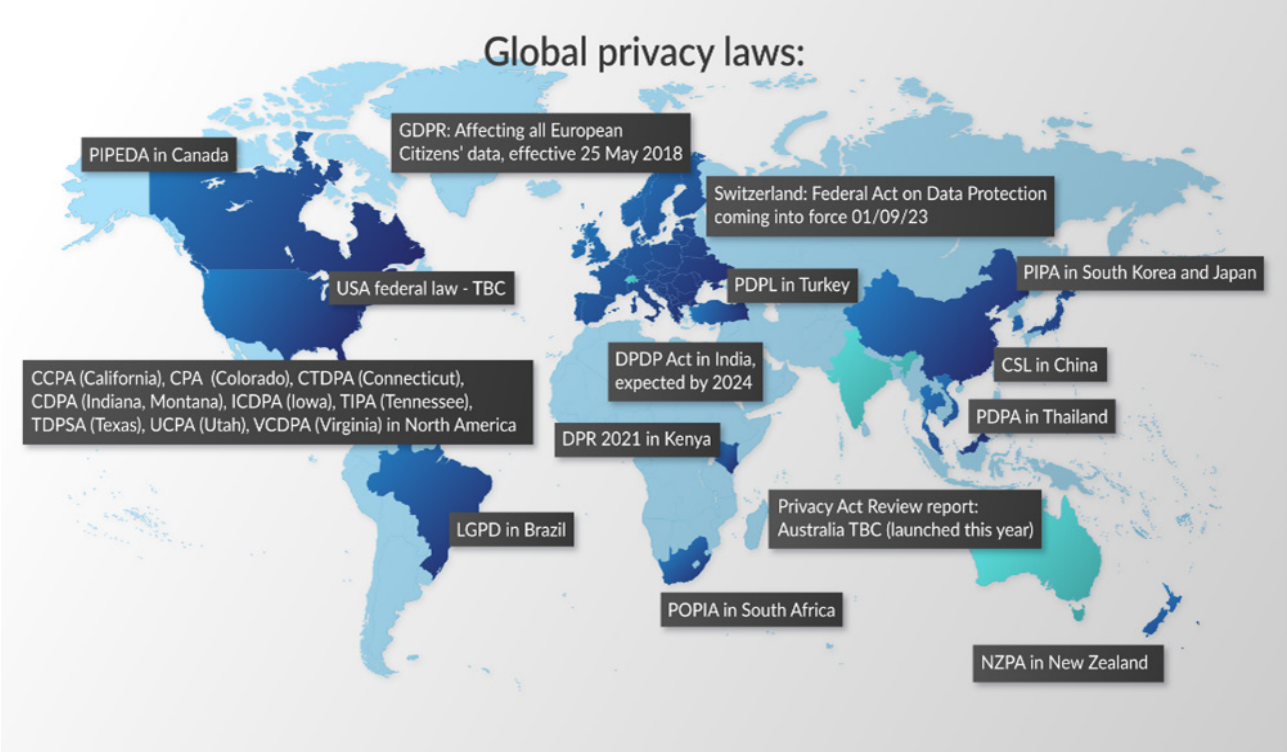
SAP는 세계에서 가장 견고한 시스템 중 하나지만, 동시에 가장 복잡한 시스템 중 하나입니다. SAP 의 구조 때문에 데이터 개인정보 보호 준수를 처리하는 것이 특히 어렵습니다. 여러 SAP 객체와 시스템의 교차 기능 통합을 이해하고 매핑하려면 세부적인 도메인 지식이 필요합니다.

EPI-USE Labs는 30년 이상 SAP 파트너로 활동하며 SAP 데이터 구조에 대한 깊은 이해를 가지고 있습니다. 전 세계의 기업들과 협력하여 GDPR(일반 데이터 보호 규정)과 같은 글로벌 데이터 개인정보 보호 법규에 맞춰 준수하도록 돕고 있습니다.

이 전자책은 다양한 복잡한 프로젝트에서 얻은 교훈을 바탕으로 SAP 시스템에서 데이터 개인정보 보호 준수를 구현하기 위한 필수 단계들을 설명하는 실용적인 가이드입니다. SAP에 대한 저의 특정 경험에 초점을 맞췄으며, 프로세스 원칙은 Microsoft Dynamics와 Oracle과 같은 다양한 애플리케이션에서도 동일하게 유지되지만, 기반 기술은 다를 것입니다.

데이터 개인정보 보호 준수 여정을 시작할 때 이 전자책이 유용한 통찰을 제공하기를 바랍니다.

글로벌 개인정보 보호법



2023년 10월 기준, 전 세계적으로 약 20개의 수정된 개인정보 보호법이 시행되었습니다::

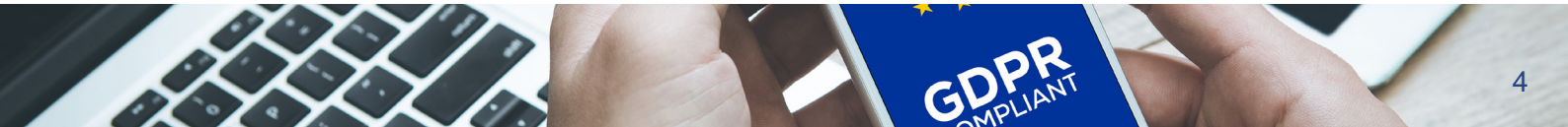
- 유럽의 GDPR
- 캘리포니아의 CCPA
- 콜로라도의 CPA
- 코네티컷의 CTDPA
- 인디애나와 몬태나의 CDPA
- 아이오와의 ICDPA
- 테네시의 TIPA
- 텍사스의 TDPSA
- 유타의 UCPA
- 버지니아의 VCDPA
- 남아프리카의 POPIA
- 태국의 PDPA
- 브라질의 LGPD
- 한국과 일본의 PIPA
- 뉴질랜드의 NZPA
- 캐나다의 PIPEDA

현재 인도의 DPDP 법안이 적극적으로 검토되고 있으며, 스위스의 연방 데이터 보호법은 거의 통과되었습니다. 캐나다, 미국, 호주를 포함하는 연방 법안은 계속 논의 중이며, 아마도 불가피할 것입니다.

각 법은 독특하며 고유한 복잡성을 포함하고 있습니다. 그러나 디지털 세계에서 고려해야 할 일반적인 주제로는 빅데이터, 개인의 개인정보 권리 및 책임이 포함됩니다. 가장 중요한 점 중 하나는 데이터 저장 위치보다는 개인의 주권에 초점을 맞춘다는 것입니다. 예를 들어, 유럽 시민은 세계 어디에서든 사업을 하거나 고용될 때 GDPR의 보호를 받습니다.

이로 인해 흥미로운 국제법적 질문이 생길 수 있지만, 저는 이러한 법적 개념을 피하고, IT 팀이 프로세스를 조정하고 운영 환경 내에서 데이터를 보존하는 기간을 설정할 때의 실용성에 집중하려 합니다.

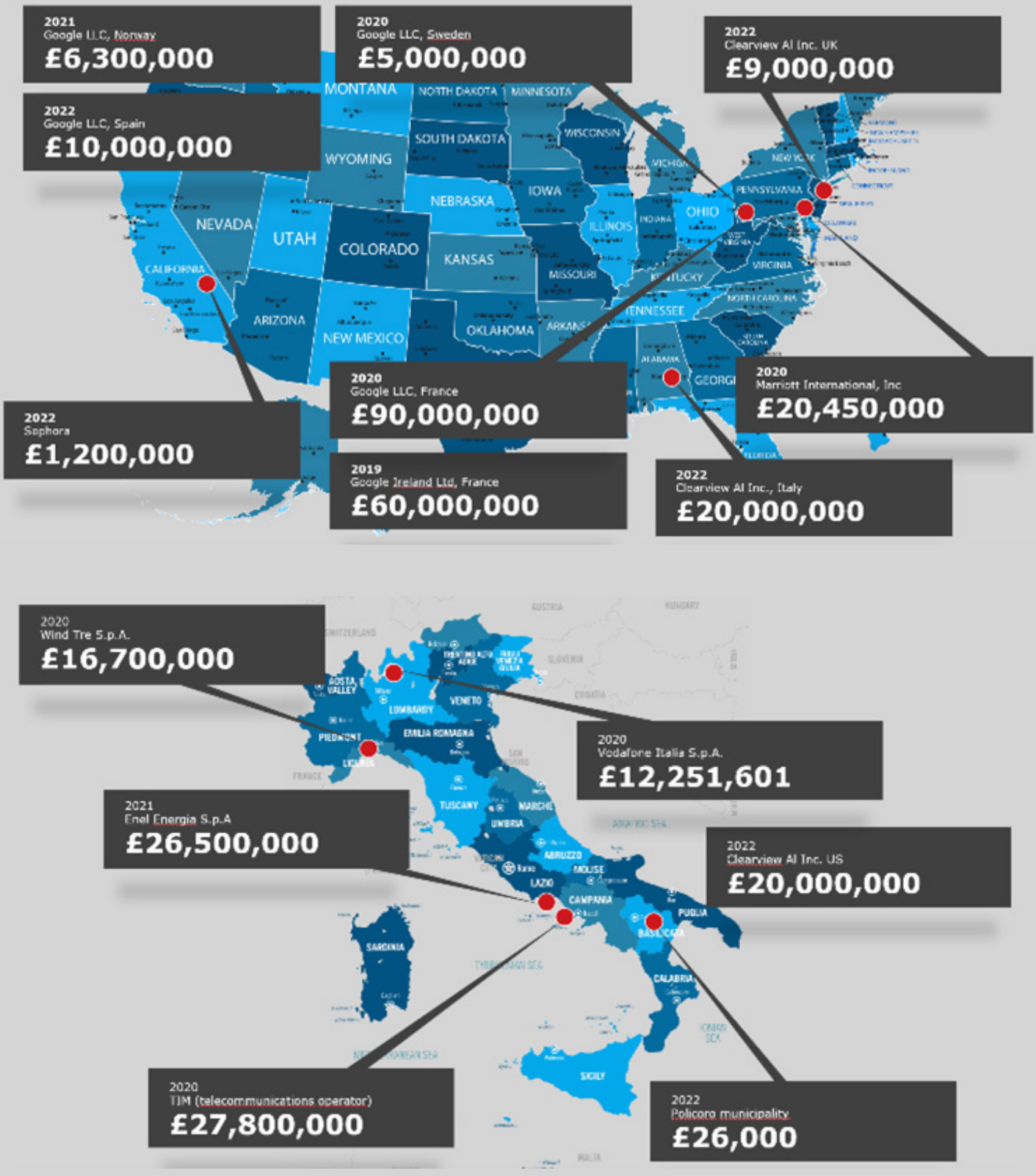
각 법에 적용되는 핵심 원칙에 대해 아래에 간단히 설명하였습니다.



개인정보 항목	설명
책임	모든 회사는 처음에 데이터 보호 책임자를 임명할 책임이 있으며, 이들은 궁극적으로 회사 내에서의 개인정보 보호에 대한 법적 책임을 지니고 있습니다. 또한, 명확한 데이터 처리자 (Data Processor) 정의를 통해 회사가 다른 출처에서 받은 데이터나 관련 사업으로 넘기는 데이터에 대한 책임을 유지합니다.
접근 권한	일반적으로 주체 접근 요청(SAR 또는 DSAR)이라고 불리며, 데이터 처리자는 사업 내에서 데이터 주체를 검색하고 식별할 수 있어야 하며, 그들의 개인 식별 정보를 요약하여 제공해야 합니다. 포괄적인 보고서는 일정 기간 내에 작성되어야 하며, 법에 따라 차이가 있지만 일반적으로 28일 또는 1개월이 언급됩니다.
삭제 권한	많은 개인정보 보호법에 대한 주요 추가 사항은 잊혀질 권리 또는 수정/삭제 권리입니다. 여기서 사업 내 PII 데이터에 대한 법적 근거를 입증할 책임이 사업에 있으며, 정당한 이유가 없는 경우 모든 데이터 주체는 정보 제거를 요청할 권리가 있습니다. 기술적인 관점에서 '삭제'의 정의는 명시적이지 않아 법무팀의 검토가 필요합니다. 그러나 삭제는 많은 관계형 데이터베이스 유형에서 어려운 과제입니다. 이 문서에서는 사용 가능한 옵션과 추천 사항을 탐구할 것입니다.
이동 권한	이것은 접근 권한과 유사하지만 주체 접근 요청과는 달리 데이터 주체의 요청에 따라 사업 간에 공유될 수 있는 모든 개인 정보를 추출할 필요성을 정의합니다. 따라서 이 데이터는 여러 사업체에서 처리할 수 있는 일반적인 읽기 가능한 형식으로 제공되어야 하며, 일부 법률에서는 명시적이지 않지만 파일 공유에 대한 충분한 검사 및 절차가 요구되어 개인을 보호해야 합니다.
적극적인 개인정보 관리	모든 기업이 고려해야 할 필수 항목으로, 데이터에 대한 보존 정책을 생성하고 더 이상 정보 유지에 대한 법적 근거가 없는 데이터 주체(및 관련 데이터)를 적극적으로 식별하고 데이터 제거를 처리해야 합니다.
국경 간 데이터 접근	종종 Schrems II라는 이름으로 언급되며, 이는 EU와 미국 간의 데이터 전송에 대한 특정 사항이지만 법적 관할권 간 데이터 공유 시나리오를 다룹니다. 자주 직면하는 간단한 시나리오는 다국적 기업의 중앙 사무소에서 관리되는 직원 데이터입니다. 이러한 기사들은 허용 가능한 데이터 전송을 정의합니다. 기업이 단일 HR 및 급여 기술/플랫폼 솔루션의 이점을 얻고자 하면서도 특정 데이터세트에 접근할 수 있는 사용자를 제한해야 하는 도전 과제를 제기할 수 있습니다.

개인정보 보호법에는 여러 공통점이 있지만, 이 문서에서는 주요 영역에 집중했습니다.

데이터 개인정보 보호 준수의 가장 설득력 있는 이유 중 하나는 벌금입니다. 새로운 법은 법적 기관이 훨씬 더 높은 재정적 제재를 가할 수 있도록 하고 있으며, 아래 예시를 통해 확인할 수 있습니다.



시작하는 방법

각 기업은 저마다 다른 특수한 도전 과제를 가지고 있으며, 모든 데이터 개인정보 보호 문제를 해결할 수 있는 '만능 해결책'은 없습니다.

'표준 기능 준수'를 제공하는 회사에 주의하시는 것을 권고합니다. 시장에 훌륭한 가속기가 있지만, 모든 프로세스는 항상 귀사의 구체적인 요구에 맞게 구현되고 맞춤화되어야 합니다.

이 점은 SAP의 기술 솔루션을 검토할 때 더욱 중요합니다. 예를 들어, AI 및 머신러닝(ML) 솔루션을 통해 환경 내의 PII를 자동으로 식별할 수 있다고 주장하는 공급업체가 있습니다. 패턴 매칭 ML은 데이터가 매핑된 테이블 필드를 찾을 수는 있지만, SAP 데이터베이스의 참조 무결성을 이해할 수는 없습니다. 최선의 경우, 데이터 스크램블링이나 제거가 일관되거나 완전하지 않을 것이며, 최악의 경우, 참조 체인에 누락된 데이터를 생성하여 SAP 시스템을 망칠 수 있습니다. 따라서 솔루션 옵션을 검토할 때는 귀하가 운영하는 시스템과 유사한 산업 및 시스템 유형에 대한 참조가 있는 전문 공급업체를 선택하는 것이 좋습니다.

그럼에도 불구하고, 실제 구현 접근 방식은 기술이나 산업에 상관없이 몇 가지 필수 단계로 표준화할 수 있습니다. 각 단계에서 수행하는 작업은 상황에 따라 매우 다를 것입니다.
EPI-USE Labs에서는 이를 '데이터 개인정보 보호 준수로 가는 길'이라고 부릅니다. 이 문서에서는 이러한 각 단계를 더 자세히 탐구합니다.

마지막으로 생각할 점: 모든 관련자를 위한 명확한 범위와 함께 견고한 요구 사항 수집 단계의 중요성을 과소평가하지 마십시오. 데이터 삭제 소프트웨어를 실행하면 예상치 못한 영향과 변경 사항을 관리해야 할 수도 있습니다. 이는 비용이 많이 들고 일정이 연장될 수 있습니다. 프로젝트의 청사진에 가능한 많은 의사 결정자를 포함하고, 사전 승인된 결과를 받으면 라이브로 전환하는 과정이 더 수월해질 것입니다.

구현을 위한 필수 단계

1) 위험 식별: 영향 및 위험 평가

앞으로 성공을 위해서는 이 단계와 다음 단계에서 정확히 설정하는 것이 중요합니다.

IT 영역 외의 위험이 있는가?

기술적인 IT 평가 요구사항에 집중하기 전에, 개인정보 프로젝트는 IT에만 집중하는 것이 아니라, 회사 운영에 관련된 사람과 비즈니스 프로세스 요소도 고려해야 한다는 점을 기억하세요.

예를 들어, 여러 고객사에서 본 두 가지 일반적인 시나리오가 있습니다:

시나리오 1
대고객 직원들(프론트 오피스)

몇 년 전 컨택 센터에서 일할 때, 저는 통화 중에 받은 중요한 정보를 기록하기 위해 정기적으로 메모장을 사용하곤 했습니다. 식별자, 계좌 번호, 전화번호 등을 기록했고, 통화를 짧게 유지하며 통화 후 이 데이터를 입력하는 행정업무를 완료했습니다.

그 후, 저는 정기적으로 근무가 끝난 후 메모장을 가방에 넣고 버스를 타고 집으로 갔습니다. 만약 그 메모장을 버스에 두고 왔다면 어떻게 되었을까요?

노트북을 사용했다면 어떨까요? 뉴스에서 여러 번 본 것처럼, 공공장소에 노트북을 두고 오면 데이터 유출로 이어질 수 있습니다.

전체 데이터 개인정보 및 보안 프로세스는 기밀 폐기, VPN/MFA 장치 등을 고려해야 합니다.

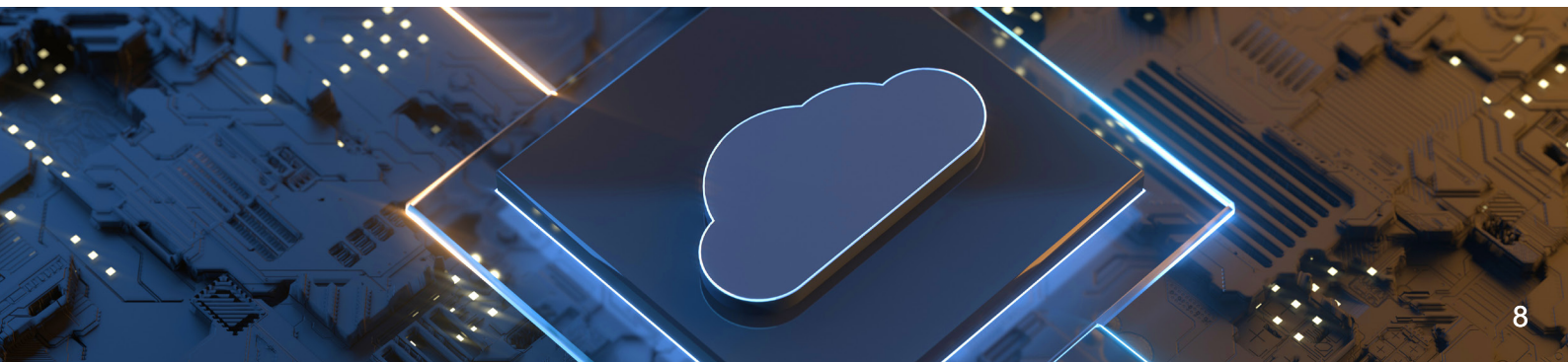
시나리오 2
사무실 방문

고객사 사이트를 방문할 때, 저는 정기적으로 출입 배지용 사진을 찍고, 신분증 증명을 요청받아 복사되어 저장될 수 있습니다. 이러한 기록을 법적으로 허용된 기간 동안 유지해야 하는 것은 무엇입니까?

제가 가장 싫어하는 것은 매우 일반적인 사이트 방명록입니다. 누구나 접근할 수 있는 공개 기록으로, 방문하는 모든 사람이 이름, 회사, 차량 등록 번호 및 연락처 전화번호를 입력하도록 요청받습니다. 전체 방명록이 도난당하거나 다른 페이지의 이미지가 찍혀서 개인정보 보호법에 위반될 수 있습니다.

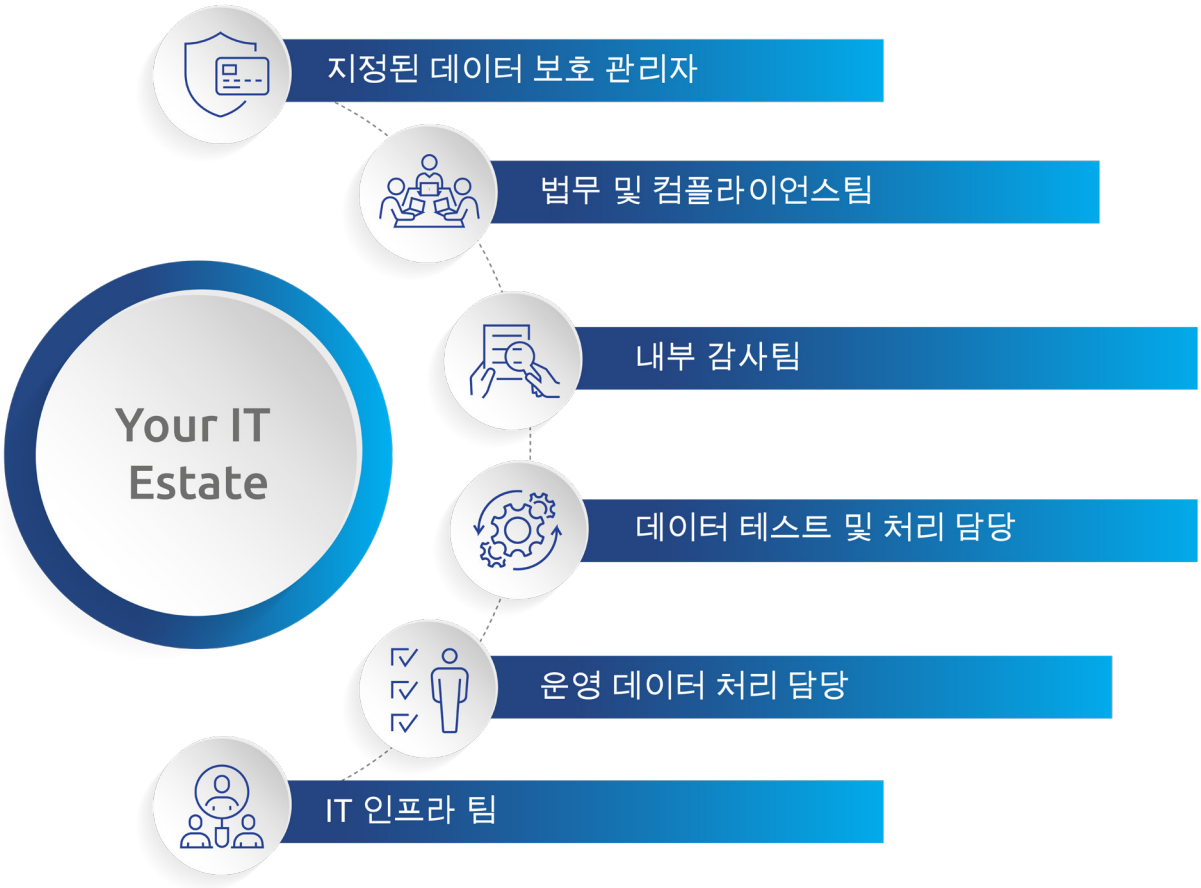
물론, 각 회사는 사건이 발생했을 경우를 대비해 일정 기간 동안 기록을 유지해야 합니다. 그러나 종이 책이 디지털 서명으로 대체될 수 있을까요? 이 데이터에 대한 보존 기간을 설정할 수 있을까요?

실제로 개인정보 보호법 내에서 IT 자산을 정의하고 관리하는 것이 더 쉬운 경우가 많으며, 이는 주요 초점이 되어야 합니다. 그러나 모든 개인정보 보호 전문가들은 IT 시스템을 정비하는 것에만 집중해서는 법률을 준수할 수 없다는 것을 깨달아야 합니다.



IT 자산: 이 단계의 참가자들

IT 자산에 관해서는, 이 단계에서 참여한 최상의 프로젝트들은 다음과 같은 참가자들이 포함되었습니다:



비즈니스와 준법 간의 교착 상태를 해결하기 위해 필수적인 역할을 하는 **데이터 보호 책임자(DPO)**는 필요할 때 이러한 결정을 내릴 수 있을 만큼의 고위직이어야 합니다. 프로젝트 중 청사진 단계가 덜 성공적이었던 경우에는 고객의 '교훈'으로 DPO를 초기에 참여시켜 데이터 익명화를 강화해야 한다는 필요성을 확인했습니다. 일반적으로 기능 팀은 고객이 돌아올 경우를 대비해 데이터를 제거하기를 원하지 않습니다.

법률 및 준법 팀은 이 단계에서 두 가지 주요 활동을 수행합니다. 첫 번째는 비즈니스의 다양한 부분이 적용받는 개인정보 보호법에 대한 의견을 제공하는 것입니다. 동일하게 중요한 것은 개인정보 보호법에 영향을 주는 다른 규정에 대한 관점입니다. 흔한 예로는 기업이 금융 거래 기록을 보관해야 하는 기간에 대한 엄격한 지침이 있는 세법이 있습니다. 이러한 추가 준법 및 법률 요구 사항을 이해하는 것은 데이터 보존 프레임워크를 식별하는 데 도움이 될 것입니다.

감사 팀은 귀중한 추가 구성원이며, 감사 시 무엇을 확인할지를 이해하여 승인할 수 있습니다. 초기부터 그들을 참여시키는 것은 나중에 비용이 많이 드는 프로젝트 문제를 피할 수 있습니다.

테스트 책임자는 매우 중요한 역할을 합니다. 모든 SAP 운영 기업은 운영 시스템에 영향을 주기 전에 프로세스 변경, 시스템 업데이트 또는 새로운 기능을 테스트할 수 있도록 운영 데이터를 복사하여 제공받습니다. 이 프로세스는 모든 기업에 필수적입니다. 대부분의 기업은 테스트를 위해 직원, 고객 및 공급업체 데이터를 사용하기 위한 정보를 제공받고 명시적 동의를 받은 상태에서 이를 신중하게 관리해야 합니다. 데이터 스크램블링의 영향을 명확히 이해해야만 준법을 준수하면서 최소한의 영향을 미치는 디자인을 개발할 수 있습니다.

마찬가지로, **운영 프로세스 관리자들**은 데이터 제거의 영향을 알리고 준수해야 합니다. 때로는 법률 및 준수 팀이 회사 보존 설계로 논쟁할 수 있는 비즈니스 정당성을 만듭니다. 또한, 준수 요구 사항을 충족하기 위해 관리해야 할 프로세스 변경이 있을 수 있으며, 이러한 소유자들은 기술 솔루션 구현과 동시에 이를 추진할 책임이 있습니다.

이 단계에서 **IT 및 인프라 팀의** 역할은 시스템 간 인터페이스를 통한 데이터 전송 및 주요 통합을 조언하는 것입니다. 예를 들어, 웹 클라이언트 솔루션에 인터페이스로 이메일 주소가 사용되는 경우, '실제' 이메일 주소 없이 이 프로세스를 계속 테스트할 기술적 옵션은 무엇인지 안내합니다. 또한 데이터가 어떻게 전송되는지에 대한 지침을 제공할 것입니다: 한 시스템에서 데이터를 전송하는가, 또는 다른 시스템에서 가져오는가? 이는 필요한 솔루션의 복잡성을 정의할 수 있습니다. 데이터가 단일 기록 시스템에서 부차적 시스템으로 가져오는 경우, '마스터' 시스템만 업데이트하면 이러한 변경이 통합 시스템에 상속됩니다. 반면에 데이터를 전송하는 경우, 업데이트를 트리거하기 위한 새로운 작업 또는 인터페이스가 필요할 수 있으며, 이는 복잡성을 증가시킵니다.

우선순위와 위험 수준

제가 본 기술 분석 중 최고의 관리수준은 시스템 아키텍처 맵으로 '신호등'을 사용하여 우선순위와 위험 수준을 표시한 것입니다:

- 빨간색은 높은 위험 시스템을 나타내며 직접 처리해야 합니다. 시스템에는 다른 시스템에서 유래되지 않은 민감한 PII가 포함되어 있으며, 제공된 개인정보 보호 기능이 없습니다. 이는 개인정보 프로젝트에서 우선순위 1인스턴스입니다.

- 노란색은 중간 위험 시스템을 나타냅니다. 시스템은 다음 중 하나입니다:
- 1. 제한된 민감한 PII를 포함
- 2. 익명화를 상속받는 기존 API 기능이 있음
- 3. 표준으로 내장된 개인정보 보호 솔루션이 있음.
- 이는 검토가 필요하지만 계획이 있는 우선순위 2로 식별됩니다.

- 녹색은 낮은 위험 시스템을 나타냅니다. 이는 PII가 처리되지 않고 비즈니스 데이터만 처리되는 시스템에 예약되어 있으며, 검토가 필요하지 않습니다.

이러한 전반적인 관리를 통해 초기 진단에서 빨간색(우선순위 1) 시스템에 집중하여 개인정보 보호 여정을 가장 잘 지원할 수 있는 공급업체를 우선적으로 식별할 준비가 되었습니다.

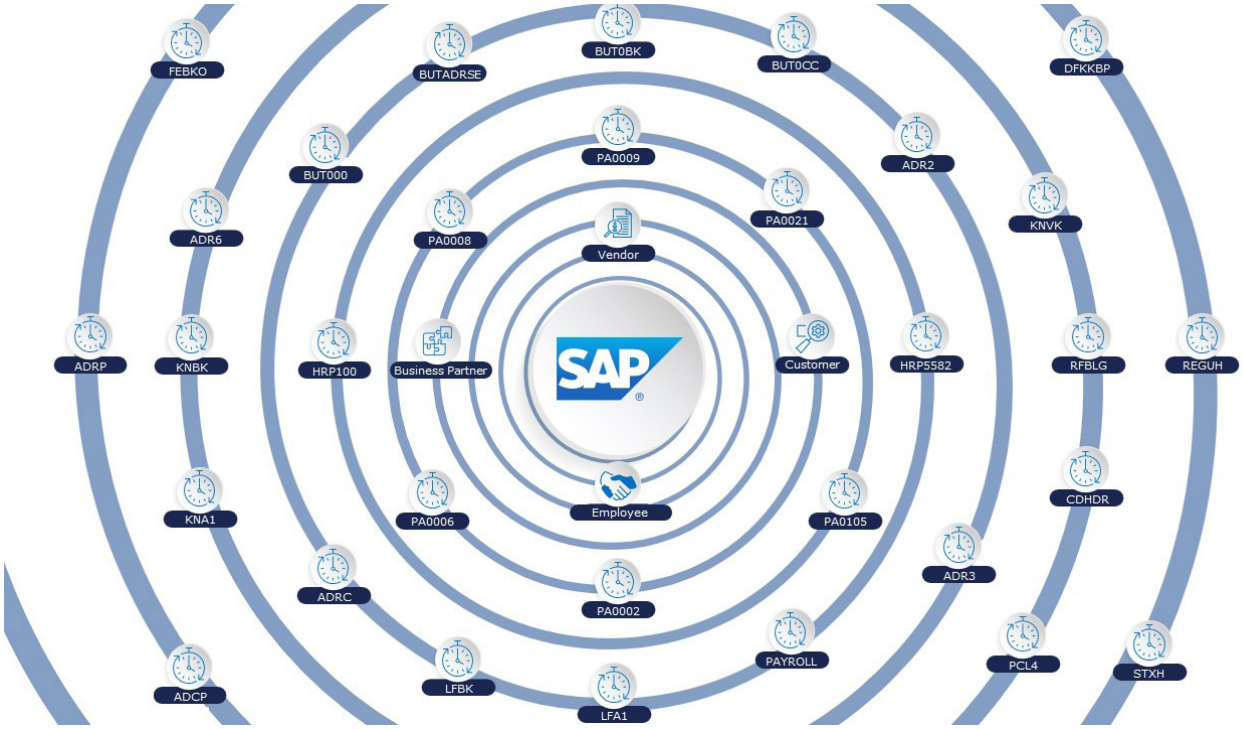
2) 개인정보를 찾아서 매핑하기

개인정보 보호법이 새롭게 도입된 시장에서는 준수를 위해 첫 번째로 중요한 단계입니다. 개인정보(PII)를 찾아서 매핑하는 것은 감사자나 준수 기관에 당신의 환경에서의 PII 위험을 명확히 이해하고 문제 해결 계획을 갖고 있음을 입증할 수 있게 합니다. 유럽의 많은 고객사에서 우리가 관찰한 바에 따르면, 프로세스를 시작했음을 증명할 수 있었던 경우에는 관리 기관이 문제를 해결할 시간을 주었으나, 문제를 완전히 무시한 회사는 벌금을 받을 가능성이 더 높았습니다.

SAP 시스템에서는 표준으로 제공되는 데이터 모델이 비교적 복잡합니다. 예를 들어, 일반적인 비즈니스 시나리오는 다음과 같습니다:

- 여러분의 시스템 환경에 직원이 있을 때, 직원의 이름, 연락처, 급여 정보, 사번, 가족 정보 등이 직원 '인포타입' 테이블에 채워집니다.
- 특정 직원은 사내의 프로젝트업무 과정에서 일합니다. 이 기간 동안 직원은 출장 중 프로젝트에 관련된 비용을 발생시킵니다. 따라서 직원의 데이터가 SAP의 벤더 테이블에 복제됩니다.
- SAP의 금융 설정이나 버전에 따라 동일한 정보가 비즈니스 파트너 객체로도 복제됩니다.
- 이 직원이 당신의 비즈니스에서 무언가를 구매하면 고객이 됩니다. 이름, 주소, 전화번호, 은행 정보 등의 개인 정보가 다른 테이블 세트에 저장됩니다.
- PII를 포함하는 테이블과 필드의 상호 연결된 웹은 쉽게 수천 개의 기술적 위치로 확장됩니다.
- 개인정보 보호법은 데이터 주체를 직원이나 벤더 또는 고객으로 존재하는 것이 아니라 단일 존재로 간주합니다. 삭제 요청 권한이 있을 경우, 데이터 주체의 전체 보유 관련성을 확실히 이해해야 결정할 수 있습니다.

이 시나리오는 SAP 데이터의 개인정보 관리를 위해 AI와 머신러닝이 효과적으로 작동할 수 없는 경우 중 하나를 설명합니다. 완전하고 일관된 데이터 제거를 달성하려면 소프트웨어에 특정 도메인 지식이 내장되어 있어야 합니다.



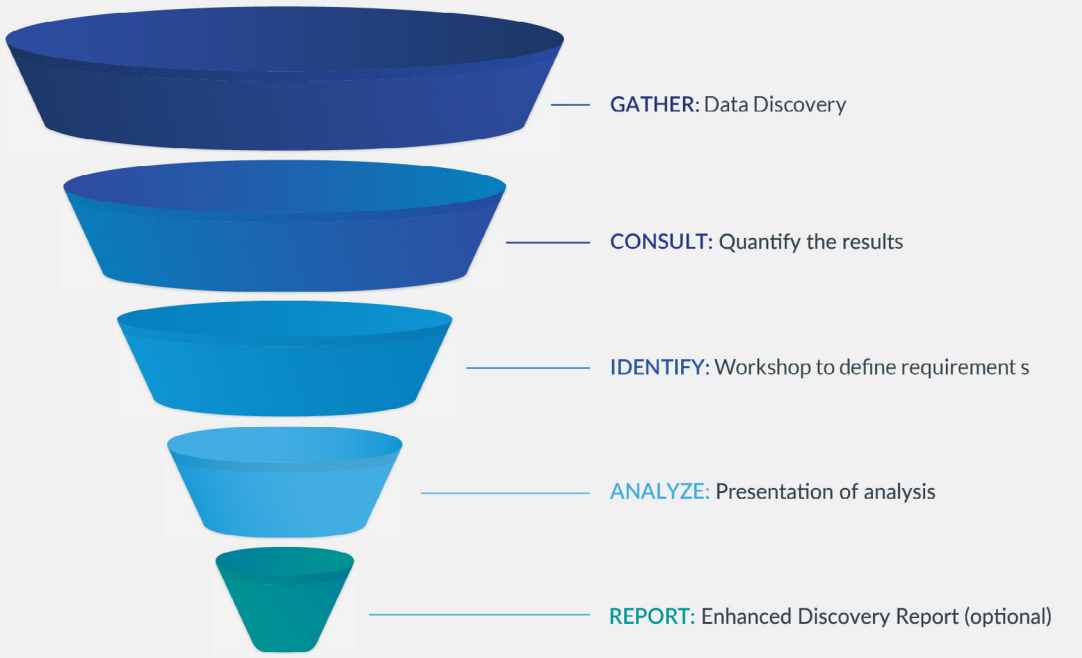
SAP의 커스터마이징 설정은 어떻게 하나요?

대부분의 회사들은 SAP 시스템을 자신들의 산업과 비즈니스에 맞게 맞춤 설정하여 필요한 프로세스를 구현해 왔습니다. SAP에서는 이를 Z 또는 Y 테이블이라고 부릅니다. 또한, PII가 포함될 수 있는 테이블과 필드를 제공하는 애드온을 구매할 수도 있습니다(이들은 항상 /로 시작합니다:
/addon/table).

그렇다면, 이를 어떻게 매핑하고 이해할 수 있을까요?

SAP 데이터 관리 전문가인 EPI-USE Labs는 이미 하나의 SAP 시스템 내에서, 그리고 여러 SAP 시스템 간의 표준 SAP 테이블과 객체 통합을 매핑했습니다. 20년 이상 일관된 데이터 복사를 완료한 우리는 SAP 솔루션의 도메인 지식을 보유하고 있어 귀하의 매핑 프로세스를 정확하게 단순화하고 가속화할 수 있습니다.

우리는 SAP에 특화된 데이터 프라이버시 평가 서비스를 설계했으며, 이 서비스를 통해 귀사의 환경 내 테이블과 필드 사전을 분석하여 PII를 포함할 가능성이 있는 필드를 강조 표시합니다. 결과에 대한 수동 분석이 완료되며, 운영 및 비생운영 유형별 PII에 대한 규정 준수 접근 방식을 정의하기 위해 영향 및 위험 평가의 주요 이해관계자와 워크숍을 개최합니다.



이 서비스에 대한 추가 정보는 저희 웹사이트에서 확인하실 수 있습니다.

이 프로젝트 단계의 결과물은 귀하의 특정 SAP 인스턴스에서 PII 위험과 위치에 대한 기술적 및 기능적 명세서가 될 것입니다. 이는 다양한 SAP 환경에서 데이터가 처리되는 방식에 대한 비즈니스 요구 사항과 민감한 데이터 유형의 기술적 PII 지도를 포함합니다. 이 문서는 감사 팀과 공유하는 것도 권장합니다. 승인이 완료되면, 다음 분석 단계로 진행할 수 있습니다.

3) 접근 위험 및 제어 검토

이제 SAP 시스템 내에서 PII가 어디에 있는지 알게 되었으므로, 첫 번째로 해야 할 것은 사용자 권한 부여와 접근 제어를 통해 PII에 접근할 수 있는 사람을 제한하고, 접근이 정당한지 확인하는 것입니다. 많은 기업들이 이미 GRC(거버넌스, 리스크 관리 및 컴플라이언스) 프로세스를 가지고 있지만, 역사적으로 이는 직무 분리(SoD)와 잠재적 사기에 초점을 맞춰왔습니다. 새로운 데이터 개인 정보 보호법은 PII 접근 위험을 포함시키도록 요구하고 있습니다.

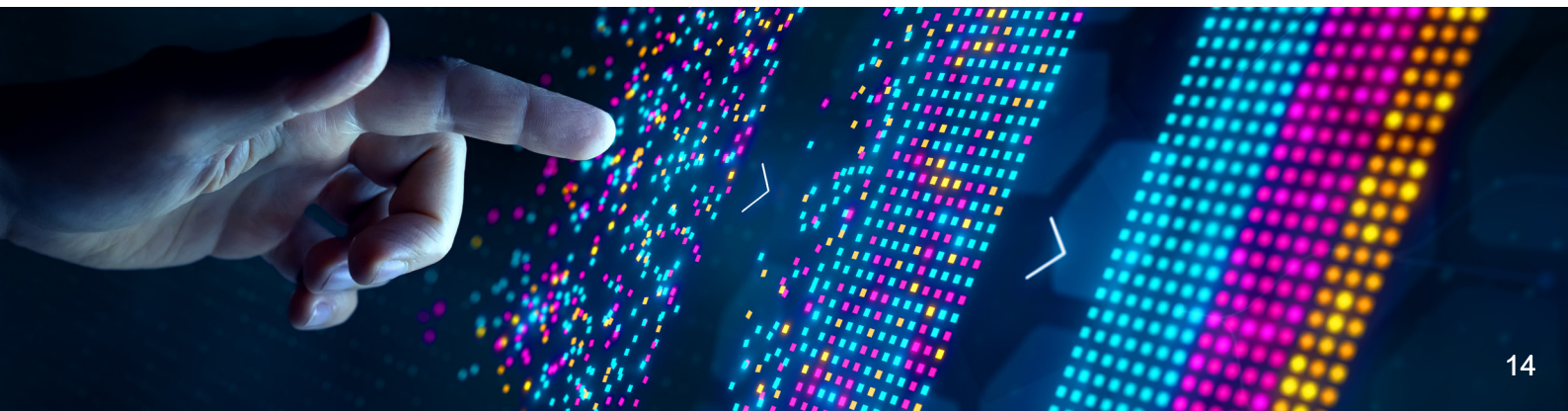
이제 다양한 유형의 PII에 누가 접근할 수 있는지를 고려해야 합니다. 예를 들어, 비인사 부서 직원이 인사 정보를 접근할 수 없도록 하고, 인사 부서 직원이 재무 정보를 접근할 수 없도록 해야 합니다. 또한, 동일한 기능적 데이터에 다양한 지리적 위치에서 접근할 수 있는지, 그리고 그 접근에 지역 개인정보 보호법이 미치는 영향을 고려해야 합니다.

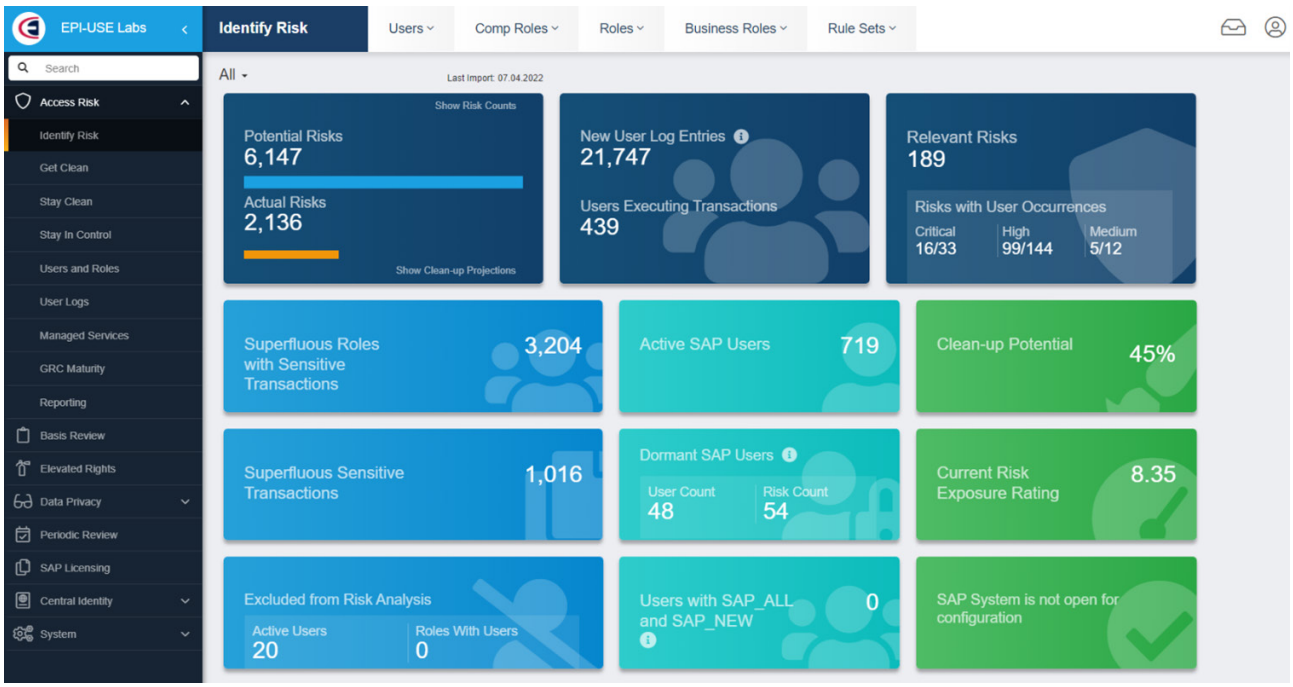
더 큰 SAP 인스턴스와 연결된 클라우드 애플리케이션의 새로운 세계에서는 여러 시스템 간의 권한을 매핑하고 볼 수 있어야 합니다.

Soterion과의 파트너십: SAP를 위한 GRC 해결

EPI-USE Labs는 Soterion과의 긴밀한 파트너십을 형성하여, SAP® 고객을 위한 GRC 문제를 해결하는 규정 준수 소프트웨어를 제공합니다. 전통적인 SAP GRC 솔루션은 쉽게 조정되지 않지만, Soterion은 완전히 커스터마이징 가능한 플랫폼에서 가속기를 제공합니다. 우리의 파트너십은 강력하고 상호 보완적인 솔루션, 지식, 경험을 결합하여 고객이 글로벌 데이터 개인정보 보호법을 준수하도록 돕습니다.

PII 매핑과 유사하게, 시작점은 누가 무엇에 접근할 수 있는지를 매핑하는 것입니다. Soterion의 솔루션은 권한 데이터와 로그를 다운로드하여 Soterion의 자체 인스턴스에 업로드함으로써 첫 번째 모습을 제공합니다. 소프트웨어에 사전 구성된 가속기 규칙 세트가 실행되어 위험의 초기 보기를 제공합니다.





Soterion 보고서는 잠재적 위험과 실제 위험의 차이를 보여줍니다. 이 차이는 위험을 초래할 수 있는 권한을 가진 사용자와 이러한 권한을 적극적으로 사용하는 사용자 간의 차이입니다. 현재 위험과 통제 조치로 인한 가능한 위험 감소를 RAG(빨강, 주황, 초록) 상태로 시각화할 수 있습니다.

Soterion은 다음을 위한 규칙 세트를 제공합니다:

개인 정보 접근 위험

대부분의 GRC 솔루션은 업무 분리와 사기 방지에 중점을 둡니다. Soterion은 이러한 기능을 수행하며, PII 데이터에 대한 접근 권한을 분석할 수 있는 규칙 세트를 구축했습니다.

업무 분리(SoD)

예를 들어, 누가 지급 제출과 승인을 모두 할 수 있는 접근 권한을 가지고 있습니까? Soterion은 시스템 내에서 상충되는 접근 권한을 가진 모든 사용자를 식별합니다.

법적 관할권을 넘는 데이터 접근

미국의 사용자가 유럽의 직원 및 고객 데이터를 액세스할 수 있습니까, 또는 그 반대로? 그렇다면, 데이터 보호막 생성에 영향을 받는 사용자는 누구입니까?

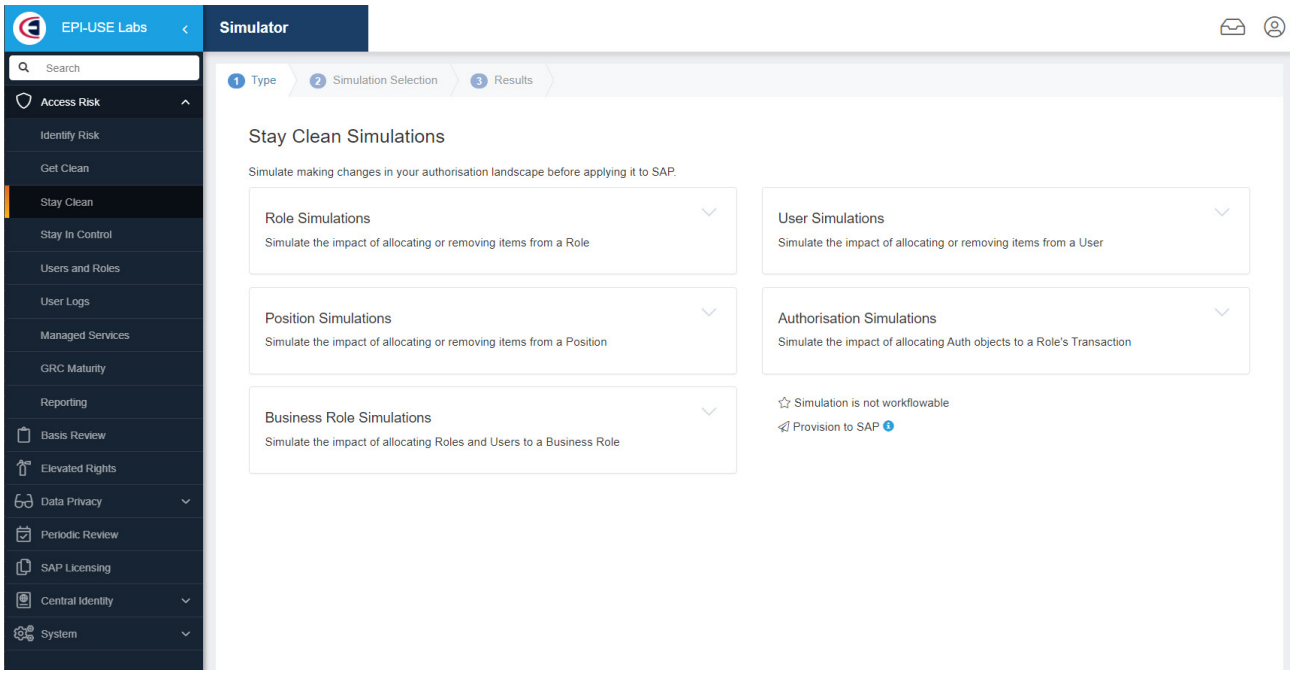
중요 거래 위험

테이블 유지보수에 직접 접근할 수 있거나 프로그램을 직접 실행할 수 있는 사람은 누구입니까? 공급업체 및 고객 관리가 올바른 사람에게 제한되어 있습니까?

초기 진단이완료되면, 이러한 리스크를 정리하는 과정을 시작해야 합니다. 잠재 리스크와 실제 리스크를 구분함으로써, 잠재 리스크를 줄이기 위한 명확한 출발점을 갖게 됩니다. 사용하지 않는 권한을 가진 사용자들을 대상으로 불필요한 역할을 제거할 수 있습니다.

실제 리스크는 더 세부적인 분석이 필요합니다. 권한을 효과적으로 재설계하기 위해서는 비즈니스와의 협력이 필수적입니다. 저는 반복적인 프로젝트를 추천하며, 동일한 리스크가 식별된 유사한 기능 영역의 사용자 그룹을 우선시하고 역할 구조와 할당을 검토하며, 리스크를 제거하기 위해 권한 모델을 재설계합니다. Soterion은 역할 시뮬레이션을 통해 변경이 리스크에 미치는 영향을 사전에 확인할 수 있도록 도와줍니다.

이러한 통제된 롤아웃을 통해 접근 리스크 관리에 대한 명확한 준수 계획과 충분한 변경 통제 포인트를 제공할 수 있습니다.



EPI-USE Labs의 고객들은 Soterion 솔루션을 사용하여 일주일 내에 소프트웨어 구현을 완료하고 리스크를 식별합니다. 그런 다음, 그들의 필요에 맞게 장기적인 역할 재설계 프로젝트를 모델링합니다. 리스크를 해결하기 위한 계획과 적극적인 관리가 마련되어 있다면, 일주일의 구현 후에 통제력을 달성하고 준수 상태를 개선할 수 있습니다.

4) 운영에서 백로그 정리

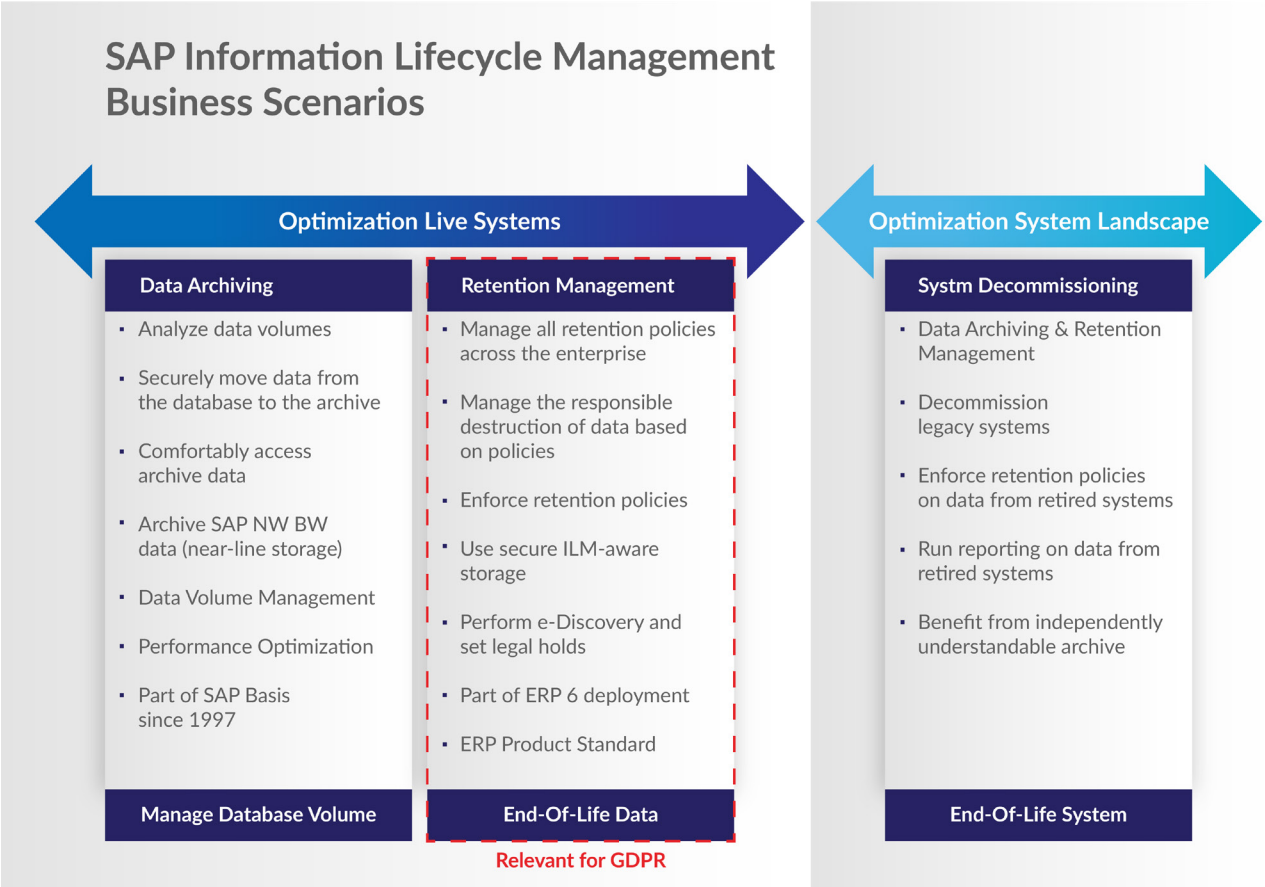
오랜 기간 SAP를 운영해온 고객들은 그동안 데이터를 적극적으로 수집하고 저장해왔습니다. 대부분의 경우, 이러한 운영 데이터가 개발, 테스트 또는 교육 목적으로 여러 복사본으로 복제되어 있음을 알 수 있습니다.

유럽에서 GDPR이 처음 도입되었을 때, 우리는 운영 복사본을 먼저 처리하도록 제안했습니다. 이는 여전히 가능한 옵션이지만, 고객들과 협력한 결과, 우선순위는 운영데이터를 통제하는 것이 되어야 한다는 것을 깨달았습니다. 이렇게 하면 다음에 복사본을 만들 때 이미 전반적으로 더 준수한 상태가 될 것입니다.

시스템 및 랜드스케이프 최적화(SLO) 프로젝트를 실행할 것을 권장합니다. 이러한 정리 작업에는 두 가지 주요 접근 방식이 있습니다:

- SAP 인프라스트럭처 라이프사이클 매니저(ILM): SAP에서 제공하며, 전체 기록과 관련된 모든 데이터를 삭제하는 작업을 생성합니다.
- 데이터 수정(EPI-USE Labs 제공): 당사의 독점 소프트웨어로, 기록의 PII만 선택적으로 제거하여 기록의 참조 무결성을 유지합니다. 비즈니스 재무 기록도 포함됩니다.

SAP ILM(7.02)은 2011년에 출시되어 SAP 데이터 아카이빙 도구로 의도되었습니다. GDPR이 2018년에 시행되면서 GDPR 솔루션으로도 발표되었습니다.



SAP 제공

데이터를 제거할 것인가 수정할 것인가?

SAP 솔루션의 참조 무결성 때문에 금융 시스템에서 고객이나 공급업체만을 단순히 제거하는 것은 불가능합니다. ILM을 사용하여 고객과 모든 관련된 판매/금융 데이터를 제거해야 하며, 그렇지 않으면 시스템 일관성 문제가 발생합니다.

귀중한 비즈니스 데이터를 잃게 되지 않도록 하기 위해, 오류를 피하려는 고객 기록과 관련된 모든 거래는 유지하지만 민감한 개인 식별 정보는 삭제하거나 분명하게 표시된 값으로 대체하는 수정 기능을 설계했습니다. 결과적으로 기록은 다음과 유사할 것입니다:

수정 접근 방식을 사용하면 전체 삭제 대신 다른 기간에 대해 서로 다른 보존 기간을 설정할 수 있습니다.

운영환경 정리를 달성하기 위해 검토해야 할 두 가지 정책이 있습니다:

- 데이터 보존 정책 – 특정 기간이 지난 후에 제거해야 할 데이터를 정의합니다. 이는 테이블별 개별 데이터일 수도 있고, 핵심 데이터 주체에 대한 목록일 수도 있습니다. 즉, 직원, 고객 또는 공급업체입니다.
- 데이터 수정 정책 – 보존 기간이 시작되면 테이블 필드별로 어떤 조치를 취해야 하는지를 정의합니다.

초기 정리를 위해, 사업체가 제거해야 할 데이터 주체 목록을 정의하는 책임을 지는 것을 추천합니다.
우리는 사업 요구에 따라 초기 입력 목록을 정의하기 위한 기술적 보존 보고서를 제공합니다. 고객은 이후 목록 검증과 사업 승인 책임을 집니다.

EPI-USE Labs는 표준 SAP 데이터에 대한 사전 제공 가속 정책을 포함한 데이터 변환 플랫폼을 제공하며, 맞춤형 요구에 맞게 완전히 확장할 수 있습니다.

일반적으로 최소한 세 번의 테스트 사이클을 추천합니다:

- 단위 테스트 – 요구 사항 확인을 위해 EPI-USE Labs에서 완료합니다.
- 수락 테스트 – 긍정 및 부정 테스트; 요청된 데이터가 제거되었음을 확인하고, 필요한 것보다 더 많은 데이터가 제거되지 않았음을 확인합니다.
- 통합 및 회귀 테스트 – 제거된 데이터가 시스템 간 연결이나 프로세스에 부정적인 영향을 미치지 않았음을 확인합니다.

두 번째 및 세 번째 테스트 사이클은 여러분과 같은 기업고객의 책임입니다.

이 첫 번째 정리는 전체 운영환경전환으로 실행하는 것이 추천되며, 백업 복원 옵션, 명확한 프로세스 제어 및 추적이 필요합니다. 제 경력에서 많은 전환을 실행해 왔기 때문에 시간별 전환 계획을 다듬기 위한 전반적인 리허설의 이점을 강조하지 않을 수 없습니다.

5) 운영 복사본에서 PII 관리

다음과 같은 변화가 있을 때
- 급여의 세금 연도 변경
- 새로운 프로세스와 발전
- 시스템 업그레이드 또는
- 기술 플랫폼 변경

비즈니스가 원활하게 운영되도록 프로세스가 영향을 받지 않도록 해야 합니다.

이를 위해, 연중 운영 데이터베이스의 전체 사본을 자주 가져와서 모든 데이터를 개발, 품질 및 사전 운영 시스템에 복제합니다. 많은 고객은 SAP 인스턴스의 교육 인스턴스 또는 별도의 장기 프로젝트 트랙을 가지고 있습니다. 이는 운영 데이터가 여러 추가 시스템으로 확산되어 데이터 수집의 다양한 사용 사례를 가집니다.

테스트 데이터에 대한 정보 제공 및 명시적 동의?

대부분의 데이터 개인정보 보호법은 비즈니스가 수집한 데이터의 사용 사례에 대한 정보 제공 및 명시적 동의를 요구합니다. 대부분의 회사는 테스트 목적으로 데이터를 사용하는 데 필요한 동의를 받지 않았습니다. 이 경로를 선택하고 모든 직원, 고객 및 공급업체에게 연락하여 동의 조건을 수집하더라도 비동의의 문제가 여전히 존재합니다. 예를 들어, 고객이 10,000명이고 그 중 100명이 동의를 거부하면 전체 데이터베이스를 복사하는 것이 유일한 실행 옵션이라면 운영에서 사본을 가져올 수 없게 됩니다.

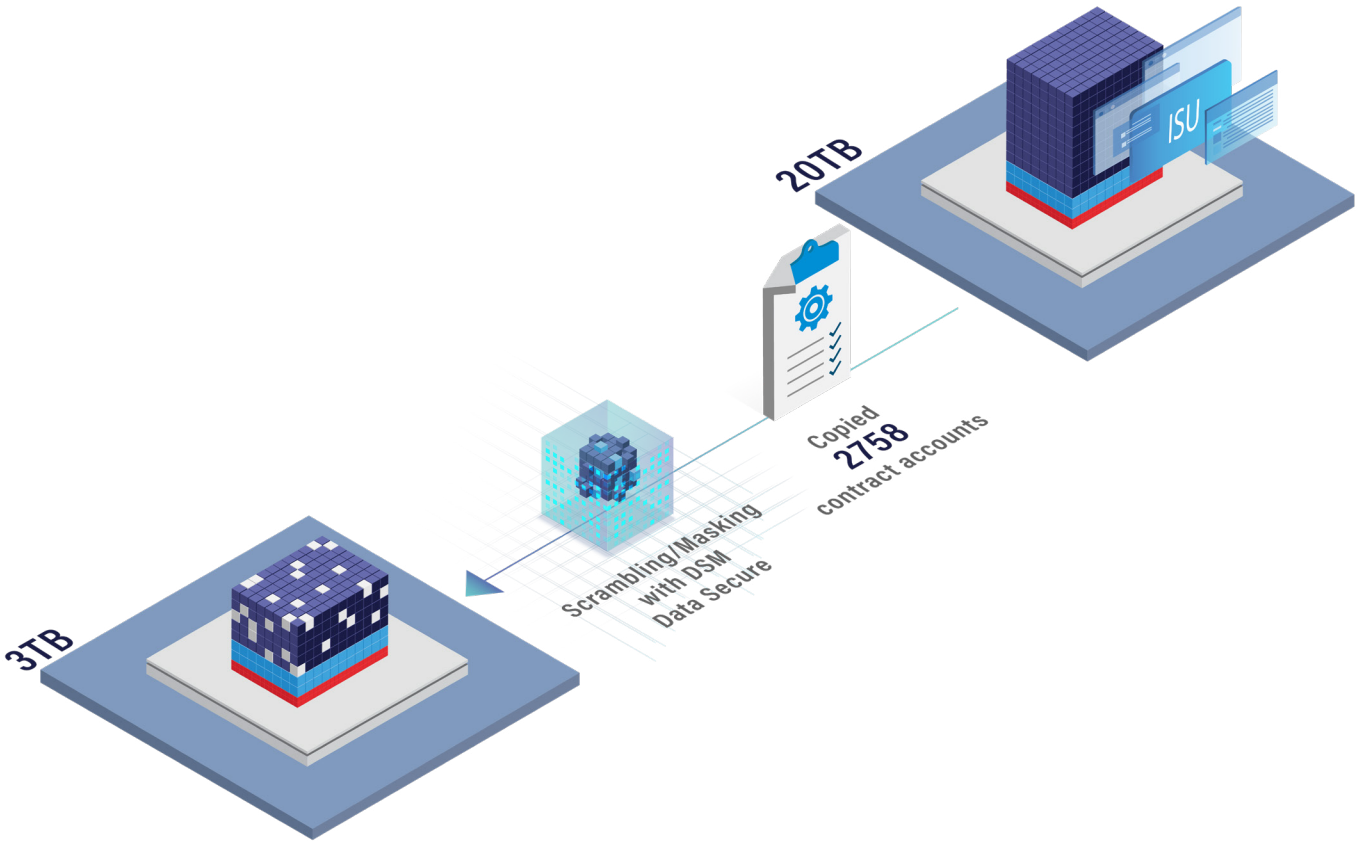
시장에 있는 일부 소프트웨어 공급업체는 사용자 인터페이스(UI) 마스킹이라고도 하는 마스킹 솔루션을 제공합니다. 이 방법은 데이터베이스에서 데이터가 변경되지 않지만 사용자가 UI를 통해 데이터를 액세스하려고 할 때 가로채어 PII의 가시성을 암호화하거나 제한하는 것입니다. UI 마스킹의 문제는 데이터베이스에 직접 액세스하면 UI를 거치지 않기 때문에 가로채기가 발생할 수 없다는 것입니다. 일반적으로 외부 데이터 유출 및 랜섬웨어 공격은 UI를 사용하지 않고 네트워크 보호가 침해되면 직접 서버 액세스를 사용합니다. 이러한 이유로 개인적으로는 UI 마스킹이 데이터 개인정보 보호법을 준수한다고 생각하지 않습니다.

안전한 대안

EPI-USE Labs의 Data Sync Manager (DSM) Suite의 일부인 Data Secure는 UI 마스킹 및 동의 관리의 대안입니다. 10년 넘게 Data Secure는 데이터베이스 내에서 PII 필드 값을 직접 수정해 왔습니다. 이 프레임워크는 암호 및 시드 테이블을 사용하지 않고, 각 필드를 독립적으로 계산하여 전문적인 도메인 매핑을 통해 정렬하는 패턴 파괴에 중점을 둡니다. 솔루션은 이름을 다른 이름으로, 은행 정보를 유효한 형식의 임의의 은행 정보로 대체하도록 설계되었습니다.

SAP 데이터가 시스템 검증을 통과할 수 있는 유효한 값을 가지도록 하면서 기록에 연관된 실제 PII 정보를 남기지 않는 것을 목표로 합니다. 표준 SAP 모델에 대한 가속 정책과 완전히 맞춤화 가능한 프레임워크가 제공되어, 비운영 환경에서 PII를 일관되게 대체하여 PII 위험을 제거할 수 있습니다.

Data Secure에 대해 더 알아보기



다양한 시스템 유형

저희가 협력하는 많은 고객들은 서로 다른 다양한 시스템들을관리하고 있습니다. 예를 들어, CONCUR, ARIBA 또는 SUCCESSFACTORS와 같은 클라우드 애플리케이션이 연결되어 있습니다.

- 첫째, OData로 연결된 클라우드 애플리케이션의 경우, 클라우드 애플리케이션에서 데이터를 복제하여 Data Secure가 제공하는 스크램블링으로 전송할 수 있는 클라우드 통합 플랫폼을 설계했습니다. 이로 인해 시스템 간 통합 스크램블링이 가능합니다.

  이 예시에서는 SAP Employee 와 SuccessFactors Entity 데이터가 동일한 새 값으로 익명화되고 있습니다.

- 그러나 다양한 유형의 시스템 및 API 연결이 존재합니다. Data Secure 솔루션은 다른 API도 사용할 수 있지만, 다른 업계 참가자들을 검토하고 Non-SAP 장치를 지원할 주요 파트너를 식별했습니다. 그래서 두 번째 권장 사항은 Non-SAP 장치에 대해 DatProf를 검토하는 것입니다. DatProf는 키와 새로운 값의 입력 목록을 받아들이며, Data Secure에 의해 완료된 SAP 스크램블링의 추출물을 가져와 모든 연결된 장치에서 새로운 스크램블 데이터를 일치시킬 수 있습니다.

6) 데이터 주체 접근 요청 처리 (DSARs)

이전의 많은 데이터 개인정보 보호법은 개인 접근 요청의 원칙을 규정하였습니다. 즉, 누구나 자신에 대해 회사가 보유한 정보를 요청할 수 있다는 것입니다. 최근 법률에서 주요한 변화는 응답해야 하는 기간이 더욱 엄격해졌다는 것입니다.

이러한 요구 사항이 오래전부터 존재해 왔기 때문에 많은 기업들은 접근 요청에 대한 대응 프로세스를 이미 갖추고 있습니다. 그러나 이러한 프로세스는 종종 수동적이고 시간이 많이 소요됩니다.

데이터 개인정보 보호법과 그 집행, 법정 사건들이 미디어의 주목을 받으면서 접근 요청의 양이 증가하고 있습니다. 저는 목표를 설정하고 동시에 회사를 접촉하는 소셜 미디어 그룹도 알고 있습니다.

일상적인 고객 대면 팀을 통해 이러한 요청의 급증을 관리하기 위해 더욱 자동화되고 효율적인 접근 요청 대응이 필요합니다. 유럽에서의 경험에 따르면 고객에게 형식화된 상세한 문서를 빠르게 응답할 수 있다면 추가 요청을 할 가능성이 훨씬 낮아집니다.

정보 주체 접근 요청에 신속하게 대응하기

EPI-USE Labs의 Data Disclose는 데이터 제거 및 암호화 솔루션에 사용된 동일한 매핑을 사용합니다. 개인 정보가 저장된 위치를 이미 알고 있으며, 여러 SAP 시스템과 클라우드 애플리케이션을 단일 출력 보고서로 검색하여 정보를 브랜드 형식의 PDF로 정리합니다.

PDF 파일은 암호화되어 저장되며, 비밀번호 보호가 필수적입니다. 파일은 요청을 한 정보 주체에게 이메일로 공유할 수 있으며, 비즈니스 프로세스에 따라 인쇄하여 우편으로 보낼 수도 있습니다. 실시간으로 개인정보 접근권에 대응할 프론트 오피스 솔루션을 찾으면 개인정보 보호법을 준수하기가 더 수월해집니다. 특히, 소매, 의료, 공공 서비스와 같은 고객 대면 사업에서는 요청이 많고 집중도가 높아 Data Disclose 같은 솔루션이 필요합니다.

Data Disclose에 대해 더 알아보기

EPI-USE LABS
value through innovation

EPI-USE Labs UK

EPI-USE Labs, Suite 11 N-B, Trafford house Manchester, M32 0RS, UK
www.epiuselabs.com
이메일: sales@labs.epiuse.com

아래 정보 대상 접근 요청에 대한 응답은 유럽 일반 데이터 보호 규정(GDPR)에 따라 발행되었습니다. 반복적이거나 과도하게 데이터를 요청하지 않는 이상, 아래와 같은 정보를 제공하는 데 별도의 비용이 청구되지 않습니다.

키: 0000401084
이름: ALAN ALBERT

비즈니스 파트너에 대한 개인 정보 검색:

CRM		
고객 관계 관리 솔루션		
데이터 유형	결과	결과 설명
전체 이름	ALAN ALBERT	
비즈니스 파트너 번호	T90CLNT090:3000	
	0000401084	
성	ALBERT	
이름	ALAN	
	ALBERT	
ID 번호	T90CLNT090:3000	
	0000401084	
생년월일	1978년 10월 15일	
도시	SALT LAKE CITY	
회사 이름	ALBERT	
전화번호	303-789-070	
	+1303789070	
도로명 주소	200 Fremont Drive	
우편/우편번호	84101	
전체 이름	ALAN ALBERT	

7) 개별 삭제 요청 처리

정보 주체는 접근 권리뿐만 아니라 삭제 권리도 이제 부여받습니다. 회사가 데이터를 보유할 합법적인 이유가 없다면, 해당 데이터를 삭제해야 합니다.

고객과 일할 때, 비즈니스와 IT 팀 간의 서로 다른 책임이 이러한 프로세스를 정의하는 데 있어 상당히 도전적이라는 점이 항상 흥미롭습니다. 대부분의 경우, 비즈니스가 데이터 소유자이며, 운영 시스템 내의 데이터 품질과 관리는 그들의 책임입니다. 그러나 데이터를 생성, 수정 또는 삭제하는 시스템 프로세스는 IT 팀이 제공합니다. 따라서 개인정보 보호 준수 프로세스는 IT 솔루션이 필요한 비즈니스 문제입니다. 많은 회의에서 비즈니스 팀이 IT에게 삭제 시스템을 운영해달라고 요청했지만, IT는 처리 요청 받은 데이터를 소유하지 않기 때문에 거절하는 경우도 있습니다.

물론 답은 공동의 노력이 필요하다는 것입니다. EPI-USE Labs에서 개발된 솔루션은 비즈니스 사용자들이 독립적으로 개별 요청을 처리할 수 있도록 설계되었습니다. 또한 IT 팀이 표준 배치 작업으로 실행할 수 있는 대규모 자동화 처리 시스템도 제공합니다. 이렇게 하면 IT는 데이터에 대한 책임을 지지 않고, 비즈니스 팀은 배치 시스템 프로세스를 책임지지 않아도 되어 모두가 만족할 수 있습니다.

이 문서의 이전 부분에서 논의한 바와 같이, 저는 민감한 데이터를 완전히 삭제하거나 UI를 통해 가리는 것보다 삭제하는 것을 강력히 추천합니다. 삭제의 정의는 민감한 데이터를 제거하거나 일정한 값으로 강제 설정하는 것입니다. 즉, 데이터베이스에서 '삭제'된다는 것입니다. 이를 통해 거래, 프로그램 또는 외부 API를 통해 접근할 때 익명화된 정보만 반환됩니다.

그러나 SAP 데이터베이스의 데이터 항목 간의 주요 값이나 관계, 비즈니스 인텔리전스는 시스템에서 유지할 수 있습니다. 간단히 말해서, 직원 기록은 여전히 존재하지만, 직원의 이름, 주소, 전화번호, 이메일 주소는 알 수 없습니다. 이 과정을 통해 비즈니스 인텔리전스는 유지되지만, 개인정보는 제거되어 개인정보 보호법을 준수합니다.

Data Disclose와 Data Redact

EPI-USE Labs의 Data Disclose를 사용하면 데이터 주체의 정보와 관련된 SAP 키를 검색할 수 있습니다. 예를 들어 이름, 전화번호, 우편번호를 검색하면 특정 데이터 주체의 직원, 고객 또는 공급업체 기록이 반환될 것입니다. 식별 후에는 개별 데이터를 삭제 워크플로우에 제출할 수 있습니다. 이 소프트웨어는 동일한 사람이 데이터 제거를 제출하고 승인할 수 없도록 역할 분리 및 권한 관리를 유지하도록 설계되었습니다.

삭제 워크플로우는 EPI-USE Labs의 Data Redact 솔루션에서 케이스를 생성합니다. Data Redact 는 유효한 키만 제출할 수 있도록 여러 가지 통제가 이루어지고 있으며, 실행된 제거 프로세스는 전용 관리자만 승인할 수 있으며, 사용자에 의해 변경될 수 없습니다. 이러한 통제는 모든 운영환경에서 제거 프로그램에 필수적입니다. 그러나 운영 사용자들이 매일 관리할 수 있는 프로세스도 필요합니다. 이러한 개인 권리에 대한 사용 편의성은 저에게 가장 높은 우선순위입니다.

Data Redact의 권한 있는 사용자가 작업 대기열을 열면, 처리 권한이 있는 객체에 대한 삭제 요청을 볼 수 있습니다. 여기서 데이터 주체의 데이터를 확인하고 삭제 요청을 수락할지 거절할지 결정할 수 있습니다. 수락되면, 모든 매핑된 PII 필드의 변경 통제 정책이 실행되어 값이 삭제되거나 대체 값으로 설정되어 시스템에서 기록이 비식별화됩니다.

다중 정책 요구사항

대부분의 기업은 다양한 데이터 항목과 서로 다른 기간에 대해 여러 데이터 수정 정책을 가지고 있습니다. 아래의 직원 예시는 일반적인 시나리오를 보여줍니다:

정책 1: 퇴사 후 6개월	정책 2: 퇴사 후 4년	정책 3: 퇴사 후 7-20년
일반적으로 제거되는 필드: 가족 정보 은행 정보 평가/메모 데이터	일반적으로 제거되는 필드: 전화번호 이메일 주소 회사 차량 등록 여권/운전면허증	일반적으로 제거되는 필드: 이름 주소 세금 정보 기타 모든 데이터

이와 같은 다중 정책 요구사항은 흔하며, 모든 데이터 제거 요구사항에 대해 이러한 접근 방식을 고려할 것을 권장합니다.

Data Redact에 대해 더 알아보기

8) 데이터 주체의 사전 식별

개별 삭제 요청 외에도, 기업은 이제 시스템에서 삭제되어야 할 데이터 주체를 사전에 파악해야 합니다. 이를 일반적으로 데이터 보존 요건이라고 합니다.

데이터 보존 질문

많은 고객으로부터 자주 받는 질문은 다음과 같습니다.

해외 직원에게는 어떤 법률이 적용됩니까?

본질적으로 이는 데이터 주체의 현재 거주지가 아닌 출신지로 귀결됩니다.

많은 경우 규정은 데이터 주체의 국적을 기준으로 적용되며, 현재 거주하는 주소는 다루지 않습니다.

데이터 보존 기간에 대해서는 다양한 국적에 적용되는 다양한 규칙 구별하는 것이 중요합니다

모든 것에 동일한 규칙이 적용되어야 합니까?

물론 아닙니다. 사실, 저는 이를 권장하지 않습니다. 직원을 예로 들어, 은행 계좌 정보와 가까운 친척/가족 구성원 정보는 고용 종료 후, 예를 들어 6개월 후에 삭제해야 합니다. 그러나 대부분의 국가에서는 세법상 주민등록번호/납세자 번호, 이름, 급여 내역을 7년에서 10년 동안 보관해야 합니다.
따라서 보존 요건을 고려할 때 정보 주체가 아닌 데이터 유형을 고려해야 합니다.

보존 정책은 누가 결정하나요?

궁극적으로 데이터 보호 책임자(DPO)는 정보 보존의 법적 정당성을 넘어 보존 기한을 정할 책임이 있습니다. 그러나 보존 기준의 기능적 및 기술적 영향을 파악하기 위해서는 DPO가 비즈니스 및 IT 팀의 도움이 필요합니다.

모든 이해관계자 간에 이러한 원칙을 논의하고 합의하며, 초기 요구 사항의 기준을 정하는 워크숍 과정을 권장합니다. 이는 제공 및 테스트를 통해 변경될 가능성이 있지만, 명확하고 실현 가능한 기준은 프로젝트의 효율성을 향상시킵니다.

EPI-USE Labs의 Data Retain 소프트웨어는 더 이상 보존 요구 사항을 충족하지 않는 SAP 데이터 주체를 자동으로 식별하고 승인된 사용자가 처리할 수 있도록 해당 데이터 주체를 Data Redact 대기열에 추가합니다.

보존 절차의 원칙

선별자:

데이터 주체의 초기 목록을 식별합니다. 예를 들어, X년 이상 전에 생성된 고객 목록이나 Y년 이상 전에 퇴사한 직원 목록을 식별합니다.

검증자:

개별 검사를 통해 식별된 데이터 주체가 편집 대상으로 처리될지 확인합니다. 이러한 검증자는 가장 많은 수를 먼저 제거하도록 설계되며, 저수준 거래 검사를 수행하기 전에 우선적으로 처리됩니다. 예를 들어, 고객 유형과 6년 이내 거래 여부에 따라 검사하는 경우, 유형 검사를 우선시하여 가장 적은 수의 기록에 대해 거래를 검사합니다.

처리자:

편집할 데이터에 적합한 정책을 선택하고 편집 워크플로우 내에서 배치 케이스를 생성합니다.

보존 보고서의 기술적 구현 일정은 요구 사항의 복잡성과 환경 내 데이터 주체의 양에 직접 비례합니다. 그러나 중요한 사항은 요구 사항의 품질을 사전에 철저히 검토하고 비즈니스 팀에 의해 서명되는 것입니다. 제가 참여했던 프로젝트 중에는 이러한 과정이 제대로 이루어지지 않아 1~2주 작업이 1~2개월의 테스트 및 재구축 과정으로 연장된 경우가 있었습니다. 요약하자면, 청사진 수립은 보존 설계에 필수적입니다.

9) 지속적인 감사 및 검토

데이터 개인 정보 보호 준수는 단기 프로젝트로 간주되어서는 안 됩니다. 사업 변화에 따라 새로운 위험이 발생할 수 있으며, 이에 대한 통제가 필요합니다.
기술 시스템 관점에서 이는 새로운 애플리케이션이나 SAP 인스턴스에 추가 기능을 구매할 때 가장 일반적으로 나타납니다. 또한 프로세스를 맞춤화하여 PII 데이터를 포함하는 새로운 커스텀 테이블을 추가하는 경우에도 발생할 수 있습니다.

저는 모든 고객에게 신뢰할 수 있는 개인정보 보호 파트너와 함께 정기적으로 6~9개월마다 시스템을 검토할 것을 권장합니다.

이 검토는 준수를 위한 미니 사이클을 요구합니다:

- 자산 내 PII 변경 사항을 매핑하기 위한 새로운 데이터 발견 완료
- 접근 권한 검토 지속 (예: 파트너 Soterion의 소프트웨어 사용)
- 원래 정책의 차이를 반영하기 위한 보존 및 수정 정책 수정
- 식별된 차이를 위한 운영환경의 백로그 처리
- 접근 권한 및 삭제 권한을 처리할 수 있도록 프론트 오피스 프로세스 업데이트 및 준비.

저는 일반적으로 SAP 시스템에 대해 6~9개월마다 이러한 활동을 완료하고 전문가가 운영환경으로 제어할 수 있도록 2~3주 기간을 허용합니다. 저는 이것을 '개인정보 보호 정책 관리'라고 부릅니다. 이 검토 주기는 사전에 합의되어 감사 검토와 연결될 수 있으며, 솔루션 전문가의 지원을 필요로 할 때 받을 수 있습니다.

> Data Secure 덕분에 우리는 직원 관련 데이터를 포함한 모든 민감한 SAP HCM 데이터를 매우 짧은 시간에 익명화할 수 있습니다.
>
> Data Disclose의 가장 큰 장점은 데이터 무결성이 보장된다는 것입니다. 고객의 민감한 데이터가 익명화되지만 모든 주문과 판매된 항목은 여전히 접근 가능합니다. 모든 테스트 시스템은 완전히 기능을 유지하며, 테스트 주문은 여전히 편집할 수 있습니다.
>
> Malte Podszus, FI/CO/HR 컨설턴트, MAPA GmbH

결론

이 문서가 여러분의 개인정보 보호 프로젝트를 구성하는 데 유용하게 사용되었기를 바랍니다. SAP와 관련하여, 자신 있게 참여할 수 있는 옵션과 파트너에 대한 정보도 포함되어 있습니다.

관리하고 있는 기술에 적합한 파트너를 찾는 것과, 법을 이해하는 법률 준수 팀의 중요성을 과소평가하지 마십시오.

개인정보 보호의 영향은 매우 광범위합니다. 기술과 데이터 공유/캡처가 빠르게 발전함에 따라 법률도 이에 맞춰 개정되어야 하며, 아마도 우리의 생애 내에 다시 변화할 것입니다. 이러한 변화에 대해 검토하고 적응하며 대처할 수 있는 적합한 팀을 구성하고 투자하는 것이 사업의 성공에 결정적일 것입니다.

이 전자책을 읽어주셔서 감사합니다. 궁금한 점이 있다면, info@labs.epiuse.com으로 연락해 주시면, 연락드리겠습니다.

저자 소개

제가 이 전자책을 쓰게 된 배경을 간단히 소개합니다.

SAP 데이터 관리 여정을 시작했을 때, 저는 레거시 시스템의 비즈니스 사용자로서 고객을 위한 SAP 설계 및 구현에 참여했습니다. 구현 이전에는 프론트엔드 시스템 사용자, 팀 리더, 트레이너였으며, 결국 SAP 구현을 위한 청구 비즈니스 분석가가 되었습니다. 이러한 프론트 및 백오피스 고객 대면 역할과 IT 구현 및 데이터 마이그레이션 경험을 통해 기능적 세계와 비즈니스 세계를 모두 이해할 수 있는 독특한 관점을 가지게 되었습니다.

2016년에 EPI-USE Labs에 기술 컨설턴트로 합류하여 SAP ALM 데이터 동기화 관리자(DSM) 소프트웨어를 구현했습니다. 데이터 동기화 관리자 솔루션의 핵심은 다양한 SAP 인스턴스 간의 교차 시스템 및 내부 통합을 매핑하는 SAP 객체 정의 라이브러리입니다. 2017년에는 유럽에서 SAP를 위한 EPI-USE Labs의 데이터 프라이버시 스위트의 시작을 담당하면서 접근 권리, 삭제 권리 및 개인 정보 보호 관리를 위한 해결책을 제공했습니다. 이 역할을 통해 고객에게 가장 적합한 프로젝트 접근 방식을 정의하여 요구 사항 수집부터 구현 및 운영까지 전 프로젝트 라이프사이클을 지원할 수 있었습니다. 2022년에는 EPI-USE Labs 비즈니스의 모든 지역 팀을 지원하는 글로벌 역할을 맡았습니다.

요약하자면, 저는 네 개의 대륙과 열세 개의 국가에서 다양한 개인정보 보호법에 따라 50개 이상의 개인정보 보호 프로젝트를 지원했습니다.

이 전자책을 통해 프로젝트를 통해 배운 교훈을 공유하고자 했습니다. 여러분의 데이터 프라이버시 여정에 도움이 되었기를 바랍니다.

James Watson
Business Owner
EPI-USE Labs 데이터 프라이버시, 리스크 및 산업 솔루션

글로벌 소프트웨어 솔루션 및 관리 서비스 회사로서, EPI-USE Labs는 SAP® 및 SAP SuccessFactors® 시스템의 성능, 관리 및 보안을 극대화하는 데 도움을 줍니다. 고객들은 매일 우리의 도움으로 비즈니스 운영이 어떻게 변화했는지 이야기합니다. 비즈니스 과제를 해결하는 방법을 알아보려면 저희에게 연락하세요.

epiuselabs.com | info@labs.epiuse.com
EPI-USE Labs는 groupelephant.com의 회원입니다.

Group Elephant™
BEYOND CORPORATE PURPOSE