7 praktische Schritte, wie Sie Ihre SAP-Systeme an die neue EU-Datenschutz-Grundverordnung (DSGVO/GDPR) anpassen

Die Erfüllung der EU-Datenschutz-Grundverordnung (DSGVO/engl. GDPR) stellt die meisten Unternehmen vor eine enorme Herausforderung. Ein Grund dafür ist die Fülle an Systemen und Prozessen, die betroffen sind – vor allem dann, wenn Unternehmen massiv in umfangreiche SAP-Lösungen (ECC, SRM, BW, CRM usw.) investiert haben. Je nach Art und Komplexität der SAP-Lösungen werden ganz unterschiedliche Speicher- und Zugriffstechniken für sensible Daten angewendet. Dazu kommen gewaltige Datenmengen, was das Finden und Verwalten sensibler Daten besonders komplex macht.

Seit dem 25. Mai 2018 müssen weltweit alle Unternehmen, die personenbezogene Daten von EU-Bürgern erheben, speichern und verarbeiten, in der Lage sein, die Daten zu einer Person offenlegen. Außerdem müssen Sie angeben können, zu welchem Zweck die Daten gespeichert und verwendet werden.

Die Einhaltung der Datenschutz-Grundverordnung ist nicht verhandelbar. Unternehmen, die dagegen verstoßen, müssen mit hohen Geldbußen rechnen: bis zu 20 Mio. EUR oder 4% des Jahresumsatzes, je nachdem, welche Summe höher ist.

Jedes Unternehmen sollte über einen Plan verfügen, wie die Anforderungen erfüllt werden können, und die zentralen Rollen und Verantwortlichkeiten hierfür festlegen. Für Kunden, die SAP als Haupterfassungssystem und auch überwiegend in ihrer IT-Landschaft einsetzen, hat EPI-USE Labs nachfolgend 7 praktische Schritte zusammengestellt, damit sie diese Aufgabe besser und strukturierter bewältigen können.

Schritt 1:
Prüfen, wo sensible Daten in SAP-Systemen gespeichert werden

- Analysieren Sie Ihre SAP-Landschaft, und ermitteln Sie, in welchen zentralen Bereichen alle personenbezogenen und sensiblen Daten gespeichert werden. Sie können Anfragen nur bearbeiten und personenbezogene Daten erst weitergeben, wenn Sie wissen, wo sensible Daten abgelegt sind.
- Die für SAP zuständigen Teams müssen wissen, wo in Ihren SAP-Systemen sensible Daten liegen (einschließlich integrierter Komponenten wie Workflow, SAP BW und Änderungsbelegen), sodass Prozesse zum Finden, Anzeigen und eventuellen Löschen von Daten entwickelt werden können.
- Überprüfen Sie die Abläufe und Blueprints Ihrer Geschäftsprozesse, und ermitteln Sie die Schritte, in denen sensible Daten von Kunden, Mitarbeitern, Lieferanten und Geschäftspartnern vorhanden sind.

Schritt 2:
Sensible Daten in nicht-produktiven SAP-Systemen reduzieren

- Mindern Sie Ihr Risiko, indem Sie Daten in nicht-produktiven Systemen intelligent maskieren.
- Ermitteln Sie ungenutzte Mandanten oder Systeme mit sensiblen Daten, die gelöscht werden können. Prüfen Sie auch sensible Daten, die in bestimmten Testmandanten nicht benötigt werden und ebenfalls gelöscht werden können.

Schritt 3:
Prozesse für das Recht auf Auskunft und Recht auf Vergessenwerden entwickeln

- Entwerfen Sie Prozesse und halten Sie in Checklisten fest, wie Sie in Ihrem Unternehmen auf Auskunftsanfragen personenbezogener Daten reagieren. Überlegen Sie sich geeignete Workflows und Prozessabläufe, und übertragen Sie die Verantwortung einem konkreten Team. Dazu könnte beispielsweise eine kundenorientierte Weblösung gehören, mit der Anfragen verfolgt und verwaltet werden.
- Legen Sie eine zentrale Mailbox an, oder führen Sie eine Kommunikationslösung ein, um Dialoge und Interaktionen der DSGVO betreffend zu dokumentieren.

Schritt 4:
Richtlinien zur Aufbewahrung von Daten überprüfen

- Überprüfen Sie Ihre Richtlinien zur Datenaufbewahrung im Hinblick auf die Anforderungen der DSGVO.
- Entwickeln Sie ein Rahmenkonzept für die Archivierung und Aufbewahrung von Daten, mit dem Sie Altdaten verwalten und aus dem deutlich hervorgeht, wann sensible Daten archiviert oder gelöscht werden können.
- Soweit möglich, automatisieren Sie Ihre Lösungen zur Archivierung und Verfremdung von Daten, sodass Datenaufbewahrung nicht mehr projektbasiert, sondern regelmäßig erfolgt.

Schritt 5:
Zugriffsrechte von Mitarbeitern auf sensible Daten im SAP-System einschränken

- Bestimmen Sie, wo Ihre sensiblen und personenbezogenen Daten gespeichert werden (Transaktionen, Tabellen und zugehörige Business-Objekte).
- Ermitteln Sie, welche Rollen und Benutzer auf diese Daten zugreifen können, und entwickeln Sie Regeln, die etwaige mit dem Zugriff verbundene Risiken berücksichtigen.
- Legen Sie einen Prozess fest, mit dem der Zugriff auf personenbezogene Daten regelmäßig überprüft wird.
- Dokumentieren Sie Zugriffsrechte und Validierungsschritte genau.

Schritt 6:
Daten verschlüsseln, die Ihr SAP-System verlassen

- Implementieren Sie eine Verschlüsselung, damit auf archivierte Daten nicht unbefugt zugegriffen werden kann. Alle Daten, die auf Fileservern gespeichert oder über Schnittstellen versendet werden, sollten vor der Übertragung verschlüsselt werden.
- Überprüfen Sie Ihr End-Point-Sicherheitskonzept. Stellen Sie sicher, dass durch die Lösungen, die Sie nutzen, das Risiko für Benutzer gemindert wird, wenn diese für Reportings, Analysen und Wissensaustausch mit Kollegen sensible Daten extrahieren.

Schritt 7:
Audit und Protokollierungen in SAP überprüfen

- SAP-Benutzer extrahieren für Reportings, Analysen und Wissensaustausch mit Kollegen, Partnern und Lieferanten eine Vielzahl sensibler Dokumente aus SAP-Systemen und -Anwendungen. Die meisten Unternehmen wissen nicht genau oder können nicht kontrollieren, wohin diese Dokumente gelangen, wer darauf zugreift und wie sie verwendet werden. Für Unternehmen besteht dadurch ein hohes Risiko, dass Daten aufgrund böswilliger Handlungen oder aus Versehen verloren gehen.
- Simulieren Sie eine Datenschutzverletzung und erstellen Sie daraufhin einen Maßnahmenplan, in dem die Zuständigkeiten und Verantwortungsbereiche aller beteiligten Personen (Basis, Netzwerksicherheit, Anwendungsverantwortliche, Risikobeauftragte) aufgeführt sind.

So kann EPI-USE Labs Ihnen helfen

EPI-USE Labs bietet eine Vielzahl an innovativen Add-On-Softwareprodukten und Services zur Optimierung von SAP-Landschaften. Diese beschleunigen, automatisieren und vereinfachen das Management von Daten mit nachweißlichem Erfolg. Außerdem bieten wir moderne Sicherheitslösungen und wissen, wie Sie die Anforderungen der DSGVO erfüllen können.

Lernen Sie die EPI-USE Labs DSGVO/GDPR Compliance Suite für SAP kennen: Data Secure (Teil der Data Sync Manager Suite) ist eine umfassende Lösung für den Schutz von Daten mit vordefinierten Maskierungsregeln, anhand deren Sie alle Nicht-Schlüsselfelder in SAP unkenntlich machen können. Mit **Data Disclose** können Sie sensible Daten in Ihrem gesamten SAP-Portfolio ermitteln und damit das Recht auf Datenzugriff erfüllen. Für das Recht auf Vergessenwerden wurde die Fiori-App **Data Redact** als Ergänzung zu Data Disclose entwickelt. Damit werden Daten, die zur Verfremdung gekennzeichnet sind, intelligent entfernt. **Data Retain** ermöglicht proaktives Finden von personenbezogenen Daten zur Verfremdung nach flexiblen Regelen. Die Ausführung erfolgt ad-hoc oder regelmäßig geplant automatisiert.