EINHALTUNG DER DATENSCHUTZGESETZE IN SAP-SYSTEMEN

Zehn Empfehlungen für Ihren Weg zur Compliance

Aufgrund unserer Erfahrung bei der Implementierung von Compliance-Lösungen für SAP-Kunden empfehlen wir:

1. FÜHREN SIE EINE DATENSCHUTZ-FOLGENABSCHÄTZUNG DURCH (DATA PRIVACY IMPACT ASSESSMENT, DPIA).

- Binden Sie Ihre Auditoren und Rechtsberater frühzeitig mit ein. Sie beraten Sie zu den wichtigsten Risikobereichen und werden einen geeigneten Handlungsrahmen für das laufende Compliance-Management bereitstellen.
- Bilden Sie ein Management Team für das Datenschutzprogramm. Ernennen Sie mindestens einen Datenschutz-verantwortlichen, und registrieren Sie diesen bei der Aufsichtsbehörde.
- Assessments können Folgendes beinhalten:
  - Personenbezogene Daten und Abbildung des Datenfluss (pro Geschäftsbereich)
  - Beurteilung von Sicherheitslücken im Datenschutz
  - Due Diligence Prüfungen von Dritten

2. SCHÄRFEN SIE DAS BEWUSSTSEIN FÜR DIE RELEVANTEN DATENSCHUTZGESETZE

- Führen Sie eine unternehmensinterne Datenschutzbewertung durch, um die Bereitschaft und den Wissensstand der Mitarbeiter zu ermitteln und sicherzustellen, dass Mitarbeiter mit Kundenkontakt die notwendigen Gesetze genau kennen.
- Informieren Sie Ihre Mitarbeiter und Stakeholder über die relevanten Datenschutzgesetze, die Anforderungen und die damit verbundenen Verantwortlichkeiten (nutzen Sie handelsübliche E-Learning-Lösungen, um die Wissensvermittlung und -aneignung zu beschleunigen).
- Werden Sie Mitglied bei professionellen Datenschutzstellen und -gremien, wie z. B. International Association for Privacy Professionals (IAPP.org), um Best-Practice-Verfahren optimal zu nutzen.

3. FÜHREN SIE EIN AUDIT DURCH, UM FESTZUSTELLEN, WO SENSIBLE DATEN IN IHREN SAP-SYSTEMEN GESPEICHERT WERDEN

- Analysieren Sie Ihre SAP-Landschaft, um Schlüsselbereiche zu ermitteln, in denen alle personenbezogenen und sensiblen Daten gespeichert sind. Wenn Sie keine klare Vorstellung davon haben, wo sensible Daten gespeichert sind, wird die Bearbeitung von Anfragen und die Offenlegung personenbezogener Daten schwierig.
- Die SAP-Fachbereiche sollten den Ablageort von sensiblen Daten in den SAP-Systemen kennen (einschl. integrierte Komponenten wie Workflow, SAP BW, Änderungsbelege usw.), sodass Vorgehensweisen zum Anzeigen und möglichen Entfernen von Daten entwickelt/konzipiert werden können.
- Überprüfen Sie die Abläufe Ihrer Geschäftprozesse, und identifizieren Sie Schritte, bei denen sensible Daten (Informationen zu Kunden, Mitarbeitern, Lieferanten und Geschäftspartnern) involviert sind.

4. REDUZIEREN SIE SENSIBLE DATEN IN IHREN NICHT-PRODUKTIVEN SAP-SYSTEMEN

- Verringern Sie Ihr Risikoprofil, indem Sie Daten in nicht-produktiven Systemen intelligent maskieren. Dadurch, dass Ihre Testsysteme maskiert sind, können Sie sich auf die wesentlichen Systeme fokussieren und den Aufwand bei der Bearbeitung von Anfragen reduzieren.
- Suchen Sie nicht verwendete Mandanten/Systeme mit sensiblen Daten, die gelöscht werden können. In Testmandanten können nicht erforderliche Daten entfernt werden.

5. SCHÜTZEN SIE IHRE INFRASTRUKTUR

- Überprüfen Sie das SAP One Launchpad regelmäßig auf Sicherheitspatches, speziell für Ihre SAP-Versionen, Ihr Betriebssystem und Ihren Datenbanktyp.
- Stellen Sie sicher, dass es innerhalb Ihres SAP-Teams eine klare Verantwortung für die Prüfung und Anwendung von SAP-Hinweisen gibt.
- Stellen Sie sicher, dass Ihr Team über die erforderlichen Fachkenntnisse zum Schutz von Systemen und hybriden Cloud-Landschaften, einschließlich Cloud- und Firewall-Regeln, verfügt.

6. ÜBERPRÜFEN ODER IMPLEMENTIEREN SIE RICHTLINIEN ZUR DATENHALTUNG, UM HISTORISCHE DATEN ZU REDUZIEREN (INNERHALB VON SAP)

- Entwickeln Sie ein Regelwerk zur Archivierung, Verfremdung und Datenhaltung für historische Daten, das eindeutig angibt, welche sensiblen Daten archiviert oder anderweitig entfernt werden können.
- Automatisieren Sie diese Verfremdungs- und Archivierungslösungen, sodass die Datenhaltung Teil Ihres normalen Geschäftszyklus wird.
- Führen Sie anhand Ihrer Datenhaltungsrichtlinien ein Clean-Up- und Archivierungsprojekt durch, um Daten, für deren Aufbewahrung keine rechtlichen Gründe mehr vorliegen, zu entfernen, zu archivieren oder zu verfremden.

7. VERWALTEN SIE ZUGRIFFSRISIKEN IN BEZUG AUF SAP-SYSTEME, UM DEN ZUGRIFF DER MITARBEITER AUF SENSIBLE DATEN ZU BESCHRÄNKEN

- Legen Sie fest, wo Ihre sensiblen und personenbezogenen Daten gespeichert werden (Transaktionen, Tabellen und zugehörige Business-Objekte).
- Identifizieren Sie Rollen und Benutzer, die Zugriff auf diese Daten haben, und entwickeln Sie Regelwerke und Warnhinweise, damit Risiken bei Zugriffsanfragen erkannt werden.
- Setzen Sie einen Prozess auf, um regelmäßig zu prüfen, wer Zugriff auf personenbezogene Daten hat.
- Dokumentieren Sie Zugriffsrichtlinien und Validierungsschritte klar und deutlich.

8. VERSCHLÜSSELN SIE DATEN, DIE IHR SAP-SYSTEM VERLASSEN

- Implementieren Sie eine Verschlüsselung, um zu verhindern, dass sensible Daten gespeichert werden: Alle auf Dateiservern gespeicherten oder über Schnittstellen bereitgestellte Daten sollten vor der Übertragung verschlüsselt werden.
- Überprüfen Sie Ihre Sicherheitsrichtlinien, um sicherzustellen, dass Sie Lösungen eingesetzt haben, die das Risiko von Benutzern verringern, die sensible Daten durch Reporting und Analysen extrahieren.

9. ÜBERPRÜFEN SIE DIE FÄLLIGKEIT IHRER AUDIT-TRACKING- UND -PROTOKOLLIERUNG IN SAP

- SAP-Benutzer extrahieren Hunderte von sensiblen Datensätzen und Dokumenten aus SAP-Systemen und Anwendungen zwecks Reporting, Analysen und Wissensaustausch mit Kollegen, Partnern und Lieferanten. Die meisten Unternehmen haben sehr wenig Kenntnis oder Kontrolle darüber, wohin diese Dokumente übermittelt werden, wer auf sie zugreift oder wie sie verwendet werden. Für Unternehmen bedeutet dies ein hohes Risiko von Datenverlusten aufgrund von böswilligen oder zufälligen Handlungen.
- Simulieren Sie eine Reaktion auf eine Datenschutzverletzung, und entwickeln Sie einen Aktionsplan, der die zentralen Verantwortlichkeiten aller beteiligten Rollenakteure skizziert (Basis, Netzwerksicherheit, Anwendungsverantwortliche und Risikomanager).

10. DEFINIEREN SIE EINE ROADMAP FÜR DIE EINHALTUNG DER COMPLIANCE

- Identifizieren Sie SAP-Lösungen und -Prozesse zur Unterstützung des Managements von Zugriffsrisiken, Infrastruktursicherheit, Risikobeurteilung und internen Kontrollen, Archivierung, Management von nicht-produktiven Daten, Benachrichtigungen bei Datenschutzverletzungen und Management von Auskunftsanfragen.

EPI-USE Labs kann Sie bei der Einhaltung der Datenschutzgesetze unterstützen.

Setzen Sie sich mit uns in Verbindung: vertrieb@epiuselabs.com | T +49 6227 6 98 98 0

epiuselabs.com/de/gdpr-compliance-suite | epiuselabs.com/de/compliance-richtlinien-erreichen | epiuselabs.com/de/gdpr-services

groupelephant.com
BEYOND CORPORATE PURPOSE