Datenschutz in ERP-Systemen aus Unternehmenssicht

Datenschutz macht vor ERP-Systemen nicht Halt. Das Inkrafttreten des neuen Schweizer Datenschutzgesetzes am 1. September 2023 ist ein guter Anlass, die Datenschutzkonformität betriebener und geplanter ERP-Systeme zu überprüfen.

>> Henriette Baumann | integratio GmbH

Das Wichtigste gleich zu Beginn: Betreibt ein Unternehmen ein ERP-System, so steht das Unternehmen gegenüber allen Personen, deren Daten im ERP-System verarbeitet werden, datenschutzrechtlich in der Verantwortung. Aussagen zur Datenschutzkonformität von Herstellern müssen vertraglich zugesichert und ggf. überprüft werden. Jeder Auftragnehmer, der Zugang zu Personendaten im ERP-System hat, wie beispielsweise Cloud-Anbieter oder Support-Dienstleister, muss überprüft und vertraglich verpflichtet werden, die Datenschutzanforderungen einzuhalten. Das neue Schweizer Datenschutzgesetz sieht zudem vor, dass Unternehmen bereits ab der Planung Datenschutzvorschriften zu berücksichtigen haben. Somit gehören Anforderungen an einen datenschutzkonformen Einsatz des geplanten ERP-Systems bereits in die Evaluation und Ausschreibung.

Beschränkung auf den Zweck und «need to know»

Wichtig für den operativen Einsatz eines ERP-Systems ist, dass Personendaten für die Zwecke bearbeitet werden, für die sie erhoben wurden. Werden in einem ERP-System Online-Käufe abgewickelt, so dürfen die dabei anfallenden Daten beispielsweise nicht für beliebige Werbezwecke verwendet werden. Entsprechend sind die Zugriffe und Verarbeitungen zu regeln. Ein Marketing-Mitarbeiter beispielsweise benötigt keinen Zugriff auf Bestell- und Rechnungsdaten einzelner Kunden. Auch bei der Übermittlung von Daten an Drittsysteme ist die Zweckbeschränkung zu berücksichtigen.

Keine beliebig lange Aufbewahrung

Ist der Zweck, für den die Daten erhoben wurden, erfüllt und sehen keine gesetzlichen Aufbewahrungsfristen eine längere Aufbewahrung vor, müssen Personendaten gelöscht oder anonymisiert werden. Eine Inaktivierung ist nicht ausreichend. Hierfür benötigt es Funktionalitäten, die eine Identifikation und datenschutzkonforme Löschung aller zu löschenden Personendaten ermöglicht.

Datensicherheit muss gewährleistet sein

Zu den datenschutzrechtlichen Anforderungen an die Datensicherheit gehören Zugriffs- und Zugangskontrollen und Protokollierungen zur Nachweisbarkeit der Bearbeitungen. Die Sicherung und rasche Wiederherstellung von Personendaten müssen gewährleistet sein. Werden Personendaten an Dritte weitergegeben, sind Massnahmen wie Verschlüsselung und Sicherstellung der korrekten Empfänger erforderlich, was auch bei der Anbindung von Drittsystemen zu beachten ist. Die Massnahmen müssen dem Risiko angemessen sein. So sind die Anforderungen an ein ERP-System, in dem besonders schützenswerte Personendaten bearbeitet werden, höher als bei einem Schraubenproduzenten. Ob ein ERP-System datenschutzkonform ist, kann demzufolge erst nach entsprechender Analyse der unternehmensspezifischen Nutzung des ERP-Systems beurteilt werden.

Meldepflicht bei Verletzungen der Datensicherheit

Ab 1. September 2023 müssen Verletzungen der Datensicherheit, bei denen ein hohes Risiko für die betroffenen Personen zu befürchten ist, so rasch als möglich gemeldet werden.

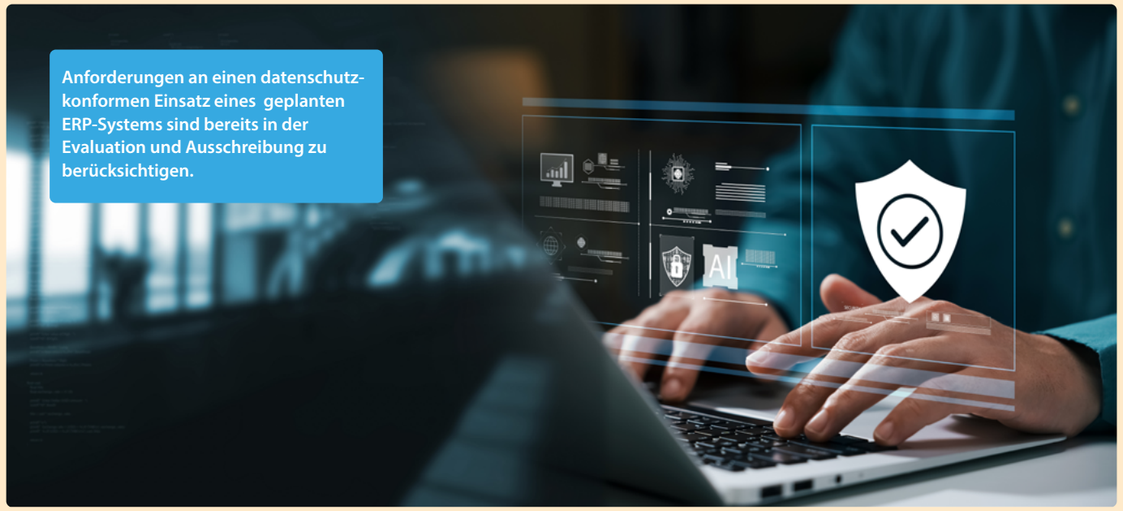
Datensicherheitsverletzung im ERP-System müssen daher schnell festgestellt, nachvollzogen und eingedämmt werden können. Das bedingt jederzeit verfügbares technisches und funktionales Know-how, entweder im eigenen Unternehmen oder von einem Dienstleister vertraglich zugesichert.

Auskunftsbegehren und weitere Rechte

Diejenigen Personen, deren Daten im ERP-System bearbeitet werden, haben das Recht auf Auskunft über die bearbeiteten Daten, auf Berichtigung, Sperrung und Löschung sowie auf die Aushändigung ihrer Daten in einem gängigen elektronischen Format. Diese Funktionalitäten muss ein ERP-System zur Verfügung stellen und eine vorgängige Überprüfung sollte durchgeführt werden, da im Falle einer Betroffenenanfrage Fristen einzuhalten sind.

Länderübergreifender Betrieb

Wird ein ERP-System länderübergreifend eingesetzt, beispielsweise bei Unternehmensgruppen, gilt es die Datenschutzgesetzgebungen der jeweiligen Länder zu berücksichtigen. Dies wäre beispielsweise der Fall, wenn eine Schweizer Muttergesellschaft ein ERP-System in der Schweiz betreibt und ihren Tochtergesellschaften in mehreren Ländern zur Verfügung stellt. Auch die Übermittlung von Personendaten zwischen Unternehmen einer Unternehmensgruppe ist nicht ohne weiteres zulässig und die Schnittstellen und Zugriffe müssen beschränkt bzw. geregelt werden.



Anforderungen an einen datenschutzkonformen Einsatz eines geplanten ERP-Systems sind bereits in der Evaluation und Ausschreibung zu berücksichtigen.

Transparenz ist unerlässlich

Datenschutzanforderungen können nur erfüllt werden, wenn ein ERP-System transparent und prüfbar ist. Nicht nur für die bereits aufgeführten Fälle, sondern auch für die Erfüllung der Informationspflicht und die Erstellung datenschutzrechtlich notwendiger Dokumentationen. Hier ist Hartnäckigkeit gefragt. Die erforderlichen Informationen müssen vom verantwortlichen Unternehmen beim Hersteller oder Dienstleister eingeholt und geprüft werden.

Die **Konsequenzen bei Verstössen** werden mit dem neuen Datenschutzgesetz verschärft. Hier sind vor allem die Bussgelder zu erwähnen, die bis maximal 250‘000 Franken gegen diejenigen Person verhängt werden können, die einen Datenschutzverstoss begeht bzw. zu verantworten hat. Nicht zu unterschätzen ist auch ein möglicher Reputationsverlust, wenn Datenschutzverletzungen in der Öffentlichkeit bekannt werden. Die sorgfältige und regelmässige Prüfung des ERP-Systems und der damit verbundenen Auftragnehmer gehört daher zu den grundlegenden Compliance-Aufgaben eines Unternehmens. <<

Datenschutz-Schulung und E-Learning

Warum müssen Schulungen für Datenschutz und Informationssicherheit durchgeführt werden?

Sowohl das Schweizer Datenschutzgesetz wie auch die EU-DSGVO geben vor, wie Personendaten verarbeitet werden dürfen. Jedes Unternehmen hat die Einhaltung dieser gesetzlichen Vorgaben sowie vertraglicher Verpflichtungen sicherzustellen. Dies kann nur mit einem datenschutzkonformen Verhalten der Mitarbeitenden und genügender Sensibilisierung im Bereich der Informationssicherheit erreicht werden: Durch entsprechende Schulung und Unterweisung.

Was bietet das E-Learning-Training der integratio?

Wir bieten E-Learning-Kurse für Schweizer Unternehmen, die von Mitarbeitenden orts- und zeitunabhängig durchlaufen werden können – am PC, Tablet oder Smartphone. Die topaktuellen Kursinhalte werden von unseren Experten und Fachanwälten entwickelt und praxisorientiert auf den Punkt gebracht. Einsatzgebiete sind die jährlich empfohlenen Mitarbeiterunterweisungen, Einweisung im Onboarding-Prozess und die vertiefte Weiterbildung einzelner Mitarbeitenden. Unternehmensspezifische Fragestellungen – auch komplexe – können eingebunden und vermittelt werden. So verfestigt sich das Wissen optimal und es können spezifische Risiken adressiert werden. Die E-Learning-Plattform wird von der integratio in der Schweiz betrieben.

integratio.com/de/elearning

Henriette Baumann ist unabhängige und zertifizierte Datenschutz-Expertin und Geschäftsleitungsmitglied der integratio GmbH, einem Beratungsunternehmen für Datenschutz und Informationssicherheit in Zürich. Nach einem Studium der Betriebswirtschaft sowie Informatik und anschliessend über zehn Jahren in verschiedenen Positionen in der Software-Entwicklung in Finanzdienstleistungsunternehmen, ist sie seit über 20 Jahren als unabhängige Beraterin für Banken und mittelständische Unternehmen tätig. Nach langjährigen Vorstandstätigkeiten in der Schweizer Informatik Gesellschaft und der Open Source Business Alliance widmet sie sich heute neben ihrer Beratungstätigkeit der Leitung des Schweizer Erfahrungsaustausch-Kreises der Gesellschaft für Datenschutz und Datensicherheit.

www.integratio.com