Versäumnisse können teuer werden

Die Datenschutz-Grundverordnung stellt HR vor neue Herausforderungen bei der Verarbeitung personenbezogener Daten. Wer sich nicht rechtzeitig mit der Anpassung seiner Prozesse und Systeme befasst, riskiert empfindliche Strafen.

▸ Mit der EU-Datenschutz-Grundverordnung (DSGVO) rollt die größte europaweit verabschiedete Gesetzesänderung im Bereich Datenschutz auf uns zu, die es seit 1995 gegeben hat. Die DSGVO regelt den Umgang mit personenbezogenen Daten umfassend. Betroffen sind insbesondere Systeme zur Verwaltung von Personaldaten wie SAP. Für die Praxis bedeuten die neuen Vorschriften Änderungen hinsichtlich Anonymisierung und Löschung von Daten in den Systemen. Hauptaugenmerk liegt hier auf inaktiven Personal- und Kundendaten, die unter bestimmten Bedingungen gelöscht beziehungsweise verfremdet werden müssen. Bei Nichtbeachtung der Richtlinie drohen Unternehmen Bußgelder von bis zu 20 Millionen Euro oder – sofern höher – vier Prozent des weltweiten Jahresumsatzes.

2018 wird es ernst

Die DSGVO ist am 24. Mai 2016 in Kraft getreten. Nach einer zweijährigen Übergangsphase löst sie am 25. Mai 2018 das aktuelle Bundesdatenschutzgesetz (BDSG) ab. Während dieser Übergangsphase gilt das BDSG weiter. Sobald die DSGVO am 25. Mai 2018 alleinig anzuwenden ist, sind alle Unternehmen verpflichtet, die neuen Vorschriften vollständig einzuhalten, auch für bereits bestehende Systeme, Prozesse und Verträge. Sich mit diesem kritischen Thema erst im Jahr 2018 zu befassen, erscheint viel zu spät.

Was bedeutet dies für die Daten Ihres Unternehmens und welchen Einfluss hat dies auf Ihr ERP-System? Durch die neue Verordnung entsteht unter anderem die Notwendigkeit, bestimmte Daten aus dem System

zu entfernen, so als ob sie nie da gewesen wären. Im Einzelnen heißt dies, dass Unternehmen branchenabhängige Datenbereiche auf Anfrage „per Knopfdruck" löschen müssen, sofern es keine triftigen Gründe gibt, diese zu halten. IT-Unternehmen und Kanzleien bieten schon heute Workshops an, sowohl die Datenbereiche als auch die Zeiträume der Pflichtlöschung zu definieren.

Datenminimierung

Grundsätzlich werden Unternehmen dazu angehalten, personenbezogene Daten zu minimieren und durch ein Sicherheitskonzept die Einsicht unbefugter Dritter zu vermeiden. In der Datenminimierung gilt es zunächst anhand der Anzahl an Datenfeldern beziehungsweise Datensätzen die Menge zu definieren. Danach werden der Umfang der Datenverarbeitung sowie die Speicherdauer entlang der gesetzlichen Aufbewahrungsfristen festgelegt. Diese hängen stark vom jeweiligen Verarbeitungszweck sowie vom Datenauswahlbereich ab. Abschließend wird anhand eines Berechtigungskonzepts der Datenzugriff dokumentiert und technisch umgesetzt. Jeder der aufgezählten Prozesse muss im Rahmen der Datenminimierung den Anforderungen der DSGVO genügen.

Datensicherheit

Bei der Datensicherheit wird zwischen Konzeption, Wirksamkeitstests und Beschaffung unterschieden: Im ersten Stadium muss ein Konzept möglicher Risikofaktoren erstellt werden. Durch Wirksamkeitstests ist in periodischen Abständen die Wirkungsweise der getroffenen technischen und organisatorischen Maßnahmen zu testen. Alle beschafften und verwendeten internen und externen Produkte und Leistungen müssen konform mit der DSGVO sein.

Meldepflichten

Alle aufbewahrten Daten werden schließlich Meldepflichten gegenüber der Datenschutzaufsichtsbehörde oder den betroffenen Personen unterliegen. So gilt es beispielsweise, eine zufällige oder unrechtmäßige Veränderung beziehungsweise einen Verlust von Daten zu melden. Meldepflichten gelten unter anderem für folgende Bereiche: Leistungserbringung, Einstellung, Fortbildung, Einsatzplanung, Marketing und Vertrieb. Die Empfänger sensibler Daten sind zu dokumentieren und mitzuteilen. Sofern Meldefristen nicht eingehalten werden, kann die Aufsichtsbehörde Informationen der Meldevorgänge gegen das Unternehmen verwenden.

> Bei Nichtbeachtung der Richtlinie drohen Bußgelder von bis zu 20 Millionen Euro.

Der Teufel steckt im Detail

Zusammenfassend gilt, dass die Bereiche der Datenerhebung, Nutzung und Löschung genau definiert und spezifiziert werden müssen. Dieser Vorgang muss bereits vor Inkrafttreten der DSGVO geschehen, um Strafen zu vermeiden. Die Beweislast zur Nutzung und Verarbeitung personenbezogener Daten liegt im Verantwortungsbereich der Unternehmen und nicht seitens der Behörde.

Aus IT-Sicht sollte es bis 2018 insbesondere bei SAP-ERP-Systemen möglich sein, ohne großen Aufwand bestimmte Datenbereiche entlang vorgegebener Kriterien aufzuspüren und gegebenenfalls zu anonymisieren. Schon heute gibt es produktseitige Ansätze, über eine einfache Nutzeroberfläche DSGVO-relevante Daten aufzuspüren und bei Bedarf zu anonymisieren. Der Teufel steckt auch hier im Detail. So sind beispielsweise Mitarbeiterdaten nicht nur im HR-Modul des ERP-Systems gespeichert, sondern auch übergreifend in Business-Warehouse-Applikationen, im CRM oder in externen Non-ERP-Lösungen.

Um das Risiko der kommenden Verordnung auch IT-seitig zu minimieren, bieten Beratungshäuser schon jetzt fertige Softwarelösungen zur Anonymisierung beziehungsweise Löschung inaktiver Personal- und Kundendaten an. ■

Die DSGVO

Nach mehr als vierjähriger Beratung hat das EU-Parlament im Mai 2016 die EU-Datenschutz-Grundverordnung (DSGVO; englisch: General Data Protection Regulation, GDPR) verabschiedet. Sie wird ab dem 25. Mai 2018 in allen EU-Mitgliedstaaten unmittelbar verbindlich sein, eine Umsetzung in nationales Recht ist nicht erforderlich. Die DSGVO vereinheitlicht EU-weit das Datenschutzrecht und regelt unter anderem die Verarbeitung von personenbezogenen Daten durch Unternehmen und öffentliche Stellen.

Für den Personalbereich macht die DSGVO eine Überprüfung seiner Prozesse und Systeme notwendig.
Sind sie nicht konform mit dem neuen Datenschutzrecht, müssen entsprechende Änderungen vorgenommen werden. Insbesondere Vertragsmuster sollten überprüft werden, etwa hinsichtlich der Einwilligungen zur Datenverarbeitung. Auch notwendige Anpassungen von Betriebsvereinbarungen kommen in Betracht.

Mehr zu den arbeitsrechtlichen Konsequenzen der DSGVO lesen Sie im Beitrag „DSGVO: Compliance ist wichtiger denn je" bei den Downloads zum Heft (www.pwgo.de/downloads).

AUTOR

Markus Schüßler, Inside Sales & Support Consultant (SAP HCM), EPI-USE Labs GmbH, Walldorf, markus.schuessler@labs.epiuse.com