KOMMENTAR

Von **Gabriele Ernst,** Allgeier ES

Lässt sich die Verantwortung für den Datenschutz auslagern?

Gabriele Ernst ist Senior Consultant für SAP Compliance Services mit dem Schwerpunkt „Datenschutz in SAP“ bei Allgeier ES.

Am Freitag, dem 25. Mai 2018, ist es so weit. Die EU-Datenschutz-Grundverordnung (EU-DSGVO) gilt. Artikel 24 regelt die „Verantwortung des für die Verarbeitung Verantwortlichen“.

Liegen personenbezogene Daten im eigenen Haus auf eigenen Servern, ist die Verantwortung klar. Der Verantwortliche, also die Organisation, die für ihre Unternehmenstätigkeit Daten von natürlichen Personen sammelt, speichert und verarbeitet, trägt die Verantwortung dafür, dass die Vorgaben der EU-DSGVO eingehalten werden. Sammelt eine Organisation Daten von natürlichen Personen, speichert und verarbeitet diese aber nicht selbst, konkretisiert der sogenannte Erwägungsgrund 074 den Artikel 24 wie folgt: „Die Verantwortung und Haftung des Verantwortlichen für jedwede Verarbeitung personenbezogener Daten, die durch ihn oder in seinem Namen erfolgt, sollte geregelt werden. Insbesondere sollte der Verantwortliche geeignete und wirksame Maßnahmen treffen müssen und nachweisen können, dass die Verarbeitungstätigkeiten im Einklang mit dieser Verordnung stehen und die Maßnahmen auch wirksam sind.“ Gemäß EU-DSGVO ist „Software as a Service“ möglich, „Verantwortung as a Service“ hingegen nicht. Der Verantwortliche kann einen Teil seiner Verantwortung an seinen Auftragsverarbeiter abgeben. In diesem Fall sollten Verantwortungsübergänge klar geregelt sein. Angesichts der empfindlich hohen Strafen, die ab 25.5.2018 auf Verantwortliche zukommen können, ist eine Überprüfung bestehender Verträge ratsam. Das betrifft neben Verträgen mit Auftragsverarbeitern auch jene mit Mitarbeitern, Banken, Kunden, Lieferanten etc. Liegt kein Rechtsgrund zur Verarbeitung personenbezogener Daten vor, ist diese verboten. Daten dürfen nur so lange im System verbleiben, wie es zur Erfüllung des Zwecks erforderlich ist. Der Verantwortliche muss die Zweckgebundenheit gegenüber der Aufsichtsbehörde belegen können.

Sind meine Daten in SAP sicher?

Angesichts des jüngsten Facebook-Datenskandals ist das Interesse der Nutzer groß, ob und bei wem ihre Daten sicher sind. Auf entsprechende Nachfragen sollten SAP-Kunden vorbereitet sein. Artikel 5 der EU-DSGVO fordert: „Personenbezogene Daten müssen [...] in einer Weise verarbeitet werden, die eine angemessene Sicherheit der Daten gewährleistet, einschließlich Schutz vor unbefugter oder unrechtmäßiger Verarbeitung und vor unbeabsichtigtem Verlust, unbeabsichtigter Zerstörung oder unbeabsichtigter Schädigung durch geeignete technische und organisatorische Maßnahmen (‚Integrität und Vertraulichkeit‘)“. Wichtige Bausteine dafür sind die Netzwerksicherheit, durchdachte Zugangskontrollen, eine hohe Systemzuverlässigkeit, die Absicherung von Schnittstellen und eine fundierte Verschlüsselung bei Datenübertragungen. Im Rahmen des Lizenz- und Wartungsvertrages stehen SAP-Kunden Bordmittel und regelmäßige Services zur Verfügung. Sie helfen, den Ist-Stand zu überwachen und die Qualität dauerhaft auf einem hohen Niveau zu halten. Dazu gehören zahlreiche Protokollmöglichkeiten, die Feinjustierung von Rollen und Berechtigungen, regelmäßige Security-Hinweise, der SAP Early Watch Report und der SAP Security Optimization Service. Auch SAP Read Access Logging kann ohne zusätzliche Lizenzkosten genutzt werden. Wichtig ist, sämtliche Maßnahmen zu dokumentieren und so nach und nach ein Datenschutz-Management-System aufzubauen. Darin werden alle Dokumente, Nachweise, Übersichten und Prozessbeschreibungen gesammelt und aktualisiert, die bei einer Überprüfung vorhanden sein müssen. Was das Datenschutz-Management-System beinhaltet, welches Budget und welche Ressourcen dafür bereitgestellt werden, entscheidet der Verantwortliche auf Basis seiner unternehmensinternen Risikoeinschätzung.

Werden meine Daten aus SAP gelöscht?

Artikel 17 regelt das „Recht auf Vergessenwerden“: „Eine betroffene Person hat das Recht, von dem Verantwortlichen zu verlangen, dass sie betreffende personenbezogene Daten unverzüglich gelöscht werden“, wenn z. B. die betroffene Person die Einwilligung zurückgezogen hat oder der Zweck, für den die Daten erhoben wurden, entfallen ist. Daten müssen nicht unverzüglich gelöscht werden, wenn gesetzliche oder sonstige glaubhaft nachvollziehbare Aufbewahrungsfristen gelten. Die Umsetzung kann toolunterstützt durchgeführt werden. So bildet etwa das SAP Information Lifecycle Management den Lebenszyklus von Daten ab. Es hilft Sperr- und Löschfristen mittels eines Regelkataloges einzuhalten und Daten automatisiert zu archivieren und zu löschen. In der Vergangenheit haben sich viele Unternehmen vor der Sperrung und Löschung gedrückt. Ab dem 25.5.2018 gilt: Der Verantwortliche kann Maßnahmen und die Überwachung zum Schutz von personenbezogenen Daten an einen IT-Partner auslagern, die Verantwortung dafür leider nicht.

www.allgeier-es.com