Kolumne Netzwerk Südbaden Ausgabe Januar 2018

DSGVO - die Uhr tickt: Diese Änderungen kommen auf Sie zu

Am 25. Mai 2018 kommt die EU-DSGVO (EU Datenschutz-Grundverordnung) zur Anwendung. Viele Unternehmen sind noch immer nicht ausreichend vorbereitet, obwohl empfindliche Strafen drohen.

Die Bezeichnung „Datenschutz“ ist eigentlich falsch und irreführend. Nicht die Daten sind vordergründig zu schützen, sondern vielmehr die Persönlichkeitsrechte und Privatsphäre der Menschen hinter den Daten. Jedem Einzelnen steht das Recht zu, über die Verwendung seiner Daten selbst zu bestimmen. Die bereits 1970 erstmalig im hessischen Datenschutzgesetz niedergeschrieben Rechte formulieren unter anderem die Vertraulichkeit, das Recht auf Korrektur der erhobenen Daten und garantiert Transparenz durch ein Auskunftsrecht. Diese Punkte bilden bis heute den Kern aller Nachfolgenden Verordnungen.

Die EU-DSVGO wurde im Sinne einer europäischen Harmonisierung auf den Weg gebracht und ist bereits seit dem 25. Mai 2016 in Kraft. Zur Anwendung in aller Konsequenz kommt sie nach zwei Jahren Schonzeit am 25. Mai 2018 – dann ersetzt europäisches Recht die bisherigen nationalen Regelungen, somit auch die deutsche Gesetzgebung zum Datenschutz. Dieser Termin sorgt nun, je nach Naturell, für Unsicherheit oder hektischem Aktionismus.

Inhaltlich orientiert sich die europäische Verordnung oft an den bisherigen deutschen Regelungen. Damit erscheint Vieles bereits vertraut. Waren die alten Regelungen zwar im internationalen Vergleich vergleichsweise streng, so waren die zu befürchteten Konsequenzen bei Verstößen zugleich jedoch relativ gering. Sanktionen wurden kaum verhängt, freiwillige Meldung führte regelmäßig zu einer Befreiung von Bußgeldern.

Viel beachtet ist daher die Höhe der zukünftig drohenden Bußgelder. Diese können sich auf bis zu 20 Millionen Euro belaufen, bei Konzernen bis zu 4% des letztjährigen Jahresumsatzes. Strafen werden nun ausdrücklich „wirksam und abschreckend“ sein.

Für Unternehmen stellt eine Nichtbeachtung oder lückenhafte Umsetzung also ein beträchtliches Risiko dar. Wenn noch nicht geschehen, so ist es allerhöchste Zeit, die aktuelle Situation im Unternehmen zu betrachten, notwendige Maßnahmen zu planen und zeitnah umzusetzen.

Das Führen von Verfahrensverzeichnissen - geeigneter Dreh- und Angelpunkt zum Management der datenschutzrechtlichen Konformität – wurde bisher vielerorts stiefmütterlich durchgeführt. Unternehmen sollten nun also spätestens ab Mai 2018 möglichst vollständig diejenigen Prozesse identifizieren, bei denen personenbezogene Daten (Kunden, Interessenten, Geschäftskontakte, Mitarbeiter, ...) eine Rolle spielen. Diese werden in einem aktuell zu haltenden Verarbeitungsverzeichnis zusammengeführt. Auf dieser Basis

kann nun, Prozess für Prozess, die Rechtmäßigkeit der Verarbeitung geprüft, gegebenenfalls nachgebessert und am Ende Datenschutzkonformität belegt werden. Zukünftig gilt eine Beweislastumkehr, es ist also im eigenen Interesse eben diese Nachweise jederzeit erbringen zu können. Zu dokumentieren sind jeweils mindestens der Zweck der Verarbeitung, rechtmäßige Herkunft und Kategorien der personenbezogenen Daten, einzuhaltende Löschfristen und Vorkehrungen zu deren Einhaltung sowie „technische und organisatorische Maßnahmen“ (TOMs) zur Datensicherheit.

Alle Prozesse sind darauf zu prüfen, ob die Betroffenenrechte umgesetzt werden können. Diese Rechte umfassen unter anderem das Recht auf Auskunft, Recht auf Löschung und zukünftig ein Recht auf „Vergessenwerden“.

Die Anforderungen an die Datensicherheit, die sich aus der EU-DSGVO ergeben, sind weitaus höher als zuvor. Auch hier gelten fortan eine Beweislastumkehr sowie eine erweiterte Haftung für Verantwortliche und Auftragsverarbeiter. Die konkret formulierten Anforderungen und Empfehlungen orientieren sich deutlich an bekannten Normen des Informationssicherheitsmanagements wie ISO/IEC 27001 oder dem vom Bundesamt für Sicherheit in der Informationstechnik formulierten BSI-Grundschutz (siehe z.B. „Standarddatenschutzmodell“). Entsprechend zertifizierte Unternehmen oder Auftragsverarbeiter tun sich daher in der Umsetzung der Anforderungen und dem Erbringen entsprechender Nachweise deutlich leichter.

Sollte es zum Beispiel, durch Schwächen der Datensicherheit zu einer Datenpanne gekommen sein, so bestehen ab dem 25. Mai 2018 eine Meldepflicht bei den Aufsichtsbehörden und eine Informationspflicht gegenüber den Betroffenen. Die zuvor gültige Einschränkung auf „sensible Daten“ und „zu erwartende schwere Beeinträchtigungen“ wird gestrichen. Alle Datenpannen sind meldepflichtig - es sei denn, ein Schaden kann ausgeschlossen werden. Dies kann der Fall sein, wenn zugänglich gewordene Daten nach dem Stand der Technik wirksam verschlüsselt waren. Meldepflichtige Ereignisse sind z.B. gehackte Server, Verlust oder Diebstahl von mobilen Datenträgern (auch Notebooks / Smartphones, wenn entsprechende Daten darauf unverschlüsselt gespeichert waren), Fehlentsorgung, Fehlversand.

Wird die Verarbeitung personenbezogener Daten ganz oder teilweise aus der Hand gegeben, z.B. in Form des Betriebs entsprechender Systeme in einem externen Rechenzentrum oder in der Cloud, so bleibt die datenschutzrechtliche Verantwortlichkeit beim Auftraggeber. Er hat sicherzustellen, dass der Auftragnehmer (Hoster, Cloudanbieter) sorgfältig ausgewählt wird. Der Auftragnehmer („Auftragsverarbeiter“) hat die Pflicht, für seinen Verantwortungsbereich angemessene TOMs zum Schutz der personenbezogenen Daten vereinbarungsgemäß umzusetzen. Der Auftraggeber seinerseits ist in der Pflicht, sich davon zu überzeugen und dies belegen zu können. Dies erfolgt durch einen Auftragsdatenverarbeitungsvertrag (ADV), in dem u.a. die relevanten TOMs beschrieben sind. Zusätzlich können Zertifikate eingefordert oder eigene Auditierungen durch den Auftraggeber durchgeführt werden.

Schon seit der Unternehmensgründung beschäftigt sich die Continum AG aus Freiburg mit den Themen Informationssicherheit und Datenschutz. Als Teil der Freicon-Gruppe ist Continum der Spezialist für hochwertiges Enterprise- und Anwendungs-Hosting und arbeitet nach höchsten Sicherheitsanforderungen. In modernsten Rechenzentren, welche ausschließlich in Deutschland positioniert sind, erbringt das Unternehmen als Auftragsdatenverarbeiter „Managed Services“ nach der EU-DSGVO und ist nach ISO/IEC 27001 sowie nach PCI-DSS (Payment Card Industry Data Security Standard) zertifiziert.

Autor: Thilo Rees, Informationssicherheitsbeauftragter

Ansprechpartner: Julian Sayer, Vorstand der Continum AG.

Kontaktieren Sie uns unter:

Continum AG
Bismarckallee 7b-d
79098 Freiburg
Tel: +49 761 217111-0
info@continum.net