Das Standard-Datenschutzmodell in der Praxis

EU-DS-GVO umsetzen

Viele Unternehmen stehen auch fast ein Jahr nach Inkrafttreten der EU-DS-GVO noch vor der Frage, wie sich die dort formulierten Datenschutzgrundsätze in der Praxis verwirklichen lassen. Oft ist unklar, wie die erforderlichen Werkzeuge und Mechanismen zur Umsetzung praktisch bereitzustellen sind und wie gegenüber Aufsichtsbehörden und berechtigten Interessenten der Nachweis einer Umsetzung erfolgen könnte. Bei der Auseinandersetzung mit dem Gesetzestext prallen die unterschiedlichen Denkweisen von Juristen einerseits und IT-Experten sowie Informationssicherheitsbeauftragten andererseits aufeinander. Um diesen Konflikt aufzulösen, ist eine Übersetzung der komplexen Anforderungen des Gesetzes in ein standardisiertes Vorgehensmodell und in praktische Maßnahmen erforderlich.

Mit dem Inkrafttreten der europäischen Datenschutz-Grundverordnung (EU-DS-GVO) am 24. Mai 2016 wurde auch eine zweijährige Übergangsfrist festgelegt, die am 25. Mai 2018 endete. Wie alle Grundverordnungen wurde auch die EU-DS-GVO direkt gültig, bedurfte also keiner Umsetzung durch die nationale Gesetzgebung. Sie bietet jedoch zahlreiche Öffnungsklauseln, über die einzelne Staaten ihre nationalen Anforderungen in die Rechtsnorm einbringen können. In Deutschland geschieht dies durch das „Gesetz zur Anpassung des Datenschutzrechts an die Verordnung (EU) 2016/679 und zur Umsetzung der Richtlinie (EU) 2016/680" (BDSG-neu), das am 5. Juli 2017 im Bundesgesetzblatt veröffentlicht wurde und zum Ende der Übergangsfrist der EU-DS-GVO in Kraft trat. Ungeachtet dieser langen Vorlaufzeiten zeigten sich viele Betroffene im Frühjahr 2018 von der Änderung der Gesetzeslage überrascht. Zu diesem Zeitpunkt hatten Umfragen unter 600 Marketing-Entscheidern zufolge erst zehn Prozent der Befragten ihre Datenschutzregeln angepasst, etwa die Hälfte wenigstens Projekte zur Umsetzung begonnen und gut ein Drittel keinerlei Aktivitäten in dieser Richtung unternommen.

Ein Grund für diese Situation liegt in der Komplexität der EU-DS-GVO, die sie für Nicht-Juristen schwer zugänglich macht und auch Fachleute verwirrt. Dabei formuliert die EU-DS-GVO im Kern einfache und vernünftige Regeln für den Umgang mit personenbezogenen Daten. Diese sind zumindest für Deutschland überwiegend auch nicht neu – viele der Inhalte waren im alten Bundesdatenschutzgesetz (BDSG) bereits enthalten. Die Grundsätze der EU-DS-GVO lassen sich folgendermaßen zusammenfassen:

- Die Verarbeitung der Daten muss rechtmäßig sein, nach gutem Treu und Glauben geschehen und in allen Teilen transparent sein.
- Die Verarbeitung ist nur für festgelegte, eindeutige und legitime Zwecke zulässig. (Zweckbindung)

- Der Umfang der erhobenen Daten muss dem Zweck angemessen sowie auf das notwendige Maß beschränkt sein (Datenminimierung).
- Die erhobenen Daten müssen korrekt sein, und es sind alle angemessenen Maßnahmen zu treffen, damit unrichtige personenbezogene Daten unverzüglich gelöscht oder berichtigt werden können.
- Daten müssen „in einer Form gespeichert werden, die die Identifizierung der betroffenen Personen nur so lange ermöglicht, wie es […] erforderlich ist" (Speicherbegrenzung).
- Daten müssen dem Dateneigentümer auf Wunsch in einem gängigen lesbaren Format unentgeltlich übergeben werden (Recht auf Datenübertragbarkeit).
- Die angemessene Sicherheit der personenbezogenen Daten, einschließlich dem Schutz vor unbefugter oder unrechtmäßiger Verarbeitung und vor unbeabsichtigtem Verlust, unbeabsichtigter Zerstörung oder unbeabsichtigter Schädigung muss gegeben sein (Integrität, Vertraulichkeit und Verfügbarkeit).

Viele Unternehmen stehen dennoch weiterhin vor der Frage, wie sich diese Grundsätze in der Praxis verwirklichen lassen. Das Standard-Datenschutzmodell (SDM) setzt genau hier an: Das SDM ist ein Vorgehensmodell, um die EU-DS-GVO in technische und organisatorische Maßnahmen zu überführen und erfüllt damit die Forderung nach einer Übersetzung der EU-DS-GVO in die Denkweise der Informationsverarbeitung. Es ist unter der Hoheit der Konferenz der unabhängigen Datenschutzbehörden des Bundes und der Länder entstanden. Die Version 1.1 wurde Ende April 2018 einstimmig beschlossen. Das SDM definiert dazu als zentrales Element sieben Gewährleistungsziele und stellt diesen die betroffenen Paragrafen der EU-DS-GVO gegenüber. Zur Erreichung der Gewährleistungsziele bietet das SDM einen Katalog von Bausteinen an, die im Detail festlegen, wie die jeweiligen Anforderungen umzusetzen sind. Die Bausteine erfinden dabei das Rad nicht neu – vielmehr stützen sie sich intensiv auf den IT-Grundschutz des Bundesamtes für Sicherheit in der Informationstechnik (BSI) und betten die Maßnahmen und Umsetzungshinweise des IT-Grundschutzes in den Kontext des Datenschutzes ein.

Was genau will das SDM nun unter dem Begriff der Gewährleistungsziele verstanden wissen und wie stellen sich die Verfasser

das Vorgehen bei der Datenschutzkonzeption vor? Der Begriff der Gewährleistungsziele ist seit Ende der 1980er Jahre in der Informationssicherheit üblich. Die drei Ziele

- Verfügbarkeit,
- Integrität und
- Vertraulichkeit

von Informationen sind die zentralen Größen, wenn es um Informationssicherheit geht und bilden auch die ersten drei Gewährleistungsziele der Datensicherheit im SDM. Hinzu kommen diejenigen Ziele, die auf den Schutz Betroffener ausgerichtet sind, nämlich die Nichtverkettung, die Transparenz und die Intervenierbarkeit.

- ***Nichtverkettung*** bedeutet die Anforderung, dass personenbezogene Daten nicht zusammengeführt (verkettet) werden dürfen.

- ***Transparenz*** bedeutet die Anforderung, dass sowohl Betroffene als auch die Betreiber von Systemen erkennen können, welche Daten für welchen Zweck erhoben und verarbeitet werden. Dazu gehört auch die Klarheit darüber, welche Systeme und Prozesse genutzt werden, welche Datenflüsse stattfinden und wer die rechtliche Verantwortung trägt.

- ***Intervenierbarkeit*** bedeutet die Anforderung, dass den Betroffenen die ihnen zustehenden Rechte jederzeit wirksam gewährt werden und die verarbeitende Stelle die dazu erforderlichen Maßnahmen umsetzt.

- ***Datenminimierung*** bedeutet die Anforderung, nicht mehr personenbezogene Daten zu erheben, zu verarbeiten und zu nutzen, als für das Erreichen des Verarbeitungszwecks benötigt werden.

Diesen Gewährleistungszielen ordnet das SDM die entsprechenden Artikel und Erwägungsgründe zu. Zur Anwendung des SDM ist es im Vorfeld erforderlich, zunächst den jeweiligen Betrachtungsgegenstand zu klären, also den Kontext, in dem personenbezogene Daten verarbeitet werden. Hier sind die Verantwortlichen und Betroffenen genauso zu identifizieren wie die tangierten Geschäftsprozesse und Verarbeitungsprozesse sowie der stattfindende Datenfluss. Sind diese Punkte bekannt, ist unter anderem zu bewerten, welche Rechtsgrundlagen für die Verarbeitung gegeben sind und welche Anforderungen und Interessen seitens der Beteiligten erfüllt werden müssen. Dies mündet in eine erste Bewertung bestehender Gefährdungen von Betroffenenrechten (also eine Risikoanalyse).

Sind diese Schritte getan, geht es daran, zu bestimmen, in welcher Ausprägung die Gewährleistungsziele erreicht werden können. Hier fließen die gesetzlich zwingenden Anforderungen genauso ein wie qualitative und quantitative Parameter und eine Bestimmung des Schutzbedarfs der Informationen, Systeme und Anwendungen. Das richtige Werkzeug hierfür stellt der IT-Grundschutz im BSI Standard 200-2 bereit. Welche organisatorischen und technischen Maßnahmen vor diesem Hintergrund zu treffen sind, beschreiben die Bausteine, die dem SDM beigestellt sind und unabhängig von diesem gepflegt werden. Für die sieben Gewährleistungsziele sind zurzeit 17 Bausteine geplant, davon liegen bereits sieben Bausteine in einer von der Konferenz der unabhängigen Datenschutzaufsichtsbehörden des Bundes und der Länder noch nicht abgestimmten Fassung vor (Stand 01/2019). Sie stellen jeweils den Bezug zu den Gewährleistungszielen her, benennen erforderliche Maßnahmen auf Ebene der Daten, der IT-Systeme und der Verarbeitungsprozesse und referenzieren die Maßnahmen und Umsetzungsempfehlungen des IT-Grundschutzes. Darin liegt auch der besondere Wert dieses Vorgehens. Es entsteht eine Brücke zwischen der juristisch geprägten Denkweise der EU-DS-GVO sowie dem technisch und organisatorisch ausgerichteten Betrachtungswinkel des Informationssicherheitsmanagements und der Informationstechnik.

Eine Schwäche des Ansatzes darf an dieser Stelle nicht verschwiegen werden – es stehen eben nur sieben der geplanten Bausteine zum SDM bereit. Erst mit einem vollständigen Baustein- und Maßnahmenkatalog ist aber eine detaillierte Abwicklung des Vorgehensmodells lückenlos möglich. Bis dahin bleibt dem „Early Adopter" nichts anderes übrig, als durch Auseinandersetzung mit dem IT-Grundschutz bestehende Lücken individuell zu füllen und darauf zu hoffen, dass die fehlenden Bausteine bald vorgelegt werden.

Trotz dieser Schwächen lohnt sich die Beschäftigung mit dem SDM und bietet in der Praxis eine gute Möglichkeit, die Forderungen der EU-DS-GVO systematisch in der Informationstechnik umzusetzen. ■

GEORG BASSE,
Senior Consultant IT-Security, Controlware GmbH