Schreckgespenst EU Datenschutzgrundverordnung (DS-GVO)?

Unsere personenbezogenen Daten gehören zu den wertvollsten Dingen, die wir besitzen. Deshalb erklärt die DS-GVO den Schutz dieser personenbezogenen Daten zu den Grundrechten der betroffenen Personen. Es stellt sich die Frage, ob mit diesen Daten demnach nicht genauso sorgfältig umzugehen ist, wie beispielsweise mit streng vertraulichen Daten zu einem Hightech Produkt vor der Markteinführung?

Datensicherheit umfasst nicht nur personenbezogene Daten sondern den gesamten Datenbestand einer Organisation und somit auch deren Know-how Schutz.
Hohe Datensicherheitsstandards können Image- und auch Standortvorteile bringen. Weil z.B. in Deutschland bislang sehr hohe Datensicherheitsstandards gelten, wählen viele Unternehmen ganz bewusst Deutschland als Sitz von Rechenzentren aus.

Datensicherheit ist also ein wichtiges Thema, dass viele Bereiche von Unternehmen und Organisationen betrifft. Aber gehen Unternehmen und Organisationen in der Realität mit „ihren“ Daten immer dementsprechend sorgfältig um?

Einerseits ja. Für Geheimhaltungsvorkehrungen spendieren Unternehmen und Organisationen in der Regel erhebliche Aufwendungen. Welche Informationen werden wann wem zur Verfügung gestellt? Und wie werden die streng vertraulichen Daten sicher vor dem Wettbewerber aufbewahrt? Weniger ist hierbei mehr.

Andererseits nein. Beim Umgang mit personenbezogenen Daten von Mitarbeitern, Kunden und Lieferanten steht oftmals die „Sammellust“ im Vordergrund. Daten werden erfasst und gespeichert, weil sie vielleicht irgendwann zu irgendeinem Zweck einmal gebraucht werden könnten. Die gesetzeskonforme Löschung dieser Daten wird vergessen usw.

Zwei unterschiedliche Vorgehensweisen für ähnlich sensible Daten!

Erschwerend kommt hinzu, dass sich Daten im modernen Zeitalter der elektronischen Medien wesentlich einfacher verbreiten lassen als noch zu Zeiten des Papiers. Die Herausforderung ist es, hierbei den Überblick zu behalten, welche personenbezogenen Daten existieren, wodurch diese Daten erzeugt werden, wie oft diese Daten an verschiedenen Stellen abgelegt sind, wer Zugriff auf die Daten hat, haben muss und eben nicht haben darf und wann und durch welche Prozesse diese Daten wieder gesetzeskonform und rückstandsfrei gelöscht werden. Ein plastisches Beispiel: Ein erheblicher Anteil an Daten, auch personenbezogene Daten, „schlummert“ heute in persönlichen E-Mail-Konten und verschiedenen Datensilos.

Um dieser Herausforderung nachhaltig zu begegnen, bedarf es zunächst einer strukturierten Datenablage mit klar definierten Zugriffsrechten. Hierbei unterstützen die Vorgehensweisen des Informationsmanagements. Informationsmanagement schafft Struktur und Überblick im Datenbestand und beinhaltet die ganzheitliche Erschließung aller Informationen in Unternehmen und Organisationen. Informationsmanagement hat das Ziel, dass die richtigen Informationen die richtige Person im richtigen Format zur richtigen Zeit erreicht.
Dabei werden sowohl die gesetzlich vorgeschriebenen Aufbewahrungsfristen nach Handelsgesetzbuch (HGB) und Abgabenordnung (AO) usw. als auch die Löschfristen nach den Vorgaben des Bundesdatenschutzgesetzes (BDSG) usw. berücksichtigt. Mit einem guten Überblick über die vorhandenen Daten und Informationen schafft das Informationsmanagement somit eine gute Grundlage für einen wirkungsvollen Schutz personenbezogener Daten.

Einen weiteren wichtigen Baustein zum zuverlässigen Schutz personenbezogener Daten liefern die neuen Regelungen der DS-GVO.

Die DS-GVO gilt ab dem 25.05.2018. Seit dem 12.05.2017 ist auch das Datenschutz-Anpassungs- und Umsetzungsgesetz (DSAnpUG-EU) mit dem BDSG-neu beschlossen. Dieses Gesetz ergänzt die DS-GVO und wird das bisherige BDSG ersetzen. Es ist unter den Datenschützern allerdings nicht unumstritten und Forderungen nach weiteren Anpassungen und Korrekturen stehen im Raum.

Worin besteht der Handlungsbedarf für Unternehmen und Organisationen?

- Zunächst erfordern die Vorgaben der DS-GVO zusätzliche Aufwendungen und verstärkte Konsequenz, die in der Vergangenheit oft achtlos oder auch mit Bedacht gesammelten und ausgewerteten Daten jetzt genauer zu betrachten und die Rechtmäßigkeit des Tuns zu hinterfragen.
- Bei den Vorgaben für die konkrete Umsetzung der DS-GVO bestehen nach wie vor Lücken, deshalb ist der Handlungsbedarf hier noch nicht eindeutig zu benennen. Zumindest sind die ersten Fragenkataloge und Checklisten der Aufsichtsbehörden inzwischen veröffentlicht, z.B. „Fragebogen zur Umsetzung der DS-GVO zum 25.05.2018“ vom Bayerischen Landesamt für Datenschutzaufsicht (BayLDA).
- Sicher ist, dass es mit der DS-GVO zu einer Umkehr der Beweislast und einer Rechenschaftspflicht durch die Unternehmen und Organisationen kommt. Das heißt, die Unternehmen und Organisationen müssen nachweisen, dass sie alle erforderlichen Maßnahmen zum Schutz der personenbezogenen Daten ergriffen haben. Um diesen Nachweis bringen zu können, werden die Dokumentationspflichten von der DS-GVO verstärkt eingefordert.
- Die Rechte der betroffenen Personen werden wesentlich gestärkt. Alle betroffenen Personen haben nach der DS-GVO klar geregelte Ansprüche z.B. auf Auskunft, Berichtigung, Löschung und Widerspruch der Verarbeitung. Diesen Ansprüchen müssen die Unternehmen und Organisationen gerecht werden. So sind der betroffenen Person Informationen über Grund der Datenerhebung, Art, Verwendungszweck, Rechte Dritter und Aufbewahrungsdauer der Daten in einer ihm verständlichen Ausdrucksweise und Sprachwahl aktiv zur Verfügung zu stellen.
- Wesentlich verschärft hat sich auch die Meldepflicht an die Aufsichtsbehörden bei Datenpannen und die Höhe der zu entrichtenden Bußgelder. Damit kommt der Datensicherheit und dem Risikomanagement ein wesentlicher Aspekt zu.
- Wichtige Bestandteile zur Erfüllung der DS-GVO werden sein:
  - das Verzeichnis der Verarbeitungstätigkeiten (Art. 30 DS-GVO).
  - die Datenschutz-Folgeabschätzungen (Art. 35 DS-GVO)
  - die Übersicht über Auftragsverarbeiter (Art.28 DS-GVO)
  - die Erfüllung der Informationspflichten (Art.12 ff DS-GVO)
  - die technisch und organisatorischen Maßnahmen zur Einhaltung der Datensicherheit (Art. 32 DS-GVO)

Welche bereits vorhandenen Dokumentationen und Verfahren können als Grundlage dienen?

Das BDSG ist eines der strengsten Datenschutzgesetze in Europa. Auch nach diesem Gesetz ist es bereits notwendig die Rechtmäßigkeit der Verarbeitung nachzuweisen und öffentliche und interne Verfahrensverzeichnisse zu führen. Das interne Verfahrensverzeichnis beinhaltet neben einer Verfahrensbeschreibung, den Zweck und die Rechtsgrundlage der Datenverarbeitung, die Art der zu verarbeitenden Daten, die Datenübermittlung, die Löschfristen, Berechtigungskonzepte und die konkreten Verfahren der getroffenen technisch organisatorischen Maßnahmen (TOM) zur Sicherstellung der Datensicherheit. Mit Auftragsdatenverarbeitern müssen Verträge abgeschlossen werden, die den Umgang mit den personenbezogenen Daten und die einzuhaltenden Maßnahmen zur Datensicherheit regeln. Datenschutzvereinbarungen auf Websites und Mitarbeiterschulungen sind ebenfalls verpflichtend.

Die DS-GVO ist folglich keine Revolution der Datenschutzgesetze und auch kein „Schreckgespenst“ sondern beinhaltet viele Aspekte des BDSG in einheitlicher durchgängiger Form und EU-weiter Verbindlichkeit. Somit kann auf die bisher vorhandenen Dokumente, Verträge und Vorgaben aufgebaut werden.

Um der verstärkten Dokumentationspflicht der DS-GVO nachzukommen, können auch andere im Unternehmen oder der Organisation vorhandene Analysen und Dokumentationen herangezogen werden, z.B.

- Analysen, die bei der Einführung von Software z.B. eines Informationsmanagementsystems durchgeführt wurden.
  Diese Analysen liefern eine Übersicht über die vorhandenen Prozesse, Speicherorte, Zugriffsrechte, Lösch- bzw. Aufbewahrungsfristen, verwendete Softwarelösungen usw. Eventuell wurden auch bereits Informations- oder Archivierungslandkarten angelegt. Diese können Angaben wie Berechtigungen, Lebenszyklus, Rechtsgrundlage der Aufbewahrung, Aufbewahrungsfrist, Vernichtungsfrist usw. über Informationen liefern.
- Verfahrensdokumentationen, die aufgrund der elektronischen Verarbeitung buchhalterischer Daten nach GoBD erstellt werden müssen.
  Die GoBD verpflichtet Unternehmen und Organisationen diese Daten bis zum Ende der Aufbewahrungsfristen revisionssicher elektronisch zu archivieren und in einer Verfahrensdokumentation zu dokumentieren. Es treten Begriffe wie Zugangs- und Zugriffsberechtigungskonzepte, Funktionstrennungen, Erfassungs-, Eingabe und Verarbeitungskontrollen, Schutzmaßnahmen gegen beabsichtigte und unbeabsichtigte Verfälschung von Programmen, Daten und Dokumenten usw. auf.

Aus den oben genannten Punkten ist erkennbar, dass es Anforderungen aus verschiedenen Quellen gibt, die gleiche Bestandteile enthalten. Aus diesem Umstand können Synergien erzeugt werden, d.h. geleistete Aufwendungen können wiederverwendet werden. So sind z.B. sowohl für die Erfüllung der GoBD als auch im Datenschutz Verfahrensbeschreibungen, Berechtigungskonzepte wie auch die Angabe von technisch organisatorischen Maßnahmen und sonstigen Datensicherheitsmaßnahmen notwendig. Begriffe wie Vertraulichkeit, Verfügbarkeit, Authentizität und Integrität der Daten sind sowohl im Informationsmanagement und in Verfahrensdokumentationen als auch im Datenschutz fester Bestandteil.

Mit der verbindlichen Einführung der DS-GVO am 25.05.2018 sollten die Dokumentationen, Verfahren und Prozesse auf die Konformität mit den Vorgaben der DS-GVO geprüft und entsprechend ergänzt bzw. geändert sein. Aus meiner Sicht empfehle ich folgende Dinge:

- In einem ersten Schritt den bisherigen Dokumentationsbestand zu recherchieren, mit dem Ziel, bereits vorhandene Dokumentationen für eine „Datenschutzverfahrensdokumentation“ als Grundlage zu verwenden.
- Verwendung eines Hauptdokuments für die einzelnen Verfahrensdokumentationen. Dieses Dokument dient der Navigation durch die einzelnen oft variableren Dokumente und enthält feststehende Informationen. Die einzelnen Dokumente sollten möglichst modulhaft aufgebaut werden, so dass es möglich wird, in den verschiedenen Verfahrensdokumentationen auf das gleiche Dokument zu verweisen. Dies erleichtert dann auch den späteren Anpassungsaufwand.
- Werden neue Softwaresysteme eingeführt, sollten die entsprechenden Prüfungen und Dokumentationen bereits im Vorfeld systematisch angegangen werden.

Fazit:

- Neben der Erfüllung gesetzlicher Vorschriften und dem Vermeiden hoher Bußgelder bringt die DS-GVO einer Organisation Vorteile, z.B. Datentransparenz, eindeutige Zugriffsberechtigungen. Die DS-GVO ist für alle 28 Mitgliedsstaaten der EU verbindlich und somit auch stringenter durchsetzbar.
- Mit immer komplexer werdenden Systemen und der Nutzung von Internet of Things fällt es immer schwerer den Überblick über die gesamte Datenverarbeitungs-Landschaft und die Datenwege zu behalten. Dabei ist eine vollständige, aktuelle und übersichtliche Dokumentation nicht nur wegen des Datenschutzes notwendig. Auch wird damit der gesamte Lebenszyklus von Daten aufgezeigt. Hier gilt es Synergieeffekte zu nutzen.
- Datensicherheit ist nicht nur ein Thema des Datenschutzes personenbezogener Daten sondern sichert auch Know-how und erfüllt weitere rechtliche Vorgaben.
- Der Datenschutz ist aus meiner Sicht ein weiterer Baustein in der Datenverarbeitungs-Landschaft, der seine Betrachtungsweise auf die personenbezogenen Daten richtet. Wer bislang die Vorgaben des BDSG erfüllt, Informationsmanagement nutzt und/oder mit einer Verfahrensdokumentation dokumentiert, kann dies als Grundlage für die Erfüllung der Vorgaben der DS-GVO nutzen.
- Es empfiehlt sich die Themen Informationsmanagement, Verfahrensdokumentation und Datenschutz nicht getrennt voneinander zu betrachten und Synergien zu nutzen.
- Die DS-GVO ist nichts komplett Neues. Die Begriffe haben sich etwas geändert, aber in der Sache sind viele Aspekte des heute für Deutschland gültigen BDSG enthalten.
- Wichtig ist es, dass die Erfüllung der Vorgaben der DS-GVO kein einmaliges Vorgehen ist, sondern dass die Dokumente sowie Verfahren und Prozesse ständig geprüft, aktuell gehalten und auch auf den technischen Stand angepasst werden müssen.

Dipl. Ing. Inf. (FH) Ute Lafrenz
geprüfte Datenschutzbeauftragte (ifdas)
Project Consult Unternehmensberatung GmbH
Bietigheim-Bissingen
Ute.Lafrenz@PROJECT-CONSULT.com