„CARTA-Verständnis“ [8] folgendermaßen zusammenfassen: „Die Strategie des Verteidigungsansatzes muss der kontinuierlichen Risikoanpassung und der kontinuierlichen Prüfung darauf, ob dem System noch vertraut werden kann, folgen.“ In komplexen Systemen funktioniert das nur über Machine-Learning-Ansätze, bei denen standardisiert und permanent auf Abweichungen überwacht wird. „CARTA“ steht für „Continuous Adaptive Risk and Trust Assessment“. *Abbildung 4* fasst diese Gesamtsicht nochmals abschließend zusammen.

Weitere Informationen

[1] IDC Perspective – „Ten Myths regarding GDPR: Sifting Fact from Fiction“, Kuan Hon, Duncan Brown, June 2017, IDC #EMEA42628217

[2] Artikel 25 „Datenschutz durch Technikgestaltung und durch datenschutzfreundliche Voreinstellungen“.

[3] Artikel 30 „Verzeichnis von Verarbeitungstätigkeiten“, Artikel 35 „Datenschutz-Folgenabschätzung“

[4] Artikel 16 „Recht auf Berichtigung“, Artikel 17 „Recht auf Löschung“, Artikel 18 „Recht auf Einschränkung der Verarbeitung“, Artikel 19 „Mitteilungspflicht im Zusammenhang mit der Berichtigung oder Löschung personenbezogener Daten oder der Einschränkung der Verarbeitung“

[5] Zum Beispiel „Health Insurance Portability and Accountability Act“ (HIPAA) oder „Sarbanes-Oxley Act“ (SOX)

[6] „Security Information and Event Management“ (SIEM)

[7] „User and Entity Behavior Analytics“ (UEBA)

[8] Gartner – „Use a CARTA Strategic Approach to embrace Digital Business Opportunities in an Era of Advanced Threats“, Neil MacDonald, Felix Gaehtgens, May 2017, ID #G00332400

Ernst Lorenz
ernst.lorenz@oracle.com

In sieben Schritten zu EU-DSGVO-Verfahrenshandbuch & Co.

Mag. Wolfgang Klinger und DI (FH) Ernst Stippl, Sphinx IT Consulting GmbH

Es gibt viele Gründe, sich nicht mit langweiliger Dokumentation zu beschäftigen. Doch die DSGVO ist in diesem Punkt ganz klar: Personenbezogene Daten und deren Verarbeitungen müssen dokumentiert sein. Dieser Leitfaden hilft in sieben Schritten, die DSGVO-relevanten Dokumente rechtzeitig fertigzustellen, um auch nach dem 25. Mai 2018 ruhig schlafen zu können.

Wie verspeist man einen Elefanten? – In kleinen Häppchen!

Die DSGVO ist ziemlich umfangreich und besser in strukturierten Teilen zu genießen; das ist bekömmlicher und kann auch sehr zum Vorteil des Unternehmens sein: Das große Aufräumen im Sinne der DSGVO bringt Übersicht, Transparenz, spart Ressourcen und schafft Platz für Neues. Ist es wirklich sinnvoll, Marketing-Aussendungen an möglichst viele Adressaten zu schicken? Ist eine kleinere, wirklich interessierte Zielgruppe nicht ohnehin die bessere Alternative? Sind die Heerscharen von Office-Dokumenten, die auf diversen Servern gestrandet sind, nicht sowieso besser in einem Dashboard mit genau geregelten Zugriffsrechten aufgehoben? Die DSGVO kann Anlass dafür sein, sich mit Projekten zu befassen, die bisher immer auf die lange Bank geschoben wurden.

Es gibt teilweise Unschärfen in der DSGVO. Wie diese letztendlich zu interpretieren sind, wird sich – wie bei jedem juristischen Text – erst in zukünftigen Gerichtsurteilen herausstellen. Es gibt aber auch Abschnitte mit klaren Vorgaben, etwa bezüglich der zu erstellenden Dokumente, allen voran das „Verzeichnis von Verarbeitungstätigkeiten". Diese Dokumente sind im Bedarfsfall vorzuweisen, also dann, wenn die Behörde eine entsprechende Anfrage stellt. Es ist jedenfalls besser, vorbereitet zu sein, um einen guten Start in der Zusammenarbeit mit der Behörde hinlegen zu können. Der Artikel stellt eine Möglichkeit vor, sich der Erstellung dieser Dokumente anzunähern.

Schritt 1: Betroffene Daten erheben

Zunächst muss klar sein, welche Daten im Unternehmen überhaupt gespeichert sind. „Personenbezogen" ist dabei sehr umfassend zu sehen – es inkludiert auch IP-Adressen, Cookies, Fotos und Kundennummern. Alles, was eine Person eindeutig identifizierbar macht, fällt darunter. Dabei sind auch harmlos erscheinende Daten zu berücksichtigen, die in Kombination miteinander plötzlich wieder zur eindeutigen Identifizierbarkeit führen können.

Zu klären ist: Welche Daten werden von Mitarbeitern, Kunden, Lieferanten oder Geschäftspartnern gespeichert? Sind auch besonders sensible Daten dabei, wie etwa Gesundheitsdaten oder Religionsbekenntnis?

Das Vorgehen: Es ist nicht ganz einfach und klingt aufwendig, kann aber durch automatisiertes Durchsuchen von Datenbeständen und geführtes Einbeziehen wissender Mitarbeiter gut unterstützt werden. Personenbezogene Daten werden von Applikationen verwaltet oder sind als identifizierbare Datenbestände (Dateien) auffindbar.

Ergebnis: die Liste der Daten, die im Unternehmen von der DSGVO betroffen sind.

Schritt 2: Verarbeitungen beschreiben

Welche Verarbeitungen werden mit den in Schritt 1 identifizierten Daten durchgeführt? Gibt es Daten, die nicht mehr verwendet werden? Dann ist es am besten, diese zu löschen. Der Grundsatz der Datenminimierung zieht sich wie ein roter Faden durch die DSGVO. Das heißt, es soll sowohl der Zugriff auf Daten als auch deren Speicherung nur im wirklich notwendigen Ausmaß erfolgen – es muss also immer einen Grund dafür geben. Zu klären ist:

- Wer ist für welche Daten verantwortlich?
- Für welchen Zweck werden welche Daten gespeichert?
- Was genau passiert mit welchen Daten (Art der Verarbeitung)?
- Wie lange werden welche Daten gespeichert und warum?
- Wer hat Zugriff auf die Daten und an wen werden sie weitergegeben?

Das Vorgehen: Jetzt beginnt die Hauptarbeit! Eine gute Vorlage für das Verfahrenshandbuch gibt es beispielsweise bei der WKO *(siehe „www.wko.at/service/wirtschaftsrecht-gewerberecht/eu-dsgvo-muster-verarbeitungsverzeichnis-verantwortliche.html")*. Die Autoren empfehlen, hier ein paar Euro in eine Software-Lösung zu investieren. Man wird damit durch die Fragen gut geführt und mehrere Leute können gleichzeitig daran arbeiten. Man kann auch einen DSGVO-Kundigen von extern hinzuziehen, der aktiv mitarbeitet oder den Fortschritt verfolgt und Tipps gibt. Auch spätere Anpassungen sind viel leichter und das Verfahrenshandbuch kann immer auf dem letzten Stand gehalten werden.

Ergebnis: das Verfahrenshandbuch (Verzeichnis der Verarbeitungstätigkeiten) mit allen vorgeschriebenen Inhalten.

Schritt 3: Richtige Reaktion bei Anfragen von Betroffenen festlegen

Es gibt eine kurze Liste an Rechten, die Betroffene, von denen das Unternehmen Daten gespeichert hat, einfordern können. Diese Liste ist zwar nicht lang, aber es ist wichtig, sich vorab zu überlegen, wie diesen Rechten entsprochen werden kann. Im Anlassfall kann ein Betroffener eines seiner folgenden Rechte einfordern:

- Informationspflicht
- Auskunftsrecht
- Recht auf Berichtigung
- Recht auf Löschung („Recht auf Vergessenwerden")
- Recht auf Einschränkung der Verarbeitung
- Recht auf Datenübertragbarkeit
- Widerspruchsrecht

Das Vorgehen: Für die Erhebung dieser Informationen ist mindestens eine Person nötig, die sich mit den Abläufen in der Firma auskennt, und eine, die mit den IT-Systemen gut vertraut ist. Moderierte Intensiv-Workshops in Kombination mit Hausaufgaben für diese Kollegen bringen aus Erfahrung der Autoren am schnellsten die gewünschten Ergebnisse.

Ergebnis: eine Prozess-Beschreibung für den DSGVO-konformen Ablauf für jede dieser Anfragen sowie Arbeitsanweisungen und Schulung für die verantwortlichen Mitarbeiter.

Schritt 4: IT-Anwendungen und -Systeme auf DSGVO-Konformität untersuchen

Die obigen Schritte auf Anfragen von Betroffenen sind in manchen Umgebungen nicht uneingeschränkt umsetzbar; vor allem das Recht auf Löschung kann eine Anpassung der Systeme erfordern. Logisches Löschen durch Setzen eines Löschkennzeichens kann zumindest als temporäre Lösung dienen, wenn physisches Löschen nicht ohne Weiteres implementierbar ist. Wichtig ist, den Zugriff auf die logisch gelöschten Daten zuverlässig zu verhindern. Vorhandene IT-Anwendungen müssen daher auf Erfüllung der DSGVO-Vorgaben geprüft werden:

- Welche Anwendungen sind im Einsatz?
- Wie werden die Betroffenenrechte mit diesen Anwendungen verwirklicht (beispielsweise die saubere Löschung von Daten)?
- Gibt es „Office-Applikationen" (Word, Excel etc.), die personenbezogene Daten verarbeiten, die oft verstreut auf den Filesystemen herumliegen?

Das Vorgehen: Auflistung der DSGVO-relevanten Funktionen in einem Applikationskatalog. Gleichzeitig wird überprüft, in welchem Maße die vorhandenen Applikationen die DSGVO-Personenrechte unterstützen.

Ergebnis: eine Liste der Applikationen, aus der ersichtlich wird, welche DSGVO-

konform sind und welche nicht. Dadurch können die Investitionen für Applikations-Versionen transparent gemacht werden, um sie DSGVO-konform zu machen.

Schritt 5: Richtige Reaktion bei Missbrauch der Daten festlegen

Wenn Daten gestohlen werden, ist rasches Handeln angesagt, denn die DSGVO schreibt enge Fristen vor. Daher ist es wichtig, für den Anlassfall vorbereitete Abläufe bei der Hand zu haben, die überlegt ausgearbeitet sind. Denn wenn es so weit ist, gibt es ohnehin Stress genug. Folgendes ist zu tun:

- Feststellen, welche Daten wie kompromittiert wurden. Hier kann in weiterer Folge forensische Arbeit nötig sein, für die eventuell Unterstützung von außen erforderlich ist.
- Meldung an die Aufsichtsbehörde, Muster siehe *„www.wko.at/service/wirtschaftsrecht-gewerberecht/eu-dsgvo-data-breach-notification-behoerde.html"*
- Meldung an die Betroffenen, Muster siehe „Muster: *www.wko.at/service/wirtschaftsrecht-gewerberecht/eu-dsgvo-data-breach-notification-betroffene.html"*

Das Vorgehen: Als Basis dient eine geeignete Vorlage (Anwalt, WKO etc.), die an das Unternehmen angepasst wird. Am wichtigsten sind die Erstellung einer Checkliste oder Arbeitsanweisung sowie die Schulung der Mitarbeiter, die an der Analyse und Aufarbeitung eines Datendiebstahls involviert sein werden. Sie müssen im Anlassfall unter Stress schnell und richtig reagieren können.

Ergebnis: Prozessbeschreibungen für die DSGVO-relevanten Meldungen, Arbeitsanweisung und Schulung für verantwortliche Mitarbeiter sowie eine Definition von Maßnahmen (technisch, organisatorisch), um das Risiko für solche Vorfälle zu senken.

Schritt 6: Sicherheit der mobilen Endgeräte überprüfen

Mobile Endgeräte führen leicht zu unkontrollierter Verbreitung von Daten, der Schutz auf diesen Geräten wird oft übersehen. Besonders kritisch sind Geräte, auf denen Apps vom Anwender frei installiert werden dürfen und die möglicherweise Daten auslesen und weiterreichen, ohne das an die große Glocke zu hängen. Das ist bei Apps leider nicht die Ausnahme, sondern fast schon die Regel. Mobile Device Management (MDM), das etwa das Löschen aus der Ferne ermöglicht, sowie die Einschränkung der Benutzerrechte am Gerät sind hier wesentliche Faktoren.

Wie sicher sind Laptops, Tablets, Handys & Co. und wie kann technisch und organisatorisch sichergestellt werden, unerlaubten Zugriff auf personenbezogene Daten zu verhindern?

Das Vorgehen: Anlegen eines Software- und Datenverzeichnisses mit Schwerpunkt auf Sicherheitsfunktionen.

Ergebnis: Definition von Maßnahmen (technisch, organisatorisch), um das Risiko für unerlaubte Zugriffe oder unbeabsichtigten Datenverlust zu senken, und ein Zeitplan für die Umsetzung.

Schritt 7: Spezialfälle prüfen

Als letzter Schritt ist zu prüfen, ob auch nichts übersehen wurde. Durch die Art der Verarbeitung (etwa Video-Aufzeichnungen oder Profiling) oder bei speziellen Daten (wie Gesundheitsdaten) können durch Kombination zusätzliche Informationen entstanden sein, die ebenfalls berücksichtigt werden müssen. Unter Umständen sind für diese Informationen eigene Dokumentationen nötig. Es ist zu klären, welche Spezialfälle auf das Unternehmen zutreffen, für die weitere Dokumente im Sinne der DSGVO vorhanden sein müssen.

Das Vorgehen: Es werden die in Schritt 1 und 2 erhobenen Informationen so kombiniert, dass dadurch mögliche Spezialfälle sichtbar werden. Beispiele dafür wären die Rechtmäßigkeit der Verarbeitung der personenbezogenen Daten oder die Frage, ob eine Datenschutz-Folgenabschätzung durchgeführt werden muss.

Ergebnis ist eines oder mehrere der folgenden Dokumente:

- Dokumentation der Einwilligungserklärungen *(siehe „https://www.wko.at/service/wirtschaftsrecht-gewerberecht/EU-Datenschutz-Grundverordnung:-Einwilligungserklaerung-.html")*
- Dokumentation der Sicherheitsmaßnahmen
- Dokumentation der Risikoabschätzung
- Dokumentation von Arbeitsanweisungen
- Mustervertrag für die Auftragsverarbeitung *(siehe „https://www.wko.at/service/wirtschaftsrecht-gewerberecht/eu-dsgvo-mustervertrag-auftragsverarbeitung.html")*
- Dokumentation der Geheimhaltungspflicht *(siehe „https://www.wko.at/service/wirtschaftsrecht-gewerberecht/eu-dsgvo-muster-verpflichtungserklaerung-datengeheimnis.html")*

Ein abschließender Tipp

Am besten ist es, alle Überlegungen und Entscheidungen, die zur DSGVO angestellt werden, gleich im Verzeichnis von Verarbeitungstätigkeiten zu dokumentieren. Es ist das zentrale Dokument zur DSGVO-Konformität und erleichtert die Nachvollziehbarkeit aller Entscheidungen in Bezug auf den Datenschutz, wenn alles an einem Ort zusammengefasst ist. Auch wenn es Überlegungen gibt, die für das Unternehmen als nicht relevant erachtet wurden, sollten diese trotzdem zu Dokumentationszwecken inklusive Begründung in das Verzeichnis aufgenommen werden.

Fazit

Das Sieben-Punkte-Programm ist eine pragmatische Vorgehensweise, die einfache Methoden, bewährte Vorlagen, eine schlanke Software-Lösung und Mitarbeiter-Schulung umfasst. Damit ist man bezüglich aller Dokumentationspflichten im Sinne der DSGVO „auf der sicheren Seite". Im Zuge des Sieben-Punkte-Programms werden zusätzliche Erkenntnisse gewonnen, die Unternehmen in Form von Verbesserungsvorschlägen und neuen Ideen viel nützen können:

- Die Verbesserung von Abläufen sorgt für höhere Effizienz und Transparenz
- Mehr Informationen aus vorhandenen Daten zu ziehen, hilft bei der laufenden Verbesserung der Dienstleistung oder der Produkte
- Ausmisten unnötiger Daten oder Verarbeitungen schafft Luft für Neues und entlastet die Mitarbeiter
- Das Schaffen der Awareness bei Mitarbeitern ist eine gute Vorbeugungsmaßnahme gegen Datenverlust durch Angriffe von innen und außen
- Das Erhöhen der Betriebssicherheit senkt das Risiko von Geschäftsausfällen

Mag. Wolfgang Klinger
wolfgang.klinger@sphinx.at

DI (FH) Ernst Stippl
ernst.stippl@sphinx.at