DSGVO und Dokumentationspflicht

Know-how Bis zum 25. Mai müssen betroffene Unternehmen ihre Datenbearbeitung, Organisation und Prozesse angepasst haben. Dieser Artikel gibt Tipps, wie sich die neuen Bestimmungen auf die Dokumentationspflichten auswirken.

Von Maria Winkler

Aufgrund der in der DSGVO verankerten Rechenschaftspflicht muss ein Unternehmen, das für eine Datenbearbeitung verantwortlich ist, nachweisen, dass es dabei die gesetzlichen Vorgaben einhält. Ein solcher Nachweis kann in erster Linie mittels Dokumentationen erbracht werden, wobei in der Regel unerheblich ist, ob diese schriftlich oder elektronisch vorliegen.

Klärung der datenschutzrechtlichen Rollen

In der Praxis hat sich die Bestimmung, welche datenschutzrechtliche Rolle ein Unternehmen bei der Verarbeitung von Personendaten einnimmt, als eine nicht immer einfach zu lösende Aufgabe erwiesen. Die DSGVO kennt neben der sogenannten betroffenen Person, also der natürlichen Person, deren Daten verarbeitet werden, noch die datenschutzrechtlichen Rollen des Verantwortlichen sowie des Auftragsverarbeiters. Beim Verantwortlichen handelt es sich um das Unternehmen, das über die Zwecke und Mittel der Datenverarbeitung bestimmt. Einfacher gesagt ist gemäss DSGVO dasjenige Unternehmen der Verantwortliche, das die Personendaten für eigene Zwecke erhebt und verarbeitet. Wenn ein Unternehmen hingegen die Personendaten als Dienstleister für ein anderes Unternehmen (den Verantwortlichen) und für dessen Zwecke verarbeitet, dann handelt es sich dabei um einen Auftragsverarbeiter.

Ein Online-Shop mit Kunden in der EU gilt gemäss DSGVO als Verantwortlicher. Speichert er seine Daten in einem externen Rechenzentrum, ist der Betreiber des Rechenzentrums der Auftragsverarbeiter. Zurzeit ist es zumindest umstritten, inwieweit ein Schweizer Auftragsverarbeiter direkt unter die DSGVO fällt, da er gemäss der Definition der DSGVO die Daten für den Verantwortlichen verarbeitet und daher seine Leistungen nicht direkt den betroffenen (natürlichen) Personen anbietet.

Kritische Datenbearbeitungen müssen sorgfältig dokumentiert werden.

Verzeichnisse von Verarbeitungstätigkeiten

Zu den in der DSGVO ausdrücklich genannten Dokumentationspflichten gehört die Verpflichtung, sogenannte Verzeichnisse von Datenverarbeitungen zu erstellen. Dabei handelt es sich um eine kurze Beschreibung der wesentlichen Elemente der in einem Unternehmen vorhandenen Geschäftsprozesse, in denen Personendaten zu einem bestimmten Zweck bearbeitet werden. Zweck dieser Verzeichnisse ist der Nachweis der Einhaltung der DSGVO. Die Mindestangaben, die in dem Verzeichnis gemacht werden müssen, sind in Art. 30 DSGVO aufgelistet, wobei der sogenannte Verantwortliche und der Auftragsverarbeiter unterschiedliche Verzeichnisse erstellen müssen.

Im oben beschriebenen Beispiel des Online-Shops muss der Anbieter des Online-Shops das Verzeichnis des Verantwortlichen ausfüllen. Der Betreiber des Rechenzentrums wird das Verzeichnis des Auftragsverarbeiters ausfüllen müssen, sofern er unter die DSGVO fällt.

Greifen mehrere Unternehmen gemeinsam auf Daten zu und werden diese für gemeinsame Zwecke verarbeitet, dann sind sie «gemeinsam Verantwortliche» und müssen das Verzeichnis entsprechend gemeinsam ausfüllen und zusätzlich eine Vereinbarung schliessen, in der sie vereinbaren müssen, wer welche Pflichten gemäss DSGVO trägt (Art. 26 DSGVO).

Ist geklärt, welches Verzeichnis zu erstellen ist, muss definiert werden, für welche Geschäftsprozesse eines ausgefüllt werden muss. Es ist zu empfehlen, sich bei der Festlegung der zu dokumentierenden Geschäftsprozesse nach dem Bearbeitungszweck zu richten. Datenverarbei-

tungen, die zu einem bestimmten Zweck erfolgen, sollen in einem Verzeichnis dokumentiert werden. Am Beispiel der Verarbeitung von Mitarbeiterdaten können beispielsweise ein, zwei oder mehr Prozesse vorliegen. Es kann der gesamte Personalprozess von der Rekrutierung über die Anstellung, die Datenbearbeitung bei aktiven Arbeitsverhältnissen bis zur Beendigung des Arbeitsverhältnisses und der Archivierung und anschliessenden Löschung der Daten als ein Prozess bezeichnet und beschrieben werden. In der Praxis ist es üblich, den HR-Prozess auf zwei oder mehr Verzeichnisse zu verteilen – den Rekrutierungsprozess und den eigentlichen HR-Prozess ab Anstellung. Einige Unternehmen führen den Lohnprozess nochmals separat. Wichtig ist, dass eine Datenverarbeitung, die zwar mit denselben Daten, aber zu einem vollkommen anderen Zweck erfolgt, in einem separaten Verzeichnis dokumentiert wird.

Die gesetzlich geforderten Mindestangaben, die in Verzeichnissen von Verantwortlichen zu dokumentieren sind, können in Angaben zum verantwortlichen Unternehmen, Angaben zur Datenverarbeitung und Informationen zu den technischen und organisatorischen Massnahmen (sogenannte TOMs) unterteilt werden. Im Hinblick auf die Datenverarbeitung wird keine detaillierte Beschreibung einzelner Prozessschritte verlangt. Vielmehr sind neben der Bezeichnung der Datenverarbeitung (z.B. Rekrutierung neuer Mitarbeitender), Angaben zu den betroffenen Personen (z.B. Bewerber), zu den Kategorien von Personendaten (z.B. Name und Adresse, Telefon, E-Mail-Adresse, Arbeitszeugnisse, etc.) anzugeben. Zudem muss erfasst werden, ob und wenn ja welchen Kategorien von Empfängern Daten weitergeleitet werden (z.B. externer Dienstleister, der das Rekrutierungstool betreibt und hostet). Werden die Daten ins Ausland weitergeleitet (z.B. wenn das Rekrutierungstool in der Cloud gehostet wird und sich die Rechenzentren im Ausland befinden), müssen Informationen zum Empfängerland erfasst werden. Ist dieses ein Land, das aus der Sicht der EU über keinen angemessenen Datenschutz verfügt, muss zudem dokumentiert werden, mit welchen Massnahmen man den Schutz der Personendaten sicherstellt (z.B. durch Verwendung der sogenannten EU Model Clauses).

Sofern möglich, müssen zusätzlich die Aufbewahrungsdauer und die technischen und organisatorischen Massnahmen dokumentiert werden, die zum Schutz der Daten ergriffen werden. Die Formulierung «wenn möglich» soll nicht darüber hinwegtäuschen, dass erwartet wird, dass diese Informationen grundsätzlich dokumentiert werden müssen. Werden diese Informationen nicht erfasst, muss es gut begründet werden.

Datenschutz-Folgenabschätzung

Sind die Verzeichnisse erstellt, muss geprüft werden, ob eine sogenannte Datenschutz-Folgenabschätzung (DSFA) durchgeführt werden muss. Dabei handelt es sich um eine risikobasierte Prüfung einer (geplanten) Datenverarbeitung, die voraussichtlich mit einem hohen Risiko für die betroffenen Personen verbunden

ist. Diese Pflicht betrifft nur den Verantwortlichen, der Auftragsverarbeiter muss den Verantwortlichen dabei aber gegebenenfalls unterstützen. Die DSFA kann in 3 Schritte unterteilt werden:

In Schritt 1 wird geprüft, ob voraussichtlich ein hohes Risiko für die betroffenen Personen vorliegt. Dies ist beispielsweise der Fall, wenn sogenannte automatisierte Einzelfallentscheidungen gefällt werden, besonders sensible Daten in einem grossen Umfang bearbeitet werden oder öffentliche Bereiche systematisch überwacht werden. Diese Aufzählung ist nicht abschliessend, ein hohes Risiko kann sich auch aus den Umständen oder der Art der geplanten Datenverarbeitung ergeben, beispielsweise, weil neue Technologien verwendet werden, bei denen die Risiken noch nicht vollständig geklärt sind. Zudem können auch die Mitgliedsstaaten vorsehen, dass bei bestimmten Datenverarbeitungen immer (oder nie) eine DSFA durchgeführt werden muss. Diese sogenannte Schwellwertanalyse muss dokumentiert und aufbewahrt werden.

Ergibt die Schwellwertanalyse ein hohes Risiko für die betroffenen Personen, dann muss als Schritt 2 die DSFA durchgeführt werden. Diese beinhaltet insbesondere die Beschreibung der Datenverarbeitung, die Bewertung der in der Schwellwertanalyse identifizierten Risiken sowie die Festlegung der Massnahmen, mit denen diese Risiken verringert oder ausgeschlossen werden. So kann beispielsweise das Risiko, dass es bei einer Datenübermittlung in ein unsicheres Drittland zu Zugriffen unberechtigter Dritter kommt, dadurch reduziert werden, dass die Daten verschlüsselt werden. Können die Risiken mit den definierten Massnahmen auf ein akzeptables Mass gesenkt oder ausgeschlossen werden, dann sind keine weiteren Schritte erforderlich. Die DSFA sollte dokumentiert und in einer beweiskräftigen Form aufbewahrt werden.

Verbleibt auch nach Ergreifen der definierten Massnahmen immer noch ein hohes Risiko für die betroffenen Personen, dann muss als Schritt 3 die zuständige Aufsichtsbehörde kontaktiert werden. Diese hat bis zu zwölf Wochen Zeit, dazu Stellung zu nehmen. Diese Frist muss gegebenenfalls bei der Planung neuer Datenverarbeitungen mitberücksichtigt werden. Grundsätzlich wird aber jedes Unternehmen ein grosses Interesse daran haben, diese Konsultationspflicht durch das Ergreifen risikoreduzierender Massnahmen zu verhindern.

Die DSFA muss in einer dokumentierten Form erfolgen, die es dem Unternehmen ermöglicht nachzuweisen, dass es seinen Pflichten nachgekommen ist. Die Form der DSFA ist nicht vorgeschrieben, sie kann daher sowohl durch das Ausfüllen von physischen Fragebogen als auch elektronisch unter Verwendung einer entsprechenden Software erfolgen. Wichtig ist, dass die Dokumentation beweiskräftig ist, also nachträglich nicht unbemerkt verändert werden kann.

Meldepflicht für Datensicherheitsverletzungen

Die DSGVO verpflichtet sowohl die Verantwortlichen als auch die Auftragsverarbeiter, angemessene Massnahmen zum Schutz von Personendaten zu ergreifen. Zweck der Schutzmassnahmen ist nicht nur die Verhinderung von unberechtigten Zugriffen, sondern beispielsweise auch deren Integrität und Verfügbarkeit zu gewährleisten. Ob die Schutzmassnahmen angemessen sind, bestimmt sich nach der Sensitivität der Daten und dem Risiko einer Persönlichkeitsverletzung – je höher das Risiko und je sensitiver die Daten, umso höher ist der anzulegende Sorgfaltsmassstab. Die ergriffenen Schutzmassnahmen müssen wiederum dokumentiert und regelmässig geprüft werden.

Passiert dennoch eine Datensicherheitsverletzung, wie beispielsweise ein Datendiebstahl, dann muss diese der Aufsichtsbehörde innerhalb von 72 Stunden nach der Entdeckung gemeldet werden. Eine Ausnahme besteht nur, wenn die Verletzung voraussichtlich zu keinem Risiko für die betroffenen Personen führt, beispielsweise, weil die Daten verschlüsselt waren und der Datendieb daher keinen Zugriff auf sie hat. Droht für die betroffenen Personen ein hohes Risiko, dann müssen diese zusätzlich über den Sicherheitsvorfall informiert werden. Diese Information muss gemäss DSGVO unverzüglich erfolgen. Damit will der Gesetzgeber erreichen, dass die vom Vorfall betroffenen Personen eventuell selbst noch allfällige Massnahmen ergreifen können, um weiteren Schaden von sich abzuwenden. Auftragsverarbeiter sind verpflichtet, den Verantwortlichen unverzüglich über allfällige Datensicherheitsverletzungen zu informieren. Eine Meldepflicht gegenüber Aufsichtsbehörden oder den betroffenen Personen besteht für sie nicht.

Schweizer KMU, die unter die DSGVO fallen, müssen daher einen entsprechenden Prozess einführen, der sicherstellt, dass Datensicherheitsvorfälle erkannt und dokumentiert werden. Auch die vorgenommene Risikobeurteilung sowie die Meldung an die Aufsichtsbehörden und, sofern nötig, an die vom Vorfall betroffenen Personen, müssen nachvollziehbar und somit dokumentiert sein. Somit müssen nicht nur die meldepflichtigen, sondern alle Sicherheitsvorfälle dokumentiert werden.

Neue Prozesse

Die in der DSGVO vorgeschriebenen neuen Dokumentationspflichten zwingen die betroffenen Unternehmen, Prozesse für die Erstellung von Verzeichnissen, die Durchführung von Datenschutz-Folgenabschätzungen und die Meldung von Datensicherheitsvorfällen einzuführen. Dabei darf nicht übersehen werden, dass es sich um eine Daueraufgabe handelt und die Dokumentationen und Prozesse auch aufrechterhalten werden müssen. Die Verzeichnisse und die Datenschutz-Folgenabschätzungen müssen daher regelmässig geprüft und aktualisiert und die Liste der Datensicherheitsvorfälle muss aktuell gehalten werden. Unternehmen, die damit noch nicht begonnen haben, sind daher gut beraten, im Hinblick auf die nur mehr kurze Zeit bis zum Inkrafttreten der DSGVO die entsprechenden Arbeiten in Angriff zu nehmen. ■

DIE AUTORIN

Maria Winkler ist Juristin mit einer Spezialisierung im IT-Recht und Datenschutzrecht und Inhaberin sowie Geschäftsführerin des Unternehmens IT & Law Consulting mit Sitz in Zürich. Das Unternehmen berät und unterstützt seit seiner Gründung im Jahr 2004 Unternehmen und Behörden beispielsweise bei der Gestaltung und Verhandlung von IT-Verträgen sowie beim Aufbau von Datenschutzmanagementsystemen. Maria Winkler unterrichtet an verschiedenen Hochschulen die Fächer Informatikrecht und Datenschutzrecht.