Newsletter Datenschutz Issue 3|2018

Aktuelles zum Grundsatz der Speicherbegrenzung

Als einen der Datenschutzgrundsätze normiert Art 5 lit e DSGVO den Grundsatz der Speicherbegrenzung: Sobald die Aufbewahrung für den Verarbeitungszweck nicht mehr erforderlich ist, sind personenbezogene Daten zu löschen, zu vernichten oder durch Anonymisierung bzw wirksame Pseudonymisierung so zu verändern, dass die Identifizierung der betroffenen Person nicht mehr möglich ist. Ausnahmen dazu bestehen nur für im öffentlichen Interesse liegende Archivzwecke, für wissenschaftliche und historische Forschungszwecke oder für statistische Zwecke.

Korrespondierend mit diesem Grundsatz, haben betroffene Personen das Recht auf Löschung ihrer personenbezogenen Daten, wenn diese für die Zwecke, für die sie erhoben oder auf sonstige Weise verarbeitet wurden, nicht mehr notwendig sind (Art 17 DSGVO). Als Ausnahme normiert die DSGVO etwa die Verarbeitung zur Erfüllung rechtlicher Verpflichtungen oder zur Geltendmachung, Ausübung oder Verteidigung von Rechtsansprüchen. Verletzt der Verantwortliche das Recht auf Löschung, steht es der betroffenen Person frei, Beschwerde bei der Aufsichtsbehörde zu erheben. Seit der Anwendbarkeit der DSGVO wurden zwei Entscheidungen veröffentlicht, in denen sich die Datenschutzbehörde mit dem Grundsatz der Speicherbegrenzung beschäftigte.

In der Entscheidung zu DSB-D216.580/0002-DSB/2018 vom 28.5.2018 hielt die Behörde fest, dass eine zeitliche unbegrenzte Speicherung von personenbezogenen Daten für eine eventuell künftige Kontaktaufnahme eine Verletzung des Grundsatzes der Speicherbegrenzung darstellt. Rechtfertigende Gründe für eine fortgesetzte Datenspeicherung bzw eine Ausnahme vom Recht auf Löschung sah die Behörde zudem nicht verwirklicht. Aus heutiger Sicht ist davon auszugehen, dass die normierten Ausnahmetatbestände daher eng auszulegen sein werden. Lehnt ein Verantwortlicher die Löschung personenbezogener Daten deshalb ab, weil sie zur Geltendmachung, Ausübung oder Verteidigung von Rechtsansprüchen erforderlich sind, ist die Datenverarbeitung jedenfalls auf das notwendige Maß – auch in zeitlicher Hinsicht – zu beschränken. Eine Datenverarbeitung, die dieses Maß überschreitet, ist unrechtmäßig und das Löschbegehren der betroffenen Person berechtigt.

In der Entscheidung zu DSB-D216.471/0001-dSB/2018 vom selben Tag setzte sich die Behörde mit der Frage auseinander, ob eine längere Aufbewahrungsdauer der personenbezogenen Daten, auch über die Beendigung der Vertragsverhältnisse und somit über die Zweckerreichung hinaus, gerechtfertigt ist. Zusammengefasst kam die Behörde zu dem Schluss, dass Verjährungsfristen (hier: § 207 Abs 2 BAO) grundsätzlich nicht dafür herangezogen werden können, gesetzliche Aufbewahrungspflichten (hier: § 97 Abs 2 TKG 2003) zu verlängern. Die weitere Aufbewahrung von Daten muss durch ein sich konkret abzeichnendes Verfahren gerechtfertigt sein. Die bloße Möglichkeit,

dass ein Verfahren eingeleitet wird, reicht hingegen nicht aus. Ebenso wenig ist es nach Ansicht der Datenschutzbehörde zulässig, die Speicherdauer um allfällige Postlaufzeiten bzw interne Prozesse zu verlängern. Aufgrund der Aufbewahrungspflichten in der Bundesabgabenordnung und im Telekommunikationsgesetz ist die Beschwerdegegnerin berechtigt, die Stammdaten der betroffenen Person für eine Dauer von sieben Jahren (§ 132 Abs 1 BAO) und deren Verkehrsdaten für die Dauer von längstens drei Monaten bzw der im TKG 2003 normierten Einspruchsfrist zu speichern. Personenbezogene Daten, deren Aufbewahrung keine gesetzliche Deckung findet, dürfen nicht über den Vertragszeitraum hinaus gespeichert werden.

Im Lichte dieser beiden Entscheidungen empfehlen wir, die im Verarbeitungsverzeichnis enthaltenen Fristen für die Löschung zu überprüfen bzw die Speicher- und Löschkonzepte differenziert nach Kategorien personenbezogener Daten auszuarbeiten bzw weiter zu verfeinern.

Claudia Fleischhacker-Hofko

Datenschutzrechtliche Bedenken beim Arbeiten via Smartphones: Abhilfe durch Mobile Device Management?

Die seit Mai 2018 anwendbare EU-Datenschutz-Grundverordnung (EU-DSGVO) schreibt eine Vielzahl an Maßnahmen zum Schutz personenbezogener Daten vor. Insbesondere Unternehmen, deren Mitarbeiter mehr und mehr mobil arbeiten, sehen sich hier großen Herausforderungen gegenüber.

<u>Beispiele aus der Praxis:</u>

- Mitarbeiter nutzen Instant Messaging für die private Kommunikation, verfügen aber über kein privates Smartphone;
- Oder umgekehrt: Mitarbeiter nutzen private Smartphones im Arbeitsumfeld und synchronisieren Unternehmensdaten;
- Mitarbeiter kommunizieren mit Kunden via WhatsApp;
- Smartphone-Betriebssysteme speichern die Daten unverschlüsselt;
- Unternehmen fordern technische Maßnahmen zur Absicherung des Firmennetzwerks bei zulässigen Zugriffen durch Mitarbeiter oder Geschäftsführer über mobile Geräte;

In all diesen Fällen kann der Einsatz einer Mobile Device Management-Lösung Abhilfe schaffen. Ein Mobile Device Management („MDM") dient der zentralen Konfiguration und Administration von Smartphones, Tablet-PCs und Laptops. Mit MDM können diese Endgeräte verwaltet, in- und außer Betrieb genommen und den unternehmensinternen Vorgaben und Richtlinien (sog. Policies) entsprechend angepasst werden. Dazu zählt zB die Auswahl der zu installierenden Apps, die Regelung der Zugriffsberechtigungen der Apps sowie die Erlaubnis zur Synchronisierung von Firmendaten.

Nutzen und Vorteile des MDM

Bei den meisten MDM Lösungen liegen die Daten am Handy in einem sogenannten Container, der optional mit einem zusätzlichen Passwort versehen werden kann. In diesem befinden sich ein eigenes Adressbuch, Mailclient und ein Kalender für Firmendaten und Kontakte. Durch MDM kommt es zu einer kompletten Trennung zwischen Firmen- und privaten Daten. Ein auf dem Gerät – außerhalb des Containers installierte Applikation (zB WhatsApp) hat somit keinen Zugriff auf Daten, insbesondere Geschäftskontakte im Container. Scheidet ein Mitarbeiter aus, kann der Container am mobilen (privaten) Gerät über das MDM Tool gelöscht werden; sämtliche private Apps, Fotos, Email etc bleiben jedoch erhalten. Für den Fall, dass das mobile Gerät verloren geht, wird es auf Werkseinstellung zurückgesetzt und alle Daten gelöscht, so können auch private Daten und Fotos nicht in falsche Hände geraten.

Ansätze zur Implementierung

Zur Implementierung von MDM kann grundsätzlich zwischen drei Ansätzen gewählt werden. Nahezu jeder Mobilfunkanbieter bietet im Rahmen seiner Zusatzservices ein MDM. Da diese Lösungen eher schlicht gehalten sind, kann auf individuelle Anforderungen kaum Rücksicht genommen werden. Als MDM für Unternehmen empfehlen wir daher eine eigene MDM-Lösung, die in der Cloud (vorzugsweise in Rechenzentren innerhalb der EU) bereits ab ca EUR 4,50 pro Monat gemietet werden kann. Diese Lösungen sind in der Funktionalität skalierbar. So kann zum Beispiel zusätzlich ein Viren- und Spywareschutz aktiviert werden. Apps können zentral auf alle Endgeräte ausgerollt oder ein gesicherter verschlüsselter Zugang in das Firmennetz (zB auf den Fileserver) ermöglicht werden. Mittels Black- und Whitelists können Verantwortliche steuern, welche Apps auf den mobilen Geräten erlaubt und welche verboten sind. Von der Verwendung der herstellerseitig angebotenen MDM-Lösungen, nämlich die Ortung und Fernlöschung über einen vom User zu aktivierenden Cloud-Service durchzuführen, ist im Unternehmensbereich hingegen eher abzuraten.

Mithilfe eines Mobile Device Management ist es Unternehmen möglich, das Risiko für die Rechte und Freiheiten natürlicher Personen infolge Datenverarbeitungen mittels mobiler Endgeräte weiter zu reduzieren.

Christian Storck
IT-Spezialist und TÜV-geprüfter Datenschutzbeauftragter

Data Breach: Rasch und richtig handeln

Kommt es zu einer Datenpanne, etwa durch einen Hackerangriff, eine zu rasch versandte Email an einen falschen Empfänger oder durch den Verlust eines Smartphones, sind Unternehmen verpflichtet,

rasch zu handeln: Die Verletzung des Schutzes der personenbezogenen Daten ist **unverzüglich und möglichst binnen 72 Stunden**, nachdem diese dem Verantwortlichen bekannt wurde, der zuständigen Aufsichtsbehörde zu melden. Nur für den Fall, dass die Verletzung voraussichtlich nicht zu einem Risiko für die Rechte und Freiheiten natürlicher Personen führt, kann die Meldung entfallen. Sofern die Verletzung des Schutzes der personenbezogenen Daten voraussichtlich ein hohes Risiko für die persönlichen Rechte und Freiheiten von natürlichen Personen zur Folge hat, ist auch die betroffene Person unverzüglich zu benachrichtigen.

Um bei einer Datenpanne DSGVO-konform reagieren zu können, ist es neben der Implementierung von technischen Maßnahmen ebenso erforderlich, ein einheitliches Verständnis für den richtigen Umgang mit personenbezogenen Daten sowie für das Vorliegen einer Datenpanne im Unternehmen zu schaffen. Nur gut geschulte und sensibilisierte Mitarbeiter werden Unregelmäßigkeiten in der Verarbeitung personenbezogener Daten erkennen und diese im Ernstfall auch an den Verantwortlichen melden.

Sollte eine Datenpanne bekannt werden, ist im Rahmen einer Risikoabschätzung zu beurteilen, ob diese festgestellte Unregelmäßigkeit tatsächlich auch eine Melde- bzw Benachrichtigungspflicht des Verantwortlichen auslöst. Als **Voraussetzung für eine Meldepflicht** definiert die DSGVO die Verletzung des Schutzes personenbezogener Daten als *„eine Verletzung der Sicherheit, die, ob unbeabsichtigt oder unrechtmäßig, zur Vernichtung, zum Verlust, zur Veränderung oder zur unbefugten Offenlegung von bzw zum unbefugten Zugang zu personenbezogenen Daten führt, die übermittelt, gespeichert oder auf sonstige Weise verarbeitet wurden*". Rechte und Freiheiten natürlicher Personen werden verletzt, wenn ein physischer, materieller oder immaterieller Schaden eintreten kann. Als Beispiele für einen Schaden für natürliche Personen nennt der Erwägungsgrund 85 den Kontrollverlust über ihre personenbezogenen Daten oder die Einschränkung ihrer Rechte, Diskriminierung, Identitätsdiebstahl oder –betrug, finanzielle Verluste, unbefugte Aufhebung der Pseudonymisierung, Rufschädigung, Verlust der Vertraulichkeit von dem Berufsgeheimnis unterliegenden Daten oder andere erheblich wirtschaftliche oder gesellschaftliche Nachteile für die betroffene natürliche Person.

Für die **Beurteilung des Risikos für die Rechte und Freiheiten natürlicher Personen** ist auf den typischen Geschehensablauf abzustellen. Im Idealfall erfolgt diese einzelfallbezogene Beurteilung (Risikoidentifikation, Abschätzung von Eintrittswahrscheinlichkeit und Schwere möglicher Schäden, Zuordnung zur Risikoabstufung) mittels vorab definierter Prozesse anhand einer Musterdokumentation. Dies, um durch eine möglichst systematische Vorgehensweise im Ernstfall rasch reagieren zu können. Orientiert sich die Musterdokumentation am Mindestinhalt der Meldung an die Aufsichtsbehörde (Art 33 Abs 3 DSGVO), können zusätzliche Synergien geschaffen werden.

Folgende Fakten sollten zügig erhoben werden:

- Beschreibung der Verletzung (Zeitpunkt oder Zeitraum, Ursache, Ort);
- Art der Verletzung (Verletzung der Vertraulichkeit, Integrität, Verfügbarkeit);
- Kategorien und ungefähre Zahl der betroffenen Personen (zB Mitarbeiter, Kunden);
- betroffene Kategorien (zB Bank- und Kreditkartendaten, Benutzererkennungen und Passwörter, Gesundheitsdaten) und ungefähre Zahl der betroffenen personenbezogenen Datensätze
- beteiligte Auftragsverarbeiter bzw gemeinsame Verantwortliche;
- mögliche/wahrscheinliche Folgen und Auswirkungen der Datenschutzverletzung (zB Kontrollverlust, Diskriminierung, finanzielle Verluste);
- ergriffene und vorgeschlagene Maßnahmen zur Behebung der Verletzung bzw zur Abmilderung der möglichen nachteiligen Auswirkungen;
- bestehende technische und organisatorische Sicherheitsmaßnahmen;
- Zeitpunkt der Feststellung der Datenpanne.

Eine detaillierte Aufarbeitung des Sachverhalts stellt nicht nur die Basis für die notwendige Risikobeurteilung dar, sondern ist zur Erfüllung der **Rechenschaftspflicht** bzw der Nachweispflicht für den Fall von Nicht-Meldungen erforderlich. Sollte der Verantwortliche im Zuge der Risikobeurteilung zum Ergebnis gelangen, dass keine „Data Breach Notification" an die Aufsichtsbehörde zu erstatten ist, weil die Verletzung voraussichtlich nicht zu einem Risiko für die Rechte und Freiheiten natürlicher Personen führt, kann die Dokumentation des Sachverhalts sowie dessen Beurteilung als Nachweis für eine ordnungsgemäße Entscheidungsfindung gegenüber der Behörde dienen.

Claudia Fleischhacker-Hofko


Information

Mag. Gernot Wilfling
T +43 1 535 8008, E g.wilfling@mplaw.at

Mag. Claudia Fleischhacker-Hofko
T + 43 1 535 8008, E c.fleischhacker@mplaw.at

Müller Partner Rechtsanwälte GmbH
Rockhgasse 6, 1010 Wien
www.mplaw.at