EU-Datenschutzgrundverordnung - Datensondermüll

Der Zeitpunkt zur verpflichtenden Umsetzung der EU-Datenschutzgrundverordnung und deren ergänzende nationale Gesetze rückt schnell näher. Am 25.5.2018 muss eine Organisation, die personenbezogene Daten verarbeitet, die Anforderungen erfüllen und „compliant" sein. Die größte Gefahr neben der Nichterfüllung der Rechte und Informationspflichten ggü. Betroffenen droht hierbei bei den zwei am meisten genutzten Anwendungen mit unstrukturierten Daten. Das sind Email und geteilte Netzlaufwerke.

Einleitung

In Email und geteilten Netzlaufwerken sind oft personenbezogene und sensible Daten vieler Betroffener (Kunden, Mitarbeiter etc) enthalten.

Diese Informationsbestände sind meist sehr intransparent oder auch „dunkel", d.h. niemand weiß, welche Dokumentation gespeichert ist und ob sie Nutzen stiftet oder ein Risiko darstellt.

Praxis

Das stellt besondere Anforderungen an Zugriff und Kontrolle, doch sind diese Systeme meist nicht speziell geschützt. In vielen Unternehmen ist es immer noch möglich, mittels (leider oft unverschlüsselter) portabler Datenträger wie USB-Sticks, große Datenmengen schnell zu kopieren. Auf Mobilgeräte synchronisierte Email ist auf Grund geringerer Sicherheitsmechanismen z. B. im Verlustfall leichter zuzugreifen. Voll verschlüsselte Mobilgeräte sind immer noch nicht weit verbreitet.

Auf Grund der Exponiertheit beider Systeme hinsichtlich Zugriff und der gespeicherten Information muss den Prinzipien der Speicherbegrenzung und Datenminimierung besondere Bedeutung beigemessen werden. Speicherbegrenzung heißt, dass klare Löschfristen gesetzt und diese auch periodisch auf Einhaltung geprüft werden müssen. Datenminimierung bedeutet, dass obsolete oder nicht relevante Information auch vor Ablauf einer Löschfrist zu löschen ist.

Bei der Prüfung dieser Datenbestände werden oft bis zu 25 Jahre alte Dateien mittels automatisierter Analysetools entdeckt, von denen meist niemand mehr weiß, dass sie existieren. Hier wuchern seit der allgemeinen Einführung zentraler Datenserver vor ca. 20 Jahren mittlerweile undurchdringliche „Datendschungel", die dringend einer Strukturierung bedürfen. Vor dem Hintergrund der Anforderungen der EU-DSGVO werden viele dieser Datenbestände als „gefährlicher Abfall" zu betrachten sein, weil in diesen Beständen mit hoher Wahrscheinlichkeit undokumentiert personenbezogene (sensible) Daten gespeichert sind.

Selektion / Umsetzung

Wie sieht nun eine Vorgehensweise zur Risikominimierung aus?

Zuerst sollte mittels automatisierter Werkzeuge eine Analyse vorgenommen werden, um eine „Landkarte" der Informationsbestände zu erstellen.

Danach kann nach folgenden Kriterien obsolete Information (ROT – für redundant, obsolete, trivial) und weiter zu speichernde Information identifiziert werden. Folgende Fragen sind zu stellen:

1. Private, persönliche oder nicht unternehmensbezogene Information oder eine Kopie?
2. Werden Geschäftsvorgänge oder Entscheidungsfindungen dokumentiert?
3. Sind gesetzliche oder regulatorische Aufbewahrungspflichten oder Löschverpflichtungen vorhanden?
4. Hat die Information historischen Wert?
5. Handelt es sich um die letzte Version des Dokumentes?
6. Wie alt ist die Information?
7. Wem „gehört" die Information oder wer ist für den Datenbestand verantwortlich?

Welche Information muss nun wie lange aufbewahrt oder sofort gelöscht werden?

ad 1.) Handelt es sich um private, persönliche oder nicht unternehmensbezogene Information (zB MP3-Musikdateien, Bilder der letzten Weihnachtsfeier etc), so ist diese Information ausnahmslos zu löschen. Das gleiche gilt für Kopien. Duplikate können mittels automatisierter Werkzeuge gefunden werden. Es gilt das SPOT-Prinzip (single point of truth).

ad 2.) Betreffen die Dokumente Geschäftsvorgänge oder Entscheidungsfindungen (zB Bestellungen, Rechnungen, Protokolle etc)? Jegliche Dokumente (Vertragsentwürfe, Emails etc), die die Entwicklung zur letztendlich vorgenommenen, Wert austauschenden Transaktion zwischen Parteien beschreibt. Oder Dokumente, die zum Nachweis von Vereinbarungen oder gesetzter Handlungen dienen, das kann gerichtlich oder außergerichtlich sein. Die meisten geschäftlichen Meinungsverschiedenheiten werden unter Nachweis der schriftlichen Vereinbarung außergerichtlich gelöst.

ad 3.) Es existieren unterschiedlichste Aufbewahrungsfristen. Diese sind abhängig von der Art des Geschäfts, der Gesellschaft und der Jurisdiktion. Geschäftserfordernisse, operative, historische Gründe etc. sind zweitrangig hinter rechtlichen und regulatorischen Anforderungen. Beispiele wären 7 Jahre für Rechnungswesenunterlagen oder 30 Jahre für bestimmte Personalunterlagen. Dokumentation kann auch Löschverpflichtungen unterliegen. Die Dokumentation kann für zukünftige rechtliche oder regulatorische Fragestellungen benötigt werden. (zB Haftungen bei Gewährleistung, Produkt-Prüfzertifikate etc)

ad 4.) Wichtige Zeitpunkte oder Entwicklungsschritte in der Firmengeschichte sollen dokumentiert werden (zB Werkeröffnung, Jubiläum etc).

ad 5.) Ersetzte oder veraltete Dokumentation muss gelöscht werden oder von aktiv verwendeten Systemen in ein Archiv transferiert werden. Es besteht sonst auch die Gefahr, in zu viel Information zu ersticken.

ad 6.) Wird die Information aktiv genutzt? Wann erfolgte der letzte Zugriff? Aufheben für den Fall des Falles ist die falsche Strategie. Nur auf Grund rechtlicher, regulatorischer oder operativer Erfordernisse sollten Dokumente aufbewahrt werden. Wenn 6 Monate kein Zugriff erfolgt, so beträgt die Wahrscheinlichkeit eines neuerlichen Zugriffs nur 0,2%!

ad 7.) Der Verantwortliche oder „Besitzer" sollte seine Dokumentationsbestände entweder selbst aufräumen oder unbedingt beigezogen werden.

Die 7 vorgenannten Fragen sollten bei der periodischen Durchführung von sog. Records Days (zB 1x / pa) gestellt werden. Im Rahmen eines Records Day wird ein Informationsbestand regelmäßig „gewartet".

Risikominimerung

Die vorgenannten Maßnahmen reduzieren folgende Risiken massiv:

1. Daten gehen durch ein Datenleck (externe Hacker, unzufriedene Mitarbeiter etc.) verloren.
2. Prüfung durch die Datenschutzbehörde. Diese wird natürlich einen ihrer Prüfschwerpunkte auf unstrukturierte Datenbestände wie Email und Netzlaufwerke legen, da dort die größten Risiken schlummern und Verstöße am wahrscheinlichsten sind.

Zusammenfassung / Conclusio

Es muss einiger Aufwand zur Bereinigung alter Informationsbestände, die personenbezogene Daten enthalten, aufgebracht werden. Bei nicht korrekter Dokumentation oder Verlust drohen hohe Strafen.

Machen Sie eine Abwägung, ob Informationsbestände noch benötigt werden. Wenn ja, dann ist aber abhängig vom Sensibilitätsgrad der Daten (zB. Religion, Geschlecht etc. - das kann bei alten Excel-Dateien der HR-Abteilung schnell der Fall sein), eine Dokumentation im Verarbeitungsverzeichnis notwendig. Bei sensiblen Daten muss auch noch eine Datenfolgeabschätzung und daraus TOMs zur Gewährleistung der Datensicherheit dieser Dokumentation abgeleitet werden. Eine Einwilligung der Betroffenen muss in jedem Fall vorliegen.

Bis Ende Mai 2018 bietet sich noch die Möglichkeit, kritische Datenbestände ganz einfach zu löschen. Das wird in den meisten Fällen der einzige ökonomisch vertretbare Weg sein.

Mag. Markus Lenotti, März 2018
Geschäftsführer
Lenotti Advisors GmbH