Datenschutz-Interview – Beispiele aus der aktuellen Umsetzung.

Herr Kevin Marschall und Herr Stephan Blazy (GDPC GbR) arbeiten als juristische Experten im Datenschutz. Sie wurden von Frau Kathrin Weber (Beraterin der I-R-M GmbH Hamburg) zu aktuellen Umsetzungsthemen befragt, die in Unternehmen und Vereinen bisher aufgetreten sind. Ein Austausch unter drei extern tätigen Datenschutzbeauftragten.

---

1. Wie sieht die grundsätzliche Datenschutzinformation aus?

Die Inhalte der Datenschutzinformation orientieren sich an den korrespondierenden Informationspflichten gemäß Art. 12, 13 und 14 DSGVO.

Neben einer möglichst vollständigen Beschreibung der zu erteilenden Informationen ist auch die adressatenorientierte Information erforderlich. Das bedeutet, dass grundsätzlich unterschiedliche Datenschutzinformationen für die jeweiligen Adressaten (Betroffenenkategorien) existieren müssen. Im betrieblichen Normalfall werden regelmäßig vier Datenschutzinformationen benötigt (Kunden, Geschäftspartner/Lieferanten, Mitarbeiter, Bewerber).

Auch der Informationskanal ist genau zu eruieren. Hierbei kommt es beispielsweise darauf an, ob die Information auf der Website abrufbar sein soll oder die Erteilung in andere feste Prozesse (z.B. im Rahmen der Auftragserteilung/Vertragsschlusses) eingebunden und hierdurch auch gewährleistet wird. Die Verantwortlichen sollten hierfür – je nach Einzelfall – mehrere Standbeine fokussieren, um eine Kenntnisnahme der betroffenen Personen von den Datenschutz-Informationen zu gewährleisten.

Beispiele:

- Freie Abrufbarkeit als pdf auf der Homepage
- Signaturverweis in der E-Mail
- Analoge Aushändigung (ggf. auch Aushang, z.B. bei Veranstaltungen etc.)

2. Ist die angekündigte Mahnwelle bezüglich fehlender Datenschutz Informationen eingetreten?

Nein, die große Abmahnwelle bezüglicher fehlender Datenschutz-Informationen – oder weiter bezüglich Verstöße gegen datenschutzrechtliche Vorgaben – hat sich bis dato nicht abgezeichnet. Es sind lediglich vereinzelte Abmahnungen bekannt, die sich beispielsweise auf fehlende SSL-Verschlüsselung, fehlerhafter und nicht vorhandener Datenschutz-Informationen auf Websites oder auf die Einbindung von Fremddiensten wie Google Analytics beziehen. Unabhängig davon, ob und inwiefern diese Abmahnungen überhaupt rechtlich zulässig sind, darf diese Situation nicht darüber hinwegtäuschen, dass das größte Risiko für Unternehmen in der Bußgeld- und Sanktionspraxis der Aufsichtsbehörden und in entsprechenden Eingaben von betroffenen Personen liegt.

3. Wo gibt es in den Unternehmen Ihrer Meinung nach die meisten Probleme?

Die aus unserer Erfahrung größten Probleme ergeben sich aus den nachfolgend aufgelisteten Punkten:

- Umsetzung der Informationspflichten (Art. 13/14 DSGVO)
- Erforderlichkeit von Joint-Controller-Agreements (z.B. bei Zeitarbeitskräften Art. 26 DSGVO), da diese oftmals fälschlich mit Auftragsverarbeitungsverhältnissen (Art. 28 DSGVO) verwechselt werden.
- Erstellung eines Verzeichnisses von Verarbeitungstätigkeiten (Art. 30 DSGVO), da vielen Verantwortlichen einerseits die Beschreibung der (Mindest-)Inhalte fremd sind und andererseits die Granularität des Verzeichnisses unbekannt sind.
- Prüfung, ob eine Pflicht zur Durchführung einer DSFA (Datenschutzfolgeabschätzung nach Art. 35 DSGVO) besteht und falls ja, wie diese durchgeführt werden muss.
- Erfassung und Bewertung von meldepflichtigen Schutzverletzungen gemäß Art. 33/34 DSGVO, da diesbezügliche eine ausführliche Analyse des Risikos (Eintrittswahrscheinlichkeit und Schwere des Schadens) und die Ergreifung hierauf bezogener abmildernder Maßnahmen durch den Verantwortlichen erforderlich sind.
- Einstufung der Schutzgrade der Daten (Art.32 z.B. interne/vertrauliche/streng vertrauliche Daten)

Einige der Probleme hängen auch mit der durch die DSGVO (wahrgenommene) verursachte Umbruchsituation zusammen, wodurch viele seit Jahren oder Jahrzehnten eingeschliffenen Prozesse geprüft und (häufig erstmals) hinterfragt und ggf. umstrukturiert werden müssen. Sätze wie „Wir machen das schon immer so“ sind hierbei häufig an der Tagesordnung.

4. Die Aufsichtsbehörden der Bundesländer sind Anlaufstelle für Problematiken im Datenschutz. Welche Situation ist derzeit wahrnehmbar?

Trotz personeller und materieller Aufstockung der einzelnen Landesaufsichtsbehörden sind viele derzeit natürlich aufgrund der massenhaften Flut von Anfragen und Beschwerden überfordert und arbeiten diese nacheinander ab. Im Falle einer Beschwerde steht der Verantwortliche jedoch sofort im Fokus der Aufsichtsbehörde, die diesen sodann zur Stellungnahme bezüglich des jeweiligen Sachverhalts auffordert. Aber auch ohne eine Beschwerde wird die Luft langsam aber sicher dünner. Einige Aufsichtsbehörden haben angekündigt, dass sie mit der Überprüfung von Unternehmen bereits im Herbst/Winter dieses Jahr beginnen werden. Andere Aufsichtsbehörden haben zudem verlauten lassen, dass Sie nur noch im Jahr 2018 zurückhaltend bezüglich der Verhängung von Bußgeldern sein werden; nicht mehr viel Zeit, um bis Jahresende noch seine Datenverarbeitungssituationen im Unternehmen zu prüfen und an die aktuelle Rechtslage anzupassen.

5. Gibt es besondere Fälle aus der Beratung, die anonym aufgeführt werden können?

Das kommt ganz auf die Zielrichtung der Frage an. Es gibt zahlreiche interessante Fälle in der alltäglichen Datenschutzpraxis.

Ein interessanter Fall beschäftigte sich beispielsweise mit der datenschutzrechtlichen Zulässigkeit von Tonaufzeichnungen im Rahmen eines Geschäftsverhältnisses. Dieser Sachverhalt wird nicht nur durch das Datenschutzrecht, sondern auch durch flankierende strafrechtliche Vorschriften geprägt. Hier kam es – insbesondere im Hinblick auf die Interessenabwägung im Rahmen von Art. 6 Abs. 1 lit. f DSGVO – wesentlich darauf an, Risiken für die Betroffenen durch entsprechende Schutzmaßnahmen zu reduzieren bzw. abzumildern. Diese Schutzmaßnahmen bezogen sich u.a. auf eine sichere Datenspeicherung

(Container) und ein strenges Zugriffskonzept (6-Augenprinzip unter Einbindung des Datenschutzbeauftragten).

Ein anderer spannender Fall beschäftigte sich mit dem Verhältnis von UWG, Datenschutzrecht und öffentlichem (Landes-)Recht und mit der Frage, ob und unter welchen Voraussetzungen eine exponierte öffentliche Stelle im Rahmen Ihrer Tätigkeit Einladungsmails zu einer Veranstaltung, die im öffentlichen Interesse liegt, verschicken kann. Der Lösungsweg lag hierbei u.a. in der juristischen Auslegung des Begriffs „Werbung“ im Sinne des UWG.

6. Das Verfahrensverzeichnis stellt immer wieder eine große Herausforderung für die Unternehmen dar. Welche Herangehensweisen haben sich aus Ihrer Sicht bisher bewährt?

Das Verzeichnis von Verarbeitungstätigkeiten gemäß Art. 30 DSGVO ist in der Tat eines der derzeit noch größten Sorgenkinder eines Unternehmens und damit auch des Datenschutzbeauftragten.

In der Praxis hat es sich definitiv bewährt, dass der Datenschutzbeauftragte in Abstimmung mit dem Verantwortlichen und den einzelnen Abteilungsleitern das Verzeichnis nach einer ausführlichen Bestandsaufnahme erstmal selbst (als Entwurf) erstellt und dieses sodann den jeweiligen Ansprechpartner zur Prüfung und Korrektur vorlegt. Hierbei darf jedoch nicht vergessen werden, dass der Datenschutzbeauftragte den Aussagen der Ansprechpartner nicht einfach blind vertrauen darf; auch bezüglich der Richtigkeit und Vollständigkeit der beschriebenen Verarbeitungstätigkeiten gilt die Überwachungs- und Kontrollpflicht des Datenschutzbeauftragten, wonach dieser sich selbst ein Bild hierüber machen muss.

Dabei ist das Verzeichnis essentiell für die Erfüllung zahlreicher Pflichten der DSGVO. So können Sie beispielsweise die einzelne Verarbeitungstätigkeiten und Prozesse nicht hinreichend und kohärent auf ihre Datenschutz-Konformität hin, etwa bzgl. der Einhaltung der Grundsätze aus Art. 5 DSGVO, überprüfen, wenn das Verzeichnis nicht existiert oder nicht vollständig ist.

7. Löschkonzepte- oft nachgefragt- Wie wichtig sind diese?

Eine strukturierte und systematische Vorgehensweise bei der Löschung von personenbezogenen Daten ist essentiell. Hierzu zählt insbesondere die Erstellung eines Löschkonzepts (dieses dient auch der Nachweispflicht) mit einigen der nachfolgend aufgelisteten Inhalte:

Löschkonzepte, z.B.

- Erfassung aller Datenarten /-kategorien im Unternehmen
- Erfassung aller Speicherorte dieser Datenarten /-kategorien
- Festlegung der Art der Löschung/Vernichtung (Programm, Extern, intern etc.)
- Berücksichtigung gesetzlicher Aufbewahrungsvorschriften für manche Datenarten
- Dokumentation der gelöschten Datensätze (z.B. in einem Löschverzeichnis)

Daneben ist die Überprüfung der Einhaltung des entworfenen Löschkonzepts ebenso wichtig wie eine hinreichende Sensibilisierung der Mitarbeiter bezüglich der Löschvoraussetzungen und den Löschverpflichtungen.

8. Auch die Archivierung ist kein neues Thema. Was ist bei einem umfassenden Archivierungssystem neu zu beachten?

Grundsätzlich ist eine Archivierung von personenbezogenen Daten an die gleichen Voraussetzungen gebunden, wie schon vor Inkrafttreten der DSGVO am 25. Mai 2018. Die einschlägigen Normen – etwa nach Handels- oder Steuerrecht – stellen sich im Verhältnis zur DSGVO als spezialgesetzliche Regelungen dar, welche deren allgemeine Vorschriften präzisieren. Das gilt freilich nur für die gesetzlich vorgeschriebenen Aufbewahrungspflichten. Die „archivierten" personenbezogenen Daten dürfen dabei nicht für andere Zwecke weiterverarbeitet werden. So ist beispielsweise ein nach §147 AO aufzubewahrender Geschäftsbrief lediglich für die Nachweiserbringung gegenüber der Finanzbehörde vorzuhalten. Beabsichtigt der Verantwortliche abseits der in den jeweiligen Vorschriften festgelegten Zwecke eine Weiterverarbeitung (etwa die Erstellung einer Kundenhistorie), so benötigt er hierfür grundsätzlich eine Einwilligung gem. Art. 6 Abs. 1 S. 1 lit. a DSGVO von den betroffenen Personen.

Die Bedeutung und Reichweite des mit der Weiterverarbeitung zu anderen Zwecken in Verbindung stehenden Kompatibilitätstests (Art. 6 Abs. 4 DSGVO) ist derzeit noch nicht abschließend geklärt.

9. Das Bundesdatenschutzgesetz gibt es schon seit den Siebziger Jahren. Welche grundlegenden Dinge sind denn seit Mai 2018 neu zu beachten?

Im Wesentlichen ist das Meiste, was die DSGVO statuiert, nicht neu und sollte bereits aus dem bisherigen Datenschutzrecht bekannt sein. Es zeigt sich jedoch in der Praxis, dass es mit dem Umsetzungsstand in Sachen Datenschutz bei einem Gros der Betriebe nicht weit her ist und vermeintlich „neue" Regelungen – etwa personenbezogene Daten nach Wegfall des Verarbeitungszwecks zu löschen – mit der bisher gelebten Praxis nicht „vereinbar" sind.

Neben altbekannten im neuen Gewand, bringt die DSGVO allerdings doch die ein oder andere Neuerung. Hier kann man beispielsweise die neu eingeführte Rechenschaftspflicht des Art. 5 Abs. 2 DSGVO anführen. Verantwortlicher und Datenschutzbeauftragter sollten nunmehr wirkungsvolle Prozesse implementieren um jede Tätigkeit mit Datenschutzrelevanz zu protokollieren um rechtskonformes Handeln auch nachweisen zu können.

Eine weitere Neuerung – zumindest in dieser globalen Form – ist die starke Risikoorientierung der DSGVO und ein damit einhergehendes risikoadäquates Vorgehen bei der Umsetzung und Einhaltung der DSGVO. Einige Pflichten, wie beispielsweise die Meldepflicht bei Schutzverletzungen, werden durch den Begriff des Risikos nicht nur dominiert, sondern hängen auch davon ab. So ist eine Meldung an die Aufsichtsbehörde bei Schutzverletzungen bspw. erst bei einem normalen/mittleren Risiko vorgesehen, ein geringes Risiko reicht hierfür nicht aus.

Vieles ist nicht neu bzw. dürfte einem nicht neu vorkommen, sofern man – wie aus unserer Erfahrung nicht allzu viele – das bisherige Datenschutzrecht schon ernst genommen hat.

Kassel/Hamburg 13.10.2018