Mandanten-Informationsblatt

Ausgabe Nr. 01/2018

Inhalt

1. 4 Monate Datenschutzverordnung (DSGVO) – und was nun?

Die Monate vor Wirksamwerden der DSGVO dürften bei vielen Onlinehändlern und anderen Unternehmen etwa so ausgesehen haben:

- **Anfang 2017** = DSGVO? Was soll das sein?!
- **Mitte 2017** = Erstmal abwarten, wie sich das Thema DSGVO entwickelt…
- **Ende 2017** = Aha, eine Bitkom Studie zum schlechten Umsetzungsstand…
- **Anfang 2018** = Die Medien sind voll vom Thema Datenschutz…
- **April 2018** = Schaffen wir das in einem Monat?!

Seien wir ehrlich, die wenigsten Unternehmen haben bis Mai 2018 das gewünschte Datenschutzniveau umgesetzt. Doch was ist seitdem passiert? Große Abmahnwellen? Beschwerden von Kunden und Kontrollen von Aufsichtsbehörden? Unzählige meldepflichtige Datenpannen? Kunden fragen täglich die Übertragung Ihrer Daten zur Konkurrenz an (Datenportabilität)?

Wohl eher nicht.

2. DSGVO – Das sollten Sie über die Datenschutz-Grundverordnung wissen

Vergangenheit: Die Realität war geprägt von vollen E-Mail Postfächern! E-Mails mit Informationen zum neuen Datenschutz, massenhafte Abfragen von Einwilligungen und genervte Verbraucher. Die Rechtsunsicherheit verbreitete sich wie ein Lauffeuer. Ein Unternehmen nach dem anderen folgte dem Beispiel anderer. Doch gerade die vielfachen Kundeninformationen über den neuen Datenschutz per E-Mail machen deutlich, wie unklar die Anforderungen für viele scheinbar waren. Ein Gebot, dass Betroffene rückwirkend über Datenerhebungen zu informieren sind, ergibt sich aus der DSGVO eher nicht. Nun denn, die meisten wollten wohl einfach auf Nummer sicher gehen. Dies kann man nicht verübeln, schon gar nicht, wenn so oft mit dem Bußgeldhammer gedroht wurde.

2.1 Veränderungen aus Sicht der Aufsichtsbehörden

Aus Perspektive der Aufsichtsbehörden kann man jedoch klar sagen, dass sich einiges getan hat: eine Fülle von Anfragen, welche aufgrund der Masse kaum zu beantworten war oder sehr lange Antwortzeiten nach sich zog. Hilfe bei der Umsetzung mussten sich Unternehmen eher bei Anwälten und Unternehmensberatern als bei den Aufsichtsbehörden holen, die schlicht keine Kapazitäten hatten. Kurz darauf haben Behörden - quasi aus eigener Überforderung - eine „Schonfrist" in den ersten Monaten ausgerufen - danach soll aber gegen alle Verstöße konsequent vorgegangen werden.

2.2 Veränderungen aus Sicht der Unternehmen

Aus Perspektive der Unternehmen ist das dennoch unzufriedenstellend. Die Rechtsunsicherheit bleibt, auch wenn die mediale Panikmache spürbar abgeflacht ist, bleiben die strengen gesetzlichen Vorgaben und die drohenden Bußgelder.

Nach wie vor weiß keiner so genau, wie strittige Fragen von Behörden und Gerichten in (ferner) Zukunft bewertet werden. Einfacher wird die Lage insbesondere auch dadurch nicht, dass sich Ministerien völlig unterschiedlich zur Anwendung und etwa auch möglicher „Abschwächungen" der DSGVO, beispielsweise für Vereine, aussprechen.

3. Datenschutzstrategie, projektbasierte Planung und Basisdokumentation

So bleibt aus Sicht vieler nur eines übrig: das Gesetz nehmen wie es ist und die neuen Anforderungen mit gesunden Menschen- und Datenschutzverstand, nach bestem Wissen und Gewissen, umsetzen. Denn eines hat sich in den letzten Monaten schon gezeigt, nämlich dass man sich nicht in komplexen Detailfragen verlieren sollte. Es gibt Bereiche, wie die zuvor angesprochene Datenportabilität, in denen erstmal wenig „Ärger" zu erwarten ist. Aufsichtsbehörden haben mehrfach verlauten lassen, dass eine grundsätzliche Datenschutzstrategie, projektbasierte Planung und Basisdokumentation zunächst maßgeblich ist.

Hinweis: Also: Management mit dem Thema Datenschutz vertraut machen („Buy-In"). Verantwortliche benennen. Datenschutzdokumentation erstellen oder auf Vordermann bringen. Mitarbeiter, insbesondere die an der Schnittstelle zu den Kunden, auf die neuen Betroffenenrechte schulen. Transparenz gegenüber den Kunden schaffen.

4. Checkliste zur Wahrnehmung der DSGVO

Zukünftig: Um das Ganze nicht bei Stichworten zu belassen und etwas zu konkretisieren, findet sich nachfolgend eine Checkliste mit den wichtigsten To Do's:

- **Ist das Management im Boot?** Unternehmen sollten sich ein Datenschutzkonzept, gerne auch eine Datenschutzrichtlinie oder ein Datenschutzhandbuch auferlegen. Das kann nur vom Management initiiert werden. Internen (Mitarbeiter, Freelancer) können hier Handlungsanweisungen gegeben und Externen (Auftraggeber, Kooperationspartner) aufgezeigt werden, warum die Daten sicher sind oder wie diese geschützt werden. Auch das Gesamtprojekt „DSGVO-Umsetzung" im eigenen Unternehmen kann hier genauer erläutert werden, auch darauf zielen etwa Fragen der Behörden ab.

- **Verantwortliche benannt?** Wichtig ist eine Datenschutzorganisation innerhalb der bestehenden Organisation. Rollen müssen benannt sein, allen voran die gesetzliche Pflicht zur Benennung eines Datenschutzbeauftragten oder – je nach Unternehmensgröße – eines Datenschutzteams. Der Datenschutzbeauftragte soll laut Gesetz die Einhaltung der DSGVO kontrollieren, das Datenschutzteam oder Koordinatoren können z.B. für die operative Umsetzung mitverantwortlich sein. Eine gute Grundlage bildet übrigens der Fragebogen der niedersächsischen Aufsichtsbehörden, der an bestimmte Unternehmen verschickt wurde.

- **Datenschutzdokumente erstellt?** Das Verzeichnis von Verarbeitungstätigkeiten ist hier das A und O – ob sehr detailliert, toolbasiert oder eher grob per Excel-Arbeitsplatt. Das Gesetz schreibt die Mindestangaben vor (Art. 30 DSGVO), die gar nicht so umfangreich sind. Im Kern geht es um eine Auflistung der datenverarbeitenden Geschäftsprozesse (z.B. Newsletter, CRM, Bewerberprozess...). Das Dokument ist auf Anfrage den Aufsichtsbehörden zur Verfügung zu stellen und wird auch in der behördlichen Praxis gerne als Erstes angefragt. Eine gute, übersichtliche Dokumentation erspart womöglich einige weitere Fragen.

- **Datenschutzerklärung auf dem neuesten Stand?** Die meisten Anfragen erhielt die Beratungswelt wohl im Bereich der Datenschutzerklärungen. Alles was nach außen sichtbar ist, sollte noch schnell „glattgezogen" werden. So viel ist sicher: Das alte BDSG sollte keine Erwähnung mehr in der Datenschutzerklärung auf der Webseite finden. Stattdessen müssen die Kunden z.B. über die erweiterten Betroffenenrechte der DSGVO aufgeklärt werden. Eine verständliche und übersichtliche Datenschutzerklärung ist integraler Bestandteil der neuen Transparenzpflichten.

- **Auftragsverarbeitungsverträge beschlossen?** Erst mit der DSGVO kam so richtig Fahrt in das Thema, obwohl auch altes Datenschutzrecht bereits die beliebten „Datenschutzverträge" fordert. Neu ist das Bewusstsein vieler Dienstleister (in der Rolle des Auftragnehmers), die nun häufig proaktiv auf ihre Auftraggeber zugehen. Das liegt nicht am besonders ausgeprägten Datenschutzbewusstsein, sondern am neuen Haftungsmodell der DSGVO. Auftraggeber und Auftragnehmer sind gleichermaßen in der Pflicht zum Abschluss der Auftragsverarbeitungsverträge. Prüfen sollte man die oft in Template-Form übersendeten Verträge allemal. Nicht selten finden sich sehr zu strenge Haftungsregelungen, die vom Gesetz gar nicht gefordert sind.

- **Mitarbeiter geschult?** Datenschutz fängt zuerst in den eigenen vier (Büro-)Wänden an. Nur wenn die eigenen Mitarbeiter sich der Verantwortung und den neuen DSGVO-Anforderungen bewusst sind, können Kundenanfragen rechtssicher beantwortet und Datenschutzvorfälle erkannt werden. Vergessen werden darf auch nicht, dass Mitarbeiter selbst „Betroffene" im Sinne des Datenschutzrechts sind und diese somit – bis zu einem gewissen Rahmen - Auskunfts- und Löschansprüche gegen den Arbeitgeber geltend machen können.

- **Betroffenenrechte und Meldepflichten** – es ist sehr zu empfehlen, gerade für Onlineshops, wo sehr häufig Anfragen bzgl. Auskunft und Löschung von Kunden reinkommen, Prozesse und Musterantworten aufzusetzen und dem Betroffen fristgemäß (innerhalb eines Monats) antworten zu können. Das gilt auch für die Meldepflichten bei „Datenpannen", hier muss sogar innerhalb von 72h nach Kenntnis der

Behörde und unter Umständen sogar den Kunden/ Betroffenen Mitteilung gemacht werden. Das ist nur mit einem entsprechenden Data-breach-response-Prozess zu schaffen! Im Hinblick auf Newsletter und Mailings sollten Einwilligungen und Hinweis auf Widerrufsrechte noch einmal genau geprüft werden, um die Abmahngefahr durch Personen und Konkurrenten zu verringern.

- **Was ist mit der Datensicherheit?** Zunächst bleibt vieles beim Alten. Falls bereits Dokumentationen zu den „technischen und organisatorischen Maßnahmen" vorliegen, sollten diese geprüft werden. Falls noch keine Dokumentation der eigenen Sicherheitsmaßnahmen und technischen Infrastruktur vorliegt, ist diese zu erstellen – Formvorgaben existieren übrigens nicht! Vorlagen und Beispiele finden sich etwa im BSI IT-Grundschutz. Neu ist, dass die DSGVO neben den Schutzzielen Integrität, Vertraulichkeit und Verfügbarkeit auch die Belastbarkeit der Systeme voraussetzt. Schwachstellenanalysen und womöglich sogar unabhängige Pentests können sinnvoll sein. Eine Verpflichtung zur Beauftragung von spezialisierten Hackern ist natürlich nicht gegeben und viele Werbemails hierzu können getrost aussortiert werden. Letztlich entscheiden der Schutzbedarf der eigenen Systeme und Daten – es ist also eine risikobasierte Entscheidung zu treffen.

Mit dem vorgenannten gesunden Menschen- und Datenschutzverstand sind diese „Hausaufgaben" machbar. Gerade der in der DSGVO immer wieder hervorgehobene risikobasierte Ansatz lässt einen gewissen Spielraum bei der Umsetzung. Eine Datenschutzorganisation wird genauso wie Rom nicht an einem Tag erbaut, die oben genannten Grundsteine sollten jetzt aber in jedem Fall gelegt werden.

Über den Autor

Robin Houben, LL.M.
Rechtsanwalt und Partner – BFMT Legal
Robin Houben berät Unternehmen vom Start-Up bis zum Marktführer im IT- und E-Commerce-Recht, und Handels- und Gesellschaftsrecht.