LOSCHELDER

Newsletter Datenschutzrecht
September 2018

Inhalt

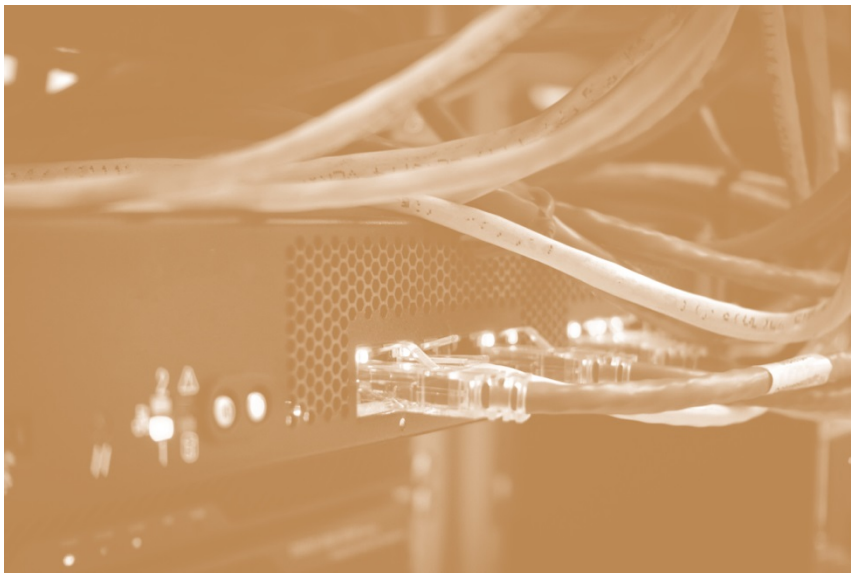
Erste Bilanz: Steigende Beschwerdezahlen, keine „Abmahnwelle“

Nach 100 Tagen DSGVO haben die Aufsichtsbehörden Anfang September eine erste Bilanz gezogen: Sie konstatieren ganz erheblich gesteigerte Beschwerdezahlen. Ausgeblieben ist aber die befürchtete Abmahnwelle jenseits des aufsichtsbehördlichen Tätigkeitsbereiches.

Die Aufsichtsbehörden haben seit dem 25.05.2018 deutlich mehr zu tun: Die Eingangszahlen haben sich teils mehr als verdoppelt, etliche Beschwerden sind anhängig. In der Behördensprache heißt dies dann, es erfolge eine deutlich stärkere Rechtewahrnehmung durch die Betroffenen. Wie Sie mit derartigen Beschwerden über die Datenverarbeitung in Ihrem Unternehmen umgehen können, erläutern wir Ihnen ebenfalls in diesem Newsletter.

Überdies sind in den vergangenen drei Monaten unter der DSGVO den Aufsichtsbehörden etliche Datenschutzverletzungen gemeldet worden, was angesichts der erheblichen Ausweitung der Meldepflichten unter der DSGVO nicht erstaunt: Zu melden ist jede Verletzung, bei der ein Risiko für die Betroffenen nicht ausgeschlossen werden kann; unter dem alten Datenschutzrecht galt die Meldepflicht nur für besonders schwerwiegende Fälle.

Nicht bewahrheitet hat sich die Befürchtung, ab dem 25.05.2018 würde eine neue Abmahnwelle rollen: Zwar kam es zu einzelnen Abmahnungen, z.B. wegen gänzlich fehlender Datenschutzerklärungen auf Homepages. Insgesamt blieb dies aber eher die Ausnahme. Womöglich – diese Vermutungen kursieren nunmehr – warten die „Abmahnspezialisten“ auf erste Sicherheit und machen Datenschutzverstöße auf diesem Weg erst dann geltend, wenn ausreichende Spruchpraxis von Behörden und Gerichten zur Konkretisierung der DSGVO-Anforderungen vorliegt.



Umgang mit Anfragen und Beschwerden

Der Datenschutz rückt nicht zuletzt mit dem Inkrafttreten der DSGVO immer mehr ins kollektive Bewusstsein. Zahlreiche Unternehmen haben dies zuletzt daran gemerkt, dass Anfragen, aber auch Beschwerden spürbar zugenommen haben. Wir geben Ihnen nachfolgende grundsätzliche Tipps zum Umgang mit derartigen Eingaben.

Im Ausgangspunkt ist es zunächst wichtig, dass alle Mitarbeiter sensibilisiert sind und das Datenschutzrecht betreffende mündliche oder schriftliche Anfragen unverzüglich an die Stellen bzw. Personen weiterleiten, die im Unternehmen hierfür zuständig sind (z.B. Datenschutzbeauftragter, Rechtsabteilung, Datenschutzkoordinator).

Wenn Sie eine Nachricht mit datenschutzrechtlichem Bezug erhalten, sollte diese auf ihren genauen Inhalt geprüft werden: Was möchte der Absender genau, Löschung, Auskunft allgemein oder für einen spezifischen Bereich oder wendet er sich gegen einen konkreten Datenverarbeitungsvorgang? Wenn das Verlangen unverständlich ist oder unklar ist, ob der Absender ein Beschäftigter, ehemaliger Beschäftigter oder Kunde ist, sollte gezielt nachgefragt werden. Dies ist auch insoweit wichtig, als eine Antwort nur dann und nur an denjenigen erfolgen darf, dessen Identität eindeutig feststeht. Im Zweifel ist ein Verlangen aber inhaltlich eher weit zu verstehen.

Wenn klar ist, wer der Absender ist und was er verlangt, sollte geprüft werden, ob das Verlangen auch erfüllt werden kann und muss sowie in welchem Umfang dies zu geschehen hat. Gerade bei Löschungsansprüchen muss genau geprüft werden, ob Angaben tatsächlich unwiederbringlich gelöscht werden dürfen (dazu auch unser Artikel in diesem Newsletter) oder ob diese nicht aufgrund gesetzlicher Vorgaben aufbewahrt werden müssen. Bei Auskunftsansprüchen muss geklärt werden, welcher tatsächliche Umfang leistbar ist und wie die zusätzlich zu übermittelnde Kopie erstellt und strukturiert wird. Immer ist zudem ein Augenmerk darauf zu richten, ob nicht ein Verweigerungsgrund oder Zahlungsanspruch besteht: Zwar sind sämtliche Betroffenenrechte grundsätzlich unverzüglich und unentgeltlich zu erfüllen. Dies gilt aber nicht im Fall exzessiver Anfragen, die verweigert werden dürfen oder für die – nach Wahl des Unternehmens – ein Entgelt verlangt werden kann. Exzessiv sind z.B. Mehrfachanfragen ohne Sachgrund oder auch offensichtlich missbräuchliche Anfragen (dazu noch weitergehend in unserem Oktober-Newsletter).

Noch nicht rechtssicher geklärt ist, wie lange solche Vorgänge im Unternehmen gespeichert werden dürfen. Die Behörden sind hier offenbar streng und gehen davon aus, dass sich der Verarbeitungszweck mit endgültiger Beantwortung erledigt hat. Das muss jedenfalls in solchen Fällen bezweifelt werden, in denen eine weitere Inanspruchnahme oder sogar ein behördliches oder gerichtliches Verfahren droht. Auch ist dies kaum in Einklang zu bringen mit dem Recht, die Erfüllung von Betroffenenrechten wegen unbegründeten Mehrfachanfragen zu verweigern oder hierfür ein Entgelt zu verlangen. In all diesen Fällen dürfte eine Speicherung aus Gründen der berechtigten Rechtsverfolgung erlaubt sein, solange eine Rechtsverfolgung möglich ist; dies dürfte regelmäßig

jedenfalls nicht länger als die regelmäßige Verjährungsfrist von drei Jahren der Fall sein.

Sollte sich ein Adressat unmittelbar an die Datenschutzaufsicht gewendet und diese entschieden haben, dass der Fall geprüft wird, wird das verantwortliche Unternehmen zunächst zur Auskunft und Anhörung aufgefordert. Das Vorgehen in einem solchen Verfahren sollte sorgsam abgewogen werden. Hierbei handelt es sich um ein Verwaltungsverfahren, in dem bestimmte Mitwirkungsobliegenheiten des Unternehmens bestehen. Erfahrungsgemäß ist dabei oft ein konstruktiverer Austausch mit der Datenschutzaufsicht als mit anderen Behörden möglich, da sich die Datenschutzaufsichtsbehörden aus ihrer historischen Entwicklung heraus vielfach auch als „Berater“ der Unternehmen verstehen. Gerne unterstützen wir Sie auch in solchen Verfahren.

Immer wieder Facebook: Neues von den Aufsichtsbehörden, Seiten-Insights und dem Like-Button

Facebook ist ein Dauerbrenner in Sachen Datenschutz und vor allem derzeit eine Fundgrunde scheinbar unlösbarer datenschutzrechtlicher Probleme. Nachdem das EuGH-Urteil vom Frühjahr 2018 zur Mitverantwortung für die Datenverarbeitung durch Facebook beim Betrieb von Fanpages für viel Unsicherheit gesorgt hat, haben sich inzwischen die Aufsichtsbehörden und auch Facebook selbst hierzu positioniert. Allerdings zeichnen sich bereits weitere offene Fragen zum Like-Button auf der eigenen Homepage sowie der Nutzung des Tracking-Tools „Custom Audience“ ab. Wir geben Ihnen hier einen ersten Überblick.

1. Fanpages: Laut EuGH ist der Fanpage-Betreiber mitverantwortlich für die Datenverarbeitung durch Facebook. Der Betreiber muss die Betroffenen also informieren und ist Adressat von Auskunfts- und ggf. Schadensersatzansprüchen bei Datenschutzverletzungen. Mit dieser

Rechtsunsicherheit lebten bisher viele Unternehmen, einige schalteten ihre Fanpages vorsorglich gleich komplett ab.

Am 5.9.2018 haben sich nun die deutschen Aufsichtsbehörden geäußert: Der Betrieb einer Fanpage ohne vertragliche Vereinbarung über die gemeinsame Verantwortlichkeit nach Art. 26 DSGVO mit Facebook sei rechtwidrig.

Hierauf hat Facebook eine Woche später reagiert und seine Bedingungen für Seiten-Insights ergänzt; sie gelten automatisch durch den weiteren Fanpage-Betrieb (https://www.facebook.com/legal/terms/page_controller_addendum). Ob dies ausreichend und angemessen ist, ist streitbar. Auffällig sind u.a. weitreichende Meldepflichten der Fanpage-Betreiber an Facebook und die Vorgabe des ausschließlichen irischen Gerichtsstands. Auch kann in Frage gestellt werden, ob damit umfassend den aufsichtsbehördlichen und gerichtlichen Anforderungen an eine wirksame Absicherung der Betroffenenrechte im Rahmen der tatsächlich gemeinsamen Verantwortung Rechnung getragen wird, denn letztlich verweist Facebook lediglich allgemein darauf, dass die DSGVO-Pflichten, insbesondere die Informationspflichten nach Art. 13, 14 DSGVO, nach „eigenem Ermessen“ erfüllt würden.

Sicher ist, dass sich hiermit das mit dem Fanpage-Betrieb verbundene datenschutzrechtliche Risiko – zumindest derzeit – deutlich reduziert hat. Wichtig ist dabei allerdings, die wesentlichen Inhalte der vertraglichen Vereinbarung nach Art. 26 DSGVO in der Datenschutzerklärung für die Fanpage zu beschreiben. Wesentlich in der aktuellen Facebook-Vereinbarung dürfte insbesondere sein, dass eine gemeinsame Verantwortlichkeit besteht, Facebook für die eigene Verarbeitung primär verantwortlich bleibt und die DSGVO-Pflichten, auch die Informationspflichten selbst erfüllt. Hier sollte dann, wie auch bisher schon empfohlen, auf die entsprechende Erklärung von Facebook verlinkt werden. Da Facebook sich weiterhin vorbehält, nach alleinigem Ermessen über die Verarbeitung der Nutzerdaten zu entscheiden, ist auch der Hinweis auf die fehlende Einflussmöglichkeit auf die Datenverarbeitung durch Facebook nach wie vor gerechtfertigt.

2. Like-Button: Vor der Tür steht indes bereits das nächste Facebook-Thema. In der vergangenen Woche verhandelte der EuGH die datenschutzrechtliche Verantwortungsfrage für den Like-Button, der auf Internetseiten integriert werden kann. Es scheint, als würde der EuGH auch hier zu einer Mitverantwortung des Website-Betreibers für die damit verbundene Datenverarbeitung durch Facebook kommen und damit auch hier eine vertragliche Vereinbarung nach Art. 26 DSGVO erforderlich werden. Dieses Thema sollte sorgsam beobachtet werden, wenn auf den von Ihrem Unternehmen verantworteten Websites „Like-Buttons“ integriert sind. Kommt es zu einer vertraglichen Vereinbarungen nach Art. 26 DSGVO, ist deren wesentlicher Inhalt in der Datenschutzerklärung zu beschreiben.

3. Facebook Custom Audience: Und zum dritten hat das Verwaltungsgericht Bayreuth Anfang Mai geurteilt, dass die Nutzung von Facebook Custom Audience für „passgenaue Werbung“ nur mit Einwilligung der

Betroffenen zulässig ist. Auch wenn diese Entscheidung noch nach altem Recht getroffen wurde, wäre sie unter Anwendung der DSGVO wohl nicht anders ausgefallen. Für eine möglichst rechtssichere Datenverarbeitung sollte eine Verwendung von Facebook Custom Audience daher nur mit Einwilligung der jeweiligen Kunden erfolgen.

Hintergrundinformationen

- EuGH, Urt. v. 05.06.2018, C-210/16 (Fanpage)
- DSK-Beschluss vom 05.09.2018 (Fanpage): https://www.datenschutz-berlin.de/pdf/publikationen/DSK/2018/2018-DSK-Facebook_Fanpages.pdf
- anhängig EuGH, C-40/17 (Like-Button)
- VG Bayreuth, Urt. v. 08.05.2018, Az. B 1 S 18.105 (Facebook Custom Audience)

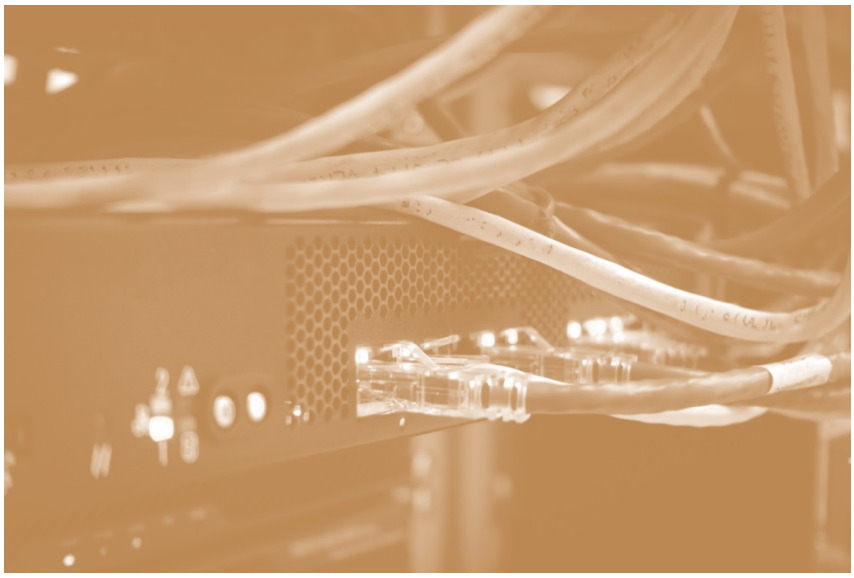
Fälle für die Datenschutzfolgenabschätzung: DSK-Blacklist

Für besonders risikoreiche Datenverarbeitungsvorgänge müssen Unternehmen eine sog. Datenschutzfolgenabschätzung durchführen. Die deutschen Aufsichtsbehörden haben hierzu inzwischen gemeinsam eine abgestimmte Liste mit einschlägigen Verarbeitungsvorgängen veröffentlicht (sog. Blacklist).

Führt eine geplante Datenverarbeitung voraussichtlich zu einem hohen Risiko für die Rechte und Freiheiten natürlicher Personen, z.B. durch die Verwendung neuer Technologien oder aufgrund von Art, Umfang, Umständen oder Zweck der Verarbeitung, so muss nach Art. 35 DSGVO vor Einführung eine Datenschutzfolgenabschätzung durchgeführt werden.

Wann von einem derart hohen Risiko ausgegangen werden muss, lässt sich ohne weitere Konkretisierung nicht rechtssicher feststellen. Hier hilft nun eine Blacklist der Datenschutzkonferenz. Die darin gelisteten Verarbeitungsvorgänge sind durch den Einsatz besonderer Techniken, einen erheblichen Umfang oder die Verarbeitung besonders sensitiver Daten gekennzeichnet, so z.B. der Betrieb eines Insolvenzverzeichnisses, Scoring durch Auskunfteien, Banken oder Versicherungen sowie die Geolokalisierung von Beschäftigten („GPS-Tracking“).

Blacklist DSK u.a. abrufbar über:
https://www.lda.brandenburg.de/media_fast/4055/DSFA_Muss_Liste_allgemein_180710.pdf



OLG Entscheidung zum Recht auf Löschung

Die – soweit ersichtlich – erste obergerichtliche Entscheidung zur Reichweite des Löschanspruchs nach Art. 17 DSGVO lehnt im Ergebnis einen Löschanspruch ab. Die Entscheidung bestätigt damit, dass eine sorgsame Prüfung im Einzelfall erforderlich ist, ob und in welchem Umfang geltend gemachte Betroffenenrechten bestehen und insbesondere, ob Daten tatsächlich unwiederbringlich gelöscht werden können und sollen.

Unter bestimmten Voraussetzungen sieht Art. 17 DSGVO einen Löschanspruch von Betroffenen vor, so insbesondere, wenn der Verarbeitungszweck entfallen ist oder die personenbezogenen Daten unrechtmäßig verarbeitet wurden. Hierauf stützte sich der Löschanspruch eines Betroffenen gegen Google, den das OLG Frankfurt mit Urteil vom 06.09.2018 ablehnte.

Laut Pressemitteilung des OLG Frankfurt kommt es für die Frage, ob ein Löschanspruch nach Art. 17 DSGVO im vorliegenden Fall besteht,

„auch nach Inkrafttreten der DS-GVO darauf an, ob das Interesse des Betroffenen im Einzelfall schwerer wiegt als das Öffentlichkeitsinteresse. Das durch die DS-GVO anerkannte „Recht auf Vergessen“ überwiegt entgegen einer Entscheidung des EuGH zum früheren Recht nicht grundsätzlich das öffentliche Informationsinteresse.“ Im Ergebnis sah das OLG Frankfurt ein Überwiegen der Kommunikationsfreiheit von Google und seinen Nutzern. Die informationelle Selbstbestimmung des Klägers musste dahinter zurücktreten, wobei auch entscheidend war, dass die ursprüngliche Presseberichterstattung rechtmäßig erfolgte.

Das Urteil ist nicht rechtskräftig, die Revision zum BGH zugelassen, „da die Rechtsfragen im Zusammenhang mit der DSGVO von grundlegender Bedeutung und höchstrichterlich nicht geklärt seien“.

Hintergrund: OLG Frankfurt, Urt. v. 06.09.2018, Az. 16 U 193/17 (Volltext noch nicht verfügbar; Ausführungen in der Pressemitteilung)

Wann dürfen Gesundheitsdaten & Co. verarbeitet werden?

Die Verarbeitung sog. „sensibler Daten“ wie z.B. Gesundheitsdaten, Angaben über politische Meinungen oder die ethnische Herkunft ist nur unter sehr engen Voraussetzungen erlaubt. Aber gelten diese erhöhten Anforderungen auch bereits für das Bild eines Brillenträgers (= Gesundheitsdatum?) oder die Filmaufnahme einer politisch motivierten Demonstration (= Angabe über politische Meinungen?)?

Der Wortlaut des Art. 9 DSGVO ist weit und differenziert nicht; das Bild des Brillenträgers informiert über die (mangelnde) Sehkraft als Gesundheitskriterium, die Teilnahme an einer bestimmten Demonstration über die politische Einstellung. Sinn und Zweck aber sprechen gegen die Einordnung solcher Angaben als Gesundheitsdatum: Art. 9 DSGVO

will die betroffenen Personen da besonders schützen, wo diese eines solchen Schutzes auch bedürfen. Die aktuelle Debatte um die Bilder von Brillenträgern und CSD-Demonstranten ist daher zu begrüßen. Gute Argumente sprechen dafür, unter Heranziehung aller anerkannten Auslegungsmethoden den Anwendungsbereich des Art. 9 DSGVO nicht möglichst weit zu fassen, sondern auf die tatsächlich sensiblen Daten zu beschränken. In vergleichbaren Fällen sollte auch über die Erlaubnis nach Art. 9 Abs. 2 lit. e DSGVO nachgedacht werden, welche die Verarbeitungssensibler Daten dann erlaubt, wenn diese Daten von der betroffenen Person „offensichtlich öffentlich gemacht“ wurden.

Es fehlt insofern allerdings bislang an einer Positionierung der Aufsichtsbehörden und die Diskussion in der Literatur zeigt, dass dies durchaus streitbar ist. Der rechtssicherste Weg führt daher dort, wo dies praktikabel ist, nach wie vor über die Einwilligung, die die womöglich sensiblen Daten auch explizit benennt.

Für alle weiteren Fragen rund um das Datenschutzrecht stehen Ihnen gerne zur Verfügung

Dr. Kristina Schreiber
+49(0)221 65065-337
kristina.schreiber@loschelder.de

Dr. Simon Kohm
+49(0)221 65065-200
simon.kohm@loschelder.de

Impressum

LOSCHELDER RECHTSANWÄLTE
Partnerschaftsgesellschaft mbB
Konrad-Adenauer-Ufer 11
50668 Köln

Tel. +49 (0)221 65065-0, Fax +49 (0)221 65065-110
info@loschelder.de
www.loschelder.de