LOSCHELDER

Newsletter Datenschutzrecht
Februar 2019

Inhalt

Zahl und Höhe der Bußgelder nimmt zu

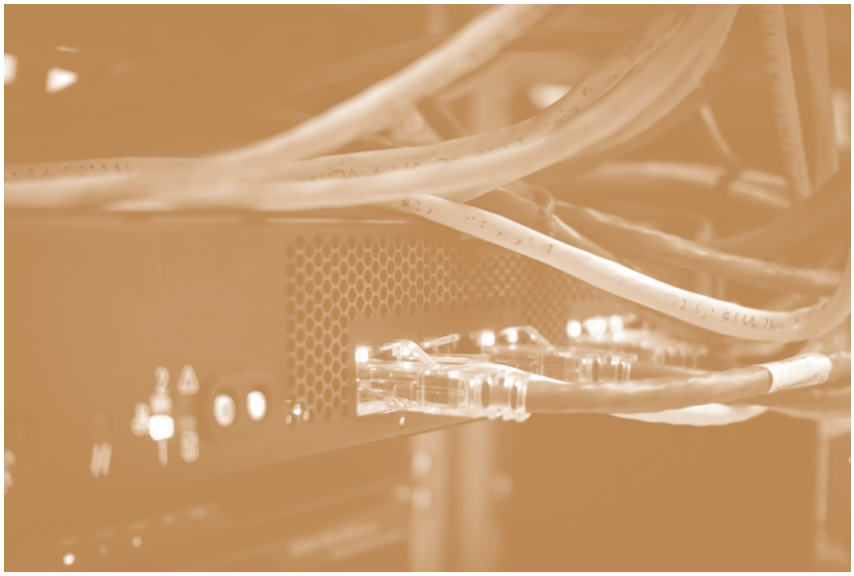
50 Millionen Euro Bußgeld gegen Google, 80.000 Euro für im Internet veröffentlichte Gesundheitsdaten, 20.000 Euro gegen die Social-Media Plattform Knuddels.de – bei Verstößen gegen die DSGVO können empfindliche Bußgelder drohen. Erst kürzlich kündigte Stefan Brink, der LfDI des Landes Baden-Württemberg, in einem Fernsehinterview an, dass im Jahr 2019 die Kontrollpraxis der Aufsichtsbehörden in ganz Deutschland zunehmen wird. Mit der Zunahme der Kontrollen steigt auch das Risiko, Adressat eines Bußgeldes zu werden. Um mögliche Bußgeldrisiken einschätzen und verhindern zu können, hilft der Blick auf die bisherige Bußgeldpraxis und laufende Verfahren.

Nach einem kürzlich erschienenen Artikel des Handelsblattes wurden bundesweit bislang 41 Bußgelder verhängt. Demnach stammten 33 der Bußgelder aus Nordrhein- Westfalen, 3 aus Hamburg, jeweils 2 aus Berlin und Baden- Württemberg und 1 aus dem Saarland. Es zeigte sich bisher also vor allem die nordrhein-westfälische Aufsichtsbehörde umtriebig bei der Verhängung von Bußgeldern. Aber auch die anderen Aufsichtsbehörden führen eine erhebliche Zahl von Verfahren. Allein der Bayerische Landesbeauftragte für den Datenschutz betreibt aktuell 85 Verfahren. Es ist also in nächster Zeit mit weiteren Bußgeldern zu rechnen.

Da die Pflichten aus der DSGVO zahlreich sind und nicht jeder Verstoß gleich schwer wiegt, muss jedes Unternehmen in der Datenschutz-Compliance Prioritäten setzen. Anhaltspunkte für die richtige Schwerpunktsetzung bietet der bisherige Fokus der Bußgeldpraxis. Dieser liegt (noch) auf dem Schutz sensibler Daten und dem Schutz vor zu invasiven Datenerhebungen:

- Unzureichender Schutz von sensiblen Daten (Kreditkarten- oder Kundendaten, Gesundheitsdaten) vor Einsichtnahme durch unbefugte Dritte:
  Bankkunden die Kontoauszüge anderer Kunden beim Online-Banking einsehen können, ein Schwerbehindertenausweis wurde einem falschen Patienten ausgehändigt oder ein ungeschütztes Speichermedium gelang in fremde Hände usw.
- Unzureichender Schutz von Webshops vor Hackerangriffen. Dadurch wurde in einem Webshop die unbefugte Kopie von Kredit- und Kundendaten möglich
- Unzulässige E-Mails mit Werbeinhalt
- Unverhältnismäßig invasive Überwachungsmaßnahmen:
  Die Aufzeichnung sämtlicher ausgehender und eingehender Anrufe bei einer Feuerwehr in Bremen oder die Videoüberwachung von ArbeitnehmerInnen und Kunden auch – aber nicht ausschließlich – in sensiblen Bereichen
- Offener und damit für jeden Adressaten sichtbarer E-Mail-Verteiler
- Dashcam-Nutzung
- Unzulässige Speicherung sensibler Daten auf Webservern, die Internet-öffentlich sind
- Fehlender Vertrag zur Auftragsverarbeitung

Das kooperative Verhalten nach Entdeckung eines Verstoßes wirkt sich im Regelfall positiv auf die Bußgeldhöhe aus. Im Fall Knuddels.de beispielsweise berücksichtigte die Aufsichtsbehörde den transparenten Umgang und die Umsetzungsbereitschaft des Unternehmens bußgeldmindern. Die Erfüllung der Meldepflichten (Art. 33, 34 DSGVO) und die Kooperation mit den Aufsichtsbehörden können sich also lohnen.



Bundeskartellamt untersagt Facebook Zusammenführung von Nutzerdaten

Auf Grundlage der Missbrauchsvorschriften reguliert das Bundeskartellamt (BKartA) mit einer jüngst erlassenen Entscheidung die Datenverarbeitung von Facebook: Bisher hat Facebook nicht nur Nutzerdaten von der Facebook-Website selbst einem Account zugeordnet, sondern auch Daten von seinen Tochterunternehmen (WhatsApp und Instagram) sowie von Webseiten Dritter, die mit Facebook verbunden sind. Verbraucher mussten dieser Praxis „freiwillig" über die Geschäftsbedingungen zustimmen, um die Facebook-Dienste WhatsApp und Instagram weiterhin nutzen zu können. Dies darf so nach Ansicht des BKartA nicht mehr weitergeführt werden.

Das Bundeskartellamt sieht einen Missbrauch einer marktbeherrschenden Stellung darin, dass Facebook die Zustimmung zur Zusammenführung der verschiedenen Daten zur Voraussetzung der Nutzung der Plattform macht. Das BKartA gibt Facebook daher vor, künftig eine „Zuordnung der Daten zum Nutzerkonto bei Facebook … nur noch mit freiwilliger Einwilligung des Nutzers" vorzusehen; ohne Einwilligung „müssen die Daten bei den anderen Diensten verbleiben und dürfen nicht kombiniert mit den Facebook-Daten verarbeitet werden". Dies gilt sowohl für WhatsApp und Instagram, als auch für Daten von Drittwebseiten.

Über das Missbrauchsverbot setzt das BKartA also faktisch Datenschutzrecht durch.BKartA Präsident Andreas Mundt fasst dies wir folgt

zusammen: „Wir nehmen bei Facebook für die Zukunft eine Art innere Entflechtung bei den Daten vor. Facebook darf seine Nutzer künftig nicht mehr zwingen, einer faktisch grenzenlosen Sammlung und Zuordnung von Nicht-Facebook-Daten zu ihrem Nutzerkonto zuzustimmen."

Die Entscheidung des BKartA ist noch nicht rechtskräftig.

Zu weiterführenden Informationen siehe die Pressemitteilung des Bundeskartellamts und das dort angefügte Hintergrundpapier unter https://www.bundeskartellamt.de/SharedDocs/Meldung/DE/Pressemitteilungen/2019/07_02_2019_Facebook.html

Notwendige Verträge im Datenschutzrecht

Das Bußgeld des Hamburgischen Beauftragten für Datenschutz und Informationsfreiheit gegen Kolibri Image in Höhe von 5.000 € ist Anlass, sich erneut der Auftragsverarbeitung und der gemeinsamen Verantwortlichkeit zu widmen. Der Hamburgische Beauftragte für Datenschutz und Informationsfreiheit verhängte ein Bußgeld gegen das Versandhaus mit der Begründung, es habe seine Pflicht, einen Auftragsverarbeitungsvertrag (AVV) zu schließen, verletzt. Für die Praxis interessant ist vor dem Hintergrund des Bußgeldes, in welchen Fällen vertragliche Regelungen nach der DSGVO erforderlich sind und wer sie zu stellen hat. Brisant an diesem Fall ist, dass ihm womöglich eine Beratung der Kolibri Image durch die hessische Aufsichtsbehörde vorangegangen ist.

Im Falle *Kolibri Image* verhängte die Aufsichtsbehörde ein Bußgeld, weil das verantwortliche Versandhaus mit seinem spanischen Dienstleister keinen Auftragsverarbeitungsvertrag (AVV) geschlossen hatte. Der Dienstleister stellte trotz mehrmaliger Aufforderung keinen AVV bereit, woraufhin sich das Unternehmen laut heise.de beim Hessischen BDI erkundigte, ob es verpflichtet sei, selbst einen AVV zu stellen. Der Hessische BDI bejahte die Frage. Das Unternehmen sah aber dennoch

von dem Abschluss eines AVV ab und kommunizierte dies wohl auch gegenüber der Behörde. Das Bußgeld seitens des Hamburgischen BDI, an den der hessische Kollege den Sachverhalt weitergeleitet hatte, folgte prompt. Ob dies zulässig ist, aus einer Beratung mithin überhaupt ein Bußgeld folgen darf, ist durchaus streitbar, da die den Aufsichtsbehörden obliegende Beratungsfunktion so in vielen Fällen wohl ad absurdum geführt würde.

Aus dem Fall lassen sich aber auch zwei Lehren ziehen.. Es ist erstens nicht sinnvoll der Aufsichtsbehörde mitzuteilen, dass man nicht beabsichtigt, einen Datenschutzverstoß abzustellen. Dies gilt – trotz „Chinese Wall" zwischen Beratung und Bußgeld – auch, wenn man sich an die Aufsichtsbehörde nur zur Beratung gewandt hat.

Zweitens entfällt die *eigene* Pflicht des Verantwortlichen zum Abschluss eines AVV nicht, nur weil der Auftragsverarbeiter der mehrmaligen Aufforderung einen unterschriebenen AVV bereitzustellen, nicht nachkommt. Denn die DSGVO verlangt in zwei Konstellationen explizit, dass die an der Verarbeitung von personenbezogenen Daten Beteiligten ihre datenschutzrechtlichen Verantwortungsbereiche in vertraglicher Form regeln. Nach Art. 26 Abs. 1 Satz 2 DSGVO müssen gemeinsam Verantwortliche in transparenter Form und genau festlegen, wer welche Pflichten aus der DSGVO, z.B. die Informationspflichten, wahrnimmt. Für die Auftragsverarbeitung folgt die Notwendigkeit einer vertraglichen Regelung aus Art. 28 Abs. 3 Satz 1 DSGVO. Im Einzelfall kann allerdings die Abgrenzung zwischen gemeinsamer Verantwortlichkeit und Auftragsverarbeitung schwierig sein:

Maßgeblich für die Qualifizierung ist, wer über den Zweck (das „ob") und die Mittel (das „wie") der Verarbeitung entscheidet. Die konkrete Unterscheidung richtet sich allerdings nicht nach den Bezeichnungen des Vertrags. Diesen kommt lediglich eine „Indiz-Wirkung" zu. Entscheidend sind die tatsächlichen Gegebenheiten, insbesondere die tatsächlichen Kontrollverhältnisse. Legen die Parteien die Zwecke der und die Mittel zur Verarbeitung gemeinsam fest und können somit beide Seiten „mitentscheiden", sind sie gemeinsam verantwortlich (z. B. gemeinsame Pflege und Nutzung einer gemeinsamen Kundendatenbank). Stellt sich das Verhältnis hingegen eher als ein weisungsgebundenes Über-/ Unterordnungsverhältnis dar, liegt eine Auftragsverarbeitung näher (Miete von softwareunterstützten Datenräumen).

Beide Beteiligungsformen haben unterschiedliche Mindestanforderungen an den vertraglichen Inhalt – der Abschluss eines Vertrages ist in beiden Fällen vorgeschrieben. Dieser ist für den Auftragsverarbeitungsvertrag bereits durch Art. 28 DSGVO selbst weitgehend vorgegeben und von den Aufsichtsbehörden bereits in verschiedenen Musterverträgen ausdekliniert worden. Gemeinsam Verantwortliche haben dagegen einen deutlich weitergehenden Gestaltungsspielraum; auch hierzu ist kürzlich ein Aufsatz von Kristina Schreiber in der Zeitschrift für Datenschutz erschienen („Gemeinsame Verantwortlichkeit gegenüber Betroffenen und Aufsichtsbehörden", in: *ZD 2/2019, S. 55 ff.*), den wir Ihnen auf Wunsch gerne auch per E-Mail übermitteln. Das aktuelle Bußgeld in Sachen Kolibri Image sollte zum Anlass genommen werden, den internen Bestand datenschutzrechtlicher Verträge unter die Lupe zu nehmen, soweit dies noch nicht geschehen ist.

Interessenabwägung muss dokumentiert werden

Wesentlicher Bestandteil einer sorgfältigen und rechtssicheren Datenschutz-Compliance ist ihre Dokumentation. Das EU-Datenschutzrecht sieht eine klare Rollenverteilung vor: Derjenige, der unternehmerisch personenbezogene Daten verarbeitet, ist zum Nachweis der ordnungsgemäßen Datenverarbeitung vollumfänglich verpflichtet, Art. 5 Abs. 2 DSGVO. Eine besondere Rechenschaftspflicht besteht auch für die Interessenabwägung, wenn eine Datenverarbeitung auf berechtigte Interessen nach Art. 6 Abs. 1 lit. f DSGVO gestützt werden soll.

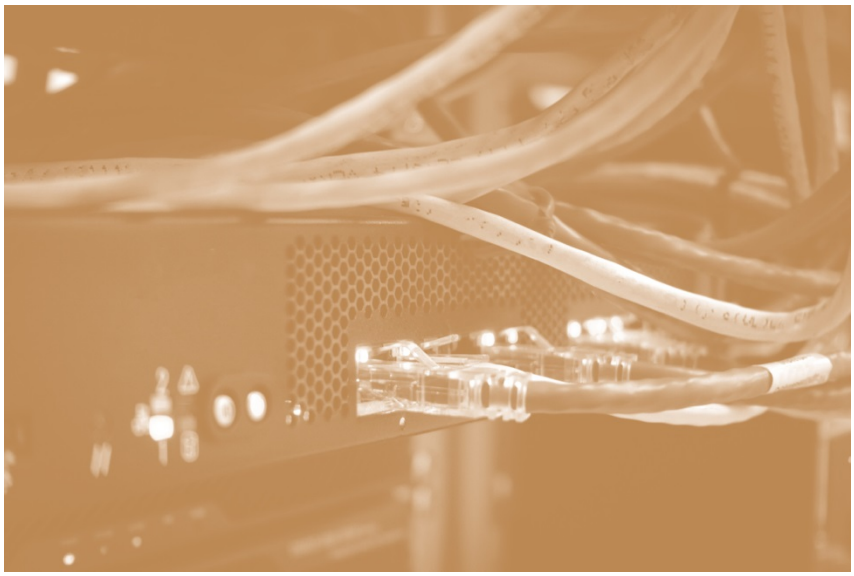
Jede Verarbeitung personenbezogener Daten ist verboten, außer sie ist gerechtfertigt. Art. 6 Abs. 1 lit. a bis f zählen hierzu verschiedene Rechtfertigungsgründe auf. So kann eine Verarbeitung z.B. gerechtfertigt sein, weil der Betroffene darin eingewilligt hat (Buchst. a)) oder die Verarbeitung zur Erfüllung einer gesetzlichen Verpflichtung erforderlich ist (Buchst. c) z. B. buchhalterische Aufbewahrungspflichten). In vielen Fällen bleibt jedoch nur der Rückgriff auf das überwiegende berechtigte Interesse zur Datenverarbeitung nach Art. 6 Abs. 1 lit. f DSGVO.

Es genügt aber nicht allein, dass die Verarbeitung tatsächlich gerechtfertigt ist. Die Ordnungsmäßigkeit der gesamten Datenverarbeitung muss zudem jederzeit durch entsprechende Dokumente nachgewiesen werden können (Art. 5 Abs. 2 DSGVO). Dies betrifft die Inhalte (wann darf ich personenbezogene Daten wie verarbeiten) ebenso, wie die Sicherstellung der Datensicherheit (technische und organisatorische Maßnahmen). Und darüber hinaus auch die für Art. 6 Abs. 1 lit. f erforderliche Interessenabwägung. Gerade an diese Dokumentationspflicht wird nach den Erfahrungen aus unserer Beratung nicht immer gedacht.

Von den Rechtfertigungsgründen erfordert das überwiegende berechtigte Interesse den größten Dokumentationsaufwand. Um das Vorliegen eines überwiegenden berechtigten Interesses prüfen zu können, muss erstens ein berechtigtes Interesse des Verantwortlichen oder eines Dritten ermittelt werden (z. B. Verarbeitung für Direktwerbung), zwei-

tens die Verarbeitung für den Zweck erforderlich sein und drittens das berechtigte Interesse des Verantwortlichen oder des Dritten die Interessen, Grundrechte und Grundfreiheiten der betroffenen Personen überwiegen. Letzteres wiederum erfordert eine Interessenabwägung, d. h. eine Ermittlung der Interessen der (potenziell) Betroffenen (z. B. Persönlichkeitsschutz) und eine Abwägung mit dem berechtigten Interesse des Verantwortlichen oder des Dritten an der Verarbeitung.

Wie nimmt man nun sinnvollerweise eine Dokumentation vor? Wesentlich ist, dass der Dreiklang für eine Anwendung des Art. 6 Abs. 1 lit. f DSGVO elektronisch oder schriftlich notiert und so in einer nachweisfähigen Form dokumentiert wird. Die Erläuterungen müssen plausibel sein; Kontrollmaßnahme mag die Lektüre eines unbeteiligten Dritten sein, etwa eines mit dem konkreten Verarbeitungsvorgang nicht befassten Kollegen. Bestätigt auch dieser die Plausibilität und ist überzeugt, spricht dies für eine hinreichende Dokumentation. Es bietet sich dabei an, bei Erstellung oder Aktualisierung des Verarbeitungsverzeichnisses direkt die Interessenabwägung zu notieren, wenn eine Verarbeitung mit dem berechtigten Interesse gerechtfertigt werden soll. Es genügt aber auch jede andere gesonderte schriftliche oder elektronische Fixierung (Email, Notizen etc.). Wichtig ist, dass die Abwägung für jeden Einzelfall, also nicht automatisiert oder pauschal erfolgt. Zudem muss sie spätestens im Fall einer aufsichtsbehördlichen Untersuchung unmittelbar auffindbar sein.



For your eyes only! Datenschutz und Geheimschutz – Veranstaltungshinweis!

Ein aktueller Gesetzentwurf lässt auch den Schutz von Betriebs- und Geschäftsgeheimnissen ohne Personenbezug für Unternehmen immer dringender werden. Interessant und mit Blick auf die Unternehmensressourcen wichtig ist, inwiefern ein wirksamer Schutz mit bereits datenschutzrechtlich gebotenen Maßnahmen verbunden werden kann,

die im Zuge der DSGVO mit regelmäßig großem Aufwand implementiert wurden.

Neu und für Unternehmen zu beachten, ist das im Entwurf vorliegende Gesetz zum Schutz von Geschäftsgeheimnissen vor rechtswidrigem Erwerb sowie rechtswidriger Nutzung und Offenlegung. Eine wesentliche Neuerung des Gesetzes ist, dass sich Unternehmen, die sich später auf einen Geheimschutz berufen wollen, nachweisen müssen, im Vorfeld aktiv schützende Maßnahmen ergriffen zu haben.

Hier stellt sich in der Praxis die Frage, welchen Handlungsbedarf es konkret gibt und etwa, ob bereits ergriffene datenschutzrechtliche Maßnahmen fruchtbar gemacht werden können. So sind Unternehmen nach der DSGVO unter anderem bereits verpflichtet, ein Verarbeitungsverzeichnis zu führen (Art. 30 DSGVO) und technisch organisatorische Maßnahmen zur Datensicherheit zu implementieren (Art. 32 DSGVO). Unternehmen, die Daten im Auftrag verarbeiten oder Datenverarbeitung als Kerntätigkeit betreiben, verfügen darüber hinaus oftmals über Zertifizierungen betreffend die Datensicherheit bzw. IT-Sicherheit. Existierende Maßnahmen, wie die Datenkategorisierung und Sicherheitseinstufung können hier auch für einen wirksamen Geheimschutz nach den neuen gesetzlichen Regelungen fruchtbar gemacht werden. Der Schutz von Betriebs- und Geschäftsgeheimnissen hat darüber hinaus eine starke arbeitsrechtliche Komponente, wenn es darum geht, Mitarbeiter entsprechend zu verpflichten bzw. die vorhandenen Mechanismen zu überprüfen.

Wir informieren Sie im Rahmen unserer Mandantenveranstaltung am 21.02.2019 in Köln über die neuen gesetzlichen Änderungen und geben praxistaugliche Ratschläge für deren Umsetzung! Über Ihre Teilnahme an unserer Veranstaltung würden wir uns freuen – möglichst mit Anmeldung bis zum 12.02.2019 per E-Mail an katrin.schwarz@loschelder.de.

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

Dr. Lucyne Ghazarian
+49 (0)221 65065-222
lucyne.ghazarian@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