LOSCHELDER

Newsletter Datenschutzrecht
Dezember 2018

Inhalt

Hilfestellung bei Datenpannen: Wann besteht eine Meldepflicht?

Wann ist ein verloren gegangener USB-Stick eine meldepflichtige Datenpanne und wann nur ein bloßes Ärgernis? Die Antworten auf diese und viele andere Fragen enthält der Leitfaden des Hamburgischen Beauftragten für Datenschutz und Informationsfreiheit.

Der Beauftragte hat den Verantwortlichen mit dem neuen Leitfaden ein hilfreiches Papier an die Hand gegeben, wie mit Verletzungen der Integrität personenbezogener Daten umzugehen ist. Insbesondere räumt der Leitfaden auch mit dem Irrtum auf, dass jeder Datenverlust oder jede Datenbeschädigung gleich den Behörden gemeldet werden muss.

Die Pflicht, sog. „Datenpannen" den Behörden zu melden oder Betroffene darüber zu informieren, folgt aus Art. 33, 34 DSGVO. Allerdings stellt nicht jede Datenverletzung, legaldefiniert in Art. 4 Nr. 12 DSGVO, eine solche Datenpanne dar. Um eine Meldepflicht auszulösen, muss zunächst eine Datenverletzung, „Data Breach", vorliegen, d. h. ein Sicherheitsbruch, bei dem Daten unrechtmäßig Dritten offenbart oder infolge eines Sicherheitsbruchs gelöscht oder zeitweise unzugänglich gemacht worden sind. Zusätzlich muss ein aus der Datenverletzung folgendes Risiko für die betroffenen Personen möglich sein.

Als Beispiele für eine Datenverletzung, Sicherheitsbrüche nennt das Papier Hacking und Datendiebstahl sowie SQL-Lücken, Bugs im Webserver, verlorengegangene USB-Sticks oder Laptops, unrechtmäßige Übermittlung sowie der Einbruch in Serverräume, die mit dem Verlust oder der Zerstörung von Hardware oder dem Auslesen von Datenträgern einhergehen. Für die Annahme einer Datenpanne muss aber nicht zwingend ein Sicherheitsmechanismus überwunden werden. Auch eine Fehladressierung von E-Mails kann eine Datenpanne darstellen. Um am Ende aber von einer Datenpanne sprechen zu können, muss ein entsprechender Erfolg eingetreten sein, d.h. es muss ein Zugriff auf die Daten stattgefunden haben.

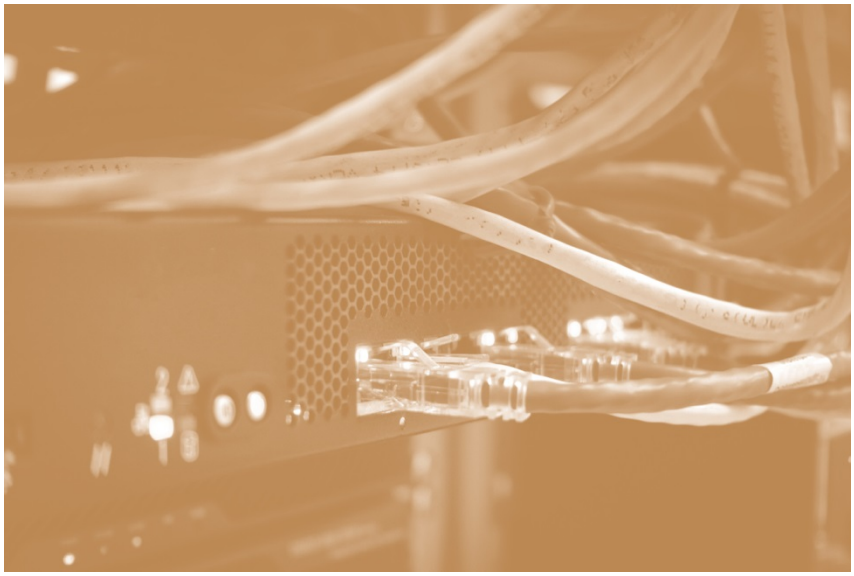
Eine Meldepflicht an die Behörde hat aber noch darüber hinausgehende Voraussetzungen. Gemeldet werden muss seine Datenpanne nur, wenn sie ein Risiko für die Rechte und Freiheiten Anderer begründet. In dem Beispiel des gestohlenen USB-Sticks nimmt die Aufsichtsbehörde z.B. kein Risiko an, wenn der Stick selbst und nicht nur die enthaltenen Dokumente passwortgeschützt ist. Nur wonach entscheidet sich, ob ein solches Risiko besteht? Schließlich gibt es auch Programme, mit denen der Passwortschutz umgangen werden kann. Das Risiko bemisst sich nach der Schwere des Schadens und dessen Eintrittswahrscheinlichkeit. Je höher der anzunehmende Schaden, desto geringer sind die Anforderung an die Wahrscheinlichkeit seines Eintritts. Hinweise, welche Kriterien bei der Risikoabwägung berücksichtigt werden dürfen, gibt das Arbeitspapier „Working Paper" 250 der Art. 29 Gruppe.

Ob zusätzlich zur Meldung bei der Aufsichtsbehörde auch noch die betroffenen Personen informiert werden müssen, richtet sich nach Art. 34 Abs. 1 DSGVO. Eine solche Informationspflicht besteht nur, wenn voraussichtlich ein *hohes* Risiko für die persönlichen Rechte und Freiheiten aus der Datenverletzung folgt. Ein solches hohes Risiko kommt ausweislich des Leitfadens z.B. in Betracht, wenn eine Werbe-E-Mail

mit offenem Mailverteiler (cc statt bcc) an eine große Empfängerzahl geschickt wird.

Der Leitfaden enthält eine Liste mit Beispielen, wann eine Meldepflicht an die Behörde und an die Betroffenen besteht, die für die Einordnung eigener Fälle hilfreich ist. Letztlich wird sich die Frage nach einer Meldepflicht (an Behörden und ggf. auch an Betroffene) in den meisten Fällen nur anhand einer Betrachtung aller Aspekte des Einzelfalls beantworten lassen. Es gilt dann, die Risiken und Gefahren für die Betroffenen nachvollziehbar einzuordnen und eine bewusste – und dokumentierte – Abwägungsentscheidung zu treffen.

Liegt nach der Beurteilung des Verantwortlichen eine meldepflichtige Datenpanne vor, muss diese möglichst unverzüglich erfolgen – spätestens jedoch nach 72 Stunden. Die Frist beginnt ab Kenntnis von der Datenpanne, ohne dass erforderlich wäre, dass bereits alle Umstände bekannt sind. Unbedingt ratsam ist es, nach Kenntnis unverzüglich den Datenschutzbeauftragten und ggf. externe technische und / oder rechtliche Unterstützung einzuholen. Darüber hinaus sind die umfangreichen internen Dokumentationspflichten zu beachten.



Erlaubnistatbestand „berechtigtes Interesse“ zur Datenverarbeitung weit zu verstehen

Die Verarbeitung personenbezogener Daten ist bekanntlich nur rechtmäßig, wenn ein Erlaubnistatbestand gefunden wird. Insbesondere Art. 6 DSGVO enthält eine ganze Reihe solcher Erlaubnistatbestände – einer von ihnen ist dabei besonders wertungsoffen und in der Verordnung selbst wenig konturiert: Das überwiegende berechtigte Interesse an einer Datenverarbeitung. Erste Rechtsprechung hilft nun bei der rechtssichereren Konkretisierung dieses Erlaubnistatbestands.

Praktische Schwierigkeiten ergeben sich oftmals bei der Frage, wann ein berechtigtes Interesse vorliegt. Das Oberlandesgericht München (Urteil vom 24. Oktober 2018, Az. 3 U 1551/17) hat sich jüngst für eine

weite Auslegung des berechtigten Interesses in Art. 6 Abs. 1 lit. f DSGVO ausgesprochen. Nicht nur rechtliche, sondern auch wirtschaftliche und ideelle Interessen können ein berechtigtes Interesse zur Datenverarbeitung begründen. Wesentliches Gewicht zugunsten eines berechtigten Interesses und damit dessen Überwiegen gegenüber den schutzwürdigen Betroffeneninteressen maß das Gericht auch der Berufsfreiheit des Verantwortlichen zu. Nebenbei gab das Gericht weitere Hinweise, welche Gesichtspunkte bei der Abwägung relevant sein können, so z.B., ob die Daten dem höchstpersönlichen Bereich der betroffenen Personen entstammen, ein besonderes Know-how von diesen betreffen oder die Verarbeitung wirtschaftliche Nachteile für die Betroffenen mit sich bringt. Wesentlich bleibt im Rahmen der Abwägung überdies weiterhin der Anhaltspunkt aus Erwägungsgrund 47 DSGVO, ob die Betroffenen mit der in Rede stehenden Verarbeitung „vernünftigerweise“ rechnen können.

Gerade der Erlaubnistatbestand eines überwiegenden berechtigten Interesses hat denn auch in der Praxis eine wesentliche Bedeutung: Er ist in Fällen, in denen die Verarbeitung weder zur Vertragserfüllung erforderlich, noch gesetzlich geboten ist, oft die einzig mögliche und gegenüber einer „Einwilligung“ der Betroffenen vorzugswürdige Alternative. Indes ist seit Einführung der DSGVO der Irrtum weit verbreitet, dass (beinahe) jede Verarbeitung personenbezogener Daten nur im Einverständnis mit dem Betroffenen erfolgen darf. Rechtlich hätte eine solche Annahme zur Folge, dass Unternehmen für jede Datenverarbeitung die Einwilligung der betroffenen Personen einholen müssten. Dies ist nicht der Fall: Zwar sieht die DSGVO vor, dass jede Datenverarbeitung erlaubt sein muss, zurückgegriffen werden kann hierfür indes alternativ zu einer oft unpraktikablen und teils – insbesondere in Kopplungsfällen – sogar unzulässigen Einwilligung auch auf einen der weiteren Erlaubnistatbestände der DSGVO. In all diesen alternativen Fällen ist eine ausdrückliche Zustimmung des Betroffenen zur Datenverarbeitung gerade nicht erforderlich.

Eine der in der Praxis relevanten Fallgruppen ist die Datenverarbeitung aufgrund des berechtigten Interesses des Verantwortlichen oder eines Dritten. Liegt ein solches berechtigtes Interesse vor überwiegen nicht gleichzeitig die Interessen des Betroffenen, ist eine Datenverarbeitung erlaubt und zulässig.

Erstes DSGVO-Bußgeld nach Datenpanne

Ende des vergangenen Monats ist das erste Bußgeld infolge eines DSGVO-Verstoßes gegen die Datensicherheitsvorgaben verhängt worden – nach einer Datenpanne mit unzähligen „verlorenen" E-Mail-Adressen und Passwörter von Nutzern eines Chat-Portals. Die Kooperations- und Investitionsbereitschaft des verantwortlichen Unternehmens wirkte sich dabei bußgeldmindernd aus.

Verhängt wurde das Bußgeld durch die LfDI Baden-Württemberg. Dem betroffene Social Media Anbieter (ein Chatportal namens Knuddels) wurde nur ein vergleichsweise niedriges Bußgeld i.H.v. 20.000 Euro auferlegt (zur Erinnerung: bis zu 20 Mio. Euro oder 4% des Jahresumsatzes wären theoretisch möglich). Das LfDI berücksichtigte bei der Bußgeldbemessung zugunsten des Unternehmens dessen umfassende Kooperationsbereitschaft sowie erhebliche bereits getätigte und vorgesehene Investitionen in eine verbesserte Datensicherheit. So ergriff der Social Media Anbieter in Kooperation mit der Behörde IT-Sicherheitsmaßnahmen, die das Unternehmen am Ende einen sechsstelligen Euro-Betrag kosten werden. In ihrer Pressemitteilung betont die Behörde explizit, dass sich das transparente und kooperative Verhalten des Unternehmens bußgeldmindernd ausgewirkt habe.

Dieser erste „Bußgeld-Fall" zeigt, dass die Behörden auch auf dieser Ebene aktiv werden. Ein Datenschutzverstoß kann Unternehmen teuer zu stehen kommen, auch wenn das Bußgeld im vorliegenden Fall und nicht zuletzt wegen der erheblichen Investitionen vergleichsweise niedrig ausgefallen ist. Mit transparentem und kooperativem Verhalten sowie einer verbesserten Datenschutz-Compliance kann also zumindest auf die Bußgeldhöhe Einfluss genommen werden.

Löschfristen und Lösch-Tools im Fokus

Mit Inkrafttreten der DSGVO sind auch Löschkonzepte in Unternehmend zunehmend wichtiger geworden; die Aufbewahrungsdauer muss für jedes personenbezogene Datum im Unternehmen bestimmt sein, Löschungen müssen datenschutzkonform möglich sein. Ob dies tatsächlich der Fall ist, untersucht derzeit das BayLDA, fokussiert auf SAP-ERP-Systeme.

Dies sollte auch für Sie Anlass sein, das Vorhandensein eines effektiven Löschkonzepts zu überprüfen und ggf. im Zuge der Erstumsetzung eingeführte allgemeine Löschgrundlagen auf ihre Umsetzung im Unternehmen zu überprüfen. Wesentliche Bausteine eines solchen Löschkonzepts sind die Vorgabe spezifischer Aufbewahrungsfristen für einzelne Datenarten, nicht undifferenziert für ganze Datensätze. Weitere Bausteine – auch in der Datenschutzrichtlinie integrierbar – müssen u.a. den Umgang mit Archivierungs- und Backup-Systemen regeln und – orientiert an der jeweiligen Schutzklasse der betroffenen Daten – in technischer Hinsicht Art und Weise der Löschung / Vernichtung regeln. Hilfestellungen bieten hierbei neben der anwaltlich- und technischen Beratung im Einzelfall der Baustein 60 des Standard-Datenschutzmodells der Aufsichtsbehörden (wir berichteten im November-Newsletter) sowie die DIN 66399.

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