LOSCHELDER

Newsletter Datenschutzrecht

Juni 2019

Inhalt

Datenpanne – und nun?

Laut DSGVO sind die für die Datenverarbeitung Verantwortlichen verpflichtet, bestimmte Datenpannen proaktiv bei der Datenschutzbehörde zu melden. Vielerorts besteht allerdings Unsicherheit, ab wann eine solche Meldepflicht eingreift, sodass oftmals geringfügige Verstöße rein vorsorglich gemeldet werden. Zu dieser Einschätzung kommt auch die Landesbeauftragte für Datenschutz und Informationsfreiheit (LDI) NRW, die laut ihrem aktuellen Jahresbericht allein seit dem 25. Mai 2018 rund 1.200 Meldungen erhalten hat. Zum Vergleich: Von Januar bis Mai 2018 wurden lediglich 61 Datenpannen gemeldet. Wie geht man also am besten mit einer Datenpanne und der Meldepflicht um und wann greift sie wirklich?

Typische Beispiele einer Datenpanne sind etwa Angriffe durch Hacker, ein verloren gegangener USB-Stick mit personenbezogenen Daten, E-Mails mit offenen Verteilerlisten oder falsch adressierte Postsendungen bzw. E-Mails. Die DSGVO sieht vor, dass der Verantwortliche derartige Vorfälle an die Aufsichtsbehörde meldet, es sei denn, dass die Verletzung des Schutzes personenbezogener Daten voraussichtlich nicht zu einem Risiko für die Rechte und Freiheiten natürlicher Personen führt (Art. 33 DSGVO). Hat die Verletzung des Schutzes personenbezogener Daten voraussichtlich ein hohes Risiko für die persönlichen Rechte und Freiheiten natürlicher Personen zur Folge, muss der Verantwortliche zudem die Betroffenen informieren (Art. 34 DSGVO). Beide Vorschriften setzen also voraus, dass der Verantwortliche die Konsequenzen und Folgen der Datenpanne prognostiziert und eine Risikoanalyse anstellt.

Eine solche Risikoanalyse bereitet in der Praxis nicht unerhebliche Schwierigkeiten. So muss der Betroffenen unter hohem Zeitdruck (die Meldung muss innerhalb von 72 Stunden nach dem Vorfall erfolgen) den zumeist technischen Sachverhalt ermitteln und daraus die zutreffenden Schlüsse ziehen. Um die Durchführung einer solchen Risikoanalyse praxistauglicher zu machen, hat die Datenschutzkonferenz hierfür drei Schritte entwickelt, an denen man sich bei Bedarf orientieren kann:

1. Risikoidentifikation,
2. Abschätzung der Eintrittswahrscheinlichkeit und Schwere möglicher Schäden und
3. Zuordnung zu Risikoabstufungen.

Die Risikoidentifikation erfordert die Ermittlung der Fragen, welche Schäden überhaupt eintreten können (z.B. Diskriminierung, Profilerstellung, wirtschaftliche/gesellschaftliche Nachteile), durch welches Ereignis es zu diesem Schaden kommen kann (z.B. unbefugte Verarbeitung, unbefugte Offenlegung von Daten, Verarbeitung nicht richtiger Daten) und wovon wiederum der Eintritt eines solchen Ereignisses abhängt (Risikoquellen wie z.B. rechtswidrig handelnde Beschäftigte des Verantwortlichen). Je nach Eintrittswahrscheinlichkeit und Schwere möglicher Schäden muss das konkrete Risiko letztlich als „geringes Risiko“, „(normales) Risiko“ oder „hohes Risiko“ eingeordnet werden können. Aus dieser Zuordnung ergibt sich dann die weitere Vorgehensweise: Eine Datenpanne muss jedenfalls dann nicht (zwingend) gemeldet werden, wenn hierdurch die Rechte der natürlichen Person gar nicht verletzt werden können oder wenn eine (zwar mögliche) Verletzung nicht wahrscheinlich ist. Aufgrund der strengen Dokumentationspflichten (vgl. Art. 5 Abs. 2 DSGVO) tun Verantwortliche gut daran, Datenpannen und die daraus folgenden Maßnahmen umfassend zu dokumentieren. Das empfiehlt sich nicht zuletzt auch aus zivil-, haftungs- und versicherungsrechtlichen Gründen, da die Konsequenzen von Datendiebstählen oder Hacking-Angriffen äußerst weitreichend sein können.

Datenschutzaufsicht: Zulässigkeit von Fragebögen?

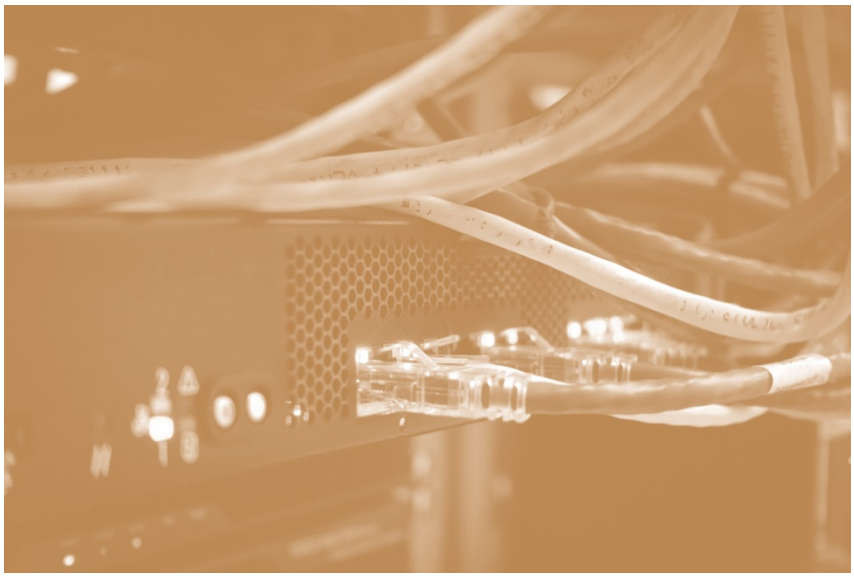
Seit Inkrafttreten der DSGVO erfragen die Datenschutzbehörden einiger Bundesländer den aktuellen Umsetzungsstand in Unternehmen und Kommunen durch Fragebögen. So wurden bereits im Juni 2018 ca. 50 niedersächsische Unternehmen kontaktiert, während in Thüringen sogar rund 17.000 Unternehmen entsprechende Anschreiben erhielten. Dieses flächendeckende Vorgehen hat jüngst die Aufmerksamkeit der Landespolitik erregt. Diskutiert wird, ob und in welchem Umfang (auch anlasslose) Fragebögen zulässig sind und ob diese beantwortet werden müssen.

Der Thüringer Landesdatenschutzbeauftragte Lutz Hasse sorgte mit seinem Fragebogen, welcher Ende 2018 an rund 17.000 Unternehmen und zahlreiche Kommunen versendet worden ist, für Aufsehen. Man wolle mit Hilfe der Fragebögen einen Überblick über die bisherige Umsetzung der DSGVO, über den Umfang der verarbeiteten personenbezogenen Daten gewinnen, so Hasse. Von Seiten der Landespolitik erntete er hierfür heftige Kritik.

In rechtlicher Hinsicht stellt sich die Frage, ob das Versenden von Fragebögen rechtlich zulässig ist und ob Unternehmen zur wahrheitsgemäßen und vollständigen Beantwortung verpflichtet sind. Einerseits verpflichtet die DSGVO Unternehmen dazu, mit den Behörden zusammenzuarbeiten. Andererseits darf niemand dazu verpflichtet werden, sich durch eine eigene Aussage selbst belasten zu müssen, § 40 Abs. 4 Satz 2 BDSG. Trifft ein Fragebogen ein, sollte dieser daher nicht voreilig ausgefüllt und zurückgeschickt, aber auch nicht ignoriert werden. Ein Bußgeld droht für die Verweigerung der Aussage zwar nicht, aber die Behörde kann die Auskunft förmlich anordnen und vollziehen. Zudem hat sie noch weitergehende Aufsichtsbefugnisse, Art. 58 DSGVO. Leitet sie dann infolge der Verweigerung ein Aufsichtsverfahren ein, kann am Ende dieses Verfahrens bei einem Verstoß gegen die DSGVO ein Bußgeld stehen. Einleiten kann sie das Aufsichtsverfahren aber auch unabhängig von der Beantwortung des Fragebogens. Die Kooperationsbereitschaft und ein lösungsorientierter Ansatz des Unternehmens wirken sich jedoch oftmals bußgeldmindernd aus.

Um sich in einem Fragebogen nicht selbst zu belasten, sollte vorab die eigene Datenschutz-Compliance in dem erfragten Punkt überprüft und gegebenenfalls Rechtsrat eingeholt werden. Dies lohnt sich zum einen vor dem Hintergrund, dass die Auskunftsersuchen ein Indikator für die zukünftigen thematischen Prioritäten der Aufsichtsbehörden sind. Vor allem aber besteht ein Auskunftsverwei-

gerungsrecht gemäß § 40 Abs. 4 Satz 2 BDSG, wenn das Unternehmen sich durch die Auskunft selbst belasten würde.



Der Umfang des Betroffenenauskunftsrechts

Die DSGVO gibt dem Betroffenen ein Recht auf Auskunft über die Verarbeitung von ihn betreffenden personenbezogenen Daten gegen den für die Datenverarbeitung Verantwortlichen. Nach dem Wortlaut des Gesetzes ist auch eine „Kopie" der personenbezogenen Daten zur Verfügung zu stellen. Der genaue Umfang dieses Rechts ist jedoch bei weitem nicht so klar, wie es scheint und wurde auch in unserem Newsletter bereits mehrfach diskutiert. Vor kurzem hatte sich das Landgericht Köln, sowie Mitte 2018 bereits das Oberlandesgericht Köln, mit der Frage zu beschäftigen, was genau das Auskunftsrecht nun umfasst.

Nach seinem Wortlaut umfasst das Auskunftsrecht Informationen über den Verarbeitungszweck, Kategorien der Daten, Drittempfänger, die geplante Speicherdauer bzw. Kriterien hierfür sowie das Bestehen eines Lösch-/Berichtigungs- und eines Beschwerderechts. Ferner hat der Verantwortliche eine Kopie der personenbezogenen Daten, die Gegenstand der Verarbeitung sind, zur Verfügung zu stellen.

Es scheint zunächst, als könne der Betroffene umfassende Kopien aller ihn betreffenden Daten und Abläufe von dem Verantwortlichen verlangen. Einem solchen Verständnis des Auskunftsrechts

erteilte das Landgericht jedoch jüngst eine Absage. Der Anspruch auf Auskunft ist umfassender Natur, bezieht sich jedoch nicht auf alle internen Vorgänge, sondern vielmehr auf die darin enthaltenen personenbezogenen Daten.

Laut LG Köln sind nicht sämtliche internen Vorgänge des verantwortlichen Unternehmens, wie z.B. Vermerke oder Schriftverkehr, die der betroffenen Person bereits bekannt sind (E-Mails, Briefe), vom Auskunftsanspruch erfasst. Das Auskunftsrecht diene nämlich „nicht der vereinfachten Buchführung des Betroffenen", sondern die Auskunft solle lediglich den Betroffenen in die Lage versetzen, „den Umfang und Inhalt der gespeicherten personenbezogenen Daten [zu] beurteilen (…)". Der Betroffene kann also aufgrund des Auskunftsanspruchs nicht etwa Ausdruck und Übermittlung des ihm bereits bekannten Schriftverkehrs verlangen (so schon OLG Köln zu § 34 BDSG a.F., Beschl. v. 26.7.2018 – Az. 9 W 15/18).

Die „Free-Flow-of-data"-Verordnung als Pendant zur DSGVO

Geht es um personenbezogene Daten, ihre Verarbeitung und ihren Schutz, denken Sie höchstwahrscheinlich – freiwillig oder unfreiwillig – an die DSGVO. Damit der freie Datenverkehr innerhalb der EU weiter vorangetrieben und die Wettbewerbsfähigkeit Europas und europäischer Unternehmen gefördert wird, ist nun ca. ein Jahr nach der DSGVO auch die Verordnung für den freien Verkehr nicht-personenbezogener Daten in

der EU (VO (EU) 2018/1807) als ergänzendes Gegenstück in Kraft getreten und bringt einige Vorteile für Unternehmen mit sich. Eine Interpretationshilfe bieten die Leitlinien der Europäischen Kommission zur „Free-Flow-of-data"-Verordnung. Nicht-personenbezogene Daten sind solche, durch die eine Person gerade nicht identifiziert werden kann, während die personenbezogenen Daten mittelbar (verbunden mit weiteren Informationen) oder unmittelbar eine Individualisierung der dahinterstehenden Person zulassen. Da oftmals auch eine Gemengelage sowohl personenbezogener als auch nicht-personenbezogener Daten besteht, kommen Abgrenzungsfragen zur Anwendbarkeit der einen, der anderen oder beider Verordnungen hinzu.

Die sog. „Free-Flow-of-data"-Verordnung ist am 18.12.2018 in Kraft getreten und gilt seit dem 28.05.2019 unmittelbar in allen Mitgliedstaaten der EU. Sie regelt den Verkehr nicht-personenbezogener Daten und stellt somit das Gegenstück zur DSGVO dar.

Nicht-personenbezogene Daten sind Daten, die sich ursprünglich nicht auf eine identifizierte oder identifizierbare natürliche Person bezogen haben oder Daten, die ursprünglich personenbezogene Daten waren, später jedoch anonymisiert wurden. Die „Anonymisierung" personenbezogener Daten unterscheidet sich von der Pseudonymisierung, denn ordnungsgemäß anonymisierte Daten können nicht einmal durch die Verwendung zusätzlicher Daten einer bestimmten Person zugeordnet werden. Technische Daten zu Produkten, maschinell generierte Wetterdaten oder Finanz- und Steuerdaten stellen beispielsweise nicht-personenbezogene Daten dar.

Durch die „Free-Flow-of-data"-Verordnung soll der freie Datenverkehr in der EU gefördert werden. Der freie Datenverkehr wiederum stärkt den EU-Binnenmarkt und senkt langfristig die IT-Kosten für Unternehmen. Sie sollen nicht mehr von z.B. einem Cloud-Anbieter abhängig sein, sondern Anbieter freier und leichter wechseln können. Eine ungehinderte Übertragbarkeit von Daten zwischen IT-Systemen verhindert den sog. „Vendor-Lock-in-Effekt", d. h. Hindernisse zwischen Dienstanbietern zu wechseln oder Daten zurück in eigene IT-Systeme zu übertragen. So können Unternehmen ihr Datenmanagement und ihre Datenanalyse flexibler gestalten.

Hierzu werden den Mitgliedstaaten Datenlokalisierungsauflagen untersagt und Mechanismen zur Absicherung dieses Verbots eingeführt. Ausnahmen sind nur aus Gründen der öffentlichen Sicherheit

zulässig. Zudem verpflichtet die Verordnung die Europäische Kommission, Anreize zur Selbstregulierung in Form von Branchen-Verhaltensregeln, insbesondere im Hinblick auf Anbieterwechsel und die Übertragung von Daten, zu fördern und zu erleichtern.

Ergänzend wirken die beiden Verordnungen („Free-Flow-of-data"-Verordnung und DSGVO), wenn es um sog. „gemischte Datensätze" geht, also solche Datensätze, in denen personenbezogene und nicht-personenbezogene Einzelangaben enthalten sind. Dies bedeutet für einen „gemischten Datensatz", dass für die nicht-personenbezogenen Daten des Datensatzes die „Free-Flow-of-data"-Verordnung gilt und für die personenbezogenen Daten des Datensatzes die den freien Verkehr betreffenden Bestimmungen der DSGVO. Sind die nicht-personenbezogenen Daten und die personenbezogenen Daten „untrennbar miteinander verbunden", gelten die Datenschutzrechte und -pflichten aus der DSGVO in vollem Umfang für den gesamten „gemischten Datensatz", und zwar auch dann, wenn die personenbezogenen Daten nur einen kleinen Teil des Datensatzes ausmachen.

Die „Free-Flow-of-data"-Verordnung ist ein wichtiger Schritt zur Förderung des digitalen EU-Binnenmarktes. In Kombination mit der DSGVO bietet sie europaweit agierenden Unternehmen entsprechende Flexibilität und Vorteile, um im zunehmend datengesteuerten Wirtschaftsleben wettbewerbsfähig zu bleiben.

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