von Rechtsanwalt **Phil Salewski**

Checkliste der IT-Recht Kanzlei: Vorgehensweise bei Datenpannen im eigenen Online-Shop + Muster

Online-Händler, die täglich über technische Systeme eine Vielzahl von Kundendaten erheben, speichern und zur Vertragsabwicklung oder zu kommerziellen Zwecken verwenden und übermitteln, sind einem grundsätzlichen Risiko dahingehend ausgesetzt, dass einzelne Verarbeitungen über die gesetzliche Rechtfertigung hinausgehen und einer wirksamen Rechtsgrundlage entbehren. Weil die DSGVO für derartige Verletzungen des Schutzes personenbezogener Daten ein strengen Ablaufplan mit Melde- und Benachrichtigungspflichten aufstellt, zeigt die IT-Recht Kanzlei auf, welche Schritte bei Datenpannen unbedingt einzuleiten sind, und stellt Mandanten nunmehr 2 hilfreiche Muster bereit.

Hinweis: Exklusiv für Mandanten hält die IT-Recht Kanzlei ein Muster-Reaktionsschreiben für betroffene Kunden nach einem Hacking-Angriff bereit, mit welchem sich die Vorfälle erläutern und eine vertragliche Haftung ablehnen lassen.

I. Was sind Datenpannen und wie ereignen sie sich?

Art. 4 Nr. 12 DSGVO definiert die Datenpanne als eine Verletzung der Sicherheit, die, ob unbeabsichtigt oder unrechtmäßig, zur Vernichtung, zum Verlust, zur Veränderung, oder zur unbefugten Offenlegung von beziehungsweise zum unbefugten Zugang zu personenbezogenen Daten führt, die übermittelt, gespeichert oder auf sonstige Weise verarbeitet wurden.

Datenpannen im Online-Shop ereignen sich, ausgehend von dieser Definition, hauptsächlich durch Verarbeitungssituationen, die nicht von einer Rechtsgrundlage des Art. 6 (bzw. bei sensiblen Daten zusätzlich des Art. 9 DSGVO) getragen werden oder durch unrechtmäßige Zugriffe erfolgen.

Ersteres ist regelmäßig der Fall, wenn die Datenverarbeitungen – gewollt oder ungewollt – der Art oder dem Umfang nach über den Bereich hinausgehen, der von einer Rechtfertigungsgrundlage abgedeckt war. Eine Verletzung des Datenschutzes liegt aber auch dann vor, wenn eine Verarbeitung auf eine einwilligungslose Rechtfertigung (etwa die Vertragsabwicklung nach Art. 6 Abs. 1 lit. b oder berechtigte Interessen nach Art. 6 Abs. 1 lit. f DSGVO) gestützt wurde, obwohl tatsächlich die Einholung einer wirksamen Einwilligung des Betroffenen erforderlich gewesen wäre.

Zur Veranschaulichung ein kleines **Beispiel**:

Online-Händler A hat mit Verbraucher B einen Kaufvertrag über eine Kaffeemaschine geschlossen. In seinem Kundenkonto hat B neben seinen Adressdaten auch seine Telefonnummer hinterlegt. A stellt nun für den Versand der Kaffeemaschine unter Nutzung eines Versandlabel-Services die ein Versandlabel aus und gibt das etikettierte Paket bei der Post auf. Aufgrund eines internen Fehlers bei der Übertragung der Daten weist das Versandlabel nun nicht nur die Lieferadresse des B, sondern auch dessen Telefonnummer aus. Rechtsfolge?

Im obigen Beispiel war die Verarbeitung der Adressdaten beim Erstellen des Etiketts für die Vertragsabwicklung, nämlich für die Erfüllung der Leistungspflicht des A, erforderlich und somit durch Art. 6 Abs. 1 lit. b DSGVO gedeckt. Der Verarbeitung der Telefonnummer als personenbezogenes Datum bedurfte es für die Vertragserfüllung aber gerade nicht, da die Zustellung freilich auch ohne deren Offenlegung durch bloße Ausweisung der Adressdaten gelingt. Für die versehentliche maschinelle Übermittlung und den Aufdruck der Telefonnummer hätte A insofern die Einwilligung des B benötigt, die nicht vorliegt. Es ist infolge zu einer Datenpanne durch Offenlegung eines personenbezogenen Datums und zur Verletzung des Schutzes der personenbezogenen Daten des B gekommen.

Unabhängig von Anfälligkeiten technischer Systeme, die für Erhebungs- und Übermittlungsfehler sorgen und so durch übermäßige Datenverarbeitungen Datenpannen nach sich ziehen können, kann die Verletzung des Schutzes personenbezogener Daten auch durch rechtswidrige Fremdzugriffe auf Datensysteme und insofern durch Hacks entstehen. Zwar haben Verantwortliche (so auch Online-Händler) zur Minimierung der Fremdzugriffsmöglichkeiten gemäß Art. 32 DSGVO originär hinreichende technische und organisatorische Maßnahmen zu etablieren. Setzen sich Dritte aber über diese hinweg und erhalten dadurch in unzulässiger Weise Zugriff auf personenbezogene Datensätze, stellen derartige Sicherheitsbrüche ebenfalls tatbestandliche Datenpannen dar, die den Verantwortlichen zu einer Reihe von Maßnahmen veranlassen.

II. Wie ist bei Aufdeckung einer Datenpanne zu reagieren?

Neben internen Maßnahmen, die Online-Händler im Falle des Auftretens von Datenpannen zwingend ergreifen sollten, sieht die DSGVO selbst einen rigiden Anforderungskatalog vor, der sich vor allem in Form von Melde- und Informationspflichten ausprägt.

1.) Frühzeitige Erkennung der Datenpanne

Grundsätzlich knüpft die DSGVO die Handlungspflichten im Falle einer Datenpanne an den Zeitpunkt der Kenntnisnahme des Online-Händlers von eben dieser. Um diesen nicht unbillig nach hinten zu verlagern und mithin den Betroffenen einem zunehmenden Risiko der Beeinträchtigung seines Datenschutzes auszusetzen, sollten Online-Händler durch technische Warnsysteme hinreichend sicherstellen, dass Datenanomalien so früh wie möglich gemeldet werden.
Insbesondere Alarmsysteme für unbefugte Fremdzugriffe und -zugriffsversuche sind als erforderliche technische und organisatorische Maßnahmen i.S.d. Art. 32 DSGVO einzurichten.

Unter den Landesdatenschutzbehörden ebenso für wirksam befunden wurde die Errichtung eines sog.

„Data Breach Notification Management“-Systems, das insbesondere Kommunikationswege, Kooperationen verschiedener Untergliederungen miteinander, den Informationsaustausch mit Auftragsverarbeitern und die rechtzeitige Einbindung von Entscheidungsträgern verbindlich und ablaufspezifisch festlegt.

2.) Dokumentation der Datenpanne

Gemäß Art. 33 Abs. 5 DSGVO hat der verantwortliche Online-Händler Datenpannen unverzüglich, also ohne schuldhaftes Zögern (§ 121 BGB), nach Kenntniserlangung hinreichend zu dokumentieren. Diese Dokumentation muss auf Verlangen der Aufsichtsbehörde (Art. 58 Abs. 1 lit. a DSGVO) vorgelegt werden können, die anhand der aufgezeichneten Fakten überprüfen können muss, ob der Online-Händler seiner Meldepflicht (dazu sogleich) hinreichend und vor allem hinreichend rechtzeitig nachgekommen ist.

Die Dokumentation muss im Zuge der Datenpanne alle mit ihr im Zusammenhang stehenden Fakten dokumentieren und so insbesondere enthalten:

- eine Beschreibung der Art der Verletzung des Schutzes personenbezogener Daten, soweit möglich mit Angabe der Kategorien und der ungefähren Zahl der betroffenen Personen, der betroffenen Kategorien und der ungefähren Zahl der betroffenen personenbezogenen Datensätze
- eine Beschreibung des konkreten Ereignisses unter Nennung der Ursache, des technischen Anknüpfungspunkts, evtl. der ausgehebelten oder fehlgegangenen technischen und organisatorischen Maßnahme, den genauen Umständen, Angaben zum Verschuldens und der Person(en), in deren Verantwortungsbereich sich die Datenpanne ereignete
- den Ort und die Zeit des Ereignisses
- eine Beschreibung der wahrscheinlichen Folgen der Verletzung des Schutzes personenbezogener Daten
- eine Beschreibung der von dem Verantwortlichen ergriffenen Maßnahmen zur Behebung der Verletzung des Schutzes personenbezogener Daten und gegebenenfalls Maßnahmen zur Abmilderung ihrer möglichen nachteiligen Auswirkungen.
- den Namen und die Kontaktdaten des Datenschutzbeauftragten oder einer sonstigen Anlaufstelle für weitere Informationen

Für Verstöße gegen die Verpflichtung zur ordnungsgemäßen Dokumentation von Datenpannen werden gemäß Art. 83 Abs. 4 lit. a DSGVO Geldbußen von bis zu 10 000 000€ oder im Falle eines Unternehmens von bis zu 2 % seines gesamten weltweit erzielten Jahresumsatzes des vorangegangenen Geschäftsjahres verhängt.

3.) Benachrichtigung der Aufsichtsbehörde

Nach erfolgter Dokumentation, die zwingend Vorrang haben muss, ist die Datenpanne sodann der nach Art. 51 DSGVO zuständigen Aufsichtsbehörde unter Einhaltung eines Mindestinformationsgehaltes und einer strengen zeitlichen Frist zu melden, Art. 33 Abs. 1 DSGVO

Die Pflicht entfällt zwar, wenn die Verletzung des Schutzes personenbezogener Daten voraussichtlich nicht zu einem Risiko für die Rechte und Freiheiten natürlicher Personen führt. Da es sich hierbei aber um eine Prognoseentscheidung des Verantwortlichen handelt, die im Zweifel behördlich überprüfbar und im Falle einer Fehlabwägung gar sanktionierbar ist, liegt es im Sinne der Rechtssicherheit, der Meldepflicht in jedem Falle einer Datenpanne nachzukommen. Dies gilt insbesondere im Online-Handel, wo primäre Personendaten Grundlage jeglicher Verarbeitungsvorgänge sind.

a) Zuständige Behörde

Die Meldung ist gegenüber der zuständigen Behörde i.S.d. Art. 51 DSGVO zu erbringen. In Deutschland ist für Unternehmen die Aufsichtsbehörde des Bundeslandes zuständig, in dem der Sitz des Unternehmens liegt.

b) Pflichtiger

Meldepflichtig ist nur der Datenverantwortliche. Dies hat insbesondere Relevanz in Fällen, in denen sich die Datenpanne bei einem Auftragsverarbeiter ereignet. Erfolgt in dessen Sphäre eine Verletzung des Schutzes personenbezogener Daten, muss der Auftragsverarbeiter nach Art. 33 Abs. 2 DSGVO unverzüglich den Verantwortlichen informieren, der dann wiederum die erforderliche Meldung bewirken muss.

c) Frist

Die Meldung hat gemäß Art. 33 Abs. 1 Satz 1 DSGVO unverzüglich, also ohne schuldhaftes Zögern (§ 121 BGB) und möglichst binnen 72 Stunden nach dem Zeitpunkt zu erfolgen, in welchem der Verantwortliche Kenntnis von der Datenpanne erlangt hat.

Unter anderem zur Sicherstellung des Fristeneinhalts kann die Behörde die nach Art. 33 Abs. 5 DSGVO zu errichtende Dokumentation anfordern.

Wird die Frist überschritten, so ist der Meldung gemäß Art. 33 Abs. 1 Satz 2 DSGVO zwingend eine hinreichende Begründung für die Verzögerung beizufügen.

d) Mindestinhalt der Meldung

Die Meldung muss gemäß Art. 33 Abs. 3 DSGVO zwingend folgende Angaben enthalten:

- eine Beschreibung der Art der Verletzung des Schutzes personenbezogener Daten, soweit möglich mit Angabe der Kategorien und der ungefähren Zahl der betroffenen Personen, der betroffenen Kategorien und der ungefähren Zahl der betroffenen personenbezogenen Datensätze;
- den Namen und die Kontaktdaten des Datenschutzbeauftragten oder einer sonstigen Anlaufstelle für weitere Informationen;
- eine Beschreibung der wahrscheinlichen Folgen der Verletzung des Schutzes personenbezogener Daten;
- eine Beschreibung der von dem Verantwortlichen ergriffenen oder vorgeschlagenen Maßnahmen zur Behebung der Verletzung des Schutzes personenbezogener Daten und gegebenenfalls Maßnahmen zur Abmilderung ihrer möglichen nachteiligen Auswirkungen.

Die bereitzustellenden Informationen sollen der Behörde eine Prüfung dahingehend ermöglichen, ob geeignete und sinnhafte Maßnahmen getroffen wurden, um die Datenpanne wirksam zu beseitigen und deren Auswirkungen so gut wie möglich einzudämmen. Kommt die Behörde zu dem Ergebnis, dass die mitgeteilten und getroffenen Maßnahmen nicht ausreichend waren, kann sie gemäß Art. 58 Abs. 2 lit. d DSGVO weitere Maßnahmen anordnen.

Gelingt es dem Verantwortlichen nicht, die Informationen innerhalb der Frist gesammelt beizubringen, etwa weil ihm unmittelbar nach Bekanntwerden der Datenpanne noch wesentliche Informationen fehlen, so kann er die Angaben auch schrittweise machen, Art. 33 Abs. 4 DSGVO. Sofern weitere Ermittlungen zur Informationsbeschaffung notwendig sind, beeinflusst dies allerdings nicht den Zeitpunkt der Meldung an sich, sondern nur den Pflichtinhalt. Dass ein Datenschutzverstoß stattgefunden hat, ist grundsätzlich zwingend binnen 72 Stunden nach Kenntniserlangung zu melden.

Wichtig:
Der Mindestgehalt der Meldung an die Behörde bleibt dem Umfang nach hinter dem zurück, was Gegenstand der Dokumentation nach Art. 33 Abs. 5 DSGVO sein muss. Die für die ordnungsgemäße Dokumentation darzulegenden Informationen sind umfangreicher.

e) Form der Meldung

Art. 33 DSGVO sieht keine bestimmte Form für die verpflichtende Meldung an die Aufsichtsbehörde vor. Sie kann daher grundsätzlich in jeder denkbaren Übermittlungsart ergehen, inbs. fernmündlich, per Fax oder Mail oder postalisch.

Aus Dokumentations- und Zugangsnachweisgründen ist allerdings zu raten, die Meldung über ein geeignetes Medium zumindest in Textform (§ 126 b BGB) ergehen zu lassen.

f) Sanktionen bei Verstößen gegen die Pflicht

Die unterlassene oder nicht rechtzeitige Tätigung einer erforderlichen Meldung kann gemäß Art. 83 Abs. 4 lit. a mit einer Geldbußen von bis zu 10 000 000€ oder im Falle eines Unternehmens von bis zu 2 % seines gesamten weltweit erzielten Jahresumsatzes des vorangegangenen Geschäftsjahres geahndet werden.

4.) Benachrichtigung des Betroffenen

In einem letzten Schritt ist gemäß Art. 34 DSGVO gegebenenfalls auch der Betroffene selbst vom Verantwortlichen in geeignetem Umfang über die Datenpanne zu informieren.

a) Voraussetzung des hohen Risikos einer Rechtsgutsverletzung

Art. 34 Abs. 1 DSGVO knüpft die Pflicht an die Prognose, dass die Datenpanne voraussichtlich ein hohes Risiko für die persönlichen Rechte und Freiheiten natürlicher Personen zur Folge hat, und befreit den Verantwortlichen insofern von einer fallunabhängigen Belehrungspflicht.

Wann ein solches Risiko besteht, kann unter Anwendung des Erwägungsgrundes 85 der DSGVO erörtert werden, und ist immerhin dann zu bejahen, wenn die Verletzung des Schutzes personenbezogener Daten einen physischen, materiellen oder immateriellen Schaden für natürliche Personen nach sich ziehen kann, wie etwa

- den Verlust der Kontrolle über ihre personenbezogenen Daten oder Einschränkung ihrer Rechte,
- Diskriminierung
- Identitätsdiebstahl oder -betrug
- finanzielle Verluste
- unbefugte Aufhebungen der Pseudonymisierung
- Rufschädigung
- Verlust der Vertraulichkeit von dem Berufsgeheimnis unterliegenden Daten
- andere erhebliche wirtschaftliche oder gesellschaftliche Nachteile für die betroffene natürliche Person

Weil bei Datenpannen im Online-Shop einerseits regelmäßig die rechtsgrundlose Verarbeitung erstrangiger, gegebenenfalls gar mehrerer Personendaten droht, die – zweckwidrig verwendet – weitreichende Beeinträchtigungen nach sich ziehen können, und andererseits das Risiko einer Fehleinschätzung und einem Absehen von der Benachrichtigung beim Verantwortlichen liegt und ein Bußgeld nach sich ziehen kann, ist zu empfehlen, den Betroffenen stets zu benachrichtigen.

Die Erfüllung dieser Informationspflicht, selbst wenn sie im Nachhinein nicht erforderlich war, zieht keine negativen Konsequenzen nach sich; die Nichterfüllung trotz eigentlicher Erforderlichkeit allerdings schon.
Gerade im Online-Handel, wo eine Datenpanne das Vertrauensverhältnis zum Kunden schwer beeinträchtigt, kann eine persönliche Benachrichtigung darüber hinaus geeignet sein, die

Kundenbindung im Zweifel aufrecht zu erhalten.

Auf die Voraussetzungen des Art. 34 Abs. 3 DSGVO, nach denen die Pflicht zur Betroffenenbenachrichtigung entfallen kann, wird insofern an dieser Stelle nicht eingegangen.

b) Frist

Der Betroffene ist gemäß Art. 34 Abs. 1 DSGVO unverzüglich, d.h. ohne schuldhaftes Zögern (§ 121 BGB), zu benachrichtigen. Hierbei steht die Unverzüglichkeit der Benachrichtigung in direkter Abhängig zur Unverzüglichkeit der Feststellung der Datenpanne.

Zeitlich sollte die Benachrichtigung des Betroffenen der Meldung an die Aufsichtsbehörde nachfolgen, da diese in ihrer Einschätzung gegebenenfalls bereits eine Prognose darüber trifft, ob der Betroffene tatsächlich zu unterrichten ist.

c) Inhalt und Form

Gemäß Art. 34 Abs. 2 DSGVO muss die Benachrichtigung in klarer und einfacher Sprache die Art der Verletzung des Schutzes personenbezogener Daten beschreiben und mindestens folgende Angaben enthalten:

- den Namen und die Kontaktdaten des Datenschutzbeauftragten oder einer sonstigen Anlaufstelle für weitere Informationen;
- eine Beschreibung der wahrscheinlichen Folgen der Verletzung des Schutzes personenbezogener Daten;
- eine Beschreibung der von dem Verantwortlichen ergriffenen oder vorgeschlagenen Maßnahmen zur Behebung der Verletzung des Schutzes personenbezogener Daten und gegebenenfalls Maßnahmen zur Abmilderung ihrer möglichen nachteiligen Auswirkungen.

Klar ist die Benachrichtigung, wenn sie übersichtlich, eindeutig, hinreichend strukturiert und in ihrem datenschutzbezogenen Informationsgehalt abschließend ist, d.h. keine weiteren themenfremden Inhalte enthält.
Eine einfache Sprache meint dahingegen die Formulierung n einer für jedermann verständlichen Weise ohne Fachvokabular (Gola, DSGVO, Art. 34 Rn. 11).

Eine besondere Form ist nicht vorgeschrieben, es empfiehlt sich zu Dokumentations- und Zugangsnachweiszwecken aber jedenfalls die Übermittlung in Textform per Brief, Fax oder Mail.

III. 2 Muster der IT-Recht Kanzlei

Die IT-Recht Kanzlei stellt ihren Mandanten zum einen ein Muster für die erforderliche Meldung gegenüber der Datenschutzbehörde bereit. Dieses Muster kann hier abgerufen werden.

Neu hinzu kommt für Mandanten nunmehr und zum anderen ein Musterschreiben für die Benachrichtigung des Betroffenen im Online-Handel, das in inhaltlicher Übereinstimmung mit Art. 34 DSGVO über eine eingetretene Datenpanne informiert. Das neue Muster kann hier abgerufen werden.

IV. Fazit

Datenpannen im Online-Shop konfrontieren Händler nicht nur mit dem Risiko eines Imageschadens und eines Vertrauensverlustes der betroffenen Kunden, sondern zwingen sie rechtlich auch dazu, weitreichende Dokumentations- und Informationspflichten zu erfüllen. Insbesondere die hohen Bußgeldandrohungen für Pflichtverstöße und die kurzen Fristen sollten Anlass geben, geeignete Methoden und Abläufe aufzustellen, um im Falle von Datenpannen kurzfristig und angemessen reagieren zu können.

Für die Benachrichtigung von betroffenen Kunden erleichtert die IT-Recht Kanzlei ihren Mandaten den erforderlichen Aufwand durch die Bereitstellung eines hilfreichen Musters.

Autor:
RA Phil Salewski
Rechtsanwalt