Kundendaten frei im Internet auffindbar – Was droht Online-Händlern bei Datenpannen?

In Großbritannien hat ein Online-Shop die Daten seiner Kunden ungesichert gespeichert und so waren diese frei über das Internet für jedermann einsehbar. Das ist ein schwerer Verstoß gegen das Datenschutzrecht. Was müssen Online-Händler in so einem Fall in Zukunft nach der DSGVO tun? Und was droht ihnen?

Schon heute gilt, dass Unternehmer personenbezogene Daten sicher speichern müssen. Die Sicherheit muss dabei nach dem Stand der Technik gewährleistet sein.

Das gilt auch in Zukunft. Art. 32 DSGVO schreibt unter anderem vor, dass personenbezogene Daten zu verschlüsseln sind.

Daten frei im Internet verfügbar

Ein Online-Shop in Großbritannien hat dies offenbar nicht gemacht. Ohne Passwortkontrolle, also quasi frei zugänglich im Internet, war es möglich, die Kundendaten dieses Shops einzusehen, wie golem.de berichtet. In dem Bericht heißt es dazu,

> *"dass sogar Großeltern, die Internet Explorer nutzen, an die Daten herangekommen wären."*

Ein solches Datenleck ist aber insbesondere für den Ruf und das Image eines Unternehmens nicht nur besonders ärgerlich, sondern hat auch rechtliche Konsequenzen. Wir wollen diesen Fall als Anlass nehmen, um Sie über die möglichen Rechtsfolgen im Fall von Datenpannen zu informieren.

Insbesondere ab 25. Mai 2018, wenn die Datenschutzgrundverordnung gilt, ändern sich hier einige Bestimmungen.

Sanktion nach DSGVO

Die unverschlüsselte Speicherung von personenbezogenen Daten stellt einen Verstoß gegen Art. 32 DSGVO dar.

Ein solcher Verstoß wird zukünftig mit einem Bußgeld von bis zu 10 Millionen Euro, oder im Fall eines Unternehmens von bis zu 2 % seines gesamten weltweit erzielten Jahresumsatzes des vorangegangenen Geschäftsjahrs verhängt, je nachdem, welcher der Beträge höher ist.

In einem solchen Fall droht Unternehmern also zunächst einmal ein hoher wirtschaftlicher Schaden.

Meldepflicht nach DSGVO

Die DSGVO kennt aber nicht nur Sanktionen und Bußgelder. Sie legt Unternehmern im Fall von Datenpannen auch Meldepflichten auf. Art. 33 DSGVO beschreibt diese näher.

Danach muss im Falle der Verletzung des Schutzes personenbezogener Daten unverzüglich und möglichst innerhalb von 72 Stunden nach dem Bekanntwerden der Verletzung die zuständige Aufsichtsbehörde informiert werden.

> *Die zuständige Aufsichtsbehörde ist die Landesdatenschutzbehörde des Bundeslandes, in dem der Unternehmer seinen Sitz hat.*

Eine Meldepflicht besteht nur dann nicht, wenn die Verletzung des Schutzes personenbezogener Daten voraussichtlich nicht zu einem Risiko für die Rechte und Freiheiten natürlicher Personen führt.

> *Diese Ausnahme greift aber nicht, wenn Kundendaten frei im Netz verfügbar sind.*

Kann man die Meldung nicht innerhalb von 72 Stunden einreichen, so muss dies der Behörde gegenüber begründet werden.

Inhalt der Meldung

Die Meldung an die Aufsichtsbehörde über die Datenpanne muss folgenden Inhalt aufweisen:

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.

Blanko-Meldungen vorbereiten, Projektplan erstellen

Damit man die vom Gesetz vorgegebene Frist von 72 Stunden einhalten kann, sollte man auf den Fall einer Datenpanne vorbereitet sein.

Dazu gehört zum einen ein detaillierter Projektplan, in dem die wichtigsten Fragen beantwortet werden. Wie zum Beispiel “Welcher Mitarbeiter macht was, wenn eine Datenpanne auftritt?” oder “Wie erreichen wir den/die Datenschutzbeauftragte?”

Zentraler Ansprechpartner in einem solchen Fall sollte immer der oder die Datenschutzbeauftragte des Unternehmens sein. Ist in dem Unternehmen kein Datenschutzbeauftragter bestellt, muss eine entsprechend qualifizierte, andere Person diese zentrale Rolle übernehmen.

Dazu empfiehlt es sich, mögliche Meldungen vorzubereiten. Es bietet sich hier eine Art Formular an, welches man dann im Falle der Datenpanne ausfüllen und an die Aufsichtsbehörden übersenden kann.

In der Meldung selbst sollte neben der genauen Beschreibung des Vorfalls auf den vierten Punkt besonderer Wert gelegt werden. Es ist wichtig, dass man den Aufsichtsbehörden detailliert mitteilt, welche Maßnahmen man ergriffen hat, um die Panne abzustellen und um sicherzustellen, dass gleiches nicht noch einmal passiert.

Information an die Betroffenen

Birgt die Verletzung sogar ein voraussichtliches hohes Risiko für die Rechte und Freiheiten der Betroffenen, so muss der Verantwortliche die Betroffenen unverzüglich informieren.

Ob ein hohes Risiko für die Rechte und Freiheiten der Betroffenen besteht, muss man immer im Einzelfall prüfen. Bei dem britischen Shop waren neben den vollständigen Namen und

Anschriftendaten der Kunden auch jeweils die letzten vier Ziffern der Kreditkartennummer in der offen einsehbaren Datenbank enthalten.

Das Risiko für die Betroffenen ist in diesem Fall also sehr hoch. Und wenn solche Datenbanken offen im Internet zugänglich sind, ist auch die Wahrscheinlichkeit recht hoch, dass Betrüger an diese Datenbank geraten und diese Daten dann missbrauchen.

Durch die Meldung an die Betroffenen können diese z.B. unverzüglich ihre Kreditkarte sperren lassen, sodass ein Missbrauch ausgeschlossen werden kann.

Die Meldung an den Betroffenen muss mindestens die Punkte 2 bis 4 der Meldung an die Behörden enthalten.

Meldung und Informationen unterbleiben? Bußgelder drohen

Die Meldung an die Aufsichtsbehörden und auch die Information der Betroffenen sollten Unternehmen sehr ernst nehmen. Denn unterbleibt dies, liegen gleich zwei Verstöße gegen die Vorschriften der DSGVO vor, die separat geahndet werden können.

Und jeder Verstoß hier kann ebenfalls mit (jeweils!) einem Bußgeld von bis zu 10 Millionen Euro, oder im Fall eines Unternehmens von bis zu 2 % seines gesamten weltweit erzielten Jahresumsatzes des vorangegangenen Geschäftsjahrs geahndet werden, je nachdem, welcher der Beträge höher ist.

Ein solcher Fall kann in Zukunft im worst case also drei sehr hohe Bußgeldbescheide nach sich ziehen:

unverschlüsselte Speicherung der Daten
unterbliebene Meldung an die Aufsichtsbehörde
unterbliebene Information der Betroffenen
Außerdem muss damit gerechnet werden, dass in einem solchen Fall die Aufsichtsbehörden einen Kontrollbesuch im Unternehmen durchführen werden. Dabei könnten dann noch weitere Verstöße “aufgedeckt” werden, die dann wieder Bußgeldbescheide nach sich ziehen können.

Fazit

Fehler können passieren, das ist menschlich. Führen diese Fehler zu Datenpannen, sollte man gut vorbereitet sein, um hier professionell und schnell handeln zu können – und auch, um verlorengegangenes Vertrauen wieder aufzubauen. Hier noch einmal eine kurze Checkliste für Sie für den Fall der Fälle:

Ruhe bewahren, keine übereilten Maßnahmen wie Mailing an Betroffene, Löschen von irgendwelchen Verläufen etc.
Dokumentieren: Was genau ist passiert? Welche Daten sind betroffen? Welche Personen (Käufer, Mitarbeiter,…) sind betroffen?
Zeitnah handeln: bei meldepflichtigen Vorfällen haben Sie bis zur Meldung an die Datenschutzbehörde nur 72 Stunden Zeit
Sofern vorhanden: Datenschutzbeauftragten frühzeitig mit einbeziehen. Es ist sein Aufgabe, Informationen zu sammeln, zu bewerten und auf dieser Grundlage anschließend zu entscheiden, was unternommen werden muss.
Bildnachweis: Bloomicon/shutterstock.com