1/2017
1 – 24

CHECKLISTE
Social-Media-Guideline
Hans-Jürgen Pollirer

DATENSCHUTZ KONKRET

Recht | Projekte | Lösungen

Chefredaktion: Rainer Knyrim

Datenschutz bei Kindern

Sensibilisierung ist der einzig wirksame Weg
Interview mit Eva Souhrada-Kirchmayer, Richterin am BVerwG

Kinderschutz in der DSGVO
Werner Pilgermair

Minderjährige in der datenschutzrechtlichen Judikatur
Viktoria Haidinger

Praxisprojekt: Handhabung von Datenpannen
Markus Oman

Networks of Control – das Ende von Freiheit und Würde?
Sarah Spiekermann

Sozialversicherungsnummer in der Rechtsprechung
Andreas Gerhartl

Mitbestimmungsrecht des Betriebsrates bei der Einführung von IT Systemen
Klaus zu Hoene/Christian Kern

ISSN 2313-5409

dako.manz.at

MANZ

Österreichische Post AG Verlag Manz, Gutheil Schoder Gasse 17, 1230 Wien

Markus Oman
O.P.P. – Beratungsgruppe

Die Handhabung von Datenpannen iSd DSGVO

Das künftige EU-Datenschutzrecht – Teil 8. Bei einer Datenpanne, auch bekannt als „data breach", können natürliche Personen einen physischen, materiellen oder immateriellen Schaden durch die Verletzung des Schutzes personenbezogener Daten erleiden. Der Beitrag zeigt den typischen Verlauf einer Datenpanne, die Schritte zur Schadensminimierung und ein Muster für die Meldung an die Aufsichtsbehörde.

„Data breaches" (Datenpannen)

Eine Datenpanne iSd DSGVO stellt den Verlust der vollständigen Kontrolle über personenbezogene Daten dar. Es ist aus Sicht des Datenschutzes unerheblich, ob der Datenabfluss mit Vorsatz oder unbewusst durch einen Fehler erfolgt ist. Diesbezügliche Regelungen finden sich in der DSGVO primär in den Art 33 und 34, die auf den ErwGr 85 bis 88 beruhen. In Art 12 Abs 1 findet man die Vorgaben, welche zur verständlichen und präzisen Auskunft verpflichten. Art 33 befasst sich mit der Meldung von Verletzungen des Schutzes personenbezogener Daten an die Aufsichtsbehörde und Art 34 mit der Benachrichtigung der von einer Verletzung des Schutzes personenbezogener Daten betroffenen Person.

Verlauf der Datenpanne

Der Verlauf einer Datenpanne hat in der Praxis typischerweise zehn Phasen, die zumeist nachfolgende Reihenfolge aufweisen.

Phase 1 – Die Datenpanne an sich

Die DSGVO definiert eine Datenpanne – oder besser bekannt als „data breach" – folgendermaßen: Es wird im ErwGr 85 die Verletzung des Schutzes personenbezogener Daten dahingehend beschrieben, dass die natürliche Person einen physischen, materiellen oder immateriellen Schaden erleiden könnte; bspw den Verlust der Kontrolle über ihre personenbezogenen Daten oder eine Einschränkung ihrer Rechte, Diskriminierung, Identitätsdiebstahl oder -betrug, finanzielle Verluste, unbefugte Aufhebung der Pseudonymisierung, Rufschädigung, Verlust der Vertraulichkeit von dem Berufsgeheimnis unterliegenden Daten oder andere erhebliche wirtschaftliche oder gesellschaftliche Nachteile für die betroffene natürliche Person.

1. Datenpanne an sich	Ungewollter Abfluss der Daten aus der Datenhoheit des für Verarbeitung Verantwortlichen an sich
2. Erkennen des ungewollten Datenabflusses	Erkennen des ungewollten Datenabflusses durch den für Verarbeitung Verantwortlichen
3. Abfluss stoppen	Verhinderung eines weiteren Datenabflusses
4. Folgen einschätzen	Einschätzen der Art und Schwere der nachteiligen Folgen für betroffene natürliche Personen
5. Minimierung der Folgeschäden	Beginn der Minimierung möglicher Folgeschäden für betroffene natürliche Personen
6. Information der betroffenen Person	Unverzügliche Information der vermeintlich betroffenen natürlichen Personen, hinsichtlich der Verletzung des Schutzes ihrer personenbezogenen Daten
7. Information an die Aufsichtsbehörde	Information über die Datenpanne an die Aufsichtsbehörde (definiert in Art 51; Österreichische Datenschutzbehörde, www.dsb.gv.at); zumeist binnen 72 Stunden)
8. Maßnahmen zur Schadensbeseitigung	Maßnahmen zur Schadensbeseitigung zu Gunsten der betroffenen natürlichen Person, eventuell unter Auflagen der Aufsichtsbehörde
9. Analyse	Analyse des kompletten Herganges der Datenpanne
10. Verbesserungen etablieren	Vorkehrungen zur Verhinderung zukünftiger Datenpannen, eventuell unter Auflagen der Aufsichtsbehörde

Abbildung: Phasen einer Datenpanne

Phase 2 – Erkennen des ungewollten Datenabflusses

Es kann unterschieden werden zwischen Datenverlust durch eine ungewollte Panne, durch grobe Fahrlässigkeit oder durch Vorsatz herbeigeführten Datenabflüssen:

- Eine **ungewollte Panne** wäre typischerweise ein Softwarefehler in einer Internetapplikation, durch den zB Bewerberdaten einer Recruiting-Plattform für andere Bewerber sichtbar sind.
- **Grobe Fahrlässigkeit** liegt jedenfalls dann vor, wenn entweder allgemein übliche technische oder organisatorische Maßnahmen zum Schutz der Daten nicht getroffen wurden; wie zB fehlender Passwortschutz, wenn unverschlüsselte Datenträger an öffentlich zugänglichen Orten verloren gehen oder wenn man nicht ausreichend aufmerksam mit Daten und va mit deren Weitergabe umgeht (bspw wenn eine Finanzbeamtin Informationen einer Prüfung in Form eines E-Mails auf Grund von Namensähnlichkeiten an den falschen Empfänger sendet).
- **Vorsatz** liegt sicherlich bei der Überwindung technischer oder organisatorischer Sicherheitsmaßnahmen unter Anwendung spezieller Techniken und Verfahren, bekannt als „hacking", vor. Vorsatz liegt auch vor, wenn anvertraute

Daten ohne Genehmigung veröffentlicht werden.

Phase 3, 4, 5 – Weitere Datenabflüsse verhindern und Schaden minimieren

Der für die Verarbeitung Verantwortliche sollte verschiedene **technische und organisatorische Maßnahmen** implementiert haben, die es ermöglichen, Datenpannen frühzeitig zu erkennen bzw zu verhindern, um schnellstmöglich Gegenmaßnahmen und die Information der vermeintlich Geschädigten und der Aufsichtsbehörde zu veranlassen. Solche Verfahren könnten durch eine laufende strukturierte Auswertung von Logging-Protokollen erfolgen. Dies setzt jedoch voraus, dass Zugriffe entsprechend auswertbar protokolliert werden und die Abweichung von sinnvollen Protokollstandards auch zu geeigneten Maßnahmen bzw Benachrichtigungen führen.

Eine strukturierte Protokollierung von Logdateien ermöglicht, Datenpannen zu erkennen.

Phase 6 – Information der betroffenen Person

Hat die Verletzung des Schutzes personenbezogener Daten voraussichtlich ein **hohes Risiko** für die persönlichen Rechte und Freiheiten natürlicher Personen zur Folge, so benachrichtigt der Verantwortliche die betroffene Person unverzüglich von der Verletzung (Art 34 Abs 1).

Ein wichtiger Begriff ist der des „hohen Risikos"; dies könnte zB die unerlaubte Veröffentlichung von Schulnoten, Einkommensdaten, Verkehrsvergehen, Bonitäten oder von Korrespondenz mit einer Finanzbehörde darstellen. Das Risiko ist jedenfalls immer dann hoch, wenn Dritte die Daten des Betroffenen, ohne selbst einen berechtigten Zweck zu haben, einsehen und daraus Ihre Schlüsse ziehen können. Auch die Gefahr der Diskriminierung und des Identitätsdiebstahls bzw des Identitätsbetrugs stellen typische Risiken dar, genauso wie finanzielle Verluste oder unbefugte Aufhebung der Pseudonymisierung (zB Namen von Teilnehmern an medizinischen Studien werden bekannt) und natürlich auch Rufschädigung.

Hinsichtlich des **Benachrichtigungszeitpunkts** sind jedenfalls die Ausführungen des ErwGr 86 letzter Satz, zu beachten: Um bspw das Risiko eines unmittelbaren Schadens mindern zu können, müssten betroffene Personen sofort benachrichtigt werden, wohingegen eine längere Benachrichtigungsfrist gerechtfertigt sein kann, wenn es darum geht, geeignete Maßnahmen gegen fortlaufende oder vergleichbare Verletzungen des Schutzes personenbezogener Daten zu treffen.

Gem Art 34 Abs 2 beschreibt die Benachrichtigung der betroffenen Person in klarer und einfacher Sprache, die die Art der Verletzung des Schutzes personenbezogener Daten und zumindest folgende Informationen enthält:

- Beschreibung der Art der Verletzung des Schutzes personenbezogener Daten;
- die ungefähre Zahl der betroffenen Datensätze;
- den Namen und die Kontaktdaten des Datenschutzbeauftragten;
- die Beschreibung der wahrscheinlichen Folgen;
- die Beschreibung der von dem Verantwortlichen ergriffenen oder vorgeschlagenen Maßnahmen zur Behebung der Verletzung;
- und gegebenenfalls die Maßnahmen zur Abmilderung der möglichen nachteiligen Auswirkungen.

Phase 7 – Information an die Aufsichtsbehörde

Art 33 behandelt die gegebenenfalls notwendige **Meldung** an die Aufsichtsbehörde über die Verletzung des Schutzes personenbezogener Daten. Wenn die Datenpanne nicht sehr wahrscheinlich für die betroffene Person risikolos ist, so ist die Aufsichtsbehörde nach Möglichkeit innerhalb von 72 Stunden zu informieren. Eine spätere Benachrichtigung ist zu begründen. Auch für einen Auftragsverarbeiter gilt, dass er eine in seiner Sphäre auftretende Datenpanne unverzüglich an den Verantwortlichen des Auftraggebers meldet.

Die Aufsichtsbehörde ist nach Möglichkeit innerhalb von 72 Stunden zu informieren.

Gem Art 33 Abs 3 sind folgende **Mindestangaben** anzuführen:

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

Wenn und soweit die Informationen nicht zur gleichen Zeit bereitgestellt werden können, kann der Verantwortliche diese Informationen ohne unangemessene weitere Verzögerung **schrittweise** zur Verfügung stellen (Art 33 Abs 4).

Der Verantwortliche dokumentiert Verletzungen des Schutzes personenbezogener Daten einschließlich aller iZm der Verletzung des Schutzes personenbezogener Daten stehenden Fakten, deren Auswirkungen und der ergriffenen Abhilfemaßnahmen (Art 33 Abs 5). Diese **Dokumentation** ermöglicht der Aufsichtsbehörde die Überprüfung der Einhaltung dieser Bestimmungen.

Ist sich der Verantwortliche unsicher, ob es zielführender ist, sofort Maßnahmen zur Schadensminimierung zu ergreifen oder zuerst die Aufsichtsbehörde zu verständigen, ist Folgendes abzuwägen: Wenn eindeutige und sinnvolle **Schadensminimierungsmaßnahmen** möglich sind, so sind diese **sofort** zu ergreifen. Hinsichtlich des Benachrichtigungszeitpunkts sind jedenfalls die Ausführungen des ErwGr 86 letzter Satz und ErwGr 87 zweiter Satz zu beachten.

Wenn sinnvolle Schadensminimierungsmaßnahmen nicht klar definiert werden können, sollte die Aufsichtsbehörde am besten am gleichen Tag informiert werden bzw innerhalb von maximal 72 Stunden. Mit dieser sollten die weiteren Maßnahmen detailliert abgestimmt werden. Die Aufsichtsbehörde kann auch mittels Beschluss Maßnahmen anordnen.

Muster für eine Meldung

Es wurden am 11. April auf der Webseite des öffentlichen „Datenfreund-Blogs" Kundendaten der Unbeschwert GmbH von Unbekannten (laut IP-Adresse von einem weißrussischen Server aus) gepostet. Die Daten stammen aus dem CRM-System, der Zugang erfolgte mittels Logindaten einer Mitarbeiterin, die am 30. März ausgeschieden war. Die Analyse der Logdaten vom 12. April ergab, dass im Zuge des unbefugten Datenabflusses vom 10. April aus der Kundendatei der Unbeschwert GmbH 1.651 Datensätze kopiert wurden. Pro Datensatz (= Firmenkunde) betrifft dies 1 bis 5 natürliche Personen von denen folgende Datenarten unbefugt abgeflossen sind: Adressdaten, Kontaktdaten, Firmenposition, bisher getätigte Käufe nach Gruppen und Euro, Hobby, Lebenspartner und Kontaktschiene zur Unbeschwert GmbH. Die Anzahl der betroffenen Personen beläuft sich voraussichtlich auf 4.386.

Anmerkung: *Namen und die Kontaktdaten des Datenschutzbeauftragten oder einer sonstigen Anlaufstelle für weitere Informationen.*

Es steht unser Privacy-Koordinator Mag. Ing. Markus Sorgenvoll als Ansprechpartner zur Verfügung unter 0777-1234567 oder markus.sorgenvoll-@unbeschwert.at

Anmerkung: *Eine Beschreibung der wahrscheinlichen Folgen der Verletzung des Schutzes personenbezogener Daten.*

Die Analyse der Datenarten ergab, dass Daten aus den Bereichen Kontaktinformation, Verhältnis zur Gesellschaft und aus der persönlichen Lebensführung stammen. Die Folgen für den Betroffenen sind dahingehend teilweise gravierend, da auch Daten aus der persönlichen Lebensführung veröffentlicht wurden und die Unbeschwert GmbH nicht einschätzen kann, inwieweit diese Offenlegung die betroffenen Personen schädigt oder sonstige negative Auswirkungen auf die Betroffenen hat.

Anmerkung: *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.*

Es wurden seitens der Unbeschwert GmbH folgende Maßnahmen ergriffen:
Es wurden alle User des CRM-Systems inaktiv gesetzt und werden nun neu vergeben. Aus Vorsichtsgründen erfolgt dies auch bei allen anderen Systemen mit User-Login.
Es wurde eine Spezialfirma beauftragt die eine physische Löschung der relevanten Daten bei der „Firma Datenfreund-Blogs INC" mit Sitz in Irland auf rechtlichem und technischem Weg erwirkt. Dies wird voraussichtlich heute, 12. April, gegen 21:00 MEZ erfolgt sein.
Es werden jede natürliche Person und die Geschäftsführung der betroffenen Gesellschaften per E-Mail verständigt und genau über Art bzw Zeitpunkt der Datenpanne und Type bzw Anzahl unlauter abgeflossenen Daten informiert. Zudem steht unser Privacy-Koordinator Mag. Ing. Markus Sorgenvoll als Ansprechpartner zur Verfügung.

Phase 8 – Maßnahmen zur Schadensbeseitigung

Wichtigste Maßnahme ist eine genaue Kenntnis von Art, Umfang und Kombinierbarkeit der ungewollt abgeflossenen Daten; dann ist zumeist ein **Mix** aus technischen, organisatorischen und medialen **Maßnahmen** zu definieren, um die Schäden für die betroffenen Personen zu minimieren oder zu beseitigen. Dies könnte im Fall von abgeflossenen Kreditkartendaten zB eine sofortige Weitergabe der (wahrscheinlich) gestohlenen Kreditkartendaten an die „payment-provider" und Kreditkarteninstitute sein, die eine sofortige Gegenmaßnahmen einleiten können wie zB ein „high level monitoring" der Nummern und/oder eine Sperrung der Kartennummern.

Phase 9 und 10 – Vollständige Analyse und Verbesserungen

Hierzu ist eine genaue Beleuchtung aller relevanten Prozesse, in denen personenbezogenen Daten ver- und bearbeitet werden, notwendig. Des Weiteren sind die **Datensicherheitsmaßnahmen** gem Art 32 (Sicherheit der Verarbeitung) genau zu erfüllen bzw ist zu evaluieren, warum die Effektivität der IT-Kontrollen nicht gegeben war. Es sind – eventuell in Abstimmung mit der Aufsichtsbehörde – nachhaltige Prozessverbesserungen und die Herstellung bzw Wiederherstellung der Sicherheit der Verarbeitung durchzuführen.

Resümee

Die neue Regelung wird in vielen Fällen dafür sorgen, dass betroffene Personen tatsächlich über einen sie betreffenden Datenabfluss informiert werden und entsprechend handeln können. Der für die Verarbeitung Verantwortliche erhält klarere Regeln und auch eine weitreichende Unterstützung bzw verpflichtende Anleitung durch die Behörde. Dies wird am Ende allen Beteiligten nützen!

Dako 2017/3

Zum Thema

Über den Autor

Mag. Ing. Markus Oman, CSE, ist geschäftsführender Gesellschafter der O.P.P. – Beratungsgruppe. Kontakt: Tel: +43 (0)699 125 180 89, E-Mail: datenschutz@opp-beratung.com, Internet: www.opp-beratung.com

Hinweis

Dieser Beitrag ist der 8. Teil der Serie zum künftigen EU-Datenschutzrecht. Bisher erschienen sind:

- ***Knyrim*, Die Datenschutz-Grundverordnung: Entwicklung und Anwendungsbereich, Dako 2015/21;**
- ***Pollirer*, Die Datenschutz-Grundverordnung: Der Datenschutzbeauftragte, Dako 2015/37;**
- ***Pollirer*, Die Datenschutz-Grundverordnung: Die Datenschutz-Folgenabschätzung, Dako 2015/47;**
- ***Wagner*, Die Datenschutz-Grundverordnung: Die Betroffenenrechte, Dako 2015/59;**
- ***Knyrim*, Die Datenschutz-Grundverordnung: Die neuen Pflichten, Dako 2016/6;**
- ***Leissler/Wolfbauer*, Die Datenschutz-Grundverordnung: Das „One-Stop-Shop"-Prinzip, Dako 2016/23;**
- ***Haidinger*, Geltendmachung der Betroffenenrechte und das Auskunftsrecht nach der EU-Datenschutzgrundverordnung, Dako 2016/73.**