SCHADEN.NEWS


07.03.2018

SO HANDELN SIE RICHTIG BEI EINER DATENPANNE

Eine Datenpanne ist schnell passiert. Egal, ob ein Hacker in das Computernetzwerk eindringt, eine E-Mail mit Kundendaten versehentlich an eine falsche – namensgleiche – Person verschickt oder der Laptop in einem Verkehrsmittel vergessen oder gestohlen wird. Worauf sollte der Betrieb bei einer solchen Panne vor dem Hintergrund der Datenschutzgrundverordnung (DSGVO) insbesondere ab 25. Mai 2018 achten?

GRUNDSÄTZLICH IST JEDE VERLETZUNG PERSONENBEZOGENER DATEN MELDEPFLICHTIG

Wenn eine Verletzung personenbezogener Daten passiert ist, muss der Verantwortliche diese, innerhalb von 72 Stunden nach Bekanntwerden bei der zuständigen Aufsichtsbehörde melden (Art. 33 Abs. 1 DSGVO). Ob ihn an der Datenschutzverletzung ein Verschulden trifft, ist dabei ebenso unerheblich, wie die Schwere. Vor der Meldung sollte unbedingt das Management oder die Geschäftsführung eingeschaltet werden. Schließlich ist Datenschutz Chefsache und nichts wäre peinlicher, als eine überhastete, aber letztendlich nicht gerechtfertigte Meldung.

Gemäß Art. 33 Abs. 3 DSGVO muss die Meldung mindestens folgende Informationen enthalten:

1. 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

2. den Namen und die Kontaktdaten des Datenschutzbeauftragten oder einer sonstigen Anlaufstelle für weitere Informationen;

3. eine Beschreibung der wahrscheinlichen Folgen der Verletzung des Schutzes personenbezogener Daten

4. 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 ERGRIFFENEN MASSNAHMEN DOKUMENTIEREN

Darüber hinaus fordert Art. 33 Abs. 5 DSGVO, dass der Verantwortliche die Verletzungen des Schutzes personenbezogener Daten einschließlich aller damit im Zusammenhang stehenden Fakten, deren Auswirkungen und die ergriffenen Abhilfemaßnahmen dokumentiert.

Sollten die Informationen nicht innerhalb der 72 Stunden Frist zur Verfügung stehen oder nicht gleichzeitig zur Verfügung gestellt werden können, kann die Meldung auch später, ohne unangemessene weitere Verzögerung erfolgen. Allerdings ist die Verzögerung der Aufsichtsbehörde gegenüber zu begründen. Der Wert eines sauber geführten Verzeichnisses der Verarbeitungstätigkeiten und einer sorgfältig durchgeführten Risikoanalyse zeigt sich spätestens jetzt. Denn für denjenigen, der gut vorbereitet ist, dürfte das „Datenleck“ nicht nur schnell zu finden, sondern auch zu schließen sein.

IN BESTIMMTEN FÄLLEN KANN DIE MELDUNG UNTERBLEIBEN

Vor einer Meldung an die Aufsichtsbehörde sollte in jedem Fall ermittelt werden, welche Daten von der Datenschutzverletzung betroffen sind. Schließlich kann die Benachrichtigung nicht unterbleiben, wenn die „Verletzung des Schutzes personenbezogener Daten voraussichtlich nicht zu einem Risiko für die Rechte und Freiheiten natürlicher Personen führt“, wie es in Art. 33 Abs. 1 DSGVO heißt.

Zunächst ist daher festzustellen, ob die Verletzung personenbezogene Daten betroffen hat. Waren „nur“ personenunabhängige Fachinformationen betroffen, ist eine Meldung nicht erforderlich.

Doch auch für den Fall, dass personenbezogene Daten betroffen waren, besteht die Meldepflicht nur dann, wenn sie zu einem Risiko für die Rechte und Freiheiten des Betroffenen führen kann. Welche Nachteile das im Einzelnen sein können, zeigt Erwägungsgrund 85:

„physischen, materiellen oder immateriellen Schaden für natürliche Personen …, wie etwa Verlust der Kontrolle über ihre personenbezogenen Daten oder 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.“

Dies kann zum Beispiel der Fall sein, wenn von der Verletzung Daten betroffen sind, die sich auf Bewertungen, wie etwa die Arbeitsleistung, wirtschaftliche Lage, Gesundheit, persönliche Vorlieben oder Interessen, die Zuverlässigkeit oder das Verhalten, den Aufenthaltsort einer Person betreffen und der Verletzer damit Profile erstellen kann. Dasselbe gilt, wenn die Daten von Kindern oder einer großen Anzahl von Personen betroffen sind.

BENACHRICHTIGEN SIE DIE BETROFFENEN PERSONEN

Gemäß Art. 34 DSGVO sind nicht nur die Aufsichtsbehörden, sondern auch die betroffenen Personen in einfacher und klar verständlicher Sprache und unverzüglich über den Vorfall zu benachrichtigen. Die Benachrichtigung sollte folgende Informationen enthalten:

• Beschreibung der Art der Verletzung des Schutzes personenbezogener Daten
• An die betroffene Person gerichtete Empfehlungen zur Minderung etwaiger nachteiliger Auswirkungen dieser Verletzung

Wenn ein unmittelbarer Schaden droht, muss die Benachrichtigung sofort erfolgen. Eine längere Frist ist nur dann gerechtfertigt, „wenn es darum geht, geeignete Maßnahmen gegen fortlaufende oder vergleichbare Verletzungen des Schutzes personenbezogener Daten zu treffen." Abhängig von den Umständen des Einzelfalls, insbesondere dem mit der Benachrichtigung verbundenen Aufwand, kann die Information der betroffenen Personen individuell, durch öffentliche Bekanntmachung oder eine ähnlich wirksame Maßnahme, z.B. in den Medien, erfolgen.

DER VERANTWORTLICHE IST IN DER PFLICHT

Die Beurteilung darüber, ob eine derartige Gefahr gegeben ist, obliegt dem Verantwortlichen. Entscheidend sind die Schwere der Verletzung und die Eintrittswahrscheinlichkeit eines Schadens ab.

Die Überlegungen, d.h. die Prognosen die zu dieser Einschätzung geführt haben, sollten unbedingt dokumentiert werden. Schließlich ist der Behörde im Zweifelsfall gegenüber nachzuweisen, dass etwa erforderliche Maßnahmen nicht aus Nachlässigkeit, sondern aufgrund einer nachvollziehbaren Analyse aufgrund des zum Zeitpunkt der Prognose verfügbaren Wissens unterblieben sind. Dies ist insbesondere deshalb wichtig, da die Entscheidung der vollen gerichtlichen Kontrolle unterliegt.

Wer geeignete technische und organisatorische Maßnahmen (TOM) nachweisen kann, weil er z.B. seine Systeme stets auf dem Stand der Technik gehalten und die Daten verschlüsselt oder pseudonymisiert verarbeitet hat, tut sich damit sicher leichter, als derjenige, der die Daten „ungeschützt im Klartext" auf seinen Systemen liegen hat.

ABSCHLIESSENDE BEMERKUNG

Das Wirksamwerden der DSGVO wird das Schattendasein, das der Datenschutz bisher vielfach geführt hat, endgültig beenden. Angesichts des Umstands, dass Abmahnungen lukrativ sind, werden vielerorts bereits jetzt die Messer gewetzt und es ist höchste Zeit, seine Datenverarbeitung an die neue Situation anzupassen. Dies gilt übrigens nicht nur für die EDV, sondern auch für „analoge" Systeme.

Dr. Wolf-Henning Hammer (Kanzlei Voigt)