Verhalten bei einer Datenpanne

Ein Verantwortlicher muss den Auf- und Anforderungen (z.B. nach Auskünften, Unterlagen oder zur Zusammenarbeit) der Aufsichtsbehörde nachkommen, die diese im Rahmen ihrer Aufgabenerfüllung und ihrer Befugnisse an ihn richtet, Art. 31 der europäischen Datenschutzgrundverordnung (DSGVO).

Unabhängig von einer Aufforderung bestehen folgende Pflichten:

Meldung eines evtl. Datenschutzbeauftragten

Mitteilung von Name und Kontaktdaten des Datenschutzbeauftragten. Seitens der Landesbeauftragten für Datenschutz und Informationsfreiheit Nordrhein-Westfalen (LDI) wird aktuell mitgeteilt, dass beabsichtigt ist, eine Möglichkeit zur Online-Meldung anzubieten und "Mitteilungen, die vor der Fertigstellung eingehen, nicht berücksichtigt werden können". Die Frist, der LDI den Datenschutzbeauftragten zu benennen, beginnt am 25.05.2018 und endet am 31.12.2018.

"Datenpanne"

Wird dem Verantwortlichen eine Datenschutzverletzung bekannt, muss er dies unverzüglich, d.h. ohne schuldhaftes Zögern, und möglichst binnen 72 Stunden der Aufsichtsbehörde melden, es sei denn, dass die Verletzung voraussichtlich nicht zu einem Risiko, z.B. der Persönlichkeitsrechte von Betroffenen, führt (Art. 33 Abs. 1 und 2 DSGVO). Erfolgt die Meldung nicht binnen 72 Stunden, muss die Verzögerung begründet werden. Die Meldung muss enthalten:

- Art der Verletzung; soweit möglich mit Angabe der Kategorien und der ungefähren Zahl der betroffenen Personen / Datensätze;
- Name, Kontaktdaten des Datenschutzbeauftragten oder einer anderen Anlaufstelle;
- Beschreibung der wahrscheinlichen Folgen;
- Beschreibung der ergriffenen oder vorgeschlagenen Maßnahmen zur Behebung bzw. Abmilderung.

Hat eine "Datenpanne" voraussichtlich ein hohes Risiko z.B. für das Persönlichkeitsrecht zur Folge, muss der Verantwortliche auch die betroffenen Personen unverzüglich informieren, Art. 34 DSGVO. Die Benachrichtigung entspricht im Wesentlichen der o.g. Meldung an die Aufsichtsbehörde (mit Ausnahme der Zahl der Betroffenen/Datensätze). Eine Pflicht zur Benachrichtigung besteht nur dann nicht, wenn eine der folgenden Bedingungen erfüllt ist, siehe Art. 34 Abs. 3 DSGVO:

- es wurden geeignete technische und organisatorische Vorkehrungen in Bezug auf die von der Datenschutzverletzung betroffenen Daten getroffen, ausdrücklich insbesondere z.B. Verschlüsselung (also ein Fehlschlagen eigentlich geeigneter, angemessener Maßnahmen);
- durch Maßnahmen nach der Datenschutzverletzung ist sichergestellt, dass ein hohes Risiko für Rechte und Freiheiten der Betroffenen "aller Wahrscheinlichkeit nach nicht mehr besteht";
- die Benachrichtigung wäre mit einem unverhältnismäßigen Aufwand verbunden - in dem Fall muss stattdessen aber eine öffentliche Bekanntmachung oder eine ähnliche Maßnahme erfolgen.

Unabhängig von oben Gesagtem ist jede Datenschutzverletzung stets zumindest zu dokumentieren, einschließlich aller damit im Zusammenhang stehenden Fakten, der Auswirkungen und ergriffenen Abhilfemaßnahmen. Dies soll der Aufsichtsbehörde z.B. die Überprüfung der Einhaltung der Melde- oder Benachrichtigungspflicht ermöglichen, Art. 33 Abs. 5 DSGVO.

Kontaktdaten der Aufsichtsbehörde

Die Landesbeauftragte für Datenschutz und Informationsfreiheit Nordrhein-Westfalen (LDI)
Postfach 20 04 44
40102 Düsseldorf
Tel.: 0211/38424-0
Fax: 0211/38424-10
E-Mail: poststelle@ldi.nrw.de

Dieses Informationsblatt wurde erarbeitet von der Arbeitsgemeinschaft der nordrhein-westfälischen Heilberufskammern (Ärztekammer Nordrhein, Ärztekammer Westfalen-Lippe, Apothekerkammer Nordrhein, Apothekerkammer Westfalen-Lippe, Kammer für Psychologische Psychotherapeuten und Kinder- und Jugendlichenpsychotherapeuten Nordrhein-Westfalen, Tierärztekammer Nordrhein, Tierärztekammer Westfalen-Lippe, Zahnärztekammer Nordrhein sowie Zahnärztekammer Westfalen-Lippe) sowie den Kassenärztlichen Vereinigungen Nordrhein und Westfalen-Lippe und gibt den Stand der Meinungsbildung vom 15.05.2018 wieder.