Meldung von Verletzungen des Schutzes personenbezogener Daten („Datenpanne“)

Für die Verarbeitung personenbezogener Daten müssen Verantwortliche wissen, dass den Auf- und Anforderungen der Aufsichtsbehörde (z.B. zur Erteilung von Auskünften bzw. Vorlage von Unterlagen oder zur Zusammenarbeit) nachzukommen ist, die diese im Rahmen ihrer Aufgabenerfüllung und ihrer Befugnisse an sie richten (Art. 31 der europäischen Datenschutzgrundverordnung - DSGVO -).

Unabhängig hiervon besteht eine umfassende Pflicht für Verantwortliche, der Aufsichtsbehörde Verletzungen des Schutzes personenbezogener Daten zu melden.

Eine Verletzung des Schutzes personenbezogener Daten liegt nicht nur dann vor, wenn diese Dritten offen gelegt wurden bzw. sie unbefugt Zugang erlangt haben, sondern auch dann, wenn personenbezogene Daten unbeabsichtigt oder unberechtigt vernichtet, verloren oder verändert wurden (Art. 4 Abs. 12 DSGVO).

Wird dem Verantwortlichen eine Verletzung des Schutzes personenbezogener Daten 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

Grundsätzlich nicht erforderlich ist es jedoch, eine Kopie der betroffenen Datensätze an die Aufsichtsbehörde zu übermitteln. Die Aufsichtsbehörden weisen zudem im Kurzpapier Nr. 18 darauf hin, dass „die Formulierung ‚nicht zu einem Risiko‘ von ihrem Sinn und Zweck ausgehend als ‚nur zu einem geringen Risiko‘ führend verstanden“ wird.

Zur Erleichterung einer den Anforderungen entsprechenden Meldung und um notwendige Rückfragen zu minimieren, hat die LDI NRW ein Meldeformular entwickelt, das unter ldi.nrw.de zur Verfügung steht.

Hat eine "Datenpanne" voraussichtlich ein hohes Risiko z.B. für das Persönlichkeitsrecht zur Folge, muss der Verantwortliche zusätzlich zur Meldung an die Aufsichtsbehörde auch die betroffenen Personen unverzüglich informieren (Art. 34 DSGVO). Die klar und einfach zu formulierende Benachrichtigung entspricht inhaltlich 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, durch die die personenbezogenen Daten für Unbefugte unzugänglich gemacht wurden.
- 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 diesem Fall muss stattdessen eine öffentliche Bekanntmachung oder eine ähnliche Maßnahme erfolgen.

Unabhängig von oben Gesagtem ist jede Datenschutzverletzung stets einschließlich aller damit im Zusammenhang stehenden Fakten, der Auswirkungen und ergriffenen Abhilfemaßnahmen zumindest zu dokumentieren. 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

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 unter Mitwirkung der Landesbeauftragten für Datenschutz und Informationsfreiheit Nordrhein-Westfalen und gibt den Stand der Meinungsbildung vom 23.11.2018 wieder.

(*) Als Heilberufler gelten die Mitglieder der vorgenannten Kammern.

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