



Wann Sie Datenlecks melden müssen

Wann Sie Datenlecks melden müssen

Die europäische Datenschutz-Grundverordnung (DSGVO) sieht vor, dass die jeweils zuständige Aufsichtsbehörde über die Verletzung des Schutzes personenbezogener Daten zu informieren ist. Aber welche Arten von Datenpannen sind den Behörden zu melden?

Artikel 33 DSGVO als Richtschnur

Artikel 33 der DSGVO besagt, dass die verantwortliche Stelle im Falle einer Verletzung des Schutzes personenbezogener Daten die Aufsichtsbehörde unterrichtet: unverzüglich, möglichst aber binnen 72 Stunden. Der Absatz 3 des Artikels beschreibt sehr umfassend, welche Informationen dabei an die Behörde zu liefern sind.

In der Praxis wirft der Artikel die Frage auf, welche Art von Datenschutz-Verletzungen zu melden sind. Denn hier hat der Gesetzgeber den verantwortlichen Stellen die Aufgabe überlassen, die Abwägung vorzunehmen.

Und das löst Unsicherheit aus. Denn nur ein Verhalten, das mit Artikel 33 konform geht, minimiert Risiken in Hinblick auf Schadensersatz und Haftung.

Bewertung nicht eindeutig formuliert

Der Gesetzestext setzt ein sehr enges Zeitfenster, innerhalb dessen die Meldung zu erfolgen hat. Deshalb sehen sich die Verantwortlichen nicht nur mit der Behebung eventueller Datenlecks konfrontiert.

Sie haben auch unter Zeitdruck die Entscheidung zu fällen, ob überhaupt zu unterrichten ist. „Bauchgefühl“ oder „gesunder Menschenverstand“ helfen hier nicht weiter.

So ist eine Attacke auf die internen Systeme eines Unternehmens nicht meldepflichtig, wenn nachweislich keine personenbezogenen Daten betroffen waren. Dabei kann die Attacke mit stundenlangem Stillstand von Systemen und damit auch finanziellen Verlusten verbunden gewesen sein.

Der Diebstahl eines USB-Sticks mit Patientenakten wird dagegen meldepflichtig sein, selbst wenn es sich dabei um ein sehr begrenztes Ereignis handelte.

Behörde nennt Praxisbeispiele

Es herrscht also Unsicherheit darüber, welche Vorfälle Verantwortliche melden müssen und ob diese auch die Information der Betroffenen nach sich ziehen.

Dieser Befangenheit will ein Leitfaden des Hamburgischen Beauftragten für Datenschutz und Informationsfreiheit begegnen.

Herzstück des Dokuments ist eine Tabelle, die einige Beispiele für Datenlecks beinhaltet. Zu jedem Eintrag finden sich Erklärungen, ob die Aufsichtsbehörde und die Betroffenen zu informieren sind.

Außerdem sind Hinweise enthalten, wie das Risiko zu bewerten ist, wenn es zu einem Datenleck kam.

Die kompakte und kostenfreie Broschüre [laden Sie sich direkt als PDF-Datei herunter](#). Sie ist (nicht nur im Ernstfall) eine hervorragende Handreichung, die mehr Sicherheit schafft.

Quelle:

www.datenschutz-praxis.de

Autor Stephan Lamprecht