

Merkblatt Meldepflicht bei Datenschutzpannen

Hinweis: Die nachfolgenden Fragen und Antworten sind sorgfältig erstellt, jedoch nicht durch die Aufsichtsbehörden geprüft worden. Die Landes Zahnärztekammer Baden-Württemberg kann daher keine Haftung für die Fragen und Antworten übernehmen. Der Fragenkatalog ersetzt keinesfalls eine Beratung durch einen Rechtsanwalt.

1. Welche Meldepflichten hat die Praxis?

Die neue EU-Datenschutz-Grundverordnung (EU-DSGVO) sieht in Art. 33 vor, dass Datenschutzpannen, die mit einem Risiko für die betroffenen Patienten einhergehen (z. B. durch Diebstahl von Computern oder Datensicherungen und Hackerangriffe auf Praxiscomputer, aber auch der Verlust des Handys, auf dem Praxis-E-Mails gelesen werden können) zu melden sind.

2. Wer muss die Information über Datenschutzpannen erhalten?

Datenschutzpannen sind der zuständigen Landesdatenschutzbehörde:

*Landesbeauftragten für den Datenschutz
und die Informationsfreiheit Baden-Württemberg
Königstraße 10 a
70173 Stuttgart*

in der Regel **innerhalb von 72 Stunden**, gerechnet ab dem Zeitpunkt, ab dem die Praxis sichere Kenntnis von der Panne erlangt hat, zu melden.

Bei der Meldung ist nach folgendem Risikoraster vorzugehen:

1. Besteht nur ein geringes Risiko für personenbezogene Daten, so ist nur eine interne Dokumentation nötig (bspw. eine gestohlene Festplatte ist physisch und kryptografisch gegen unbefugten Zugriff gesichert)
2. Besteht ein mittleres Risiko für personenbezogene Daten, so ist dies intern zu dokumentieren und es muss eine Meldung an den Landesbeauftragten für Datenschutz erfolgen (bspw. Angriff mittels Verschlüsselungstrojaner, bei dem der Zugriff auf personenbezogene Daten nicht ausgeschlossen werden kann)
3. Besteht ein hohes Risiko für personenbezogene Daten, so ist dies intern zu dokumentieren und es muss neben einer Meldung an den Landesbeauftragten für Datenschutz auch eine Information an die betroffenen Patienten erfolgen (z. B. eine unverschlüsselte und auch nicht anderweitig gegen unbefugte Zugriffe geschützte Festplatte mit Patientendaten wird entwendet bzw. geht verloren). Eine solche Meldung sollte in Absprache mit der Landesdatenschutzbehörde erfolgen – siehe letzter Abschnitt „Wann muss der Patient informiert werden?“.

3. Wann muss der Patient informiert werden?

Die EU-DSGVO sieht in Art. 34 auch eine Mitteilung der Datenschutzpanne an die durch die Panne betroffenen Patienten vor. Diese Meldung ist aber nur dann erforderlich, wenn ein hohes Risiko mit der Datenschutzpanne für die betroffenen Patienten verbunden ist. Eine solche Meldung sollte in **Absprache mit der Landesdatenschutzbehörde** erfolgen. Nur wenn diese eine Notwendigkeit für die Information der betroffenen Patienten sieht, muss eine entsprechende Mitteilung versandt werden. Eine Frist gibt es für diese Mitteilung an die Patienten, anders als bei der Meldung an die Behörde, nicht.

Ein Mustertext für diese Meldung steht Ihnen auf unserer Webseite zum Download zur Verfügung. Alternativ kann eine Datenpanne auch online unter:

<https://www.baden-wuerttemberg.datenschutz.de/datenpanne-melden/>

gemeldet werden.

Ihre
LZK-Geschäftsstelle