INCIDENT-PLAYBOOK DAT-05

Verdacht auf Datenschutzverletzung

Daten & Datenschutz

Personenbezogene Daten sind möglicherweise verloren gegangen, an Unbefugte gelangt, verändert worden oder nicht mehr verfügbar. Der Verdacht genügt für die Meldung. Die Bewertung übernehmen andere.

- Kundenliste an den falschen Empfänger geschickt
- Ordner mit Personaldaten offen freigegeben
- Unterlagen mit Kundendaten verloren
- Bewerbungsunterlagen im falschen Postfach gelandet

Sofortmaßnahmen

ERSTE 15 MINUTEN

01 Sofort melden. Die gesetzliche Frist des Unternehmens beginnt mit dem Moment, in dem es Kenntnis erlangt, also mit deiner Meldung.

02 Den Zustand einfrieren: nichts löschen, nichts überschreiben, keine Freigabe stillschweigend zurückziehen.

03 Belege sichern: Screenshot der Freigabe, Kopie der gesendeten Nachricht, Notiz zur Uhrzeit.

04 Notieren, welche Personengruppen und welche Datenarten betroffen sein könnten und wie viele Personen es ungefähr sind.

05 Ist die Ursache noch aktiv, etwa ein offener Link, das der IT beim Melden ausdrücklich sagen.

Melden

SOFORT

WEN

Datenschutz-Ansprechperson und IT-Verantwortliche gemeinsam. Fehlt eine benannte Datenschutz-Ansprechperson, geht die Meldung an die Geschäftsführung.

WIE

Über den internen Meldeweg aus dem Kontaktblatt, ohne Umweg über Zwischenstationen. Bei Unsicherheit telefonisch.

WAS BEREITHALTEN

- Was passiert ist und wann du es bemerkt hast
- Welche Datenarten betroffen sind
- Wie viele Personen ungefähr betroffen sind
- Wer die Daten erhalten haben könnte
- Ob die Ursache noch besteht

Nicht tun

HÄUFIGE FEHLER

- × Erst selbst prüfen, ob es wirklich schlimm ist. Die Bewertung ist Aufgabe der Datenschutz-Ansprechperson.
- × Betroffene Personen auf eigene Faust informieren, bevor das Vorgehen abgestimmt ist.
- × Empfänger bitten, die Nachricht einfach zu löschen, und den Fall damit für erledigt halten.
- × Belege löschen, um die Sache unauffällig zu bereinigen.

Was danach passiert

IT · DATENSCHUTZ · LEITUNG

- → Die Datenschutz-Ansprechperson bewertet, ob eine Verletzung des Schutzes personenbezogener Daten vorliegt und welches Risiko für die betroffenen Personen entsteht.
- → Ergibt die Bewertung ein Risiko, meldet das Unternehmen unverzüglich und möglichst binnen 72 Stunden nach Bekanntwerden an die Datenschutzbehörde (Art. 33 DSGVO).
- → Bei voraussichtlich hohem Risiko werden zusätzlich die betroffenen Personen unverzüglich benachrichtigt (Art. 34 DSGVO).
- → Auch Verletzungen ohne Meldepflicht werden intern dokumentiert. Die Dokumentation ist selbst eine gesetzliche Pflicht.

Verweise: Incident-Kontaktblatt (PDF) · Gesetze und Regulierung im Wissensbereich · Interne Kontakte siehe Incident-Kontaktblatt

Playbooks sind der Anfang. Der Prozess dahinter ist Führungsarbeit.

Alle Playbooks, Kontaktblatt und Hintergründe online — kostenfrei und ohne Anmeldung.

wermescher.com/tools/it-notfallplan