WHITEPAPER – letzte Überarbeitung März 2024

Wo & was melde ich? Wie verhalte ich mich?

Datenpannen Management – Wir erklären, was Sie nach Art. 33 DSGVO zu tun haben

GLENDE CONSULTING

In diesem Whitepaper geht es darum, wie Sie Datenschutzpannen in Ihrem Unternehmen effektiv handhaben – von der Vorbeugung über das gezielte Krisenmanagement bis hin zur sorgfältigen Aufarbeitung des Vorfalls. Datenschutzpannen sind heutzutage leider allgegenwärtig und verlangen nach einer prompten und besonnenen Reaktion. Es spielt keine Rolle, ob das Problem von innen kommt oder von außen verursacht wurde; wichtig ist, dass Sie schnell verstehen, was passiert ist. Das bedeutet, Sie müssen sofort entscheiden, ob Sie den Vorfall den Datenschutzbehörden melden und ob Sie die betroffenen Personen informieren müssen. Auch eine gründliche Risikobeurteilung gehört dazu.

Vergessen Sie nicht: Wenn durch den Vorfall die Rechte und Freiheiten der betroffenen Personen Übergebühr bedroht sind, haben Sie 72 Stunden Zeit, die Behörden zu informieren, nachdem Sie von der Panne erfahren haben.

Vorbeugung

Ergreifen Sie proaktive Schritte, um auf eine mögliche Datenschutzpanne vorbereitet zu sein:

- Zuweisung klarer Zuständigkeiten
- Bereitstellung von Mustern und Checklisten zur Bewertung eines Datenschutzvorfalls
- Sensibilisierung für die Einhaltung der 72-Stunden-Meldefrist
- Festlegung interner Abläufe im Falle einer Datenschutzpanne
- Durchführung zielgerichteter Schulungen für die Belegschaft

KOMMUNIKATION UND BENACHRICHTIGUNGSREGELN

Definieren Sie Regeln, wer in welcher Form und Frist informiert wird. Die Kommunikation mit Betroffenen ist erforderlich, wenn ihre Daten durch die Panne einem hohen Risiko ausgesetzt sind, wie bei besonderen Kategorien personenbezogener Daten oder bei Bank- und Kreditkarteninformationen. In bestimmten Situationen kann von einer Benachrichtigung abgesehen werden, etwa wenn durch ergriffene Maßnahmen das Risiko nicht mehr besteht. Benachrichtigungen sollten unverzüglich und in klarer, einfacher Sprache erfolgen.

Während einer Datenschutzpanne

- Koordination mit IT-Verantwortlichen
- Ergreifen von Sofortmaßnahmen, z. B. Abschaltung betroffener Systeme
- Nachverfolgung verlorener Geräte
- Änderung von Passwörtern und Sperren von Fernzugriffen
- Ermitteln der Rechtsverletzung Dritter

Ziehen Sie Experten hinzu, um den Vorfall zu bewältigen, einzudämmen und zu dokumentieren.

Interne Erstmeldung: Nutzen Sie vorgefertigte Formblätter für die interne Dokumentation des Vorfalls.

DOKUMENTATION UND RISIKOERMITTLUNG

Dokumentieren Sie alle Aspekte des Vorfalls und bewerten Sie das Risiko für die betroffenen Personen. Hierzu kann als Leitfaden das Kurzpapier Nr. 18 der Datenschutzkonferenz dienen.

Kurzpapier Nr. 18 der Datenschutzkonferenz

Bitte entnehmen Sie weitere Informationen und die erforderlichen Schritte zur Meldung aus dem Anhang und der bereitgestellten Linksammlung. Beachten Sie dabei, dass bei grenzüberschreitenden Sachverhalten die Aufsichtsbehörde am Hauptsitz des Verantwortlichen zuständig ist und bei Unsicherheiten die Behörde kontaktiert werden sollte, in deren Zuständigkeitsbereich sich der Vorfall ereignet hat.

Nach einer Datenpanne

Nach einer Datenschutzverletzung und deren Meldung ist die Nachbereitung des Vorfalls von entscheidender Bedeutung, um das Ausmaß des Schadens zu begrenzen, zukünftige Vorfälle zu verhindern und das Vertrauen der betroffenen Personen sowie der Öffentlichkeit wiederherzustellen. Hier sind einige sinnvolle Maßnahmen:

Interne Untersuchung
Führen Sie eine gründliche Untersuchung durch, um die Ursache und den Umfang der Datenschutzverletzung zu verstehen. Dokumentieren Sie, welche Daten betroffen waren, wie die Verletzung passieren konnte und warum sie nicht verhindert wurde.

Überarbeitung der Datenschutzrichtlinien
Überprüfen und aktualisieren Sie Ihre Datenschutzrichtlinien und Verfahren, um eventuelle Schwachstellen zu beheben, die zu der Verletzung geführt haben. Stellen Sie sicher, dass alle Richtlinien den aktuellen gesetzlichen Anforderungen entsprechen.

ggf. Schulung der Mitarbeiter
Verstärken Sie die Schulungsmaßnahmen für Mitarbeiter in Bezug auf Datenschutz und Sicherheit. Stellen Sie sicher, dass alle Mitarbeiter die Bedeutung des Datenschutzes verstehen und wissen, wie sie Daten richtig handhaben müssen.

Technische Sicherheitsmaßnahmen
Verbessern Sie die technischen Sicherheitsmaßnahmen, wie z. B. die Implementierung von Multi-Faktor-Authentifizierung, Verschlüsselung von Daten und regelmäßige Sicherheitsüberprüfungen.

Beziehung zu Dienstleistern überprüfen
Falls Dritte an der Verletzung beteiligt waren, überprüfen und bewerten Sie die Sicherheitsmaßnahmen Ihrer Dienstleister. Schließen Sie gegebenenfalls neue Vereinbarungen ab oder wechseln Sie zu Dienstleistern mit höheren Sicherheitsstandards.

Incident Response Plan
Überarbeiten Sie Ihren Incident Response Plan, um sicherzustellen, dass Sie für zukünftige Vorfälle besser gerüstet sind. Der Plan sollte klare Verantwortlichkeiten und Abläufe für den Fall einer Datenschutzverletzung festlegen.

Evaluierung und kontinuierliche Verbesserung
Bewerten Sie regelmäßig Ihre Datenschutzpraktiken und -verfahren, um kontinuierliche Verbesserungen sicherzustellen. Nehmen Sie die Datenschutzverletzung als Anlass, Ihre Prozesse zu überdenken und zu stärken.

Beispiele für Datenpannen

E-Mail Leck
Ein Mitarbeiter sendet versehentlich eine Massen-E-Mail mit sichtbaren E-Mail-Adressen aller Empfänger, statt die BCC-Funktion zu nutzen.

Verlorener Laptop
Ein Firmenlaptop mit unverschlüsselten sensiblen Kundeninformationen geht auf einer Geschäftsreise verloren.

Hackerangriff
Cyberkriminelle erlangen durch eine Sicherheitslücke Zugriff auf die Kundendatenbank eines Unternehmens.

Phishing Betrug
Ein Mitarbeiter gibt versehentlich Anmeldedaten auf einer gefälschten Webseite ein, was zu einem Datenleck führt.

Unsichere Speicherung
Sensible Dokumente werden auf einem ungesicherten Netzlaufwerk gespeichert, auf das alle Mitarbeiter Zugriff haben.

Malware Infektion
Ein Virus infiziert das Netzwerk eines Unternehmens und sammelt vertrauliche Informationen von verschiedenen Arbeitsstationen.

Datenverkauf durch Mitarbeiter
Ein Mitarbeiter verkauft vertrauliche Kundendaten an Dritte.

Unsachgemäße Datenentsorgung
Ausgemusterte Firmencomputer werden verkauft, ohne die Festplatten zuvor ordnungsgemäß zu löschen.

Software Fehler
Ein Update einer Anwendungssoftware führt dazu, dass private Kundeninformationen öffentlich zugänglich werden.

Social Engineering
Ein Betrüger überzeugt einen Mitarbeiter am Telefon, vertrauliche Informationen preiszugeben, indem er sich als IT-Support ausgibt.

Die EDSA hat Leitlinien mit Beispielen für die Meldung von Verletzungen des Schutzes personenbezogener Daten erstellt.

Leitlinien mit Beispielen für die Meldung von Datenpannen

Entscheiden Sie sich für uns, ist es plötzlich ganz einfach.

WIR KÜMMERN UNS UM DATENSCHUTZ UND INFORMATIONSSICHERHEIT IN IHREM UNTERNEHMEN:

SO KONFORM WIE NÖTIG - SO PROZESSORIENTIERT WIE MÖGLICH!

glende-consulting.de

» BESUCHEN SIE UNS

GLENDE.CONSULTING GmbH & Co. KG
Friedrich-Barnewitz-Str. 7
18119 Rostock-Warnemünde

» SPRECHEN SIE MIT UNS

Tel.: 0381.7787 468-0

» SCHREIBEN SIE UNS

info@glende-consulting.de