VINQO®
RECHTSANWÄLTE

Handlungsempfehlungen bei Datenschutzpannen in kleinen und mittelständischen Unternehmen.

Die Gefahr durch Hacker-Angriffe, Fehler von Mitarbeitenden und sonstige Cybervorfälle nimmt für Unternehmen immer weiter zu. Dabei können Datenschutzverletzungen (auch Datenlecks oder Cyber Security Incidents, Databreaches oder DSGVO-Verstöße genannt) insbesondere für kleine und mittelständische Unternehmen mit Bußgeldern in Höhe von bis zu 20 Mio. Euro oder 4% Jahresumsatz existenzbedrohend sein. 2023 sind durchschnittlich pro Verstoß Bußgelder in Höhe von 2,8 Millionen Euro verhängt worden - 2019 waren es noch etwa 500.000 Euro.

Die Einhaltung datenschutzrechtlicher Vorschriften ist im vielschichten Unternehmeralltag ohne Zweifel kein Lieblingsthema. Insbesondere in kleinen und mittelständischen Unternehmen, in denen kein dezidiertes Personal für IT-Sicherheit vorhanden ist, können Datenschutzvorfälle ein existenzbedrohendes Szenario darstellen.

Wir zeigen, welche rechtliche Risiken bei einem Datenschutzverstoß bestehen und wie Sie als Geschäftsführer oder Vorstand vorgehen sollten, um Bußgelder und Schäden für Ihr Unternehmen möglichst gering zu halten.

Folgen eines Datenschutzverstoßes

Die DSGVO konfrontiert Unternehmen bei Datenschutzvorfällen mit gleich mehreren Fronten: einem Bußgeldverfahren, Schadenersatzansprüchen, Reputationsschäden – und einer Meldefrist von gerade einmal 72 Stunden.

Bußgeldverfahren

Mit der Verpflichtung zur Meldung eines potenziellen Datenschutzverstoßes innerhalb von 72 Stunden (Art. 33 DSGVO), wird ein Ordnungswidrigkeitenverfahren eingeleitet. Stellt sich im weiteren Verfahren heraus, dass die Meldung ohne Rechtfertigung verspätet oder unvollständig erfolgte, droht ein weiteres Bußgeld. Die Sanktionierung im Rahmen des Bußgeldverfahrens soll dabei „*wirksam, verhältnismäßig und abschreckend*" sein (Art. 83 DSGVO).

Deshalb sollten Sie die Meldung an die Aufsichtsbehörde keinesfalls selbständig vornehmen.

Es kommt ganz entscheidend darauf an, was in dieser Meldung kommuniziert wird. Fehlen wichtige Informationen, wird dies die Aufsichtsbehörde bußgelderhöhend werten. Tätigen Sie zu viele Angaben zum potenziellen Datenschutzverstoß, belasten Sie Ihr Unternehmen unnötig selbst. Auch dies kann dann zu einem erhöhten Bußgeld führen. Dabei wird der Aufsichtsbehörde weitreichende Befugnisse eingeräumt, um eigene Untersuchungsmaßnahmen durchzusetzen, bei denen betroffene Unternehmen umfangreich kooperieren müssen (Art. 58 DGSVO).

Das Bußgeld kann dabei, abhängig vom Verstoß, bis zu 40 Mio. Euro bzw. bis zu 4% des weltweiten Jahresumsatzes betragen.

Das Bußgeldverfahren wird bei größeren oder bekannteren Unternehmen zusätzlich regelmäßig veröffentlicht. Damit einher geht ein Reputationsschaden, der unternehmerisch abgefangen werden muss.

Benachrichtigungspflichten

Abhängig von der Datenpanne können Unternehmen verpflichtet sein, nicht nur die Aufsichtsbehörde, sondern auch die Betroffenen zu informieren. Auswahl und Umsetzung des Verfahrens sind ganz besonders kritisch, da hierdurch Reputationsschäden, Schadenersatzansprüche und Beeinträchtigungen in laufenden Geschäftsbeziehungen drohen können.

Die Kommunikation muss deshalb gut vorbereitet und rechtlich sehr genau geprüft werden.

Schmerzensgeld für Betroffene

Ein besonderes Risiko nach Datenschutzpannen ist der in der DSGVO eingeführte Schmerzensgeldanspruch, auch immaterieller Schadenersatzanspruch genannt. Betroffenen eines Datenschutzvorfalls kann ein Anspruch auf Schmerzensgeld zustehen. Der Europäische Gerichtshof (EuGH) hat 2023 noch einmal das sehr weite Verständnis dieses Schmerzensgeldanspruchs betont. Deutsche Gerichte sind im europäischen Vergleich noch etwas zurückhaltender bei der Zuerkennung, allerdings sollte das Risiko eines Masseschadens unternehmerisch nicht verkannt werden:

Abhängig vom Verstoß erkennen Gerichte in Deutschland – arbeitsgerichtliche Verfahren sind hierbei bewusst ausgenommen – Schmerzensgelder in Höhe von 300,00 € ca. 1.000,00 € pro Person zu. Wenn Ihre Kundendatenbank von Hackern im Internet veröffentlicht und nur 10.000 Kunden betroffen sind, besteht ein wirtschaftliches Risiko von **10 Mio. Euro pro Datenpanne** - wohlgemerkt neben dem Bußgeld. Wenn auch noch die Pflicht zur Benachrichtigung der Betroffenen besteht, machen Sie die Betroffenen auf ihren

möglichen Schmerzensgeldanspruch auch noch aufmerksam. Diese Risiken müssen dann ggfs. in der Bilanz mit Rückstellungen abgebildet werden.
Die Rechtsfolgen eines Datenschutzverstoßes sind damit weitreichend und müssen unternehmerisch sehr ernst genommen werden.

Handlungsleitfaden für Unternehmer

Wenn sich der Eindruck festigt, dass Ihr Unternehmen von einer Datenpanne betroffen sein könnte, heißt es erst einmal: Ruhe bewahren. Keinesfalls sollten vorschnell oder panisch E-Mail oder andere Mitteilungen verfasst und versendet werden. Dabei ist zu berücksichtigen, dass sich unsere Empfehlungen an kleinere und mittelständische Unternehmen richten, in denen kein vorher eingerichtetes *Cybersecurity Incident Response Teams* besteht.

1. Verstoß erfassen

Grundlage für die weiteren Schritte ist, das Ausmaß einer Datenschutzverletzung näher eingrenzen zu können. Handelt es sich um die Unachtsamkeit eines Mitarbeiters oder um verschlüsselte Server mit tausenden Kundendaten? Woher kommt die Meldung?
Zeichnet sich ab, dass ein Verstoß vorlegen könnte, bedeutet dies je nach Umfang der Verletzung eine Taskforce zusammenstellen und Termine frühzeitig zu verschieben. Im Falle eines Verstoßes muss die 72 Stunden Frist eingehalten werden.

2. Taskforce zusammenstellen und ergänzen

Stellen Sie eine Taskforce zusammen, die sich prioritär um das Überprüfen und Erfassen des Ausmaßes der Datenpanne bemüht.
Hierzu zählen:

- Mitglied der Geschäftsführung / des Vorstandes
- Leitender Systemadministrator
- Datenschutzbeauftragter (soweit vorhanden)
- Externes IT-Systemhaus, das Ihre IT-Infrastruktur eingerichtet hat oder verwaltet (soweit vorhanden)
- Ansprechpartner Ihrer Cyberversicherung (soweit vorhanden)
- Rechtsanwalt für Datenschutz
- Head of PR (soweit vorhanden)

Aufgrund der besonders zeitkritischen Erledigung von Meldungen, Benachrichtigungen etc. sollte auf eine Kanzlei mit ausreichendem Personal zurückgegriffen werden.

Wir stellen deshalb abhängig von der Größe des betroffenen Unternehmens ein Team von 2 bis 12 Rechtsanwälten und Informatikern bereit, das innerhalb weniger Stunden alle datenschutzrechtlichen Maßnahmen für Sie umsetzt und aufgrund der eigenen inhouse Informatik-Unit auch IT-forensische Maßnahmen in Echtzeit berücksichtigen und juristisch übersetzen kann.

3. Checkliste abarbeiten

Steht die Taskforce fest, sollten die datenschutzrechtlichen Maßnahmen systematisch umgesetzt werden. Dabei ergänzt sich die Checkliste abhängig von der datenschutzrechtlichen Vorarbeit des Unternehmens:

- Gibt es eine Dokumentation über die TOM (Technisch-Organisatorische Maßnahmen?
- Wie ist der dokumentierte Stand der IT-Systeme (Cybersecurity)?
- Gibt es eine konsolidierte Liste der Auftragsdatenverarbeiter?

Fehlen diese Dokumentationen, wirkt sich dies nachteilig auf die Verteidigung nach einer Datenpanne aus, sodass die Dokumentationen schnellstmöglich und noch vor Meldung an die Aufsichtsbehörde nachgeholt werden müssen. Die Reaktion auf einen Datenschutzvorfall sollte dann grundlegend wie folgt aufgebaut werden:

a) Ausmaß des Datenschutzvorfalls konkretisieren. Mitarbeitende nach Auffälligkeiten befragen um ein erstes Bild zusammenzufügen.

b) Betroffene IT-Infrastruktur ermitteln
    a. Gibt es Logs, die noch gesichert werden können?
    b. Welcher Datenverkehr kann in Echtzeit festgestellt werden?
    c. Prüfung, ob Teile der IT-Infrastruktur isoliert oder vollständig heruntergefahren werden kann bzw. soll ohne Beweismittel zu zerstören oder Verschlüsselungen anzustoßen.

c) Bei schweren Systempannen: IT-Cybersecurity-Unternehmen hinzuziehen. Hierzu sollte Kontakt mit dem Service Center des BSI aufgenommen werden.

d) Betroffene Datenkategorien erfassen
    a. Welche Kategorien personenbezogener Daten?
    b. Besondere Kategorien (Gesundheitsdaten o.ä.)?
    c. Welche Datenpunkte sind konkret betroffen?

e) Art der Datenpanne ermitteln
    a. Um was für eine Datenpanne handelt es sich technisch (Scraping, Datenbankdump, offene API, Fehlläufer etc.)?
    b. Wie lange könnte der Vorfall bereits angedauert haben?

f) Quantitativer Umfang?

   a. Wie viele Personen sind vom Vorfall ggfs. betroffen?
   b. Kann eine Liste der Betroffenen rekonstruiert werden?
   c. Können die Datensätze insgesamt rekonstruiert werden?

g) Wann ist der Vorfall erstmals bekannt geworden? (72 Std. Frist)
h) Vorbereitende Maßnahmen für die DSGVO Meldung
   a. Gab es ein dokumentiertes Datenschutzkonzept?
   b. Gab es Unterweisungen oder Schulungen?
   c. Wie war der Stand der Technik im betroffenen Unternehmen?
   d. Welche positiven Umstände können angeführt werden?
   e. Schriftliche und begründete Risikoabwägung im Hinblick auf Meldung und Benachrichtigung
i) Abstimmung und Entwicklung der DSGVO-Meldung zwischen allen Beteiligten der Taskforce
j) Ggfs. Benachrichtigung an Betroffene
k) Einreichung der DSGVO-Meldung
l) Ggfs. Abstimmung Umsetzung von PR-Maßnahmen bei Totalausfällen, insbesondere juristische Abstimmung der Sprachregelungen

Damit sind die ersten 72 Stunden nach einem Datenschutzvorfall strukturiert genutzt. Die weitere Abarbeitung dient der Schadenbegrenzung für das Unternehmen und ggfs. die Wiederherstellung der IT-Systeme.

Anwaltliche Unterstützung nach einer Datenpanne

Wir empfehlen Ihnen aufgrund der erheblichen Risiken unverzüglich anwaltliche Hilfe hinzuziehen. Als Geschäftsführer oder Vorstand stellen Sie so sicher, dass Sie Ihren eigenen Sorgfaltspflichten entsprechen und Schaden für Gesellschafter und Aktionäre bestmöglich abwenden.

Die juristische Beratung und Verteidigung beginnen bei der Meldung und der ggfs. erforderlichen Benachrichtigung von Betroffenen. Der zweite Abschnitt stellt die Verteidigung im Ordnungswidrigkeitenverfahren dar, um die Höhe des Bußgeldes deutlich zu verringern. Hierbei ist insbesondere eine umfassende Darstellung der technologischen Infrastruktur und Schutzmaßnahmen sinnvoll, die bei Bedarf von unserer Informatik-Unit aufgearbeitet wird, um belastbare Verteidigungsansätze zu bündeln.

Der dritte Abschnitt ist die Abwehr von möglichen Schmerzensgeldansprüchen. Hierfür ist nicht nur eine gut abgestimmte juristische Strategie erforderlich, abhängig von der Vielzahl der Betroffenen müssen tausende Verfahren innerhalb eines kleinen Zeitfensters koordiniert und ggfs. streitig geführt werden. Der letzte Abschnitt ist die Kommunikationsstrategie. Sprachregelungen und Presseerklärungen müssen juristisch überprüft werden, damit sie keine Angriffsfläche für nachgelagerte Prozesse oder weitere Aufsichtsverfahren bieten. Mit diesen Handlungsempfehlungen sind Sie dann in der Lage, Millionenschäden für Ihr Unternehmen zu verhindern oder zu minimieren.

Ihr Ansprechpartner

Tim Platner

Chief Operating Officer

E-Mail: info@vinqo.de

Telefon: 0202 25625 000