

Der datenschutzrechtliche Meldeprozess

Pflicht zur Meldung von Datensicherheitsverletzungen stets im Griff

Fehler im Umgang mit personenbezogenen Daten können jedem passieren. Maßgeblich ist nur, wie wir mit diesen umgehen. Ein strukturierter Meldeprozess hilft den Verantwortlichen, ihrer gesetzlichen Pflicht zur Meldung von Datensicherheitsverletzungen ordnungsgemäß nachzukommen und das Risiko von Bußgeldern und Reputationsschäden zu verringern.

Die Herausforderung

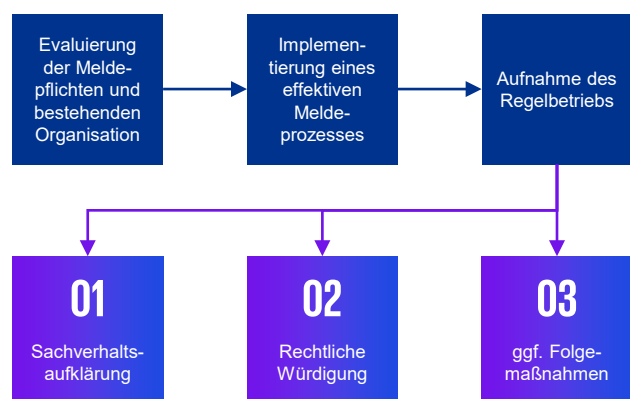
Gemäß Art. 33 Abs. 1 S. 1 DSGVO ist der Verantwortliche verpflichtet, jede Datensicherheitsverletzung an die zuständige Aufsichtsbehörde zu melden; wenn nicht ausnahmsweise nach einer entsprechenden Risikoanalyse ein nur sehr geringes Risiko für die Rechte und Freiheiten der betroffenen Personen besteht. Wird dieser Pflicht nicht ordnungsgemäß nachgekommen, sind Unternehmen dem Risiko von Bußgeldern, Schadenersatzansprüchen und damit verbundenen erhebliche Reputationsschäden ausgesetzt. In der Praxis ergeben sich im Umgang mit (potenziellen) Datensicherheitsverletzungen eine Reihe von Herausforderungen:

- Sensibilisierung aller Beschäftigten zur Sicherstellung der frühzeitigen Erkennung potenziell meldepflichtiger Datensicherheitsverletzungen
- Ein individuell auf die organisatorischen Gegebenheiten und Anforderungen Ihres Unternehmens zugeschnittener Prozess (keine Einheitslösung)
- Schnelle und zuverlässige Kategorisierung, Priorisierung und Bewertung eingehender Hinweise
- Bindung an eine kurze gesetzliche Frist (maximal 72 Stunden) zur Ermittlung und Bewertung sowie, bei Bedarf, Meldung des Vorfalls
- Bestimmung der Rolle des Unternehmens als Verantwortlicher, gemeinsam Verantwortlicher oder als Auftragsverarbeiter
- Rechtssichere Differenzierung zwischen unrechtmäßigen Datenverarbeitungen und Datensicherheitsverletzungen

- Der Wunsch nach Standardisierung und Vereinfachung zur Stärkung der Effizienz im Spannungsfeld zu Flexibilität und dem zwingenden Erfordernis der Einzelfallbetrachtung

Weg zu einem effektiven datenschutzrechtlichen Meldeprozess

Ein strukturiertes Vorgehen macht den Unterschied. Ein flexibler, zuverlässiger und anpassungsfähiger Meldeprozess ermöglicht es Unternehmen, die Herausforderungen effektiv zu meistern und ihren gesetzlichen Verpflichtungen fristgerecht nachzukommen. So können Aufwands- und Fehlerpotenziale reduziert und ein höheres Maß an Rechtssicherheit hergestellt werden.



Implementierung eines effektiven datenschutzrechtlichen Meldeprozesses

Zuerst sollte analysiert werden, welche Strukturen für den Umgang mit potenziellen Datensicherheitsverletzungen ggf. schon bestehen.

Dann kann der datenschutzrechtliche Meldeprozess unter Berücksichtigung der individuellen Anforderungen Ihres Unternehmens konzipiert werden. Damit werden die notwendigen Strukturen für ein rechts-sicheres und effizientes Vorgehen geschaffen.

Zu den wesentlichen Elementen zählen:

- Wissenstransfer an Beschäftigte
- Standardisierung
- Entwicklung eines Eskalationsprozesses
- Digitale Anbindung

Regelbetrieb

Nach erfolgreicher Implementierung ist der sichere Betrieb des Meldeprozesses entscheidend, um dauerhaft und nachhaltig die Reaktionsfähigkeit und Rechtskonformität sicherzustellen. Dieser Regelbetrieb lässt sich in drei zentrale Bereiche gliedern:

- **Sachverhaltsaufklärung:** Unterstützung bei der Ermittlung der Hintergründe und tatsächlichen Umstände des Vorfalls.
- **Rechtliche Würdigung:** Rechtliche Bewertung des Sachverhalts einschließlich der stets notwendigen Risikoanalyse hinsichtlich etwaiger Melde-, Benachrichtigungs- oder Informationspflichten.
- **Folgemaßnahmen:** Entwicklung und Vorschlag von Handlungsempfehlungen sowie Unterstützung bei der Umsetzung der gesetzlichen und vertraglichen Pflichten und der Kommunikation mit der Aufsichtsbehörde und den Betroffenen.

Adaption des Prozesses auf weitere Meldepflichten

Mit der zunehmenden Regulierung von Technologien und zur Sicherstellung der Cyber Security werden Unternehmen weiteren Meldepflichten ausgesetzt. Dazu gehören zum Beispiel die Pflicht von Telekommunikationsanbietern zur Meldung von Sicherheitsvorfällen mit beträchtlichen

Auswirkungen auf den Betrieb der Netze oder die Erbringung der Dienste (§ 168 Abs. 1 TKG), oder des Herstellers zur Meldung ausgenutzter Schwachstellen und schwerwiegender Sicherheitsvorfälle (Art. 14 Abs. 1, Abs. 3 CRA). Auch wenn die Meldepflichten unterschiedliche Adressaten und verschiedene Stoßrichtungen haben können, haben sie einige Gemeinsamkeiten: Kurze Fristen, hohe Bußgelder und große Relevanz für die Außenwirkung.

Bestens für Sie aufgestellt

Wir begleiten Sie gerne bei der Implementierung und dem Betrieb eines effektiven und effizienten Meldeprozesses. Haben Sie bereits einen Meldeprozess, können wir Sie bei der Optimierung der Prozesse sowie im Regelbetrieb unterstützen.

Wir verfügen über umfassende Erfahrung mit dem Aufbau und der operativen Tätigkeit im Meldeprozess und können Priorisierungsempfehlungen bei hohem Fallaufkommen geben. Mit unseren Partnern können wir den datenschutzrechtlichen Meldeprozess praxiserprobt und effizient als Gesamtkonzept mit einer technischen Lösung anbieten. Dabei unterstützen wir Sie von der Konzeptionierung bis zum Regelbetrieb mit unserem Rechts-, Prozess- und Tool-Know-how.

Ihre Vorteile auf einen Blick



Optimierte Prozesse schützen und Ihre Beschäftigten sensibilisieren



Standardisierung und Digitalisierung entbürokratisieren und Fehlerpotenziale reduzieren



Das praxiserprobte KPMG Law Experten-Team unterstützt flexibel bei Einrichtung und Betrieb Ihres Meldeprozesses.

Kontakt

KPMG Law Rechtsanwaltsgesellschaft mbH



Dr. Bernd Federmann, LL.M.
Partner, Rechtsanwalt
Leiter Compliance & Wirtschaftsstrafrecht
T +49 711 78192-3418
bfedermann@kpmg-law.com



Maik Ringel
Senior Manager, Rechtsanwalt
Compliance & Wirtschaftsstrafrecht
T +49 341 2257-2546
mringel@kpmg-law.com

www.kpmg-law.de

KPMG Law in den sozialen Netzwerken



Die enthaltenen Informationen sind allgemeiner Natur und nicht auf die spezielle Situation einer Einzelperson oder einer juristischen Person ausgerichtet. Obwohl wir uns bemühen, zuverlässige und aktuelle Informationen zu liefern, können wir nicht garantieren, dass diese Informationen so zutreffend sind wie zum Zeitpunkt ihres Eingangs oder dass sie auch in Zukunft so zutreffend sein werden. Niemand sollte aufgrund dieser Informationen handeln ohne geeigneten fachlichen Rat und ohne gründliche Analyse der betreffenden Situation.

Rechtsdienstleistungen sind für bestimmte Prüfungsmandanten nicht zulässig oder können aus anderen berufsrechtlichen Gründen ausgeschlossen sein.

© 2025 KPMG Law Rechtsanwaltsgesellschaft mbH, assoziiert mit der KPMG AG Wirtschaftsprüfungsgesellschaft, einer Aktiengesellschaft nach deutschem Recht und ein Mitglied der globalen KPMG-Organisation unabhängiger Mitgliedsfirmen, die KPMG International Limited, einer Private English Company Limited by Guarantee, angeschlossen sind. Alle Rechte vorbehalten. Der Name KPMG und das Logo sind Marken, die die unabhängigen Mitgliedsfirmen der globalen KPMG-Organisation unter Lizenz verwenden.