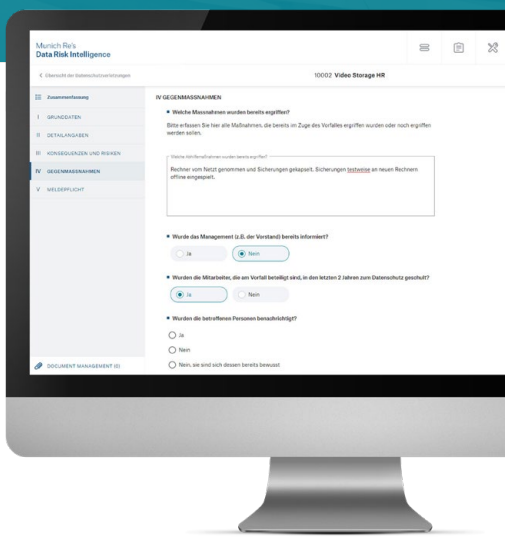
NOT IF, BUT HOW

Munich RE

Munich Re's Data Risk Intelligence **Data Breach Edition**

Fact Sheet Version 2020/07



Die Data Breach Edition der Data Risk Intelligence Platform ist ein Risikomanagement-Software-Tool, mit dem aktuelle Datenschutzverletzungen erfasst, dokumentiert und bestehende Datenschutzverletzungen verwaltet werden können.

Datenschutzpannen in Unternehmen entstehen zum Teil aufgrund interner Fehler, zum Teil durch Attacken von außen oder Schwachstellen bei Dienstleistern. Mit der Data Breach Edition können Vorfälle dieser Art DSGVO-konform erfasst, dokumentiert und der Aufsichtsbehörde gemeldet werden. Der gezielt entwickelte Fragebogen der Data Breach Edition deckt die behördlichen Anforderungen ab und ermöglicht eine einheitliche Dokumentation an zentraler Stelle. Sie haben stets den Überblick, welche Datenpannen erfasst wurden und ob diese bereits an die Aufsicht gemeldet wurden.

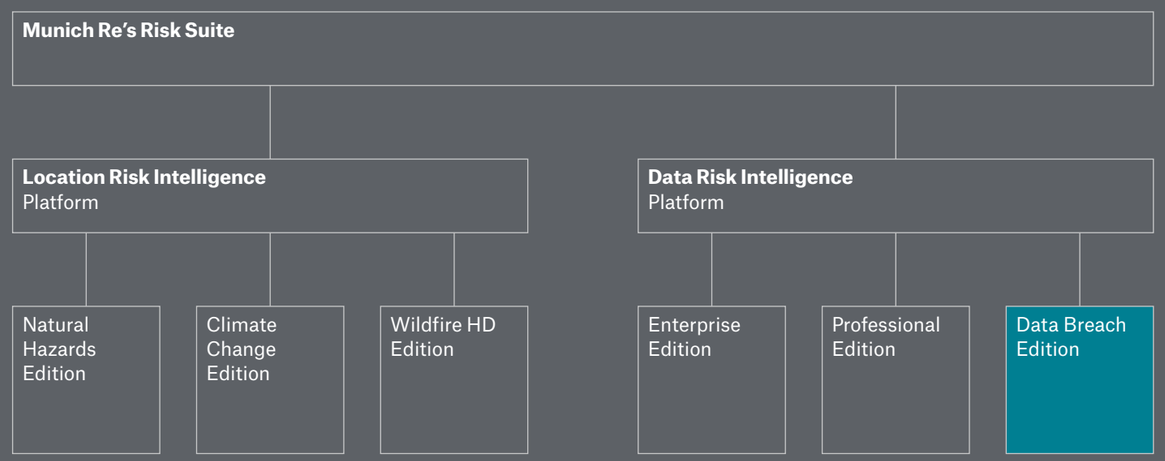
Alternativ zur Standalone-Lösung kann das Data Breach Modul in die Enterprise oder Professional Edition der Data Risk Intelligence nahtlos integriert werden.

Munich Re's Risk Suite

Munich Re's Risk Suite ist eine Reihe von Risikolösungen, die als Software-Portfolio von Munich Re Service GmbH, einer hundertprozentigen Tochtergesellschaft des weltweit führenden Rückversicherers Munich Re, bereitgestellt wird.

Unternehmen erhalten damit Zugang zu den inhouse entwickelten Risikomanagement-Tools sowie dem Wissen und der Erfahrung aus 140 Jahren des weltweit führenden Anbieters von Rückversicherung, Erstversicherung und versicherungsnahen Risikolösungen. Seit der Einführung von NATHAN (jetzt Natural Hazards Edition) ist Munich Re Vorreiter bei der weltweiten Bewertung von Naturgefahrenrisiken. Munich Re's Risk Suite baut auf diesem Expertenwissen auf und bietet eine Auswahl ausgereifter Risikobewertungslösungen für das technische Underwriting, für Investitionsentscheidungen und zur Klimawandel-Analyse.

Andererseits nutzt Munich Re's Risk Suite die jahrelange Erfahrung im globalen Datentransfer unter regulatorischen Anforderungen. Vor diesem umfangreichen Erfahrungshintergrund entstanden, ursprünglich für den internen Bedarf bei Munich Re entwickelt, hocheffiziente Lösungen zum Datenschutz- und IT-Sicherheitsmanagement, die Munich Re's Risk Suite ideal ergänzen. Damit wird Unternehmen ein umfassendes Tool-Set zur Verfügung gestellt, das das Management aller relevanten Risikoaspekte abdeckt und zudem im Hinblick auf die zu erwartende, weiter steigende Komplexität im Bereich Daten- und IT-Sicherheitsschutz kontinuierlich weiterentwickelt wird.



Inhaltsverzeichnis

1. Potenzial und Vorteile der Data Breach Edition der Data Risk Intelligence

Die Data Breach Edition versetzt Sie in die Lage, Datenschutzverletzungen zu dokumentieren und deren Meldepflicht einzuschätzen. Die Einträge können im Zeitablauf ergänzt und eine Referenznummer kann für die weitere Bearbeitung im System hinterlegt werden.

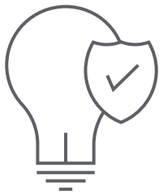
Die Data Breach Edition ist einfach und intuitiv zu bedienen, wandelt Datenschutzverletzungen in klare Strukturen um und ermöglicht eine einheitliche Dokumentation. Optimieren Sie Ihr Risiko- und Schadenmanagement durch die Dokumentation individueller technischer und organisatorischer Maßnahmen sowie die Erfüllung der Nachweis- und Dokumentationspflichten. Die rechtlich erforderlichen Dokumente werden automatisch und DSGVO-konform durch die Software-Lösung erstellt sowie die Korrespondenz mit den Aufsichtsbehörden transparent dokumentiert.

100 % vollständige Erfassung

aller Datenschutzverletzungen durch intelligenten Fragenkatalog: Nichts kann vergessen oder übersehen werden!

Schnellerer Überblick

über alle erfassten Datenschutzverletzungen und ob diese bereits der Aufsichtsbehörde gemeldet wurden.



140 Jahre Erfahrung in Risiko-bewertung und -management

verleiht Munich Re das weltweit größte und umfassendste Experten-Know-how für die Entwicklung hochwertiger Software-Lösungen in diesem Bereich.

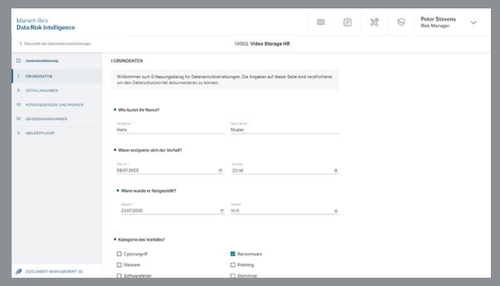
Maximale Rechtssicherheit

durch Erfüllung der Nachweis- und Dokumentationspflichten und DSGVO-Konformität.

2. Schritt für Schritt – der Data Breach Edition Workflow

Die Data Breach Edition führt Sie Schritt für Schritt durch einen Fragebogen und erstellt daraus alle wichtigen Dokumente sowie eine strukturierte Übersicht aller Datenschutzverletzungen.

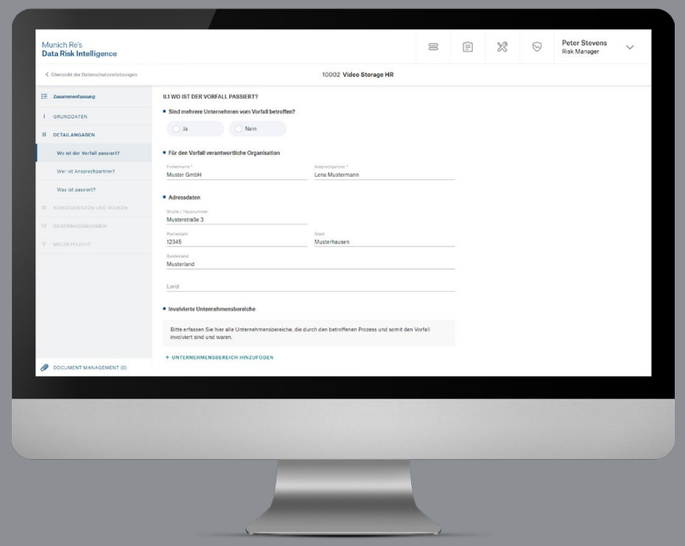
Wie geht man mit Vorfällen um? Als Erstes ist es wichtig, dass die Datenpanne abgestellt wird. In der Regel agiert die IT-Abteilung unverzüglich und setzt technische Maßnahmen zur Behebung um. Denken Sie jedoch gleich daran, dies zu dokumentieren und die Datenpanne auf die Notwendigkeit einer Meldung an die Aufsichtsbehörde zu prüfen. Es bleibt Ihnen nur wenig Zeit.



Schritt 1
Grunddaten erfassen

Wo und wann ist der Vorfall passiert, wer ist Ihr Ansprechpartner, was ist es für ein Vorfall und was ist genau passiert? Diese und eine Fülle weiterer Fragen werden automatisch gestellt.

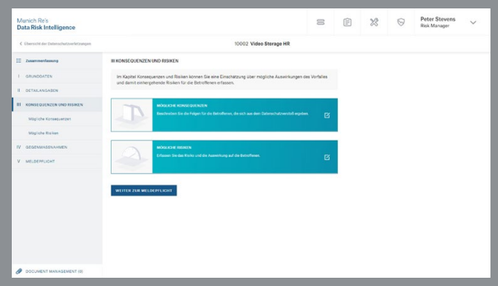
Die Beschreibung leitet Sie durch den Fragenkatalog, sodass keine relevanten Punkte in dieser Stresssituation übersehen werden. Zudem erhalten Sie eine umfassende Dokumentation der Vorfälle.



Schritt 2
Detailangaben ergänzen / Überblick behalten

In welchem Unternehmen passierte der Vorfall? Im eigenen oder bei einem Ihrer Dienstleister/Zulieferer? Behalten Sie den Überblick über alle Vorfälle und schaffen Sie die Möglichkeit eines einheitlichen Berichtswesens. Auch über Ihre Ansprechpartner auf Seiten der Aufsichtsbehörden haben Sie eine stets aktuelle Übersicht.

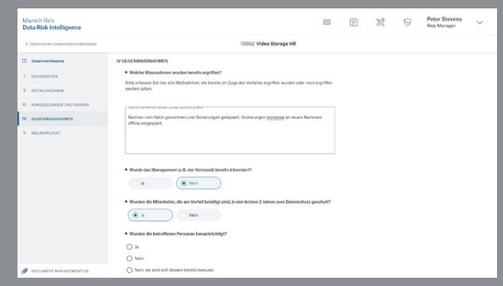
Zudem behalten Sie auch den Überblick über Ihre Dienstleister und Zulieferer, bei denen Datenschutzpannen auftreten. Häufen sich diese, können Sie frühzeitig Gegenmaßnahmen ergreifen.



Schritt 3
Konsequenzen und Risiken

Nicht nur der Vorfall an sich und die technischen Maßnahmen sind von Bedeutung. Auch die Art der Daten ist wichtig. Sind sensible personenbezogene Daten (Art. 9 DSGVO) betroffen, dürfte das Risiko für die Betroffenen deutlich größer sein, als wenn nur Kontaktdaten in die Hände Unbefugter gelangen.

Verfügbarkeit, Vertraulichkeit und Integrität der Daten – welche Folgen ergeben sich hier aus der Datenpanne? Sind Sie Opfer einer Ransomware-Attacke, sind die personenbezogenen Daten nicht mehr verfügbar? Was bedeutet dies? Können Sie Ihre Dienste dem Betroffenen nicht mehr anbieten? Ist dies ein Newsletter-Mailing-System, so dürften die Konsequenzen gering sein. Kann der Betroffene aber keine Bankgeschäfte mehr ausüben, weil sein Konto verschlüsselt ist und er damit keinen Zugang mehr hat, kann dies erheblich Folgen haben. Diese Risiken für die Betroffenen beschreiben Sie und legen fest, welche Auswirkungen die Datenpanne auf den Betroffenen hat.



Schritt 4
Gegenmaßnahmen

Ihre IT-Abteilung hat die Sicherheitslücke geschlossen. Das Vorgehen und die Maßnahmen sollten dem Datenschutzbeauftragten bekannt sein, da er dies zu dokumentieren hat. An Hand der Maßnahmen kann der Datenschutzbeauftragte feststellen, ob weiterhin ein Risiko besteht oder ob dieses inzwischen nicht mehr eintreten kann. Je nach Schwere der Datenpanne sind interne Abteilungen zu informieren. Ist die Geschäftsleitung bereits eingebunden? Aber nicht nur intern, sondern auch die Betroffenen müssen ggf. benachrichtigt werden. Sollte dies der Fall sein, so müssen Sie die Betroffenen auf Maßnahmen hinweisen, die ein Risiko für sie reduzieren kann. Wurden Zugangsdaten kompromittiert, muss der Betroffene diese ändern. Damit senken Sie gleichzeitig das Risiko, dass die Datenpanne erhebliche Risiken für den Betroffenen hat. Noch besser wäre eine technische Maßnahme, sodass Sie die Zugangsdaten von Ihrer Seite sperren.

Abschließend können Sie festlegen, ob der Vorfall an eine Aufsichtsbehörde gemeldet werden soll oder nicht.

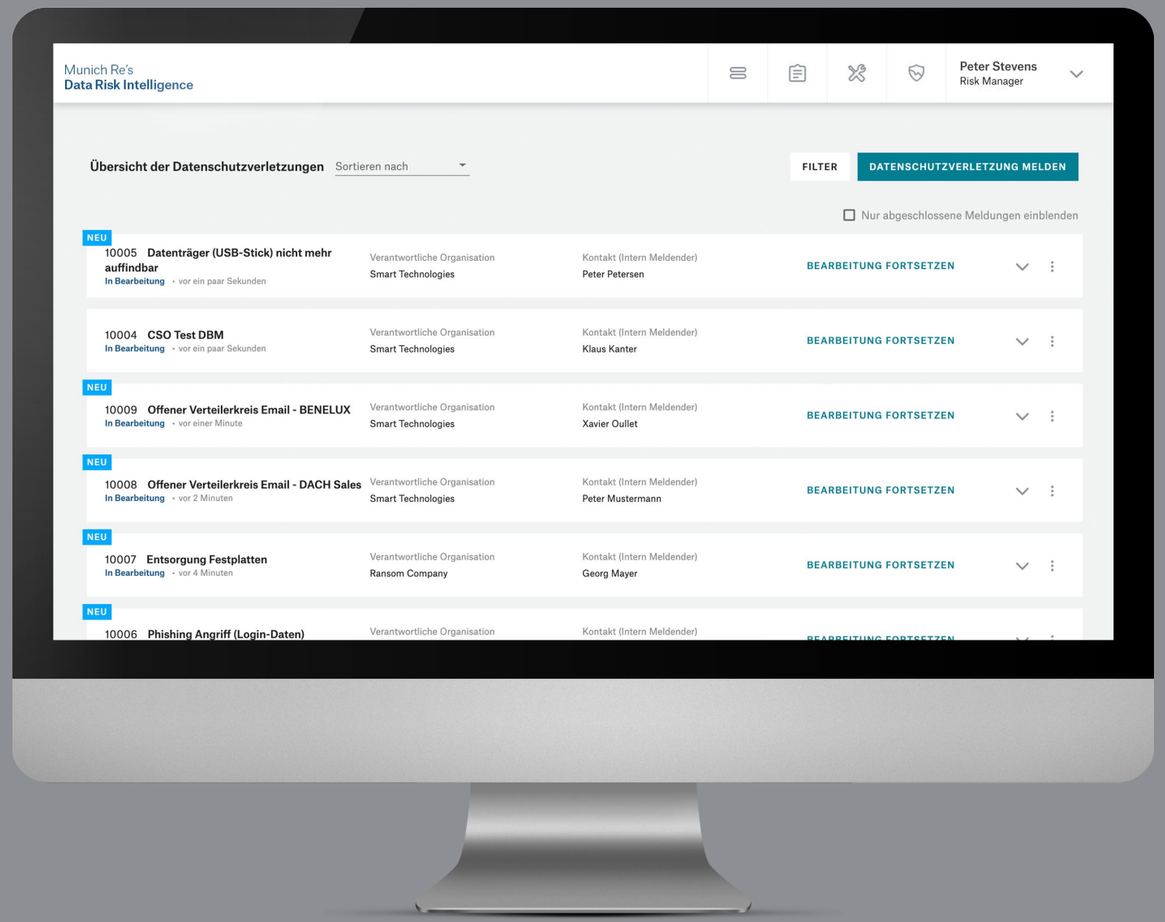
3. Vorfälle der Aufsichtsbehörde melden

Liegt eine Verletzung des Schutzes personenbezogener Daten vor, müssen Sie als verantwortliche Stelle unverzüglich und möglichst binnen 72 Stunden nach Bekanntwerden der Verletzung eine Meldung an die Aufsichtsbehörden abgeben (Art. 33 DSGVO).

Können Sie diese Frist nicht einhalten, muss diese Verzögerung zusammen mit der Meldung begründet werden. Diese Meldung müssen Sie nur abgeben, wenn das Risiko für den Betroffenen hoch ist. Gibt es kein oder nur ein geringes Risiko, so muss die Aufsicht nicht eingebunden werden. Trotzdem müssen Sie den Vorfall dokumentieren und auch begründen, warum Sie zu dieser Risikoeinschätzung kommen. Um die Angaben überprüfen und komprimiert ansehen zu können, erhalten Sie eine Übersicht der Angaben, die Sie der Aufsichtsbehörde zur Verfügung stellen können.

Haben Sie eine Meldung an die Aufsichtsbehörde abgegeben, erhalten Sie in der Regel eine Referenznummer. Diese kann, sobald sie von der Aufsichtsbehörde ausgegeben wurde, nachdokumentiert werden.

Weiterhin können Sie einen dokumentierten Vorfall durch einen (optionalen) Zusatzbericht ergänzen. Ist bspw. die Anzahl der betroffenen Datensätze geringer als in der initialen Dokumentation angegeben, kann diese Tatsache nachdokumentiert und (optional) an die Aufsichtsbehörde gemeldet werden.



Das Modul verfügt zudem über eine Übersicht der Datenschutzverletzungen, die eine Anzeige zu Details sowie ein Filtern und Suchen nach spezifischen Attributen ermöglicht.

Munich Re Service GmbH
Königinstr. 107, 80802 München, Germany

Tel.: +49 (0)89 3891-0
Fax: +49 (0)89 399056
E-mail: Risk-Management-Partners@munichre.com

Geschäftsführer: Christof Reinert, Joachim Mathe

Handelsregister des Amtsgerichts München:
HRB 241444

Munich Re Service GmbH ist eine 100% Tochtergesellschaft der Münchener Rückversicherungs-Gesellschaft Aktiengesellschaft in München. Das Unternehmen ist verantwortlich für die Entwicklung, Vermarktung sowie den Vertrieb von Produkten und Dienstleistungen im Bereich digitaler Technologien, insbesondere zur Risikomessung, Risikosteuerung und allgemeinen Geschäftsoptimierung.

Umsatzsteuer-Identifikationsnummer: DE 318853378

Bildnachweis: Getty Images