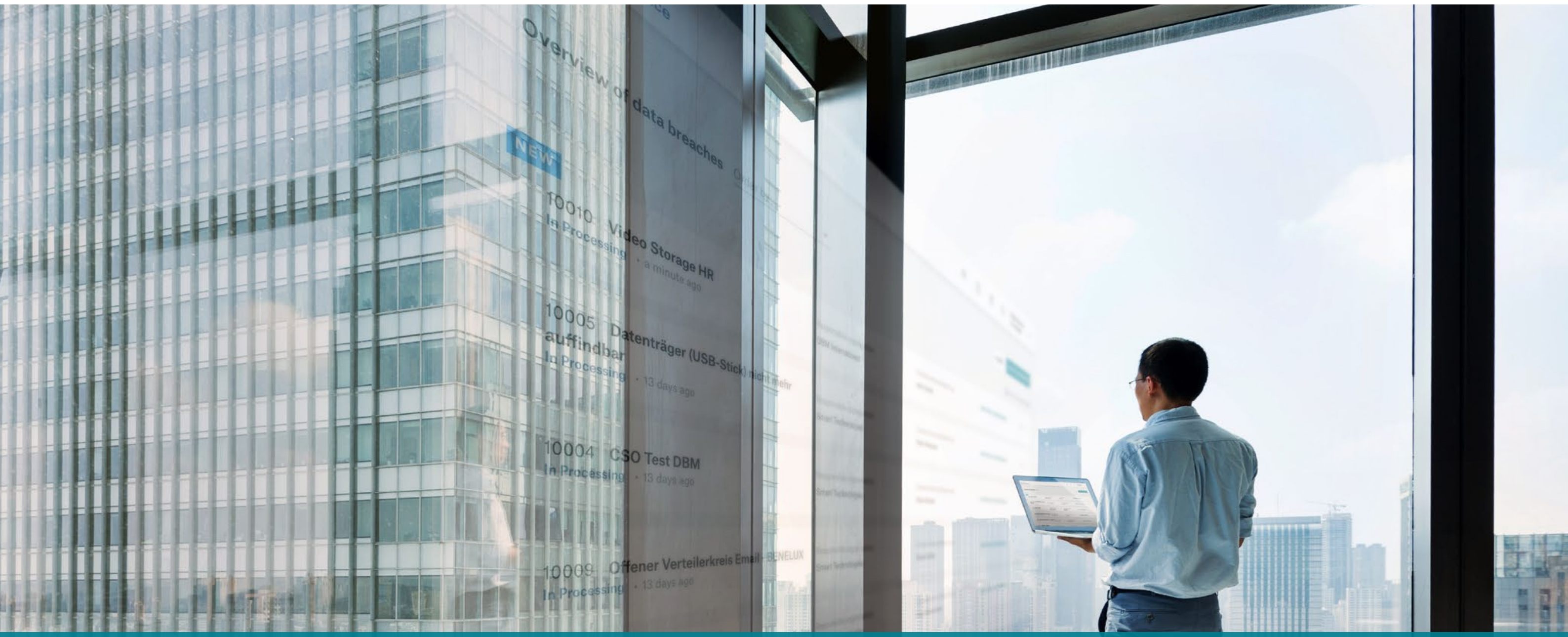
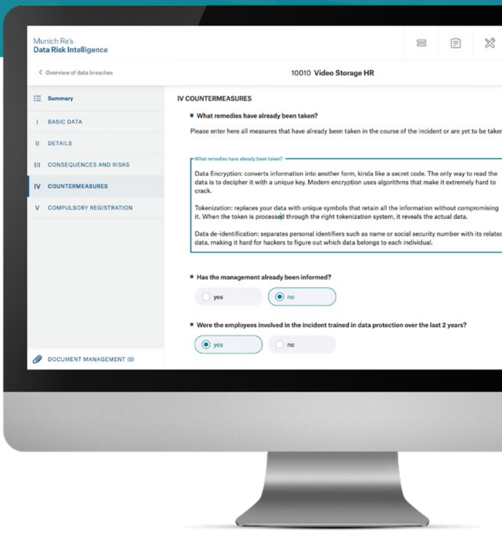
NOT IF, BUT HOW

Munich RE


Overview of data breaches
NEW
10010 Video Storage HR
In Processing · a minute ago
10005 Datenträger (USB-Stick) nicht mehr auffindbar
In Processing · 13 days ago
10004 CSO Test DBM
In Processing · 13 days ago
10009 Offener Verteilerkreis Email - BENELUX
In Processing · 13 days ago

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

Fact Sheet Version 2020/07



10010 Video Storage HR

IV COUNTERMEASURES

- What remedies have already been taken?

Please enter here all measures that have already been taken in the course of the incident or are yet to be taker

What remedies have already been taken?

Data Encryption: converts information into another form, kinda like a secret code. The only way to read the data is to decipher it with a unique key. Modern encryption uses algorithms that make it extremely hard to crack.

Tokenization: replaces your data with unique symbols that retain all the information without compromising it. When the token is processed through the right tokenization system, it reveals the actual data.

Data de-identification: separates personal identifiers such as name or social security number with its relatec data, making it hard for hackers to figure out which data belongs to each individual.

- Has the management already been informed?

○ yes ● no

- Were the employees involved in the incident trained in data protection over the last 2 years?

● yes ○ no

Data Breach Edition of Data Risk Intelligence Platform is a risk management software tool that can be used to record and document current data breaches as well as to manage existing ones.

Data protection breakdowns in companies are caused partly by internal errors and partly by attacks from outside or vulnerabilities on the part of service providers. With Data Breach Edition, incidents of this type can be recorded, documented and reported to the supervisory authorities in compliance with the GDPR. The specifically developed questionnaire of Data Breach Edition covers the relevant official requirements and enables uniform documentation at a central location. You always have an overview of what data breaches have been recorded and whether these have already been reported to the supervisory authorities.

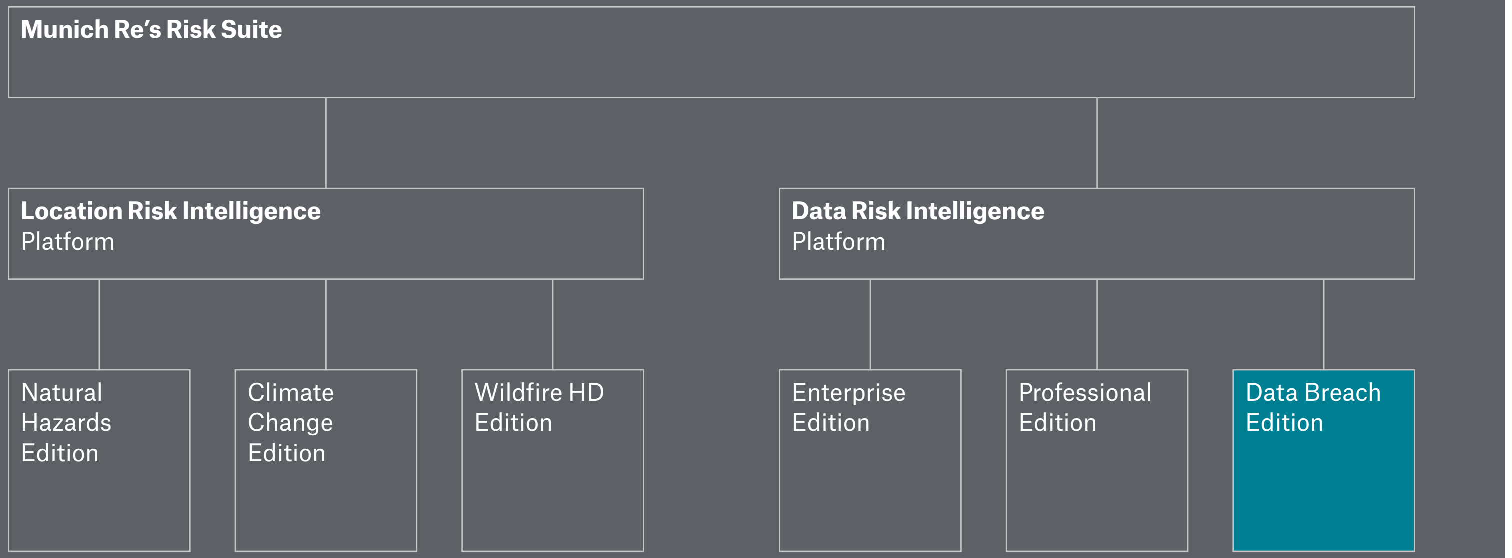
As an alternative to the stand-alone solution, the Data Breach module can be seamlessly integrated into Enterprise or Professional Edition of Data Risk Intelligence Platform.

Munich Re’s Risk Suite

Munich Re’s Risk Suite is a range of modular risk solutions provided as a software portfolio by Munich Re Service GmbH, a wholly owned subsidiary of the world’s leading reinsurer.

It offers companies access to the risk management tools developed in-house and the knowledge and experience of 140 years of one of the world’s leading providers of reinsurance, primary insurance and insurance-related risk solutions. Since the introduction of Nathan (Natural Hazards Assessment Network), Munich Re has been a pioneer in the global assessment of natural hazard risks. Munich Re’s Risk Suite builds on this expertise and offers a selection of well-engineered risk assessment solutions for technical underwriting, data protection, investment decisions and climate change analysis.

On the other hand, Munich Re’s Risk Suite draws on years of experience in global data transfer under regulatory requirements. Against this extensive background of experience, highly efficient solutions for data protection and IT security management were developed, originally for internal use, which ideally complement Munich Re’s Risk Suite and thus provide companies with a comprehensive set of tools that covers the management of all risk aspects relevant to a company and is continually being developed further in view of the expected further increase in complexity in the field of data and IT security protection.



Munich Re’s Risk Suite

Location Risk Intelligence Platform

Natural Hazards Edition

Climate Change Edition

Wildfire HD Edition

Data Risk Intelligence Platform

Enterprise Edition

Professional Edition

Data Breach Edition

Table of Contents

1. Potential and advantages of Data Breach Edition of Data Risk Intelligence Platform

Data Breach Edition enables you to document data breaches and assess the obligation to report them. The entries can be supplemented over time and reference numbers can be stored in the system for further processing.

Data Breach Edition is easy and intuitive to use, converts data breaches into clear structures and enables uniform documentation. Optimise your risk and claims management by documenting individual technical and organisational measures as well as the fulfillment of verification and documentation obligations. The software solution automatically creates the legally required records in compliance with the GDPR, and transparently documents all correspondence with the supervisory authorities.

100 % complete recording

of all data breaches by means of an intelligent questionnaire: nothing can be forgotten or overlooked!

A faster overview

of all recorded data protection violations and whether these have already been reported to the supervisory authorities.

With 140 years of experience in risk assessment and risk management

Munich Re has the world's largest and most comprehensive expert know-how for the development of high-quality software solutions in this field.

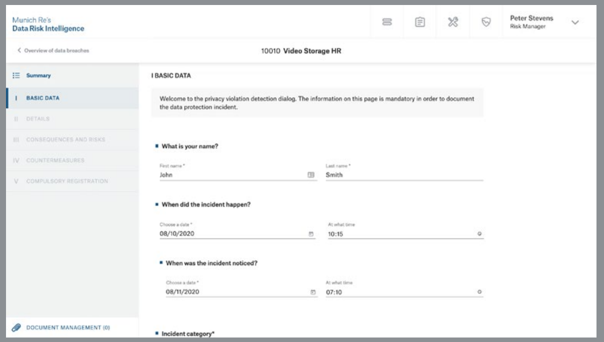
Maximum legal security

ensured by compliance with the verification and documentation requirements of the GDPR.

2. Step by step – the Data Breach Edition workflow

Data Breach Edition guides you step by step through a questionnaire and creates all the required documents as well as a structured overview of all data breaches.

How should incidents be dealt with? First of all, it is important that the data breach should be remedied. As a rule the IT department acts immediately and implements technical measures to correct the situation. However, you should remember to document this and check whether the data breach needs to be reported to the supervisory authorities. Little time is available for this.



10010 Video Storage HR

I BASIC DATA

Welcome to the privacy violation detection dialog. The information on this page is mandatory in order to document the data protection incident.

- What is your name?

First name * John

Last name * Smith

- When did the incident happen?

Choose a date * 08/10/2020

At what time 10:15

- When was the incident noticed?

Choose a date * 08/11/2020

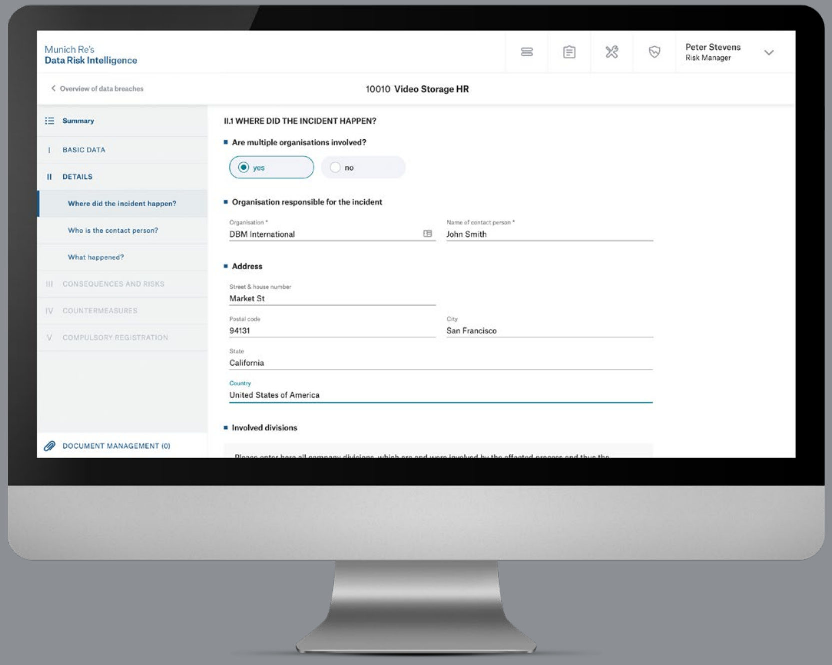
At what time 07:10

- Incident category*

Step 1
Recording the basic data

Where and when did the incident occur, who is the relevant contact person, what kind of incident is it and what happened exactly? These and many more questions are asked automatically.

The description guides you through the questionnaire, so that no relevant points in this critical situation are overlooked. You also receive comprehensive documentation of the incidents.



10010 Video Storage HR

II.1 WHERE DID THE INCIDENT HAPPEN?

- Are multiple organisations involved?

● yes ○ no

- Organisation responsible for the incident

Organisation * DBM International

Name of contact person * John Smith

- Address

Street & house number Market St

Postal code 94131

City San Francisco

State California

Country United States of America

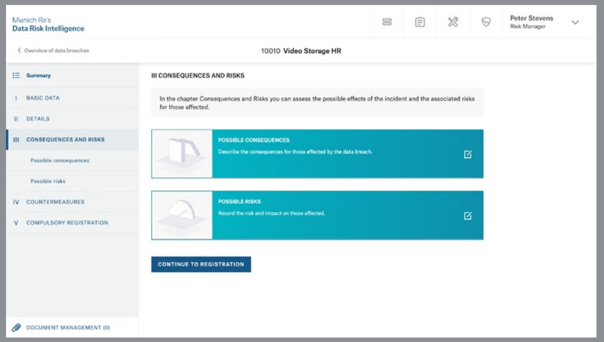
- Involved divisions

Please enter here all company divisions, which are and were involved by the affected process and thus the

Step 2
Adding details / keeping an overview

In which company did the incident occur? In your own company or at one of your service providers/suppliers? Keep an overview of all incidents and create the possibility of a uniform reporting system. You also have an up-to-date overview of your contacts on the part of the supervisory authorities.

In addition you can keep an eye on any service providers and suppliers where data breaches occur. If these occur regularly you can take corrective measures at an early stage.



10010 Video Storage HR

III CONSEQUENCES AND RISKS

In the chapter Consequences and Risks you can assess the possible effects of the incident and the associated risks for those affected.

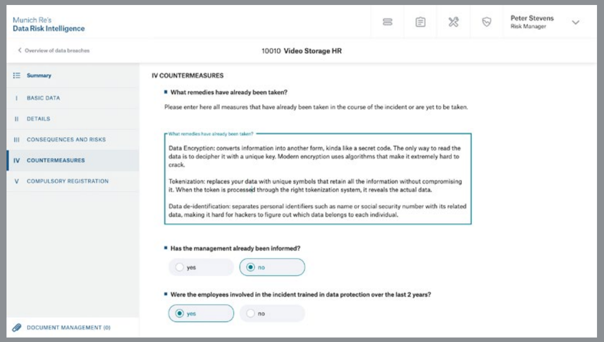
POSSIBLE CONSEQUENCES
Describe the consequences for those affected by the data breach.

POSSIBLE RISKS
Record the risk and impact on those affected.

Step 3
Consequences and risks

It isn't only the incident itself and the resulting technical measures that are important. The type of data also matters. If sensitive personal data (Art. 9 GDPR) is involved, the risk for those affected is likely to be much greater than if only contact data falls into the hands of unauthorised persons.

Availability, confidentiality and integrity of data – what are the consequences of a data breach? If you are the victim of a ransomware attack, is the personal data no longer available? What does this mean? Are you no longer able to offer your services to the persons affected? If this is a newsletter mailing system, the consequences will probably be minor. However, if the persons concerned can no longer carry out banking transactions because their account is encrypted and they therefore no longer have access, this can have serious consequences. You describe these risks for those who are affected and define what effects the data breach has on them.



10010 Video Storage HR

IV COUNTERMEASURES

- What remedies have already been taken?

Please enter here all measures that have already been taken in the course of the incident or are yet to be taken.

What remedies have already been taken?

Data Encryption: converts information into another form, kinda like a secret code. The only way to read the data is to decipher it with a unique key. Modern encryption uses algorithms that make it extremely hard to crack.

Tokenization: replaces your data with unique symbols that retain all the information without compromising it. When the token is processed through the right tokenization system, it reveals the actual data.

Data de-identification: separates personal identifiers such as name or social security number with its related data, making it hard for hackers to figure out which data belongs to each individual.

- Has the management already been informed?

○ yes ● no

- Were the employees involved in the incident trained in data protection over the last 2 years?

● yes ○ no

Step 4
Countermeasures

Your IT department has closed the security gap. The necessary procedure and measures should be known to the data protection officer, as it is his/her responsibility to document this. On the basis of such measures the data protection officer can determine whether a risk still exists or whether it has now been eliminated. Depending on the severity of the data breach, internal departments should be informed. Is management already involved? Information has to be shared not just internally, but also if necessary with the persons who are affected. If this is the case, you have to inform them about measures that can reduce the risk for them. If access data has been compromised, the individuals concerned have to change it. This also reduces the risk of the data breach posing a significant risk to such persons. Even better would be a technical measure so that you can block the access data from your side.

Finally, you can determine whether or not the incident should be reported to the supervisory authorities.

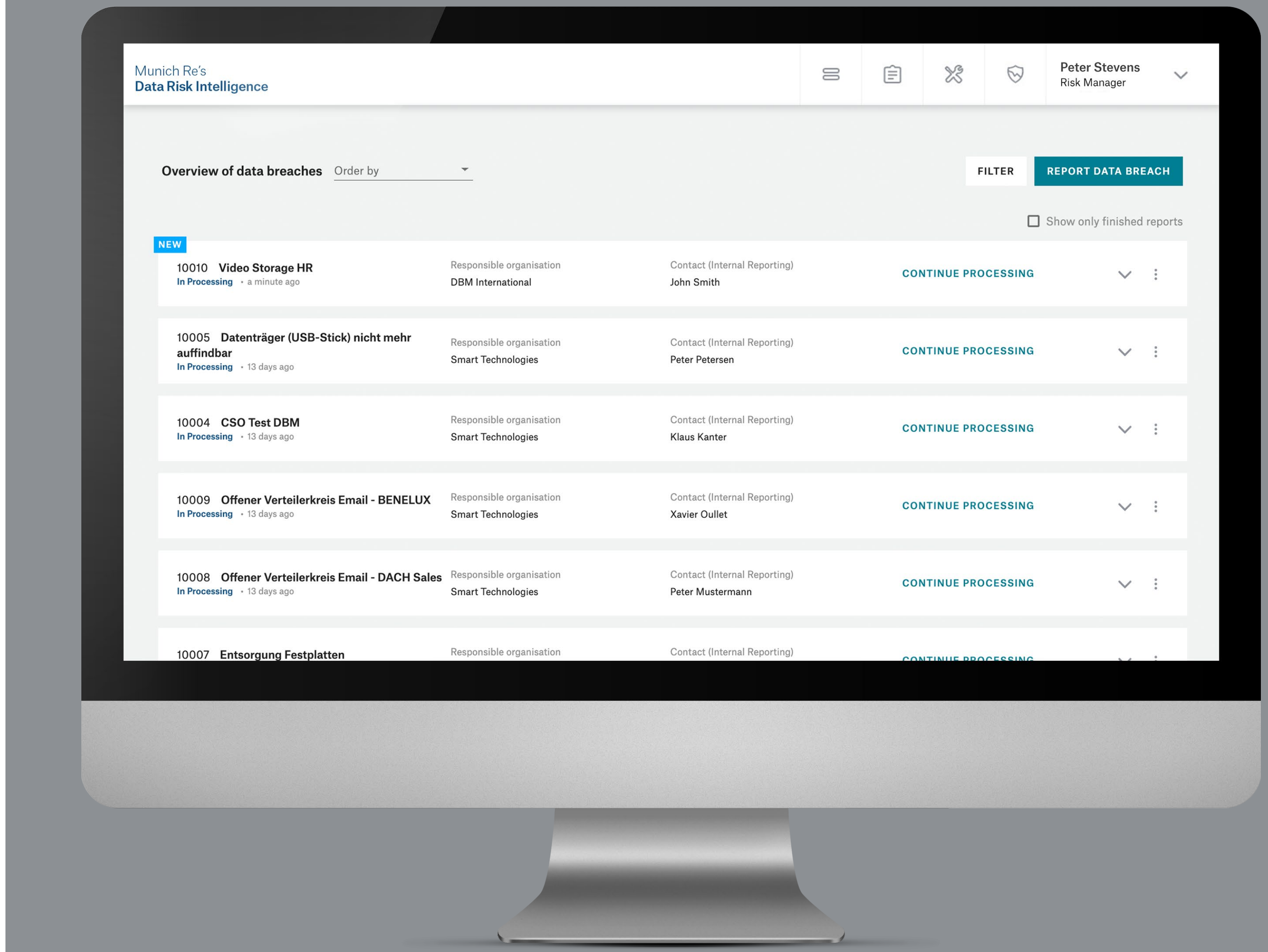
3. Reporting incidents to the supervisory authorities

If there is a breach of personal data protection you, as the responsible party, have to notify the supervisory authorities immediately and, if possible, within 72 hours of becoming aware of the breach (Art. 33 GDPR).

If you cannot meet this deadline, you have to justify this delay in your report. You only have to submit this report if the risk to the persons concerned is high. If there is no risk or only a slight risk, the supervisory authorities do not need to be involved. Nevertheless, you have to document the incident and also justify why you have assessed the risk in this way. In order to be able to check the information and view it in condensed form, you will be given an overview of the information that you can provide to the supervisory authority.

If you have submitted a report to the supervisory authorities, you will usually receive a reference number. This reference number can be documented as soon as it has been issued by the supervisory authorities.

You can also add an (optional) additional report to a documented incident. If, for example, the number of affected data records is less than the number specified in the initial documentation, this fact can be subsequently documented and (optionally) reported to the supervisory authorities.



Munich Re's
Data Risk Intelligence

Peter Stevens
Risk Manager

Overview of data breaches Order by

□ Show only finished reports

NEW 10010 Video Storage HR In Processing • a minute ago	Responsible organisation DBM International	Contact (Internal Reporting) John Smith	CONTINUE PROCESSING
10005 Datenträger (USB-Stick) nicht mehr auffindbar In Processing • 13 days ago	Responsible organisation Smart Technologies	Contact (Internal Reporting) Peter Petersen	CONTINUE PROCESSING
10004 CSO Test DBM In Processing • 13 days ago	Responsible organisation Smart Technologies	Contact (Internal Reporting) Klaus Kanter	CONTINUE PROCESSING
10009 Offener Verteilerkreis Email - BENELUX In Processing • 13 days ago	Responsible organisation Smart Technologies	Contact (Internal Reporting) Xavier Oullet	CONTINUE PROCESSING
10008 Offener Verteilerkreis Email - DACH Sales In Processing • 13 days ago	Responsible organisation Smart Technologies	Contact (Internal Reporting) Peter Mustermann	CONTINUE PROCESSING
10007 Entsorgung Festplatten	Responsible organisation	Contact (Internal Reporting)	CONTINUE PROCESSING

The module also has a data breach overview which enables you to view details as well as filter and search for specific attributes.

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

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

Managing Directors: Christof Reinert, Joachim Mathe

Commercial Register of the Local Court of Munich:
HRB 241444

Munich Re Service GmbH is a 100% affiliate company of Münchener Rückversicherungs-Gesellschaft Aktiengesellschaft in München (Munich Reinsurance Company). It is a capital company with limited liability with the following object: Development, marketing and distribution of products and services in the field of digital technologies, in particular for risk measurement, risk management and general business optimization.

VAT registration number: DE 318853378

Picture credits: Getty Images