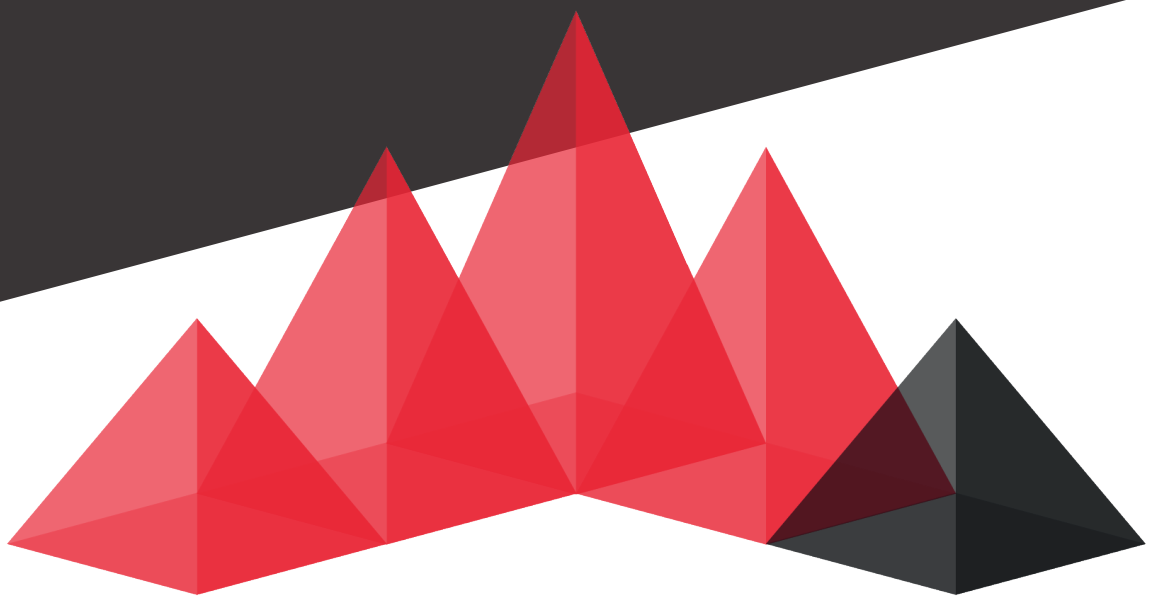
TALOS

Publication



Personal Data Breach Notification as a Service
Recommendations for the Financial Service Industry

by Christian Scholten and Thomas Eustorgi

In today's digitalized world, personal data breaches are being discovered and reported more and more frequently.[1] Particularly vulnerable is the financial service industry as it deals with large amounts of sensitive data and heightened scrutiny from regulators. The consequences of a data breach can be severe, causing drastic operational, financial and reputational damage.

Banks and other financial institutions require technical incident response processes for breach detection, containment/eradication and data recovery. From an operational of view, financial institutions need a process to communicate with supervisory authorities, affected clients, and the public to provide concerned individuals with relevant information and access to affected data. These processes bear substantial operational and financial risks wherefore organizations are well advised to build on expertise of professional service providers for legal advice, planning and execution.

TALOS

Publication

Personal Data Breach and GDPR

The General Data Protection Regulation (GDPR) defines the rights of clients and employees in case of a personal data breach. Pursuant to GDPR art. 32, the data controller (e.g. a bank) must report any personal data breach to the supervisory authority within 72 hours after becoming aware of it. The data controller is also legally bound to notify the affected data subjects (clients, employees, etc.), if the personal data breach is likely to result in a high risk to the rights and freedoms[2] of natural persons (GDPR art. 33).

The personal data breach must be communicated to the data subjects via appropriate channels to ensure that the adequate level of detail is conveyed in a concise, transparent and intelligible manner. The data controller must notify each data subjects individually and preferably in writing, unless this constitutes a disproportionate effort in which case the data controller might communicate the breach publicly. Moreover, the data controller is obligated to establish a point of contact (helpline) and to provide access to personal data including a copy of the data that undergoes processing (GDPR art. 15). In certain circumstances, this may include handing out a document containing personal data such as a copy of an email.[3]

Footnotes:
1 Some EU Data Protection Authorities receive as many as 70 data breach notifications per 100.000 inhabitants and year (GDPR Today, www.gdprtoday.org/gdpr-in-numbers-4)

2 The risk to the rights and freedoms includes risk of discrimination, identity theft, financial loss, or damage of reputation (cp. GDPR recital 75)

3 For more details, see Activity Report Data Protection Authority Hessen, Germany

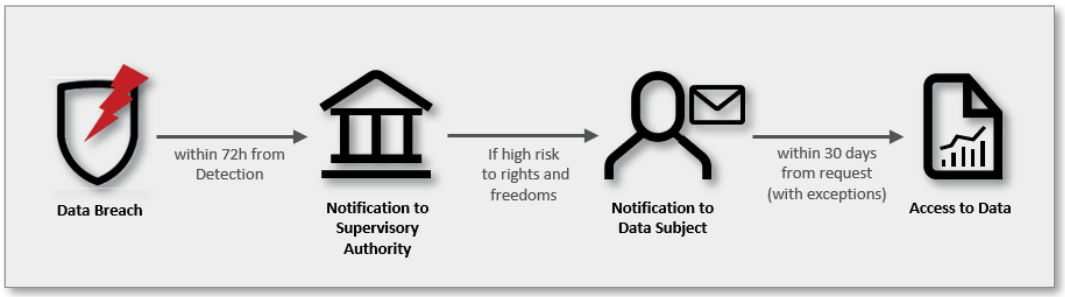


Figure 1:
Notification process under GDPR

Data Breach Notification as a Service

The data breach response process can be broken down into six main process steps (fig. 2).

Step 1 is the technical incident response process for the detection of a breach, its containment as well as eradication and data recovery. It is also part of the technical incident response process to analyse the breach, identify the affected data, and to implement customized improvement actions.

In a next step (step 2), the organization will assess how the breach has to be reported to the data protection authorities and other regulators. A data breach must be reported to the supervisory authority without undue delay, usually within 72 hours after having become aware of the breach. This is not a one-off reporting, rather, the organization needs to maintain an effective relationship with authorities from this point forward. Profound professional legal advice is key in this step of the process. A legal assessment will provide practical guidance on whether and how to notify the affected data subjects (i.e. via mail or publicly) and answer more pragmatic questions, such as which role holders of an account are to be notified or how to contact former clients with electronic mail

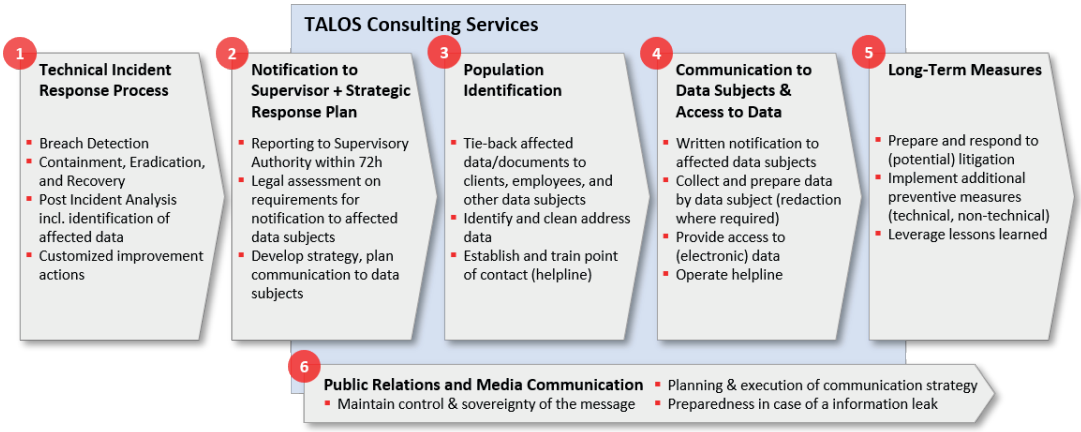


Figure 2:
The required 6 steps following a personal data breach

Footnotes:
4 That period may be extended by another 60 days taking into account the complexity and number of requests (GDPR art. 12)

delivery. The organization will use the results from the legal assessment to develop an appropriate response strategy and to plan the communication of the breach to affected data subjects and the public.

In step 3, the organization requires a methodology for the identification of the affected population of data subjects, which usually combines automated data analysis with manual reviews. As a simple example, an organization could search the breached data for account numbers followed by a false-positive review. Once the population is identified, address data of affected subjects will need to be queried, cleaned or even manually supplemented. This is particularly relevant for former clients and if the notification address differs from the regular mailing address.

Prior to the actual notification of data subjects, organisations need to nominate a point of contact for the data subjects and develop appropriate talking points. Some organizations implement a two-layered approach so that the first level point of contact can filter complex situations to a more experienced second level support. To ensure and control the consistency of messages to data subjects, only the dedicated point of contact should be authorized to communicate about matters concerning the breach.

In step 4, all affected data subjects are notified, typically either via electronical or physical mail. This may be conducted with a staggered approach to better handle the amount of potential replies. A certain proportion of data subjects will request access to the affected data or even all data and the organization must be prepared to deliver access to data within a reasonable timeframe, usually within 30 days from the request[4]. To do so, the organization requires a standardized method on collecting the data and preparing the information by data subject. Data relating to a third parties may need to be redacted – usually by a combination of auto-redaction and manual review to hide references to third parties. Access to data is to be provided in the most efficient way, preferably in an electronic format. All activities in this step, i.e. any mailing, client contact, request or provision of access, are tracked on an individual basis and, ideally, integrated into a workflow management tool.

It may take several months from becoming aware of the breach until completion of step 4. Still, some of the measures are even more long-term. These measures include the preparation and response to litigation or the implementation of additional preventive measures to reduce the risk of a future breach (step 5).

TALOS

Publication

As discussed in the introductory paragraph, a data breach may result in significant reputational risks. It is key that the organization keeps control and sovereignty of the message to clients and the public even before the actual notification to data subjects. This is achieved with an effective public relation and media communication (step 6).

Use Case

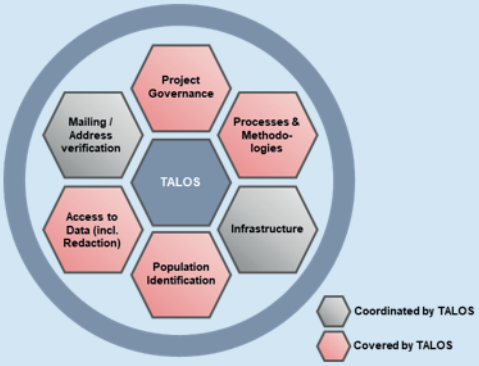
The Client Challenge

Our client suffered from a data breach in Switzerland and an EU country, leading to personal data of customers and employees being accessible to authorities in a foreign jurisdiction. Consequently, the client had to notify the affected individuals about the breach. In addition, several of the affected individuals in Switzerland and the EU contacted our client and requested access to data and documents.

Our Contribution

We designed and implemented the end-to-end notification and disclosure process, including the identification of affected individuals, sending of notification mails, operation of a help desk, as well as disclosure and redaction of relevant documents. As project implementers, TALOS defined the role of client teams, developed guidelines and working instructions, coordinated mailings and address reviews, and implemented tools for monitoring the status of each individual request. Temporarily TALOS supported the tie-back of affected data to affected individuals, provided quality assurance prior to the disclosure of data, and supported the redaction of references to third parties, where required.

With our ability to team up with specialized providers for identifying the affected data and individuals, for auto-redaction of documents and for maintaining virtual data rooms for a paperless disclosure of data and documents, TALOS became the entrusted partner to our client, coordinating all aspects of the notification in Switzerland and abroad.



Client's Benefit

The client could rely on a centralized function with the ability to partner with the organization as well as specialized providers to design, implement, and operate all aspects of the notification - from the identifying affected data subjects to providing access to data.

Conclusion

A personal data breach triggers a number of mandatory operational processes, including the notification to supervisory authorities, the identification of affected data and individuals, the communication to clients and the provision of access to data. If these operational processes are not managed and staffed properly, errors and other inefficiencies will result in further financial loss and reputational damage. Managing these processes requires an interdisciplinary approach, the knowledge and tools of specialized providers, legal expertise and project management skills. Organizations are well advised to build on the expertise and experience of professional providers, which are capable to manage and coordinate the interdisciplinary aspects of a data breach notification.

TALOS

Publication

Who we are

TALOS is continuously striving to shape new standards in management consulting. As a specialized consulting boutique of Swiss origin, we are serving the European financial services industry from our local offices in Zurich and Luxembourg.

Founded by experienced management consultants in 2008, we have grown since then to a renowned consulting company with a complementary service offering across various disciplines.

With our tailored hands-on approach, we accompany our clients in mastering the fundamental challenges the industry is facing.

We are a trusted partner for our clients helping them to increase their organizational effectiveness and operational efficiency.

We strive to be recognized as one of the leading management consulting boutiques for the European financial services industry.

Zurich
TALOS Management Consultants
Bleicherweg 45
CH-8002 Zürich
Tel. +41 44 380 14 40

Luxembourg
TALOS Management Consultants
6, Rives de Clausen
L-2165 Luxembourg
Tel. +352 26 20 23 54

www.talos-consultants.com
www.shapenewstandards.com

Your Contact

Christian is Partner at TALOS and has been working as an internal consultant for a German logistics group since 2005 and as a management consultant since 2007 (Accenture, TALOS).

Christian Scholten
Partner
christian.scholten@talos-consultants.ch

Thomas is Manager and joined TALOS in 2016. He has over 8 years of experience in the financial services industry with a global career in Switzerland, USA, Spain and South Korea. Thomas brings in functional expertise and project experience in the fields of regulatory compliance, outsourcing, and financial management.

Thomas Eustorgi
Manager
thomas.eustorgi@talos-consultants.ch