Breach Notification Under the General Data Protection Regulation:

New Capabilities in the IBM Resilient Incident Response Platform

Introduction

As of May 25, 2018, the European Union's General Data Protection Regulation (GDPR) has come into effect and with it comes new challenges for organisations dealing with the personal data and potential information loss of European Union (EU) citizens. There are many complexities to how an organisation is now required to respond to a data breach, and organisations need to ensure that their incident response team is fully prepared for the GDPR mandate.

The Key Points of GDPR

Any organisation globally that collects personal data in relation to offering goods or services to data subjects in the EU – whether the company is based in the EU or not – will have 72 hours to notify the relevant Supervisory Authority (SA) of a breach, and may need to notify their impacted customers without undue delay after becoming aware of the breach based on the level of potential risk to the affected customers.[1] If an organisation does not meet these requirements, it risks being fined. This strict, mandatory regulation will require proper planning and situational awareness to stay compliant.

Required Incident Response Plan

GDPR brings additional requirements for individual companies beyond the timeline. Among these, companies that fall under GDPR will need a documented incident response plan and an audit of incident response activities.[2] They will also need to maintain a detailed log of all relevant cyber security incidents, even if this does not trigger a notification requirement.

> *"Very few organizations from our latest Cyber Resilience study reported confidence in their ability to comply with GDPR. What's more is* ***77 percent admitted they do not have a formal cybersecurity incident response plan*** *that is applied consistently across the organization."*
>
> – Dr. Larry Ponemon, Chairman and Founder of the Ponemon Institute

For many companies, this will be the first mandatory breach notification regulation they must follow. Preparation has become more complex as individual member states in the EU have added their own laws in addition to the GDPR baseline. With the globalisation of business today, many companies will have to continue to adapt their incident response processes to account for customer breaches in different countries and work closely with the relevant Data Protection Authorities (DPAs) and specific regulations in different countries.

[1] GDPR Article 34: https://www.eugdpr.org/article-summaries.html

[2] GDPR Article 33: https://www.eugdpr.org/article-summaries.html

> ***83 percent** of organisations in the United States and Europe say that data breach notifications is the most difficult GDPR obligation to meet.*
>
> – IAPP Study, April 2018

Seventy-Two-Hour Breach Notification Requirement

As mentioned, a notable challenge for organisations is the new 72-hour data breach notification requirement. For IR teams facing this shortened window, preparation is more important than ever. Responders will need clear and consistent processes to guide them through response and notification quickly and effectively.

What is a Data Breach Under GDPR?

Another complication from GDPR is that multiple types of data breaches need to be reported. Under GDPR, a breach is defined as "*a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data transmitted, stored or otherwise processed.*"[3]

For example, any breach that is more than the loss of personal data – or, more technically, if the breach could result in a risk to the rights and freedoms of individuals – needs to be reported. In the Article 29 Working Party (WP29) guidelines on personal data breach notification, this can include loss of control over their personal data, limitation of their rights, discrimination, identity theft or fraud, financial loss, unauthorized reversal of pseudonymization, damage to reputation, and loss of confidentiality of personal data protected by professional secrecy. It can also include any other significant economic or social disadvantage to those individuals. If there is a high risk of these outcomes, then GDPR requires that the affected individuals be notified 'as soon as is reasonably feasible'.[4]

The WP29 guidance also calls out an "availability breach" that must be reported. This is a type of security incident that results in personal data made unavailable for a period of time, such as the unavailability of critical medical data in a hospital could cause risk to an individual.

Gaining an innate knowledge of what to flag and when to flag will be necessary – and can best be learned and effectively addressed through simulations and practice well in advance of breaches.

> *"Our research shows that most companies globally do not feel confident in their ability to comply with the upcoming data breach notification requirements that GDPR will bring. Organizations should be **proactive now, and establish processes and owners** for ensuring compliance with the new requirements."*
>
> – Dr. Larry Ponemon, Chairman and Founder of the Ponemon Institute

How Intelligent Orchestration Helps with GDPR

To help overcome this uncertainty of the new regulations – such as what types of breaches need to be reported, when to report them, and who to report them to – Intelligent Orchestration can be effective.

Intelligent Orchestration aligns the people, process, and technology involved in incident response – empowering responders to triage and resolve incidents intelligently, quickly, and effectively. When faced with uncertainty, incident response orchestration is crucial to ensuring that the humans in the loop can address an incident on hand, decide what needs to be done, and take remedial actions quickly and accurately.

[3] GDPR Article 4: https://www.eugdpr.org/article-summaries.html

[4] https://gdpr-info.eu/recitals/no-86/

> *"Orchestrating the people, process, and technology involved in data breach response and notification is essential to facing the challenges of GDPR. The Resilient Incident Response Platform is uniquely qualified on this front – as it* ***empowers response teams to quickly and efficiently respond to a breach*** *while staying in compliance with the breach notification obligations that GDPR will require."*
>
> **– Gant Redmon, Program Director, Cyber Security and Privacy, IBM Resilient**

When managing a privacy breach, response involves more than the security team. Privacy, legal, marketing, and key executives may all need to play a role. Intelligent Orchestration facilitates collaboration across the company – making your organisation-wide compliance efforts more effective.

Speed and accuracy are critical given the new breach notification deadlines – and orchestrating the incident response and breach notification processes are key to meeting the tight deadlines imposed by GDPR. By automating the right technological processes to empower people in the process can help ensure the organisation's response is efficient and accurate.

How IBM Resilient Efficiently Supports Compliance Efforts, Fast GDPR Breach Response

IBM Resilient has one of the world's largest breach notification databases integrated into our Incident Response Platform (IRP), and provides detailed workflows to support compliance efforts with specific regulations in the event of a breach. The Resilient Privacy Module, launched in 2011, supports more than 300 deployed customers and tracks more than 150 global privacy-reporting regulations to help improve the incident response and breach notification process. It is adapted regularly to meet the changing regulations and the growing needs of our customers and prospects, including GDPR.

By leveraging the Resilient IRP, customers will be better able to meet the new GDPR incident response regulations. The GDPR-enhanced Privacy Module provides customers with the information to assist their reporting requirements under GDPR.

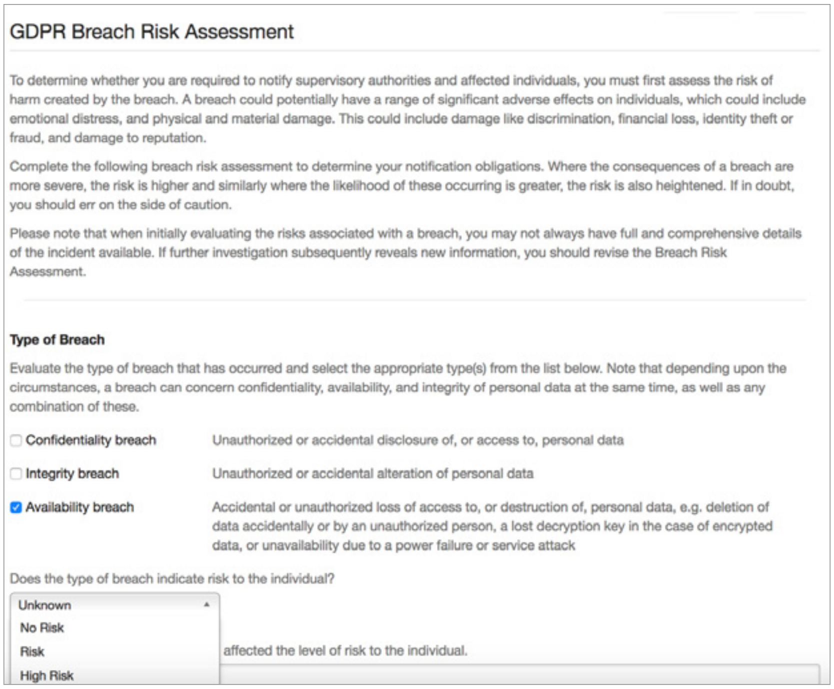
> ***66 percent*** *of organisations in the US and Europe that feel confident in their ability to comply with GDPR credit having an effective incident response plan in place, the highest of any factor.*
>
> **– IAPP Study, April 2018**

IBM Resilient Tools for GDPR Breach Notification:

GDPR Breach Risk Assessment

The new GDPR Breach Risk Assessment tools help to guide the IR and Privacy teams through the risk associated with a security incident. The tool walks the team through the WP29 guidelines, providing examples and additional guidance to help determine the level of risk and the correct notification strategy.

The Privacy team can generate a clean report to share with the relevant SA to demonstrate that work has been done to ascertain the level of risk – a GDPR requirement.



GDPR Breach Risk Assessment

To determine whether you are required to notify supervisory authorities and affected individuals, you must first assess the risk of harm created by the breach. A breach could potentially have a range of significant adverse effects on individuals, which could include emotional distress, and physical and material damage. This could include damage like discrimination, financial loss, identity theft or fraud, and damage to reputation.

Complete the following breach risk assessment to determine your notification obligations. Where the consequences of a breach are more severe, the risk is higher and similarly where the likelihood of these occurring is greater, the risk is also heightened. If in doubt, you should err on the side of caution.

Please note that when initially evaluating the risks associated with a breach, you may not always have full and comprehensive details of the incident available. If further investigation subsequently reveals new information, you should revise the Breach Risk Assessment.

Type of Breach

Evaluate the type of breach that has occurred and select the appropriate type(s) from the list below. Note that depending upon the circumstances, a breach can concern confidentiality, availability, and integrity of personal data at the same time, as well as any combination of these.

☐ Confidentiality breach	Unauthorized or accidental disclosure of, or access to, personal data
☐ Integrity breach	Unauthorized or accidental alteration of personal data
☑ Availability breach	Accidental or unauthorized loss of access to, or destruction of, personal data, e.g. deletion of data accidentally or by an unauthorized person, a lost decryption key in the case of encrypted data, or unavailability due to a power failure or service attack

Does the type of breach indicate risk to the individual?

affected the level of risk to the individual.

Updated Privacy Module

Now updated in the Resilient IRP with GDPR reporting requirements for the 28 EU member states

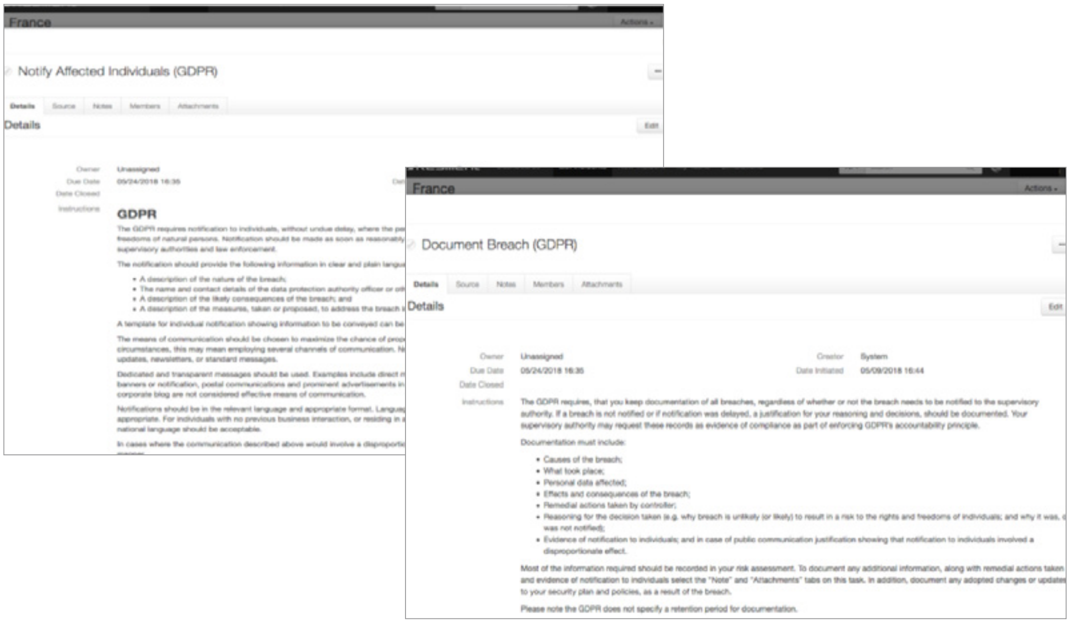
The Resilient Privacy Module guides organizations through the correct response to data loss incidents, helping to meet the regulatory deadlines and best practices for responding to an incident under GDPR.

Updated to include final GDPR reporting requirements for the 28 EU member states, the Privacy Module provides specific notification requirements for the different supervisory authorities, how they should be notified, and what information is required. Templates for this process are provided in the Privacy Module where applicable. Instructions are also provided on what must be included if individual notifications are also required. In addition to this, Resilient provides prompts and guidelines on what information is needed to document the incident for GDPR purposes.

With the Resilient Privacy Module, breach notification is integrated with the wider cyber security incident response plan, providing one central hub of incident management. GDPR reporting requirements and security incidents can now be completed in a fraction of the time of manual processes – and with greater confidence that your organization has followed the new regulations.

New Tasks for GDPR Compliance

In addition to the new GDPR Breach Risk Assessment tool, IBM Resilient has added three new tasks to help organisations with compliance. The **Notify Supervisory Authority Task** was added to provide instructions on who to notify, what must be included in the notification, and how to notify. This also provides a notification template and an option to provide subsequent notification if doing so in phases. The **Notify Affected Individuals Task** provides instructions on what must be included in the notification, and guidance on acceptable formats. The task also provides a notification template for users. Finally, the **Document Breach Task** prompts and guides users on how to document the incident throughout the response process.



Notify Affected Individuals (GDPR)

Details

Owner Unassigned
Due Date 05/24/2018 16:35
Date Closed
Instructions

GDPR

The GDPR requires notification to individuals, without undue delay, where the pe
freedoms of natural persons. Notification should be made as soon as reasonably
supervisory authorities and law enforcement.

The notification should provide the following information in clear and plain langu

- A description of the nature of the breach;
- The name and contact details of the data protection authority officer or oth
- A description of the likely consequences of the breach; and
- A description of the measures, taken or proposed, to address the breach i

A template for individual notification showing information to be conveyed can be

The means of communication should be chosen to maximize the chance of prop
circumstances, this may mean employing several channels of communication. N
updates, newsletters, or standard messages.

Dedicated and transparent messages should be used. Examples include direct m
banners or notification, postal communications and prominent advertisements in
corporate blog are not considered effective means of communication.

Notifications should be in the relevant language and appropriate format. Languag
appropriate. For individuals with no previous business interaction, or residing in a
national language should be acceptable.

In cases where the communication described above would involve a disproportio

Document Breach (GDPR)

Details

Owner Unassigned
Due Date 05/24/2018 16:35
Date Closed
Creator System
Date Initiated 05/09/2018 16:44

Instructions

The GDPR requires, that you keep documentation of all breaches, regardless of whether or not the breach needs to be notified to the supervisory authority. If a breach is not notified or if notification was delayed, a justification for your reasoning and decisions, should be documented. Your supervisory authority may request these records as evidence of compliance as part of enforcing GDPR's accountability principle.

Documentation must include:

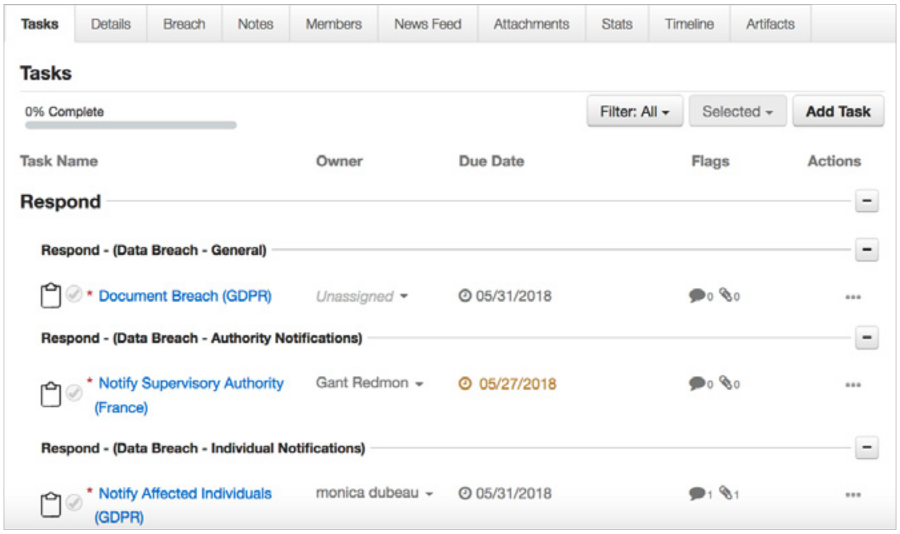
- Causes of the breach;
- What took place;
- Personal data affected;
- Effects and consequences of the breach;
- Remedial actions taken by controller;
- Reasoning for the decision taken (e.g. why breach is unlikely (or likely) to result in a risk to the rights and freedoms of individuals; and why it was, o was not notified);
- Evidence of notification to individuals; and in case of public communication justification showing that notification to individuals involved a disproportionate effect.

Most of the information required should be recorded in your risk assessment. To document any additional information, along with remedial actions taken and evidence of notification to individuals select the "Note" and "Attachments" tabs on this task. In addition, document any adopted changes or updates to your security plan and policies, as a result of the breach.

Please note the GDPR does not specify a retention period for documentation.

GDPR Simulation

Simulating GDPR privacy breaches empowers organizations to proactively rehearse the actions required based on a breach under GDPR. It helps both people and processes to be battle-tested and well-practiced before a real data breach occurs. Organizations can use this too as an effective way to iterate on the process and make changes as needed.



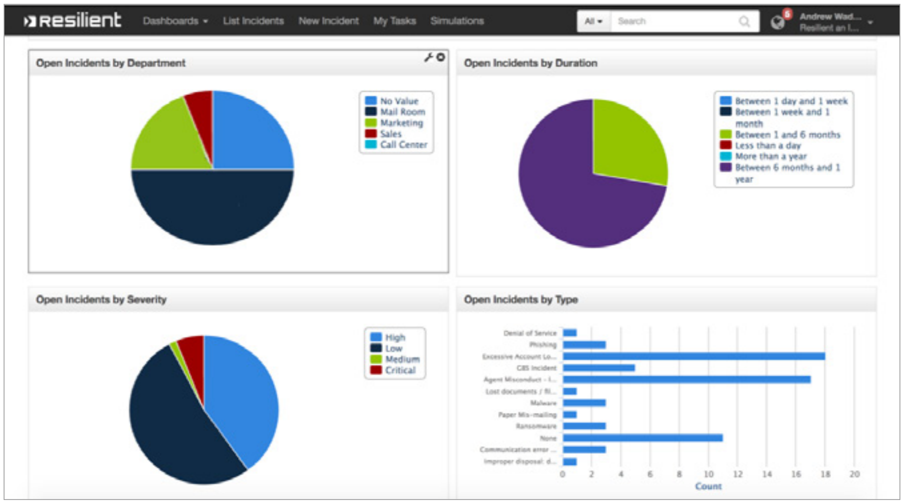
Tasks

0% Complete

Task Name	Owner	Due Date	Flags	Actions
Respond				
Respond - (Data Breach - General)				
* Document Breach (GDPR)	*Unassigned*	05/31/2018	0 0	•••
Respond - (Data Breach - Authority Notifications)				
* Notify Supervisory Authority (France)	Gant Redmon	05/27/2018	0 0	•••
Respond - (Data Breach - Individual Notifications)				
* Notify Affected Individuals (GDPR)	monica dubeau	05/31/2018	1 1	•••

Reporting

Users also have access to IBM Resilient's dashboards and reporting tools. These become useful for keeping IR leadership and organisation executives informed of the effectiveness of the overall response process, including GDPR compliance efforts. These tools also provide new insight needed for conversations about what processes need additional resources.



The key to being fully prepared to meet the new breach reporting requirements is to have a system where organisations can orchestrate and practice their incident response plan across the business. GDPR will require that your team not only have an incident response plan in place, but in order to tackle incidents effectively, it also needs to be fully orchestrated across the organisation's people, processes, and technologies. By leveraging guided response from Intelligent Orchestration, IBM Resilient provides security teams with the speed, agility, and intelligence for contending with increasingly complex attacks and navigating the new regulatory world of GDPR compliance.

- Learn more about IBM Resilient's offerings and best practices to prepare for GDPR
- Learn more about IBM's own GDPR readiness journey and our GDPR capabilities and offerings

Notice: Clients are responsible for ensuring their own compliance with various laws and regulations, including the European Union General Data Protection Regulation. Clients are solely responsible for obtaining advice of competent legal counsel as to the identification and interpretation of any relevant laws and regulations that may affect the clients' business and any actions the clients may need to take to comply with such laws and regulations.

The products, services, and other capabilities described herein are not suitable for all client situations and may have restricted availability. IBM does not provide legal, accounting or auditing advice or represent or warrant that its services or products will ensure that clients are in compliance with any law or regulation.