GDPR Incident Response Process
25 September 2016

The EU General Data Protection Regulation (GDPR) establishes security breach notification requirements for data controllers and processors. This document explores these obligations, taking into account lessons learned from breach notification requirements in the United States. It offers a template Incident Response Policy that may assist companies as they revise their internal policies to meet GDPR requirements.

A. GDPR Background

"Personal Data Breach" is defined in Article 4 of the GDPR as follows:

> (12) 'personal data breach' means 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[.]

The substantive obligations in the event of a personal data breach are set forth in Articles 33 and 34, which require notification of personal data breaches to supervisory authorizes and data subjects respectively.

> ***Article 33:*** **Notification of a personal data breach to the supervisory authority**
>
> 1. In the case of a personal data breach, the controller shall without undue delay and, where feasible, not later than 72 hours after having become aware of it, notify the personal data breach to the supervisory authority competent in accordance with Article 55, unless the personal data breach is unlikely to result in a risk to the rights and freedoms of natural persons. Where the notification to the supervisory authority is not made within 72 hours, it shall be accompanied by reasons for the delay.
>
> 2. The processor shall notify the controller without undue delay after becoming aware of a personal data breach.
>
> 3. The notification referred to in paragraph 1 shall at least:
>
>   (a) describe the nature of the personal data breach including where possible, the categories and approximate number of data subjects concerned and the categories and approximate number of personal data records concerned;
>
>   (b) communicate the name and contact details of the data protection officer or other contact point where more information can be obtained;
>
>   (c) describe the likely consequences of the personal data breach;
>
>   (d) describe the measures taken or proposed to be taken by the controller to address the personal data breach, including, where appropriate, measures to mitigate its possible adverse effects.

4. Where, and in so far as, it is not possible to provide the information at the same time, the information may be provided in phases without undue further delay.

5. The controller shall document any personal data breaches, comprising the facts relating to the personal data breach, its effects and the remedial action taken. That documentation shall enable the supervisory authority to verify compliance with this Article.

Article 34: **Communication of a personal data breach to the data subject**

1. When the personal data breach is likely to result in a high risk to the rights and freedoms of natural persons, the controller shall communicate the personal data breach to the data subject without undue delay.

2. The communication to the data subject referred to in paragraph 1 of this Article shall describe in clear and plain language the nature of the personal data breach and contain at least the information and measures referred to in points (b), (c) and (d) of Article 33(3).

3. The communication to the data subject referred to in paragraph 1 shall not be required if any of the following conditions are met:

   (a) the controller has implemented appropriate technical and organisational protection measures, and those measures were applied to the personal data affected by the personal data breach, in particular those that render the personal data unintelligible to any person who is not authorised to access it, such as encryption;

   (b) the controller has taken subsequent measures which ensure that the high risk to the rights and freedoms of data subjects referred to in paragraph 1 is no longer likely to materialise;

   (c) it would involve disproportionate effort. In such a case, there shall instead be a public communication or similar measure whereby the data subjects are informed in an equally effective manner.

4. If the controller has not already communicated the personal data breach to the data subject, the supervisory authority, having considered the likelihood of the personal data breach resulting in a high risk, may require it to do so or may decide that any of the conditions referred to in paragraph 3 are met.

Guidance around the personal data breach notification provisions is found in GDPR Recital paragraphs 85 – 88.[1] This guidance may helpful to companies as them implement policies to comply with the notification rules. The guidance may also be used by national data protection authorities (DPAs) as they manage incidents reported to them by companies and other organizations.

[1] The full text of these recital paragraphs is provided at the end of this document for reference. Highlighted sections are taken from these paragraphs.

As with the original US breach notification laws, the GDOR's breach notification provisions are clearly motivated by a desire to enable data subjects to mitigate the possible harms that may result from a personal data breach. However, it is also clear that the harms envisioned by the GDPR are broader than those generally considered when evaluating data breaches in the US As you can see from paragraph 85, the harms that must be considered include: "physical, material or non-material damage to natural persons such as loss of control over their personal data or limitation of their rights, discrimination, identity theft or fraud, financial loss, unauthorised reversal of pseudonymisation, damage to reputation, loss of confidentiality of personal data protected by professional secrecy or any other significant economic or social disadvantage to the natural person concerned."

The GDPR balances this extremely broad definition of harm by defining a 2-step notification process. If there is any "risk" of harm, the controller must notify its supervisory authority regarding the breach per Article 33. We understand from paragraph 85 that this enables the authority to evaluate the incident and determine if data subject notification is warranted.

The GDPR reflects the regulatory consensus that speed is of the essence. Paragraph 85 states: "as soon as the controller becomes aware that a personal data breach has occurred, the controller should notify the personal data breach to the supervisory authority without undue delay." If the controller cannot provide this initial notification to the authority within 72 hours, it must provide an explanation for the delay.

Article 33 provides that DPA notification is not required if the breach is "unlikely to result in a risk to the rights and freedoms of natural persons." Paragraph 85 adds that the controller must be able to demonstrate that there is unlikely to be risk "in accordance with the accountability principle."

If the controller realizes that there is a "high risk" of harm, it must notify the affected data subjects without undue delay. Paragraph 86 provides some additional insights into the Article 34 obligation, specifically that these notifications should be made "in close cooperation with the supervisory authority." From this, we understand that the Article 33 DPA notification must always occur prior to the Article 34 data subject notifications.

Paragraph 86 also notes certain factors that may impact the timing of the data subject notification. Notification should occur as soon as reasonably feasible, taking into account guidance from relevant authorities and other facts. "For example, the need to mitigate an immediate risk of damage would call for prompt communication with data subjects whereas the need to implement appropriate measures against continuing or similar personal data breaches may justify more time for communication." Paragraph 87 extends this concept, explicitly recognizing that notifications may need to be delayed to "take into account the legitimate interests of law-enforcement authorities where early disclosure could unnecessarily hamper the investigation of the circumstances of a personal data breach."

Paragraphs 87 and 88 illustrate the importance of using appropriate security measures (such as encryption) to protect personal data. Following the trend in the US for new breach notification laws, the GDPR does not provide a blanket exception to the breach notification rules for encrypted data.[2] Additionally, paragraph 87 says: "It should be ascertained whether all appropriate technological

[2] Of course, if data is strongly encrypted, the controller should have a basis for concluding that risk is unlikely, so that no notification is required under Article 33.

protection and organisational measures have been implemented to establish immediately whether a personal data breach has taken place."

Paragraph 88 further advises that: "[i]n setting detailed rules concerning the format and procedures applicable to the notification of personal data breaches, due consideration should be given to the circumstances of that breach, including whether or not personal data had been protected by appropriate technical protection measures, effectively limiting the likelihood of identity fraud or other forms of misuse."

As in the US, it seems reasonable to anticipate that EU DPAs will use breach notifications as a starting point to consider the appropriateness of the reporting organizations' security measures[3] generally. Accordingly, organizations consider the appropriateness of their controls given the Article 32 (Security of Personal Data) requirements, it is useful to understand that encryption and similar technologies can provide benefits for incident responses programs as well. Data retention measures may also be evaluated, if the breach involves data that the DPAs believe should have been retained.

B. Compliance Challenges

While the breach notification provisions in the GDPR are very specific in certain respects, such as timing and content of notices, there are other areas where the expectations are undefined. This uncertainty creates risks for organizations, and potentially undermines the effectiveness and timeliness of the notification process. Accordingly, this paper notes the challenges and offers some options that may enable breach notification process to operate more efficiently across the EU.

1. Determination of Competent Supervisory Authority

One of the most difficult issues for companies that are subject to the GDPR will be determining which DPA(s) to notify regarding breach. Article 33 requires notification of breaches to the "to the supervisory authority competent in accordance with Article 55." Article 55, however, provides that each supervisory authority is competent in its own Member State. The text thus raises the possibility that, if a personal data breach impacts individuals in multiple member states, multiple DPAs may be competent to advise on the matter. Depending on the circumstances, the breach could justify involvement of many DPAs.

> *Consider a company whose main establishment and EU DPO are located in France, whose German affiliate experienced a personal data breach, and the breach impacted data subjects in all of the EU member states. It is highly unlikely that the company could effectively respond to the incident in the desired timeframes, if it had to notify and consult with all EU DPAs.*

In the US, companies are often obligated to notify multiple regulators in those states where impacted individuals reside, but these notifications are generally made in parallel with the data subject notifications. In this model, the regulators learn of the breaches, so they can provide assistance to individuals who contract them after receiving a notification letter. For large breaches, it is also common for companies to consult with its primary regulator or law enforcement authority as the incident is evaluated, but companies engage in these consultations in the context of ongoing relationships.

3

To ensure that EU breaches are handled appropriately and in a timely manner, it would be prudent to establish that companies should provide the notice required by Article 33 initially only to the DPA that is most effectively able to analyze and evaluate the incident. In most cases, this "lead DPA" would be the authority that regulates the company in the territory of its main establishment, although, if a large affiliate experienced the breach, it might elect to work with the DPA in its country of presence, particularly if the internal response was being managed from that location. If there is a large population of data subjects in another jurisdiction, the primary DPA might conclude that the DPA in that territory should be notified as well, particularly if the risk to the individuals is uncertain. Companies should also notify applicable DPAs generally if they are sending notification letters to data subjects in other countries.

> *In the example above, the company could notify either the French or the German DPA, taking into account which DPA generally advises the company, the location of internal personal (such as the DPO and security personnel) that are overseeing the investigation, and other factors. If the DPA recommends data subject notification, the company would notify other DPAs regarding the incident so that they could be prepared to address any questions that might arise from data subjects.*

This approach also has the advantage that companies can prepare in advance for any notifications that might need to be made, by being familiar with the primary DPA's notification processes and forms, for example. If notifications are required to DPAs with whom the organization is not familiar, some delay for research regarding the notification process, language, *et. al.* is inevitable. To facilitate additional regulatory notifications that may be appropriate, the DPAs should consider establishing standard notification processes and forms.

2. Determination of "risk" and "high risk"

As discussed above, it clear that companies must consider "risk to the rights and freedoms of natural persons" very broadly, encompassing "physical, material or non-material damage to natural persons such as loss of control over their personal data or limitation of their rights, discrimination, identity theft or fraud, financial loss, unauthorised reversal of pseudonymisation, damage to reputation, loss of confidentiality of personal data protected by professional secrecy or any other significant economic or social disadvantage to the natural person concerned" (Paragraph 85). Unfortunately, the GDPR does not offer guidance on how to evaluate these risks or when it would be appropriate to conclude that a breach is unlikely to result in such risk.

US laws generally provide certain exceptions for when incidents are *not* security breaches that trigger notification. For example, most US state laws state that the "good faith acquisition of personal information by an employee or agent of the business" is not a breach, provided that the personal information is not misused. This type of provision reflects the common sense view that coworkers and vendors are all bound by confidentiality obligations, trained and subject to oversight. (This also organization allocate security resources effectively, understanding that inadvertent internal disclosures do not present the same risk as other threats.) Similarly, many US laws explicitly allow companies to avoid notification if the compromised personal data are encrypted, as long as the encryption keys are not also exposed.

US regulators have also published guidance regarding breaches, including how to determine if personal data has been compromised, triggering an obligation to notify. New York state's breach notification

law,[4] for example, instructs companies to consider the following factors (among others) to determine if personal information has been acquired by an unauthorized person (triggering the notification rule):

(1) Indications that the information is in the physical possession and control of an unauthorized person, such as a lost or stolen computer or other device containing information; or

(2) Indications that the information has been downloaded or copied; or

(3) Indications that the information was used by an unauthorized person, such as fraudulent accounts opened or instances of identity theft reported.

Most helpfully, the US Department of Health & Human Services' HIPAA Breach Notification Rule[5] provides a four-factor test that entities use to determine whether protected health information is compromised in the event of a security breach. These factors are

(1) The nature and extent of the information involved, including the types of identifiers and the likelihood of re-identification;

(2) The unauthorized person who used the information or to whom the disclosure was made;

(3) Whether the information was actually acquired or viewed; and

(4) The extent to which the risk to the information has been mitigated.

This model is highly useful for companies, as it provides an objective standard and enables consistency in conducting breach assessments. In particular, use of these factors provides makes it clear that the acquisition of sensitive personal data by an untrusted recipient creates a high risk of harm; while also allowing companies to demonstrate that there is no or low risk, even if sensitive personal information is exposed, if the recipient is trusted, the data is recovered, and any residual harm is mitigated.

As a practical matter, much attention is spent on documenting the types of incidents that put individuals at risk of harm, but many security incidents do not create such risk. For example, many companies have invested heavily in encryption technology, precisely to protect data if it is exposed. Ensuring that companies who use strong encryption have a path to avoid costly breach notification will encourage even greater deployment of that technology.

Similarly, companies and individuals need to focus on sending breach notifications where there are steps that should be taken to reduce risk. If the risk of an incident is fully mitigated, the company should not notify individuals. Over-notification (particularly where there is no risk to mitigate) can create notification fatigue and reduce the likelihood that individuals will act on a notification letter, even when action is needed. For example, a company employee may inadvertently transmit a file containing personal data to the wrong recipient. (A file intended for one company vendor may be accidently sent to another vendor.) If the recipient is trustworthy, the mistake is reported, and the data is recovered with credible assurances that it was not stored or used, there is no or very low risk to the individual. These types of incidents should not trigger notification, as there is no further risk to be managed.

[4] New York General Business Law §899-aa. (See: http://codes.findlaw.com/ny/general-business-law/gbs-sect-899-aa.html)

[5] 45 CFR §§ 164.400-414 (See: http://www.hhs.gov/hipaa/for-professionals/breach-notification/)

Attachment 1 below contains a template incident response policy that incorporates a scorecard (based on the US Health & Human Service model) that can be used to evaluate personal data breaches for risk of harm. The policy follows the industry best practice of a three-step approach to privacy breaches:

> 1st: Are individuals at real risk of harm? If so, notify the individuals as soon as possible, and provide assistance to mitigate the risk. Notify regulators and others (such as law enforcement agencies, payment card fraud teams, *etc.*) as appropriate or necessary. (if there is real risk, individuals are notified even if there is no legal obligation to do so.)
>
> 2nd: If individuals are not at real risk of harm, provide notifications as may be required by law.
>
> 3rd: If there is no risk of harm and no legal obligation to notify anyone, document the findings and implement any organization learning needed to reduce the likelihood of this type of incident reoccurring.

This template may provide companies and regulators with a foundation from which to evaluate and standardize incident response program expectations.

3. Practical Considerations for Breach Notification in the EU

From our experience with breach notification programs in the US, we have learned many important lessons regarding the practical implications of these programs. EU companies, DPAs, NGOs and other stakeholders should collaborate to offer answers to the practical questions that will arise as companies implement breach notification programs in the EU. Three particular challenges involve determining the best ways to mitigate risk from breaches, effectively communicating with data subject about breaches, and enabling data processors to support controllers in large, multi-client breaches.

a) What are acceptable ways to mitigation risk?

While it certainly appropriate to understand the risks that come from personal data breaches broadly, we must recognize that there are not always easy (or standard) ways to mitigate the different types of risk. In the US, breach notification laws focus on alerting individuals to risks of identity theft or financial fraud. These risks can be mitigated using services that are widely available in the US, such as credit monitoring, fraud resolution services, and id theft insurance. The success of these products is such that they are commonly provided to individuals, even when a breach does not compromise financial data or identifiers.

The problem with this "always-offer-credit-monitoring" approach, however, is that the remedy often does not fit the risk. If online account credentials are compromised, credit monitoring does not help. The better remedy would be to offer an online protection program, such as antivirus or malware software, along with educational materials about how to avoid phishing attacks. In other situations, such as the disclosure of a private fact (such as salary or a medical condition), there may be no real way to mitigate that harm. In this case, the company can only apologize and take measures to prevent that type of breach from happening again.

The important lesson to learn from the U, is that companies, regulators, NGOs, and others need to be flexible and creative when considering ways to mitigate harm. The mitigation strategies need to reflect

the specific situation. It would be useful to have a comprehensive risk mitigation toolbox with various tools: such as:

- Agreed-upon standards for obtaining assurances from unauthorized third parties recipients that they will not use or further disclose personal data;

- Credit monitoring products (where available) and similar "identity protection" products for personal data breaches involving national identifiers, financial account data, and the like – *companies may need to be encouraged to develop these products for Europe, where they do not organically exist today;*

- Online protection products, such as anti-virus software, for personal data breaches that compromise online accounts;

- Consumer education materials, providing specific information that individuals can use to address any harms they experience. For example, if a breach may put an individual at risk of discrimination, the company should educate the consumer regarding they types of discrimination that might be encountered and what legal recourse the person might have against the entity engaged in the illegal conduct; and

- Consumer education regarding data protection rights generally, and information on how to obtain assistance with access requests, so the individual can locate and request deletion of any personal data that may have been acquired by others.

b) How do we effectively communicate with data subjects?

In the US, breach notification laws have become very specific with regard to the content that must be provided to data subjects, including in many cases information about credit reporting, police reports, *etc.* While each of these types of content can be very useful, as noted above, the content provided needs to be tailored to the specific types of incident.

For example, in the US, notification letters "assume" that the data elements breached put the individual at risk of traditional identity theft. However, if a breach compromises a personal's credit card number, the person needs to review the credit card account statements, report any fraudulent charges, and obtain a new card (with a new number) if the compromised number is being misused. A compromised credit card number does not create a risk that a person's identity will be used to create new accounts. The legal requirements for letters result in individuals receiving letters with information that does not fit the situation. These letters are confusing and counterproductive because they do not clearly and concisely instruct the individual about steps that need to be taken.

The notification requirements set forth in Article 34 (and 33, by reference) seem to provide appropriate parameters for data subject notification. As part of building the toolkit discussed above, the various stakeholders may wish to develop some standard templates to help assure that data subjects get appropriate and effective information tailored to the risks presented by the breach. Notification letter contents should not be dictated, however, to avoid creating the problems experienced by US companies when inappropriate (and inapplicable) content is mandated.

Additionally, companies providing breach notification in the EU will need to consider the various challenges posed by the multitude of languages spoken by EU residents. In situations where a company

has a direct relationship with the individual, the notification letters can be made in the language that the company generally uses to communicate with the person. In other cases, however, the entity may have personal data on individuals without knowing what language the person comfortably speaks. (Public agencies, hospitals, and common carriers, for example, all likely have this challenge.) In the event o large breaches, companies may need to work with DPAs and NGOs to effectively communicate with individuals who have language or other personal barriers to understanding the notifications.

c) How can processors effectively support controllers in multi-client breaches?

Lastly, it is important to also consider the practical challenges that exist for stakeholders when a large breach occurs at a data processor. As in the US, the breach notification rules anticipate that processors will notify controllers, so that the controller can notify the DPAs and consumers. However, when a processor breach involves many controllers, the response process becomes mired. The processor may be trying to communicate with dozens or hundreds of its clients; these clients will all be reporting the facts second-hand to their competent authorities, and the authorities will be receiving multiple reports regarding the same incident.

Controllers and DPA must find ways to ensure that processor breaches are handled efficiently. For multi-client breaches, it may be sensible for the processors to provide initial notification to the DPA, if they and their clients agree. This approach allows the DPAs receive first hand information about the situation as well. The companies may also prefer the processor to handle the administrative aspects of data subject notification, such as printing letters, setting up informational websites and call centers and arranging for remediation services.[6] If the processor is an entity that is known directly to the data subjects, it may even be appropriate for the notification to be made by the processor itself.[7]

In the US, regulators provide *as hoc* flexibility to enable processor-led breach response. (Some regulators, including the Department of Health & Human Services, formally enable processor reporting of breaches to them via the web reporting mechanisms.) In large, multi-client breach situations, this approach is clearly more efficient for all partiers (including the regulators). However, given the potential penalties associates with GDPR non-compliance, EU-based controllers may need more formal guidance from DPAs before they will allow their processors to assist with meeting the breach notification obligations.

[6] Processors also prefer to oversee these aspects of the response, as they can save money and ensure quality control by contracting for services that cover the entire population of data subjects.

[7] If the processor is not known to the data subject directly then the notification should be made in the controller's name, to avoid confusion.

Attachment 1 – Template Incident Response Policy [8]

Acme is fully committed to protecting the security and confidentiality of all of the personal information that is entrusted to us. As part of this commitment, Acme has documented and implemented this incident response policy to guide our internal handling of events and incidents that may impact "**Personal Data**," which is any information that can be used identify, locate or contact an individual, such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person.

A "**Personal Data Breach**" means 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.

Acme defines a **"Privacy Event"** as *any* occurrence that *could* compromise the privacy, confidentiality, security or integrity of Personal Data. Privacy Events include any deviation from Acme's privacy or security policies, loss of Personal Data as well as any unauthorized use or disclosure of Personal Data.

Examples of Privacy Events:

- Lost or stolen device containing Personal Data
- Misdirected package, email or fax containing Personal Data
- Presence of malware on a computer or device containing Personal Data
- Transmission of Personal Data other than as permitted by company policy

Acme requires all employees and contractors to report Privacy Events via an established process. We investigate all Privacy Events, to determine what happened, establish if any Personal Data was compromised, and (if so) evaluate the risk of harm that could result from the situation. *In many cases Privacy Events do not actually expose any Personal Data to any unauthorized individuals. For example, Personal Data on a lost laptop may have been encrypted so that it could not be viewed by any unauthorized person.*

In some cases, Privacy Events do impact Personal Data. For example, a lost device may contain unencrypted information. Or an employee may have accidently transmitted a file containing Personal Data to the wrong recipient. If the recipient was able to view the Personal Data in the file, that information, it is an unauthorized disclosure. These events are Personal Data Breaches.

In responding to Personal Data Breaches, it is essential that we quickly and accurately assess the risk of harm. If individuals are at risk of harm, Acme policy is to notify the individuals as soon as possible and to help them mitigate the harm. If individuals are risk, we notify them even if there is no specific legal obligation to do so. If individuals are not a real risk of harm, Acme policy is to provide notification as may be required by law.

---

[8] This template is provided for reference purposes only. Many countries have enacted laws with specific requirements for incident response, including steps that need to be taken to analyze the event, and the contents and timing of individual and regulatory notifications. This template is NOT designed to address all possible applicable requirements of these laws. If you experience a privacy or security incident, you should consult your own legal counsel to determine the specific requirements that will be applicable, given your particular situation.

All Personal Data Breaches must be evaluated using the following 3 step process to determine the proper company response.[9]

STEP 1: Determine if there is a high risk to the impacted individuals as a result of the incident.

If so, notification of individuals and the appropriate Supervisory Authority is required without undue delay.

Generally speaking, a breach creates high risk for an individual when, if unaddressed, such a breach is likely to have a significant detrimental effect on the individual – for example, result in discrimination, damage to reputation, financial loss, loss of confidentiality or any other significant economic or social disadvantage.

Risk has to be assessed on a case by case basis, taking into account the circumstance of the incident and the nature of the personal data that has been compromised. For example, if sensitive data elements, such as bank account details, that could put someone at risk of financial crime are lost, there is high risk. Even less sensitive data elements, such as email addresses, may result in high risk, if the loss of the data element puts the individual at risk of phishing. On the other hand, the loss of a staff directory containing the types of data elements found on employee business cards, would not normally result in high risk. Similarly, if the personal data is strongly encrypted, and the encryption keys are not compromised, it is unlikely that the incident will result in high risk of harm.

As a matter of policy, we assume that a high risk of harm exists if unencrypted sensitive data is stolen. We also assume that a high risk of harm exists if sensitive Personal Data (such as national identification numbers, tax identification numbers or financial account information) or Special Categories of Personal Data have been transmitted to an unknown or untrusted recipient.

If there is a high real risk of harm, the following steps must be taken immediately: *Time is of the essence.*

1. Acme must notify the competent Supervisory Authority immediately. [This notice is made by the Chief Privacy Officer, the General Counsel or the Regional Data Protection Officer.] If applicable and appropriate, notification may also need to be made to (i) law enforcement, (ii) other regulatory agencies, (iii) PCI fraud teams, and (iv) the company insurance carrier.

2. Acme must notify the affected individual as quickly as possible.

    - The notification letter should alert individuals about the possible harm as well as steps that the individuals should take to minimize the risks.

    - The notification letters must fully comply with all GDPR requirements as well as any other applicable legal requirements, depending on the residency location of the data subject:

[9] This process describes the steps required to manage Personal Data Breaches where Acme is the data controller. If Acme is a data processor, it must notify the data controller as soon as possible. Acme will cooperate with the data controller to assess and manage the incident response process.

a) describe the nature of the personal data breach including where possible, the categories and approximate number of data subjects concerned and the categories and approximate number of personal data records concerned;
b) communicate the name and contact details of the data protection officer or other contact point where more information can be obtained;
c) describe the likely consequences of the personal data breach;
d) describe the measures taken or proposed to be taken by the controller to address the personal data breach, including, where appropriate, measures to mitigate its possible adverse effects.

- *If it not possible to send letters in a timely manner, Acme must consider other ways to making individuals aware of the high risk of harm. For example, Acme may post a notice regarding the incident on its website homepage and send information about the incident to individuals via email.*

3. Acme should notify other authorities as maybe appropriate given the situation. For example, if data subjects are located in multiple countries, Acme should notify relevant data protection authorities in these countries so they can provide appropriate support to individuals as may be needed.

If there does not appear to be a high risk to the rights and freedoms of an individual, move to step 2.

STEP 2: Determine the level of possible risk to the impacted individuals.

If a risk of harm exists, notification to the Supervisory Authorities is required within 72 hours (if feasible). Individual notifications will be made if requested by the Authorities.

Use the Incident Response Scorecard attached below to evaluate the risk of harm based on established factors that determine the likelihood of risk if Personal Data have been compromised. If the score generated by Incident Response Scorecard is 4 or less, there is a low risk of harm to the individuals. (Move to Step 3.)

To complete this analysis, Acme must consider (1) the specific data elements that were exposed, (2) the countries of residence of the impacted individuals, and, if applicable, (3) the specific country laws or national guidance. The company's Chief Privacy Officer or DPO will complete this analysis.

If security, confidentiality or integrity of the Personal Data has been compromised (*i.e., the score is 5 or more)*, there is risk of harm. In this case, the following steps must be taken:

1. Acme must notify the competent Supervisory Authority within 72 hours if feasible.[10] [This notice is made by the Chief Privacy Officer, the General Counsel or the Regional Data Protection Officer.] If applicable and appropriate, notification may also need to be made to (i) law enforcement, (ii) other regulatory agencies, (iii) PCI fraud teams, and (iv) the company insurance carrier.

[10] If notification to the Authority is delayed, Acme must explain the reasons for the delay in its notification.

2. Upon instructions from the Supervisory Authority, Acme may be required to notify the impacted individuals. If notification is required, the contents of the letter shall reflect the GDPR requirements noted above as well as any additional information recommended by the Supervisory Authority.

If the Incident has not compromised the security, confidentiality or integrity of Personal Data, move to step 3.

STEP 3: Document that there is no risk of harm to individuals that requires notification of Supervisory Authorities or Individuals.

Maintain documentation regarding the investigation in accordance with Acme's document retention policy.

1. When individual notifications are not required either to alert individuals to a real risk of harm or to comply with a legal notification requirement, Acme will not notify individuals of the incident.

    - Acme is committed to ensuring that individuals' interests are protected in connection with security incidents. Our policy is to notify regulators and individuals (and provide appropriate remediation) any time individuals are at any real risk of harm as a result of our mistakes – regardless of whether there is any legal obligation to notify them.

    - Acme is also committed to complying with applicable legal requirements, which sometimes require breach notification even when there is no risk of harm. We will always provide breach notification as required by law. We will cooperate with Supervisory Authorities, should they determine that notification is needed even if the risk of harm is moderate or low.

    - Article 34 of the GDPR explicitly states that a notification does not need to be made when the risk to individual rights and freedoms is not "high". This Article reflects the public policy view that individuals should not be needlessly alarmed about events that have not and will not put them at risk of harm.

    - When there is not a risk to individual rights and freedoms, there is no reason to send notification letters. Sending the letters will likely cause individuals to speculate that they are at risk of harm, as there is no other reason for the letter. It may also numb them to important notification letters, which puts them at greater risk of harm in the future.

    - Should any person have any concerns about the security of his/her information, Acme will address those concerns.

2. Acme retains records of all privacy incident investigations for a minimum of five (5) years. Send copies of your documentation (including the completed Incident Response Scorecard and any notification letter templates) [to where] for retention.

Incident Response Scorecard – Discussion Draft

Acme evaluates all incidents to determine if there is a risk that Personal Data have been compromised or that individuals have otherwise been made vulnerable to risk of harm. We consider four factors that must be considered to determine the risk of harm.[11] These factors are:

1. The nature and extent of the Personal Data involved, including the types of identifiers and the likelihood of re-identification;
2. The unauthorized person who used the Personal Data or to whom the disclosure was made;
3. Whether the Personal Data was actually acquired or viewed; and
4. The extent to which the risk to the Personal Data has been mitigated.

Personal Data (PD) is defined as:

> Any information relating to an identified or identifiable natural person ('data subject'); an identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person.
>
> Any information (alone or when used in combination with other information within Acme's direct control) can be used to identify, locate or contact an individual, together with all information related to such Individual.
>
> Personal Data includes all Sensitive Personal Data (including Special Categories of Data) and other obvious information, such as person's name or email address, as well as less obvious information such as any Internet Protocol (IP) address or biometric data, if such data could possibly be associated with an Individual.
>
> Personal Data can be in any media or format, including computerized or electronic records as well as paper-based files.

Sensitive Personal Data (SPD) has been impacted. SPD are a subset of PD, which due to their nature have been classified by law or policy as deserving additional privacy and security protections. Sensitive Personal Data consist of:

- All government-issued identification numbers (including social insurance or similar numbers, driver's license numbers, passport numbers and national identification numbers),
- Individual financial account numbers (bank account numbers, credit card numbers, other information if that information would permit access to an Individual's financial account),
- Account login credentials (such as usernames and/or passwords),
- Individual medical records, genetic information and biometric information.

[11] These factors are articulated in United State Federal law, in the breach notification rule promulgated by the Department of Health & Human Services. See 45 CFR §164.402.

- Consumer reporting data, including employment background screening reports, and

- Data regarding EU-residents that are classified as "Special Categories of Data" under European laws and consisting of (a) race or ethnic origin, (b) political opinions, (c) religion, (d) trade union membership, (e) sex life or sexual orientation, (f) physical or mental health, and (g) criminal charges or records related to criminal offenses and allegations of crimes.

The scorecard below enables us to assess the risk of harm to individual from a Personal Data Breach. If you have any questions about this Scorecard, please contact [NAME]. This document should be attached to the [incident report file].

1. The nature and extent of the Personal Data involved, including the types of identifiers and the likelihood of re-identification:

0. Low Risk	1. Possible Risk	2. High Risk
PD but no SPD and/or low risk of association	PD associated with an individual (but no SPD)	Unencrypted SPI
For example: individual name associated with public information (postal address, company name or title) or demographic data Any PD or SPD if encrypted using an industry standard encryption provided that the encryption keys are not compromised	Individual name associated with any other types of Personal Data, such as email address or telephone number, purchase history, employment details or salary information	Government-issued identifiers Individual financial account numbers User Account credentials (email address and passwords, security questions/answers)

THIS EVENT: Circle Risk Rating Points: 0 1 2

EXPLAIN:_____

2. The unauthorized person who used the PD or to whom the disclosure was made:

0. Low Risk	1. Possible Risk	2. High Risk
Trusted Recipient	Trustworthy Recipient	Untrusted Recipient
Acme Affiliate Current Acme Vendor Current Acme Client Current Acme Business Partner Government Agency	Third party with whom Acme does not have a contractual relationship, but who provides credible assurances that the data will not be misused (*e.g.*, a former vendor or client) A regulated entity, such as a financial institution, insurance company or healthcare provider	Unknown recipient (*e.g.,* public disclosure or loss of data) Recipients with known or suspected malicious intent (*e.g,* theft of data)

THIS EVENT: Circle Risk Rating Points: 0 1 2

EXPLAIN:_____

3. Whether the PD was actually viewed or acquired:

0. Low Risk	1. Possible Risk	2. High Risk
Not viewed or acquired	Viewed (or partially viewed) but not acquired	Acquired
Acme determines that file has been sent to the wrong recipient and retrieves the data prior to its being accessed Recipient reports receiving an incorrect file without viewing contents and deletes (returns or destroys) the file without reading/copying/printing Lost device/media is recovered and forensic analysis demonstrates that data was not accessed	Recipient opens package or file but realizes that it has been incorrectly directed and deletes (returns or destroys) the file without using or further disclosing the information	Acme cannot recover the data from the recipient

THIS EVENT: Circle Risk Rating Points: 0 1 2

EXPLAIN:_____

4. The extent to which the risk to the PD has been mitigated:

0. Low Risk	1. Possible Risk	2. High Risk
Acme has good-faith reason to believe that that PD have not and will not be used, disclosed or retained.	Acme has good-faith reason to believe that that PD have not and will not be used or disclosed.	No mitigation
PD have been fully recovered. Trusted or trust-worthy recipient has provided credible written assurances that the data has not been used or disclosed and that no instance of the data has been retained. PD was encrypted and the encryption keys were not compromised.	PD have been recovered from active recipient systems. Trusted or trust-worthy recipient has provided credible written assurances that the data has not been used or disclosed (but retention in back-ups may occur). The trusted or trust-worthy recipient has established program to protect similar information internally.	Acme does not have any assurances regarding use, disclosure or retention of the PD

THIS EVENT: Circle Risk Rating Points: 0 1 2

EXPLAIN: .

5. Any other factors or information which can assist in determining the risk of harm:

EXPLAIN:

C. Calculate Risk Assessment Score

Add the total risk assessment score points from factors 1-4 above.

Total score 7 or 8: The Personal Data Breach puts individuals at high risk of harm. The Supervisory Authority and the impacted individuals must be notified as soon as possible.

Total score 5 or 6: The Personal Data Breach creates a risk of harm. The Chief Privacy Officer [or DPO] should notify the appropriate supervisory authority to determine if notification of data subjects is warranted. If the incident includes data elements that trigger breach notification laws in the United States, notification will likely be required in some states as well.

Total score 4 or less: There is no or a very low risk of harm. Although you may have one or 2 high risk factors (such as sensitive PD on a stolen device), the probability of compromise must be low (such as if the data is encrypted). Risk may also be low if the data were viewed by a trusted third party with appropriate mitigation of the event.

Total Score: _____

Reference Materials – GDPR Recitals 85-88

(85) A personal data breach may, if not addressed in an appropriate and timely manner, result in physical, material or non-material damage to natural persons such as loss of control over their personal data or limitation of their rights, discrimination, identity theft or fraud, financial loss, unauthorised reversal of pseudonymisation, damage to reputation, loss of confidentiality of personal data protected by professional secrecy or any other significant economic or social disadvantage to the natural person concerned. Therefore, as soon as the controller becomes aware that a personal data breach has occurred, the controller should notify the personal data breach to the supervisory authority without undue delay and, where feasible, not later than 72 hours after having become aware of it, unless the controller is able to demonstrate, in accordance with the accountability principle, that the personal data breach is unlikely to result in a risk to the rights and freedoms of natural persons. Where such notification cannot be achieved within 72 hours, the reasons for the delay should accompany the notification and information may be provided in phases without undue further delay.

(86) The controller should communicate to the data subject a personal data breach, without undue delay, where that personal data breach is likely to result in a high risk to the rights and freedoms of the natural person in order to allow him or her to take the necessary precautions. The communication should describe the nature of the personal data breach as well as recommendations for the natural person concerned to mitigate potential adverse effects. Such communications to data subjects should be made as soon as reasonably feasible and in close cooperation with the supervisory authority, respecting guidance provided by it or by other relevant authorities such as law-enforcement authorities. For example, the need to mitigate an immediate risk of damage would call for prompt communication with data subjects whereas the need to implement appropriate measures against continuing or similar personal data breaches may justify more time for communication.

(87) It should be ascertained whether all appropriate technological protection and organisational measures have been implemented to establish immediately whether a personal data breach has taken place and to inform promptly the supervisory authority and the data subject. The fact that the notification was made without undue delay should be established taking into account in particular the nature and gravity of the personal data breach and its consequences and adverse effects for the data subject. Such notification may result in an intervention of the supervisory authority in accordance with its tasks and powers laid down in this Regulation.

(88) In setting detailed rules concerning the format and procedures applicable to the notification of personal data breaches, due consideration should be given to the circumstances of that breach, including whether or not personal data had been protected by appropriate technical protection measures, effectively limiting the likelihood of identity fraud or other forms of misuse. Moreover, such rules and procedures should take into account the legitimate interests of law-enforcement authorities where early disclosure could unnecessarily hamper the investigation of the circumstances of a personal data breach.