ARTICLE 29 DATA PROTECTION WORKING PARTY

18/EN

WP250rev.01

Guidelines on Personal data breach notification under Regulation 2016/679

Adopted on 3 October 2017

As last Revised and Adopted on 6 February 2018

THE WORKING PARTY ON THE PROTECTION OF INDIVIDUALS WITH REGARD TO THE PROCESSING OF PERSONAL DATA

set up by Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995,

having regard to Articles 29 and 30 thereof,

having regard to its Rules of Procedure,

HAS ADOPTED THE PRESENT GUIDELINES:

TABLE OF CONTENTS

INTRODUCTION

The General Data Protection Regulation (the GDPR) introduces the requirement for a personal data breach (henceforth "breach") to be notified to the competent national supervisory authority[1] (or in the case of a cross-border breach, to the lead authority) and, in certain cases, to communicate the breach to the individuals whose personal data have been affected by the breach.

Obligations to notify in cases of breaches presently exist for certain organisations, such as providers of publicly-available electronic communications services (as specified in Directive 2009/136/EC and Regulation (EU) No 611/2013)[2]. There are also some EU Member States that already have their own national breach notification obligation. This may include the obligation to notify breaches involving categories of controllers in addition to providers of publicly available electronic communication services (for example in Germany and Italy), or an obligation to report all breaches involving personal data (such as in the Netherlands). Other Member States may have relevant Codes of Practice (for example, in Ireland[3]). Whilst a number of EU data protection authorities currently encourage controllers to report breaches, the Data Protection Directive 95/46/EC[4], which the GDPR replaces, does not contain a specific breach notification obligation and therefore such a requirement will be new for many organisations. The GDPR now makes notification mandatory for all controllers unless a breach is unlikely to result in a risk to the rights and freedoms of individuals[5]. Processors also have an important role to play and they must notify any breach to their controller[6].

The Article 29 Working Party (WP29) considers that the new notification requirement has a number of benefits. When notifying the supervisory authority, controllers can obtain advice on whether the affected individuals need to be informed. Indeed, the supervisory authority may order the controller to inform those individuals about the breach[7]. Communicating a breach to individuals allows the controller to provide information on the risks presented as a result of the breach and the steps those individuals can take to protect themselves from its potential consequences. The focus of any breach response plan should be on protecting individuals and their personal data. Consequently, breach notification should be seen as a tool enhancing compliance in relation to the protection of personal data. At the same time, it should be noted that failure to report a breach to either an individual or a supervisory authority may mean that under Article 83 a possible sanction is applicable to the controller.

---

[1] See Article 4(21) of the GDPR

[2] See http://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex:32009L0136 and http://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A32013R0611

[3] See https://www.dataprotection.ie/docs/Data_Security_Breach_Code_of_Practice/1082.htm

[4] See http://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex:31995L0046

[5] The rights enshrined in the Charter of Fundamental Rights of the EU, available at http://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:12012P/TXT

[6] See Article 33(2). This is similar in concept to Article 5 of Regulation (EU) No 611/2013 which states that a provider that is contracted to deliver part of an electronic communications service (without having a direct contractual relationship with subscribers) is obliged to notify the contracting provider in the event of a personal data breach.

[7] See Articles 34(4) and 58(2)(e)

Controllers and processors are therefore encouraged to plan in advance and put in place processes to be able to detect and promptly contain a breach, to assess the risk to individuals[8], and then to determine whether it is necessary to notify the competent supervisory authority, and to communicate the breach to the individuals concerned when necessary. Notification to the supervisory authority should form a part of that incident response plan.

The GDPR contains provisions on when a breach needs to be notified, and to whom, as well as what information should be provided as part of the notification. Information required for the notification can be provided in phases, but in any event controllers should act on any breach in a timely manner.

In its Opinion 03/2014 on personal data breach notification[9], WP29 provided guidance to controllers in order to help them to decide whether to notify data subjects in case of a breach. The opinion considered the obligation of providers of electronic communications regarding Directive 2002/58/EC and provided examples from multiple sectors, in the context of the then draft GDPR, and presented good practices for all controllers.

The current Guidelines explain the mandatory breach notification and communication requirements of the GDPR and some of the steps controllers and processors can take to meet these new obligations. They also give examples of various types of breaches and who would need to be notified in different scenarios.

I. Personal data breach notification under the GDPR

A. Basic security considerations

One of the requirements of the GDPR is that, by using appropriate technical and organisational measures, personal data shall be processed in a manner to ensure the appropriate security of the personal data, including protection against unauthorised or unlawful processing and against accidental loss, destruction or damage[10].

Accordingly, the GDPR requires both controllers and processors to have in place appropriate technical and organisational measures to ensure a level of security appropriate to the risk posed to the personal data being processed. They should take into account the state of the art, the costs of implementation and the nature, the scope, context and purposes of processing, as well as the risk of varying likelihood and severity for the rights and freedoms of natural persons[11]. Also, the GDPR requires all appropriate technological protection an organisational measures to be in place to establish immediately whether a breach has taken place, which then determines whether the notification obligation is engaged[12].

Consequently, a key element of any data security policy is being able, where possible, to prevent a breach and, where it nevertheless occurs, to react to it in a timely manner.

---

[8] This can be ensured under the monitoring and review requirement of a DPIA, which is required for processing operations likely to result in a high risk to the rights and freedoms of natural persons (Article 35(1) and (11).

[9] See Opinion 03/2014 on Personal Data Breach Notification http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2014/wp213_en.pdf

[10] See Articles 5(1)(f) and 32.

[11] Article 32; see also Recital 83

[12] See Recital 87

B. What is a personal data breach?

1. Definition

As part of any attempt to address a breach the controller should first be able to recognise one. The GDPR defines a "personal data breach" in Article 4(12) 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."

What is meant by "destruction" of personal data should be quite clear: this is where the data no longer exists, or no longer exists in a form that is of any use to the controller. "Damage" should also be relatively clear: this is where personal data has been altered, corrupted, or is no longer complete. In terms of "loss" of personal data, this should be interpreted as the data may still exist, but the controller has lost control or access to it, or no longer has it in its possession. Finally, unauthorised or unlawful processing may include disclosure of personal data to (or access by) recipients who are not authorised to receive (or access) the data, or any other form of processing which violates the GDPR.

Example

An example of loss of personal data can include where a device containing a copy of a controller's customer database has been lost or stolen. A further example of loss may be where the only copy of a set of personal data has been encrypted by ransomware, or has been encrypted by the controller using a key that is no longer in its possession.

What should be clear is that a breach is a type of security incident. However, as indicated by Article 4(12), the GDPR only applies where there is a breach of *personal data*. The consequence of such a breach is that the controller will be unable to ensure compliance with the principles relating to the processing of personal data as outlined in Article 5 of the GDPR. This highlights the difference between a security incident and a personal data breach – in essence, whilst all personal data breaches are security incidents, not all security incidents are necessarily personal data breaches[13].

The potential adverse effects of a breach on individuals are considered below.

2. Types of personal data breaches

In its Opinion 03/2014 on breach notification, WP29 explained that breaches can be categorised according to the following three well-known information security principles[14]:

- "Confidentiality breach" - where there is an unauthorised or accidental disclosure of, or access to, personal data.
- "Integrity breach" - where there is an unauthorised or accidental alteration of personal data.
- "Availability breach" - where there is an accidental or unauthorised loss of access[15] to, or destruction of, personal data.

[13] It should be noted that a security incident is not limited to threat models where an attack is made on an organisation from an external source, but includes incidents from internal processing that breach security principles.

[14] See Opinion 03/2014

[15] It is well established that "access" is fundamentally part of "availability". See, for example, NIST SP800-53rev4, which defines "availability" as: "Ensuring timely and reliable access to and use of information,"

It should also be noted that, depending on the circumstances, a breach can concern confidentiality, integrity and availability of personal data at the same time, as well as any combination of these.

Whereas determining if there has been a breach of confidentiality or integrity is relatively clear, whether there has been an availability breach may be less obvious. A breach will always be regarded as an availability breach when there has been a permanent loss of, or destruction of, personal data.

Example

Examples of a loss of availability include where data has been deleted either accidentally or by an unauthorised person, or, in the example of securely encrypted data, the decryption key has been lost. In the event that the controller cannot restore access to the data, for example, from a backup, then this is regarded as a permanent loss of availability.

A loss of availability may also occur where there has been significant disruption to the normal service of an organisation, for example, experiencing a power failure or denial of service attack, rendering personal data unavailable.

The question may be asked whether a temporary loss of availability of personal data should be considered as a breach and, if so, one which needs to be notified. Article 32 of the GDPR, "security of processing," explains that when implementing technical and organisational measures to ensure a level of security appropriate to the risk, consideration should be given, amongst other things, to "the ability to ensure the ongoing confidentiality, integrity, availability and resilience of processing systems and services," and "the ability to restore the availability and access to personal data in a timely manner in the event of a physical or technical incident".

Therefore, a security incident resulting in personal data being made unavailable for a period of time is also a type of breach, as the lack of access to the data can have a significant impact on the rights and freedoms of natural persons. To be clear, where personal data is unavailable due to planned system maintenance being carried out this is not a 'breach of security' as defined in Article 4(12).

As with a permanent loss or destruction of personal data (or indeed any other type of breach), a breach involving the temporary loss of availability should be documented in accordance with Article 33(5). This assists the controller in demonstrating accountability to the supervisory authority, which may ask to see those records[16].However, depending on the circumstances of the breach, it may or may not require notification to the supervisory authority and communication to affected individuals. The controller will need to assess the likelihood and severity of the impact on the rights and freedoms of natural persons as a result of the lack of availability of personal data. In accordance with Article 33, the controller will need to notify unless the breach is unlikely to result in a risk to individuals' rights and freedoms. Of course, this will need to be assessed on a case-by-case basis.

Examples

available at http://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-53r4.pdf. CNSSI-4009 also refers to: " Timely, reliable access to data and information services for authorized users." See https://rmf.org/wp-content/uploads/2017/10/CNSSI-4009.pdf. ISO/IEC 27000:2016 also defines "availability" as "Property of being accessible and usable upon demand by an authorized entity": https://www.iso.org/obp/ui/#iso:std:iso-iec:27000:ed-4:v1:en

[16] See Article 33(5)

In the context of a hospital, if critical medical data about patients are unavailable, even temporarily, this could present a risk to individuals' rights and freedoms; for example, operations may be cancelled and lives put at risk.

Conversely, in the case of a media company's systems being unavailable for several hours (e.g. due to a power outage), if that company is then prevented from sending newsletters to its subscribers, this is unlikely to present a risk to individuals' rights and freedoms.

It should be noted that although a loss of availability of a controller's systems might be only temporary and may not have an impact on individuals, it is important for the controller to consider all possible consequences of a breach, as it may still require notification for other reasons.

Example

Infection by ransomware (malicious software which encrypts the controller's data until a ransom is paid) could lead to a temporary loss of availability if the data can be restored from backup. However, a network intrusion still occurred, and notification could be required if the incident is qualified as confidentiality breach (i.e. personal data is accessed by the attacker) and this presents a risk to the rights and freedoms of individuals.

3. The possible consequences of a personal data breach

A breach can potentially have a range of significant adverse effects on individuals, which can result in physical, material, or non-material damage. The GDPR explains that this can include loss of control over their personal data, limitation of their rights, discrimination, identity theft or fraud, financial loss, unauthorised reversal of pseudonymisation, 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[17].

Accordingly, the GDPR requires the controller to notify a breach to the competent supervisory authority, unless it is unlikely to result in a risk of such adverse effects taking place. Where there is a likely high risk of these adverse effects occurring, the GDPR requires the controller to communicate the breach to the affected individuals as soon as is reasonably feasible[18].

The importance of being able to identify a breach, to assess the risk to individuals, and then notify if required, is emphasised in Recital 87 of the GDPR:

"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."

Further guidelines on assessing the risk of adverse effects to individuals are considered in section IV.

If controllers fail to notify either the supervisory authority or data subjects of a data breach or both even though the requirements of Articles 33 and/or 34 are fulfilled, then the supervisory authority is

[17] See also Recitals 85 and 75

[18] See also Recital 86.

presented with a choice that must include consideration of all of the corrective measures at its disposal, which would include consideration of the imposition of the appropriate administrative fine[19], either accompanying a corrective measure under Article 58(2) or on its own. Where an administrative fine is chosen, its value can be up to 10,000,000 EUR or up to 2 % if the total worldwide annual turnover of an undertaking under Article 83(4)(a) of the GDPR. It is also important to bear in mind that in some cases, the failure to notify a breach could reveal either an absence of existing security measures or an inadequacy of the existing security measures. The WP29 guidelines on administrative fines state: "The occurrence of several different infringements committed together in any particular single case means that the supervisory authority is able to apply the administrative fines at a level which is effective, proportionate and dissuasive within the limit of the gravest infringement". In that case, the supervisory authority will also have the possibility to issue sanctions for failure to notify or communicate the breach (Articles 33 and 34) on the one hand, and absence of (adequate) security measures (Article 32) on the other hand, as they are two separate infringements.

II. Article 33 - Notification to the supervisory authority

A. When to notify

1. Article 33 requirements

Article 33(1) provides that:

> "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."

Recital 87 states[20]:

> "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."

2. When does a controller become "aware"?

As detailed above, the GDPR requires that, in the case of a breach, the controller shall notify the breach without undue delay and, where feasible, not later than 72 hours after having become aware of it. This may raise the question of when a controller can be considered to have become "aware" of a breach. WP29 considers that a controller should be regarded as having become "aware" when that

[19] For further details, please see WP29 Guidelines on the application and setting of administrative fines, available here: http://ec.europa.eu/newsroom/just/document.cfm?doc_id=47889

[20] Recital 85 is also important here.

controller has a reasonable degree of certainty that a security incident has occurred that has led to personal data being compromised.

However, as indicated earlier, the GDPR requires the controller to implement all appropriate technical protection and organisational measures to establish immediately whether a breach has taken place and to inform promptly the supervisory authority and the data subjects. It also states that the fact that the notification was made without undue delay should be established taking into account in particular the nature and gravity of the breach and its consequences and adverse effects for the data subject[21]. This puts an obligation on the controller to ensure that they will be "aware" of any breaches in a timely manner so that they can take appropriate action.

When, exactly, a controller can be considered to be "aware" of a particular breach will depend on the circumstances of the specific breach. In some cases, it will be relatively clear from the outset that there has been a breach, whereas in others, it may take some time to establish if personal data have been compromised. However, the emphasis should be on prompt action to investigate an incident to determine whether personal data have indeed been breached, and if so, to take remedial action and notify if required.

Examples

1. In the case of a loss of a USB key with unencrypted personal data it is often not possible to ascertain whether unauthorised persons gained access to that data. Nevertheless, even though the controller may not be able to establish if a confidentiality breach has taken place, such a case has to be notified as there is a reasonable degree of certainty that an availability breach has occurred; the controller would become "aware" when it realised the USB key had been lost.

2. A third party informs a controller that they have accidentally received the personal data of one of its customers and provides evidence of the unauthorised disclosure. As the controller has been presented with clear evidence of a confidentiality breach then there can be no doubt that it has become "aware".

3. A controller detects that there has been a possible intrusion into its network. The controller checks its systems to establish whether personal data held on that system has been compromised and confirms this is the case. Once again, as the controller now has clear evidence of a breach there can be no doubt that it has become "aware".

4. A cybercriminal contacts the controller after having hacked its system in order to ask for a ransom. In that case, after checking its system to confirm it has been attacked the controller has clear evidence that a breach has occurred and there is no doubt that it has become aware.

After first being informed of a potential breach by an individual, a media organisation, or another source, or when it has itself detected a security incident, the controller may undertake a short period of investigation in order to establish whether or not a breach has in fact occurred. During this period of investigation the controller may not be regarded as being "aware". However, it is expected that the initial investigation should begin as soon as possible and establish with a reasonable degree of certainty whether a breach has taken place; a more detailed investigation can then follow.

Once the controller has become aware, a notifiable breach must be notified without undue delay, and where feasible, not later than 72 hours. During this period, the controller should assess the likely risk to individuals in order to determine whether the requirement for notification has been triggered, as well as the action(s) needed to address the breach. However, a controller may already have an initial assessment of the potential risk that could result from a breach as part of a data protection impact

[21] See Recital 87

assessment (DPIA)[22] made prior to carrying out the processing operation concerned. However, the DPIA may be more generalised in comparison to the specific circumstances of any actual breach, and so in any event an additional assessment taking into account those circumstances will need to be made. For more detail on assessing risk, see section IV.

In most cases these preliminary actions should be completed soon after the initial alert (i.e. when the controller or processor suspects there has been a security incident which may involve personal data.) – it should take longer than this only in exceptional cases.

Example

An individual informs the controller that they have received an email impersonating the controller which contains personal data relating to his (actual) use of the controller's service, suggesting that the security of the controller has been compromised. The controller conducts a short period of investigation and identifies an intrusion into their network and evidence of unauthorised access to personal data. The controller would now be considered as "aware" and notification to the supervisory authority is required unless this is unlikely to present a risk to the rights and freedoms of individuals. The controller will need to take appropriate remedial action to address the breach.

The controller should therefore have internal processes in place to be able to detect and address a breach. For example, for finding some irregularities in data processing the controller or processor may use certain technical measures such as data flow and log analysers, from which is possible to define events and alerts by correlating any log data[23]. It is important that when a breach is detected it is reported upwards to the appropriate level of management so it can be addressed and, if required, notified in accordance with Article 33 and, if necessary, Article 34. Such measures and reporting mechanisms could be detailed in the controller's incident response plans and/or governance arrangements. These will help the controller to plan effectively and determine who has operational responsibility within the organisation for managing a breach and how or whether to escalate an incident as appropriate.

The controller should also have in place arrangements with any processors the controller uses, which themselves have an obligation to notify the controller in the event of a breach (see below).

Whilst it is the responsibility of controllers and processors to put in place suitable measures to be able to prevent, react and address a breach, there are some practical steps that should be taken in all cases.

- Information concerning all security-related events should be directed towards a responsible person or persons with the task of addressing incidents, establishing the existence of a breach and assessing risk.
- Risk to individuals as a result of a breach should then be assessed (likelihood of no risk, risk or high risk), with relevant sections of the organisation being informed.
- Notification to the supervisory authority, and potentially communication of the breach to the affected individuals should be made, if required.
- At the same time, the controller should act to contain and recover the breach.
- Documentation of the breach should take place as it develops.

Accordingly, it should be clear that there is an obligation on the controller to act on any initial alert and establish whether or not a breach has, in fact, occurred. This brief period allows for some

[22] See WP29 Guidelines on DPIAs here: http://ec.europa.eu/newsroom/document.cfm?doc_id=44137

[23] It should be noted that log data facilitating auditability of, e.g., storage, modifications or erasure of data may also qualify as personal data relating to the person who initiated the respective processing operation.

investigation, and for the controller to gather evidence and other relevant details. However, once the controller has established with a reasonable degree of certainty that a breach has occurred, if the conditions in Article 33(1) have been met, it must then notify the supervisory authority without undue delay and, where feasible, not later than 72 hours[24]. If a controller fails to act in a timely manner and it becomes apparent that a breach did occur, this could be considered as a failure to notify in accordance with Article 33.

Article 32 makes clear that the controller and processor should have appropriate technical and organisational measures in place to ensure an appropriate level of security of personal data: the ability to detect, address, and report a breach in a timely manner should be seen as essential elements of these measures.

3. Joint controllers

Article 26 concerns joint controllers and specifies that joint controllers shall determine their respective responsibilities for compliance with the GDPR[25]. This will include determining which party will have responsibility for complying with the obligations under Articles 33 and 34. WP29 recommends that the contractual arrangements between joint controllers include provisions that determine which controller will take the lead on, or be responsible for, compliance with the GDPR's breach notification obligations.

4. Processor obligations

The controller retains overall responsibility for the protection of personal data, but the processor has an important role to play to enable the controller to comply with its obligations; and this includes breach notification. Indeed, Article 28(3) specifies that the processing by a processor shall be governed by a contract or other legal act. Article 28(3)(f) states that the contract or other legal act shall stipulate that the processor "assists the controller in ensuring compliance with the obligations pursuant to Articles 32 to 36 taking into account the nature of processing and the information available to the processor".

Article 33(2) makes it clear that if a processor is used by a controller and the processor becomes aware of a breach of the personal data it is processing on behalf of the controller, it must notify the controller "without undue delay". It should be noted that the processor does not need to first assess the likelihood of risk arising from a breach before notifying the controller; it is the controller that must make this assessment on becoming aware of the breach. The processor just needs to establish whether a breach has occurred and then notify the controller. The controller uses the processor to achieve its purposes; therefore, in principle, the controller should be considered as "aware" once the processor has informed it of the breach. The obligation on the processor to notify its controller allows the controller to address the breach and to determine whether or not it is required to notify the supervisory authority in accordance with Article 33(1) and the affected individuals in accordance with Article 34(1). The controller might also want to investigate the breach, as the processor might not be in a position to know all the relevant facts relating to the matter, for example, if a copy or backup of personal data destroyed or lost by the processor is still held by the controller. This may affect whether the controller would then need to notify.

The GDPR does not provide an explicit time limit within which the processor must alert the controller, except that it must do so "without undue delay". Therefore, WP29 recommends the

[24] See Regulation No 1182/71 determining the rules applicable to periods, dates and time limits, available at: http://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=CELEX:31971R1182&from=EN

[25] See also Recital 79.

processor promptly notifies the controller, with further information about the breach provided in phases as more details become available. This is important in order to help the controller to meet the requirement of notification to the supervisory authority within 72 hours.

As is explained above, the contract between the controller and processor should specify how the requirements expressed in Article 33(2) should be met in addition to other provisions in the GDPR. This can include requirements for early notification by the processor that in turn support the controller's obligations to report to the supervisory authority within 72 hours.

Where the processor provides services to multiple controllers that are all affected by the same incident, the processor will have to report details of the incident to each controller.

A processor could make a notification on behalf of the controller, if the controller has given the processor the proper authorisation and this is part of the contractual arrangements between controller and processor. Such notification must be made in accordance with Article 33 and 34. However, it is important to note that the legal responsibility to notify remains with the controller.

B. Providing information to the supervisory authority

1. Information to be provided

When a controller notifies a breach to the supervisory authority, Article 33(3) states that, at the minimum, it should:

> "(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."

The GDPR does not define categories of data subjects or personal data records. However, WP29 suggests categories of data subjects to refer to the various types of individuals whose personal data has been affected by a breach: depending on the descriptors used, this could include, amongst others, children and other vulnerable groups, people with disabilities, employees or customers. Similarly, categories of personal data records can refer to the different types of records that the controller may process, such as health data, educational records, social care information, financial details, bank account numbers, passport numbers and so on.

Recital 85 makes it clear that one of the purposes of notification is limiting damage to individuals. Accordingly, if the types of data subjects or the types of personal data indicate a risk of particular damage occurring as a result of a breach (e.g. identity theft, fraud, financial loss, threat to professional secrecy), then it is important the notification indicates these categories. In this way, it is linked to the requirement of describing the likely consequences of the breach.

Where precise information is not available (e.g. exact number of data subjects affected) this should not be a barrier to timely breach notification. The GDPR allows for approximations to be made in the number of individuals affected and the number of personal data records concerned. The focus should be directed towards addressing the adverse effects of the breach rather than providing precise figures.

Thus, when it has become clear that here has been a breach, but the extent of it is not yet known, a notification in phases (see below) is a safe way to meet the notification obligations.

Article 33(3) states that the controller "shall at least" provide this information with a notification, so a controller can, if necessary, choose to provide further details. Different types of breaches (confidentiality, integrity or availability) might require further information to be provided to fully explain the circumstances of each case.

Example

As part of its notification to the supervisory authority, a controller may find it useful to name its processor if it is at the root cause of a breach, particularly if this has led to an incident affecting the personal data records of many other controllers that use the same processor.

In any event, the supervisory authority may request further details as part of its investigation into a breach.

2. Notification in phases

Depending on the nature of a breach, further investigation by the controller may be necessary to establish all of the relevant facts relating to the incident. Article 33(4) therefore states:

"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."

This means that the GDPR recognises that controllers will not always have all of the necessary information concerning a breach within 72 hours of becoming aware of it, as full and comprehensive details of the incident may not always be available during this initial period. As such, it allows for a notification in phases. It is more likely this will be the case for more complex breaches, such as some types of cyber security incidents where, for example, an in-depth forensic investigation may be necessary to fully establish the nature of the breach and the extent to which personal data have been compromised. Consequently, in many cases the controller will have to do more investigation and follow-up with additional information at a later point. This is permissible, providing the controller gives reasons for the delay, in accordance with Article 33(1). WP29 recommends that when the controller first notifies the supervisory authority, the controller should also inform the supervisory authority if the controller does not yet have all the required information and will provide more details later on. The supervisory authority should agree how and when additional information should be provided. This does not prevent the controller from providing further information at any other stage, if it becomes aware of additional relevant details about the breach that need to be provided to the supervisory authority.

The focus of the notification requirement is to encourage controllers to act promptly on a breach, contain it and, if possible, recover the compromised personal data, and to seek relevant advice from the supervisory authority. Notifying the supervisory authority within the first 72 hours can allow the controller to make sure that decisions about notifying or not notifying individuals are correct.

However, the purpose of notifying the supervisory authority is not solely to obtain guidance on whether to notify the affected individuals. It will be obvious in some cases that, due to the nature of the breach and the severity of the risk, the controller will need to notify the affected individuals without delay. For example, if there is an immediate threat of identity theft, or if special categories of personal data[26] are disclosed online, the controller should act without undue delay to contain the

[26] See Article 9.

breach and to communicate it to the individuals concerned (see section III). In exceptional circumstances, this might even take place before notifying the supervisory authority. More generally, notification of the supervisory authority may not serve as a justification for failure to communicate the breach to the data subject where it is required.

It should also be clear that after making an initial notification, a controller could update the supervisory authority if a follow-up investigation uncovers evidence that the security incident was contained and no breach actually occurred. This information could then be added to the information already given to the supervisory authority and the incident recorded accordingly as not being a breach. There is no penalty for reporting an incident that ultimately transpires not to be a breach.

Example

A controller notifies the supervisory authority within 72 hours of detecting a breach that it has lost a USB key containing a copy of the personal data of some of its customers. The USB key is later found misfiled within the controller's premises and recovered. The controller updates the supervisory authority and requests the notification be amended.

It should be noted that a phased approach to notification is already the case under the existing obligations of Directive 2002/58/EC, Regulation 611/2013 and other self-reported incidents.

3. Delayed notifications

Article 33(1) makes it clear that where notification to the supervisory authority is not made within 72 hours, it shall be accompanied by reasons for the delay. This, along with the concept of notification in phases, recognises that a controller may not always be able to notify a breach within that time period, and that a delayed notification may be permissible.

Such a scenario might take place where, for example, a controller experiences multiple, similar confidentiality breaches over a short period of time, affecting large numbers of data subjects in the same way. A controller could become aware of a breach and, whilst beginning its investigation, and before notification, detect further similar breaches, which have different causes. Depending on the circumstances, it may take the controller some time to establish the extent of the breaches and, rather than notify each breach individually, the controller instead organises a meaningful notification that represents several very similar breaches, with possible different causes. This could lead to notification to the supervisory authority being delayed by more than 72 hours after the controller first becomes aware of these breaches.

Strictly speaking, each individual breach is a reportable incident. However, to avoid being overly burdensome, the controller may be able to submit a "bundled" notification representing all these breaches, provided that they concern the same type of personal data breached in the same way, over a relatively short space of time. If a series of breaches take place that concern different types of personal data, breached in different ways, then notification should proceed in the normal way, with each breach being reported in accordance with Article 33.

Whilst the GDPR allows for delayed notifications to an extent, this should not be seen as something that regularly takes place. It is worth pointing out that bundled notifications can also be made for multiple similar breaches reported within 72 hours.

C. Cross-border breaches and breaches at non-EU establishments

1. Cross-border breaches

Where there is cross-border processing[27] of personal data, a breach may affect data subjects in more than one Member State. Article 33(1) makes it clear that when a breach has occurred, the controller should notify the supervisory authority competent in accordance with Article 55 of the GDPR[28]. Article 55(1) says that:

> "Each supervisory authority shall be competent for the performance of the tasks assigned to and the exercise of the powers conferred on it in accordance with this Regulation on the territory of its own Member State."

However, Article 56(1) states:

> "Without prejudice to Article 55, the supervisory authority of the main establishment or of the single establishment of the controller or processor shall be competent to act as lead supervisory authority for the cross-border processing carried out by that controller or processor in accordance with the procedure provided in Article 60."

Furthermore, Article 56(6) states:

> "The lead supervisory authority shall be the sole interlocutor of the controller or processor for the cross-border processing carried out by that controller or processor."

This means that whenever a breach takes place in the context of cross-border processing and notification is required, the controller will need to notify the lead supervisory authority[29]. Therefore, when drafting its breach response plan, a controller must make an assessment as to which supervisory authority is the lead supervisory authority that it will need to notify[30]. This will allow the controller to respond promptly to a breach and to meet its obligations in respect of Article 33. It should be clear that in the event of a breach involving cross-border processing, notification must be made to the lead supervisory authority, which is not necessarily where the affected data subjects are located, or indeed where the breach has taken place. When notifying the lead authority, the controller should indicate, where appropriate, whether the breach involves establishments located in other Member States, and in which Member States data subjects are likely to have been affected by the breach. If the controller has any doubt as to the identity of the lead supervisory authority then it should, at a minimum, notify the local supervisory authority where the breach has taken place.

2. Breaches at non-EU establishments

Article 3 concerns the territorial scope of the GDPR, including when it applies to the processing of personal data by a controller or processor that is not established in the EU. In particular, Article 3(2) states[31]:

---

[27] See Article 4(23)

[28] See also Recital 122.

[29] See WP29 Guidelines for identifying a controller or processor's lead supervisory authority, available at http://ec.europa.eu/newsroom/document.cfm?doc_id=44102

[30] A list of contact details for all European national data protection authorities can be found at: http://ec.europa.eu/justice/data-protection/bodies/authorities/index_en.htm

[31] See also Recitals 23 and 24

"This Regulation applies to the processing of personal data of data subjects who are in the Union by a controller or processor not established in the Union, where the processing activities are related to:

(a) the offering of goods or services, irrespective of whether a payment of the data subject is required, to such data subjects in the Union; or

(b) the monitoring of their behaviour as far as their behaviour takes place within the Union."

Article 3(3) is also relevant and states[32]:

"This Regulation applies to the processing of personal data by a controller not established in the Union, but in a place where Member State law applies by virtue of public international law."

Where a controller not established in the EU is subject to Article 3(2) or Article 3(3) and experiences a breach, it is therefore still bound by the notification obligations under Articles 33 and 34. Article 27 requires a controller (and processor) to designate a representative in the EU where Article 3(2) applies. In such cases, WP29 recommends that notification should be made to the supervisory authority in the Member State where the controller's representative in the EU is established[33]. Similarly, where a processor is subject to Article 3(2), it will be bound by the obligations on processors, of particular relevance here, the duty to notify a breach to the controller under Article 33(2).

D. Conditions where notification is not required

Article 33(1) makes it clear that breaches that are "unlikely to result in a risk to the rights and freedoms of natural persons" do not require notification to the supervisory authority. An example might be where personal data are already publically available and a disclosure of such data does not constitute a likely risk to the individual. This is in contrast to existing breach notification requirements for providers of publically available electronic communications services in Directive 2009/136/EC that state all relevant breaches have to be notified to the competent authority.

In its Opinion 03/2014 on breach notification[34], WP29 explained that a confidentiality breach of personal data that were encrypted with a state of the art algorithm is still a personal data breach, and has to be notified. However, if the confidentiality of the key is intact – i.e., the key was not compromised in any security breach, and was generated so that it cannot be ascertained by available technical means by any person who is not authorised to access it – then the data are in principle unintelligible. Thus, the breach is unlikely to adversely affect individuals and therefore would not require communication to those individuals[35]. However, even where data is encrypted, a loss or alteration can have negative consequences for data subjects where the controller has no adequate backups. In that instance communication to data subjects would be required, even if the data itself was subject to adequate encryption measures.

---

[32] See also Recital 25

[33] See Recital 80 and Article 27

[34] WP29, Opinion 03/2014 on breach notification, http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2014/wp213_en.pdf

[35] See also Article 4(1) and (2) of Regulation 611/2013.

WP29 also explained this would similarly be the case if personal data, such as passwords, were securely hashed and salted, the hashed value was calculated with a state of the art cryptographic keyed hash function, the key used to hash the data was not compromised in any breach, and the key used to hash the data has been generated in a way that it cannot be ascertained by available technological means by any person who is not authorised to access it.

Consequently, if personal data have been made essentially unintelligible to unauthorised parties and where the data are a copy or a backup exists, a confidentiality breach involving properly encrypted personal data may not need to be notified to the supervisory authority. This is because such a breach is unlikely to pose a risk to individuals' rights and freedoms. This of course means that the individual would not need to be informed either as there is likely no high risk. However, it should be borne in mind that while notification may initially not be required if there is no likely risk to the rights and freedoms of individuals, this may change over time and the risk would have to be re-evaluated. For example, if the key is subsequently found to be compromised, or a vulnerability in the encryption software is exposed, then notification may still be required.

Furthermore, it should be noted that if there is a breach where there are no backups of the encrypted personal data then there will have been an availability breach, which could pose risks to individuals and therefore may require notification. Similarly, where a breach occurs involving the loss of encrypted data, even if a backup of the personal data exists this may still be a reportable breach, depending on the length of time taken to restore the data from that backup and the effect that lack of availability has on individuals. As Article 32(1)(c) states, an important factor of security is the "the ability to restore the availability and access to personal data in a timely manner in the event of a physical or technical incident".

Example

A breach that would not require notification to the supervisory authority would be the loss of a securely encrypted mobile device, utilised by the controller and its staff. Provided the encryption key remains within the secure possession of the controller and this is not the sole copy of the personal data then the personal data would be inaccessible to an attacker. This means the breach is unlikely to result in a risk to the rights and freedoms of the data subjects in question. If it later becomes evident that the encryption key was compromised or that the encryption software or algorithm is vulnerable, then the risk to the rights and freedoms of natural persons will change and thus notification may now be required.

However, a failure to comply with Article 33 will exist where a controller does not notify the supervisory authority in a situation where the data has not actually been securely encrypted. Therefore, when selecting encryption software controllers should carefully weigh the quality and the proper implementation of the encryption offered, understand what level of protection it actually provides and whether this is appropriate to the risks presented. Controllers should also be familiar with the specifics of how their encryption product functions. For instance, a device may be encrypted once it is switched off, but not while it is in stand-by mode. Some products using encryption have "default keys" that need to be changed by each customer to be effective. The encryption may also be considered currently adequate by security experts, but may become outdated in a few years' time, meaning it is questionable whether the data would be sufficiently encrypted by that product and provide an appropriate level of protection.

III. Article 34 – Communication to the data subject

A. Informing individuals

In certain cases, as well as notifying the supervisory authority, the controller is also required to communicate a breach to the affected individuals.

Article 34(1) states:

> "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."

Controllers should recall that notification to the supervisory authority is mandatory unless there is unlikely to be a risk to the rights and freedoms of individuals as a result of a breach. In addition, where there is likely a high risk to the rights and freedoms of individuals as the result of a breach, individuals must also be informed. The threshold for communicating a breach to individuals is therefore higher than for notifying supervisory authorities and not all breaches will therefore be required to be communicated to individuals, thus protecting them from unnecessary notification fatigue.

The GDPR states that communication of a breach to individuals should be made "without undue delay," which means as soon as possible. The main objective of notification to individuals is to provide specific information about steps they should take to protect themselves[36]. As noted above, depending on the nature of the breach and the risk posed, timely communication will help individuals to take steps to protect themselves from any negative consequences of the breach.

Annex B of these Guidelines provides a non-exhaustive list of examples of when a breach may be likely to result in high risk to individuals and consequently instances when a controller will have to notify a breach to those affected.

B. Information to be provided

When notifying individuals, Article 34(2) specifies that:

> "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)."

According to this provision, the controller should at least provide the following information:

- a description of the nature of the breach;
- the name and contact details of the data protection officer or other contact point;
- a description of the likely consequences of the breach; and
- a description of the measures taken or proposed to be taken by the controller to address the breach, including, where appropriate, measures to mitigate its possible adverse effects.

As an example of the measures taken to address the breach and to mitigate its possible adverse effects, the controller could state that, after having notified the breach to the relevant supervisory authority, the controller has received advice on managing the breach and lessening its impact. The controller should also, where appropriate, provide specific advice to individuals to protect themselves from possible adverse consequences of the breach, such as resetting passwords in the case where their access credentials have been compromised. Again, a controller can choose to provide information in addition to what is required here.

[36] See also Recital 86.

C. Contacting individuals

In principle, the relevant breach should be communicated to the affected data subjects directly, unless doing so would involve a 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 (Article 34(3)c).

Dedicated messages should be used when communicating a breach to data subjects and they should not be sent with other information, such as regular updates, newsletters, or standard messages. This helps to make the communication of the breach to be clear and transparent.

Examples of transparent communication methods include direct messaging (e.g. email, SMS, direct message), prominent website banners or notification, postal communications and prominent advertisements in print media. A notification solely confined within a press release or corporate blog would not be an effective means of communicating a breach to an individual. WP29 recommends that controllers should choose a means that maximizes the chance of properly communicating information to all affected individuals. Depending on the circumstances, this may mean the controller employs several methods of communication, as opposed to using a single contact channel.

Controllers may also need to ensure that the communication is accessible in appropriate alternative formats and relevant languages to ensure individuals are able to understand the information being provided to them. For example, when communicating a breach to an individual, the language used during the previous normal course of business with the recipient will generally be appropriate. However, if the breach affects data subjects who the controller has not previously interacted with, or particularly those who reside in a different Member State or other non-EU country from where the controller is established, communication in the local national language could be acceptable, taking into account the resource required. The key is to help data subjects understand the nature of the breach and steps they can take to protect themselves.

Controllers are best placed to determine the most appropriate contact channel to communicate a breach to individuals, particularly if they interact with their customers on a frequent basis. However, clearly a controller should be wary of using a contact channel compromised by the breach as this channel could also be used by attackers impersonating the controller.

At the same time, Recital 86 explains that:

> "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."

Controllers might therefore wish to contact and consult the supervisory authority not only to seek advice about informing data subjects about a breach in accordance with Article 34, but also on the appropriate messages to be sent to, and the most appropriate way to contact, individuals.

Linked to this is the advice given in Recital 88 that notification of a breach 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". This may mean that in certain circumstances, where justified, and on the advice of law-enforcement authorities, the controller may delay communicating the breach to the affected individuals until such time as it would not prejudice such investigations. However, data subjects would still need to be promptly informed after this time.

Whenever it is not possible for the controller to communicate a breach to an individual because there is insufficient data stored to contact the individual, in that particular circumstance the controller should inform the individual as soon as it is reasonably feasible to do so (e.g. when an individual exercises their Article 15 right to access personal data and provides the controller with necessary additional information to contact them).

D. Conditions where communication is not required

Article 34(3) states three conditions that, if met, do not require notification to individuals in the event of a breach. These are:

- The controller has applied appropriate technical and organisational measures to protect personal data prior to the breach, in particular those measures that render personal data unintelligible to any person who is not authorised to access it. This could, for example, include protecting personal data with state-of-the-art encryption, or by tokenization.
- Immediately following a breach, the controller has taken steps to ensure that the high risk posed to individuals' rights and freedoms is no longer likely to materialise. For example, depending on the circumstances of the case, the controller may have immediately identified and taken action against the individual who has accessed personal data before they were able to do anything with it. Due regard still needs to be given to the possible consequences of any breach of confidentiality, again, depending on the nature of the data concerned.
- It would involve disproportionate effort[37] to contact individuals, perhaps where their contact details have been lost as a result of the breach or are not known in the first place. For example, the warehouse of a statistical office has flooded and the documents containing personal data were stored only in paper form. Instead, the controller must make a public communication or take a similar measure, whereby the individuals are informed in an equally effective manner. In the case of disproportionate effort, technical arrangements could also be envisaged to make information about the breach available on demand, which could prove useful to those individuals who may be affected by a breach, but the controller cannot otherwise contact.

In accordance with the accountability principle controllers should be able to demonstrate to the supervisory authority that they meet one or more of these conditions [38]. It should be borne in mind that while notification may initially not be required if there is no risk to the rights and freedoms of natural persons, this may change over time and the risk would have to be re-evaluated.

If a controller decides not to communicate a breach to the individual, Article 34(4) explains that the supervisory authority can require it to do so, if it considers the breach is likely to result in a high risk to individuals. Alternatively, it may consider that the conditions in Article 34(3) have been met in which case notification to individuals is not required. If the supervisory authority determines that the decision not to notify data subjects is not well founded, it may consider employing its available powers and sanctions.

IV. Assessing risk and high risk

A. Risk as a trigger for notification

[37] See WP29 Guidelines on transparency, which will consider the issue of disproportionate effort, available at http://ec.europa.eu/newsroom/just/document.cfm?doc_id=48850

[38] See Article 5(2)

Although the GDPR introduces the obligation to notify a breach, it is not a requirement to do so in all circumstances:

- Notification to the competent supervisory authority is required unless a breach is unlikely to result in a risk to the rights and freedoms of individuals.
- Communication of a breach to the individual is only triggered where it is likely to result in a high risk to their rights and freedoms.

This means that immediately upon becoming aware of a breach, it is vitally important that the controller should not only seek to contain the incident but it should also assess the risk that could result from it. There are two important reasons for this: firstly, knowing the likelihood and the potential severity of the impact on the individual will help the controller to take effective steps to contain and address the breach; secondly, it will help it to determine whether notification is required to the supervisory authority and, if necessary, to the individuals concerned.

As explained above, notification of a breach is required unless it is unlikely to result in a risk to the rights and freedoms of individuals, and the key trigger requiring communication of a breach to data subjects is where it is likely to result in a *high* risk to the rights and freedoms of individuals. This risk exists when the breach may lead to physical, material or non-material damage for the individuals whose data have been breached. Examples of such damage are discrimination, identity theft or fraud, financial loss and damage to reputation. When the breach involves personal data that reveals racial or ethnic origin, political opinion, religion or philosophical beliefs, or trade union membership, or includes genetic data, data concerning health or data concerning sex life, or criminal convictions and offences or related security measures, such damage should be considered likely to occur[39].

B. Factors to consider when assessing risk

Recitals 75 and 76 of the GDPR suggest that generally when assessing risk, consideration should be given to both the likelihood and severity of the risk to the rights and freedoms of data subjects. It further states that risk should be evaluated on the basis of an objective assessment.

It should be noted that assessing the risk to people's rights and freedoms as a result of a breach has a different focus to the risk considered in a DPIA)[40]. The DPIA considers both the risks of the data processing being carried out as planned, and the risks in case of a breach. When considering a potential breach, it looks in general terms at the likelihood of this occurring, and the damage to the data subject that might ensue; in other words, it is an assessment of a hypothetical event. With an actual breach, the event has already occurred, and so the focus is wholly about the resulting risk of the impact of the breach on individuals.

Example

A DPIA suggests that the proposed use of a particular security software product to protect personal data is a suitable measure to ensure a level of security appropriate to the risk the processing would otherwise present to individuals. However, if a vulnerability becomes subsequently known, this would change the software's suitability to contain the risk to the personal data protected and so it would need to be re-assessed as part of an ongoing DPIA.

[39] See Recital 75 and Recital 85.

[40] See WP Guidelines on DPIAs here: http://ec.europa.eu/newsroom/document.cfm?doc_id=44137

A vulnerability in the product is later exploited and a breach occurs. The controller should assess the specific circumstances of the breach, the data affected, and the potential level of impact on individuals, as well as how likely this risk will materialise.

Accordingly, when assessing the risk to individuals as a result of a breach, the controller should consider the specific circumstances of the breach, including the severity of the potential impact and the likelihood of this occurring. WP29 therefore recommends the assessment should take into account the following criteria[41]:

- The type of breach

The type of breach that has occurred may affect the level of risk presented to individuals. For example, a confidentiality breach whereby medical information has been disclosed to unauthorised parties may have a different set of consequences for an individual to a breach where an individual's medical details have been lost, and are no longer available.

- The nature, sensitivity, and volume of personal data

Of course, when assessing risk, a key factor is the type and sensitivity of personal data that has been compromised by the breach. Usually, the more sensitive the data, the higher the risk of harm will be to the people affected, but consideration should also be given to other personal data that may already be available about the data subject. For example, the disclosure of the name and address of an individual in ordinary circumstances is unlikely to cause substantial damage. However, if the name and address of an adoptive parent is disclosed to a birth parent, the consequences could be very severe for both the adoptive parent and child.

Breaches involving health data, identity documents, or financial data such as credit card details, can all cause harm on their own, but if used together they could be used for identity theft. A combination of personal data is typically more sensitive than a single piece of personal data.

Some types of personal data may seem at first relatively innocuous, however, what that data may reveal about the affected individual should be carefully considered. A list of customers accepting regular deliveries may not be particularly sensitive, but the same data about customers who have requested that their deliveries be stopped while on holiday would be useful information to criminals.

Similarly, a small amount of highly sensitive personal data can have a high impact on an individual, and a large range of details can reveal a greater range of information about that individual. Also, a breach affecting large volumes of personal data about many data subjects can have an effect on a corresponding large number of individuals.

- Ease of identification of individuals

An important factor to consider is how easy it will be for a party who has access to compromised personal data to identify specific individuals, or match the data with other information to identify individuals. Depending on the circumstances, identification could be possible directly from the personal data breached with no special research needed to discover the individual's identity, or it may be extremely difficult to match personal data to a particular individual, but it could still be possible

[41] Article 3.2 of Regulation 611/2013 provides guidance the factors that should be taken into consideration in relation to the notification of breaches in the electronic communication services sector, which may be useful in the context of notification under the GDPR. See http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:L:2013:173:0002:0008:en:PDF

under certain conditions. Identification may be directly or indirectly possible from the breached data, but it may also depend on the specific context of the breach, and public availability of related personal details. This may be more relevant for confidentiality and availability breaches.

As stated above, personal data protected by an appropriate level of encryption will be unintelligible to unauthorised persons without the decryption key. Additionally, appropriately-implemented pseudonymisation (defined in Article 4(5) as "the processing of personal data in such a manner that the personal data can no longer be attributed to a specific data subject without the use of additional information, provided that such additional information is kept separately and is subject to technical and organisational measures to ensure that the personal data are not attributed to an identified or identifiable natural person") can also reduce the likelihood of individuals being identified in the event of a breach. However, pseudonymisation techniques alone cannot be regarded as making the data unintelligible.

- Severity of consequences for individuals.

Depending on the nature of the personal data involved in a breach, for example, special categories of data, the potential damage to individuals that could result can be especially severe, in particular where the breach could result in identity theft or fraud, physical harm, psychological distress, humiliation or damage to reputation. If the breach concerns personal data about vulnerable individuals, they could be placed at greater risk of harm.

Whether the controller is aware that personal data is in the hands of people whose intentions are unknown or possibly malicious can have a bearing on the level of potential risk. There may be a confidentiality breach, whereby personal data is disclosed to a third party, as defined in Article 4(10), or other recipient in error. This may occur, for example, where personal data is sent accidentally to the wrong department of an organisation, or to a commonly used supplier organisation. The controller may request the recipient to either return or securely destroy the data it has received. In both cases, given that the controller has an ongoing relationship with them, and it may be aware of their procedures, history and other relevant details, the recipient may be considered "trusted". In other words, the controller may have a level of assurance with the recipient so that it can reasonably expect that party not to read or access the data sent in error, and to comply with its instructions to return it. Even if the data has been accessed, the controller could still possibly trust the recipient not to take any further action with it and to return the data to the controller promptly and to co-operate with its recovery. In such cases, this may be factored into the risk assessment the controller carries out following the breach – the fact that the recipient is trusted may eradicate the severity of the consequences of the breach but does not mean that a breach has not occurred. However, this in turn may remove the likelihood of risk to individuals, thus no longer requiring notification to the supervisory authority, or to the affected individuals. Again, this will depend on case-by-case basis. Nevertheless, the controller still has to keep information concerning the breach as part of the general duty to maintain records of breaches (see section V, below).

Consideration should also be given to the permanence of the consequences for individuals, where the impact may be viewed as greater if the effects are long-term.

- Special characteristics of the individual

A breach may affect personal data concerning children or other vulnerable individuals, who may be placed at greater risk of danger as a result. There may be other factors about the individual that may affect the level of impact of the breach on them.

- Special characteristics of the data controller

The nature and role of the controller and its activities may affect the level of risk to individuals as a result of a breach. For example, a medical organisation will process special categories of personal

data, meaning that there is a greater threat to individuals if their personal data is breached, compared with a mailing list of a newspaper.

- The number of affected individuals

A breach may affect only one or a few individuals or several thousand, if not many more. Generally, the higher the number of individuals affected, the greater the impact of a breach can have. However, a breach can have a severe impact on even one individual, depending on the nature of the personal data and the context in which it has been compromised. Again, the key is to consider the likelihood and severity of the impact on those affected.

- General points

Therefore, when assessing the risk that is likely to result from a breach, the controller should consider a combination of the severity of the potential impact on the rights and freedoms of individuals and the likelihood of these occurring. Clearly, 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, the controller should err on the side of caution and notify. Annex B provides some useful examples of different types of breaches involving risk or high risk to individuals.

The European Union Agency for Network and Information Security (ENISA) has produced recommendations for a methodology of assessing the severity of a breach, which controllers and processors may find useful when designing their breach management response plan[42].

V. Accountability and record keeping

A. Documenting breaches

Regardless of whether or not a breach needs to be notified to the supervisory authority, the controller must keep documentation of all breaches, as Article 33(5) explains:

> "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."

This is linked to the accountability principle of the GDPR, contained in Article 5(2). The purpose of recording non-notifiable breaches, as well notifiable breaches, also relates to the controller's obligations under Article 24, and the supervisory authority can request to see these records. Controllers are therefore encouraged to establish an internal register of breaches, regardless of whether they are required to notify or not[43].

Whilst it is up to the controller to determine what method and structure to use when documenting a breach, in terms of recordable information there are key elements that should be included in all cases. As is required by Article 33(5), the controller needs to record details concerning the breach, which

[42] ENISA, Recommendations for a methodology of the assessment of severity of personal data breaches, https://www.enisa.europa.eu/publications/dbn-severity

[43] The controller may choose to document breaches as part of if its record of processing activities which is maintained pursuant to article 30. A separate register is not required, provided the information relevant to the breach is clearly identifiable as such and can be extracted upon request.

should include its causes, what took place and the personal data affected. It should also include the effects and consequences of the breach, along with the remedial action taken by the controller.

The GDPR does not specify a retention period for such documentation. Where such records contain personal data, it will be incumbent on the controller to determine the appropriate period of retention in accordance with the principles in relation to the processing of personal data[44] and to meet a lawful basis for processing[45]. It will need to retain documentation in accordance with Article 33(5) insofar as it may be called to provide evidence of compliance with that Article, or with the accountability principle more generally, to the supervisory authority. Clearly, if the records themselves contain no personal data then the storage limitation principle[46] of the GDPR does not apply.

In addition to these details, WP29 recommends that the controller also document its reasoning for the decisions taken in response to a breach. In particular, if a breach is not notified, a justification for that decision should be documented. This should include reasons why the controller considers the breach is unlikely to result in a risk to the rights and freedoms of individuals[47]. Alternatively, if the controller considers that any of the conditions in Article 34(3) are met, then it should be able to provide appropriate evidence that this is the case.

Where the controller does notify a breach to the supervisory authority, but the notification is delayed, the controller must be able to provide reasons for that delay; documentation relating to this could help to demonstrate that the delay in reporting is justified and not excessive.

Where the controller communicates a breach to the affected individuals, it should be transparent about the breach and communicate in an effective and timely manner. Accordingly, it would help the controller to demonstrate accountability and compliance by retaining evidence of such communication.

To aid compliance with Articles 33 and 34, it would be advantageous to both controllers and processors to have a documented notification procedure in place, setting out the process to follow once a breach has been detected, including how to contain, manage and recover the incident, as well as assessing risk, and notifying the breach. In this regard, to show compliance with GDPR it might also be useful to demonstrate that employees have been informed about the existence of such procedures and mechanisms and that they know how to react to breaches.

It should be noted that failure to properly document a breach can lead to the supervisory authority exercising its powers under Article 58 and, or imposing an administrative fine in accordance with Article 83.

B. Role of the Data Protection Officer

A controller or processor may have a Data Protection Officer (DPO)[48], either as required by Article 37, or voluntarily as a matter of good practice. Article 39 of the GDPR sets a number of mandatory tasks for the DPO, but does not prevent further tasks being allocated by the controller, if appropriate.

---

[44] See Article 5

[45] See Article 6 and also Article 9.

[46] See Article 5(1)(e).

[47] See Recital 85

[48] See WP Guidelines on DPOs here: http://ec.europa.eu/newsroom/just/item-detail.cfm?item_id=50083

Of particular relevance to breach notification, the mandatory tasks of the DPO includes, amongst other duties, providing data protection advice and information to the controller or processor, monitoring compliance with the GDPR, and providing advice in relation to DPIAs. The DPO must also cooperate with the supervisory authority and act as a contact point for the supervisory authority and for data subjects. It should also be noted that, when notifying the breach to the supervisory authority, Article 33(3)(b) requires the controller to provide the name and contact details of its DPO, or other contact point.

In terms of documenting breaches, the controller or processor may wish to obtain the opinion of its DPO as to the structure, the setting up and the administration of this documentation. The DPO could also be additionally tasked with maintaining such records.

These factors mean that the DPO should play an key role in assisting the prevention of or preparation for a breach by providing advice and monitoring compliance, as well as during a breach (i.e. when notifying the supervisory authority), and during any subsequent investigation by the supervisory authority. In this light, WP29 recommends that the DPO is promptly informed about the existence of a breach and is involved throughout the breach management and notification process.

VI. Notification obligations under other legal instruments

In addition to, and separate from, the notification and communication of breaches under the GDPR, controllers should also be aware of any requirement to notify security incidents under other associated legislation that may apply to them and whether this may also require them to notify the supervisory authority of a personal data breach at the same time. Such requirements can vary between Member States, but examples of notification requirements in other legal instruments, and how these inter-relate with the GDPR, include the following:

- Regulation (EU) 910/2014 on electronic identification and trust services for electronic transactions in the internal market (eIDAS Regulation)[49].

Article 19(2) of the eIDAS Regulation requires trust service providers to notify their supervisory body of a breach of security or loss of integrity that has a significant impact on the trust service provided or on the personal data maintained therein. Where applicable—i.e., where such a breach or loss is also a personal data breach under the GDPR—the trust service provider should also notify the supervisory authority.

- Directive (EU) 2016/1148 concerning measures for a high common level of security of network and information systems across the Union (NIS Directive)[50].

Articles 14 and 16 of the NIS Directive require operators of essential services and digital service providers to notify security incidents to their competent authority. As recognised by Recital 63 of NIS[51], security incidents can often include a compromise of personal data. Whilst NIS requires competent authorities and supervisory authorities to co-operate and exchange information that context, it remains the case that where such incidents are, or become, personal data breaches under the

[49] See http://eur-lex.europa.eu/legal-content/EN/TXT/?uri=uriserv%3AOJ.L_.2014.257.01.0073.01.ENG

[50] See http://eur-lex.europa.eu/legal-content/EN/TXT/?uri=uriserv:OJ.L_.2016.194.01.0001.01.ENG

51 Recital 63: *"Personal data are in many cases compromised as a result of incidents. In this context, competent authorities and data protection authorities should cooperate and exchange information on all relevant matters to tackle any personal data breaches resulting from incidents."*

GDPR, those operators and/or providers would be required to notify the supervisory authority separately from the incident notification requirements of NIS.

Example

A cloud service provider notifying a breach under the NIS Directive may also need to notify a controller, if this includes a personal data breach. Similarly, a trust service provider notifying under eIDAS may also be required to notify the relevant data protection authority in the event of a breach.

- Directive 2009/136/EC (the Citizens' Rights Directive) and Regulation 611/2013 (the Breach Notification Regulation).

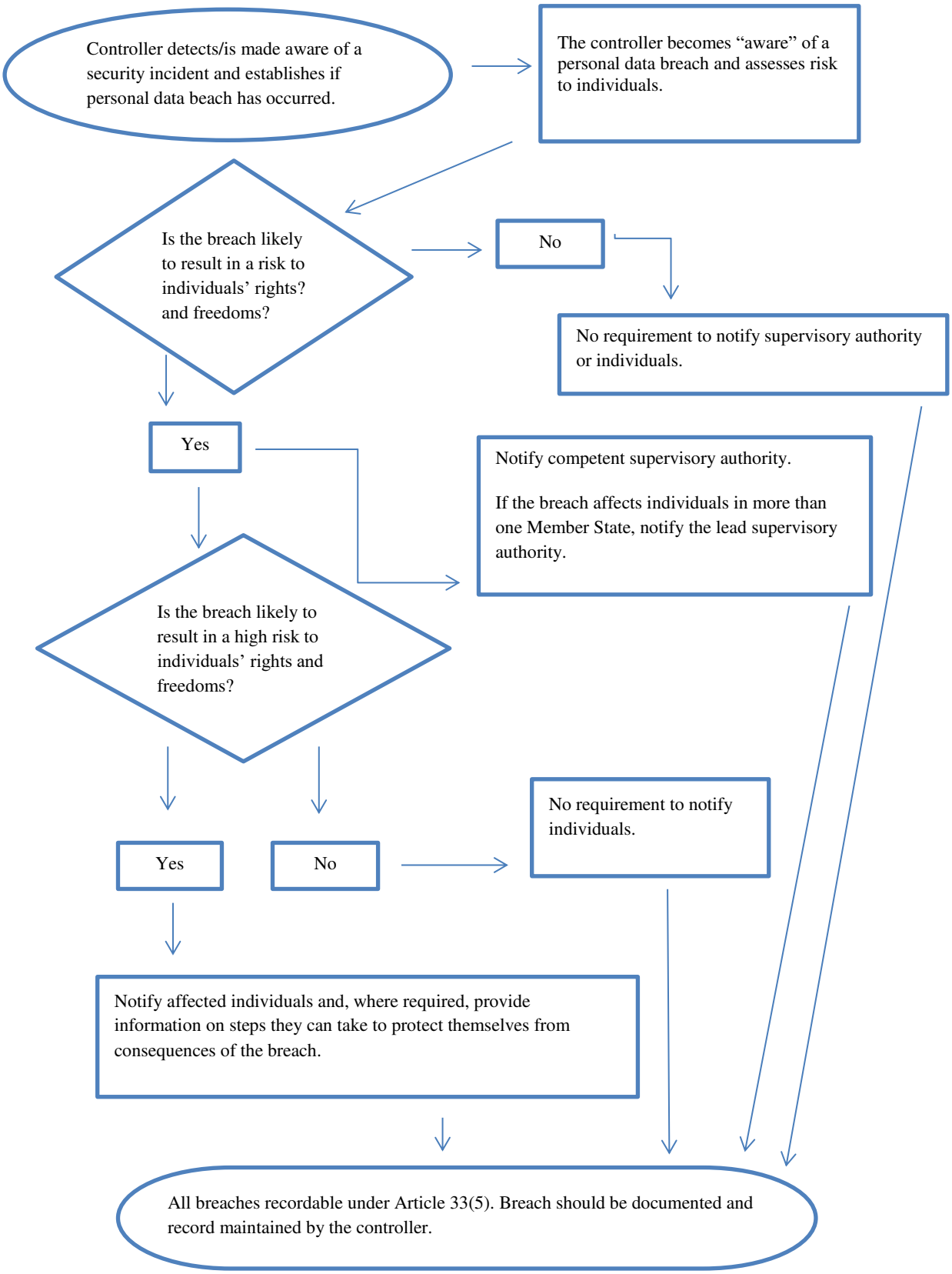
Providers of publicly available electronic communication services within the context of Directive 2002/58/EC[52] must notify breaches to the competent national authorities.

Controllers should also be aware of any additional legal, medical, or professional notification duties under other applicable regimes.

[52] On 10 January 2017, the European Commission proposed a Regulation on Privacy and Electronic Communications which will replace Directive 2009/136/EC and remove notification requirements. However, until this proposal is approved by the European Parliament the existing notification requirement remains in force, see https://ec.europa.eu/digital-single-market/en/news/proposal-regulation-privacy-and-electronic-communications

VII. Annex

A. Flowchart showing notification requirements



B. Examples of personal data breaches and who to notify

The following non-exhaustive examples will assist controllers in determining whether they need to notify in different personal data breach scenarios. These examples may also help to distinguish between risk and high risk to the rights and freedoms of individuals.

Example	**Notify the supervisory authority?**	**Notify the data subject?**	**Notes/recommendations**
i. A controller stored a backup of an archive of personal data encrypted on a USB key. The key is stolen during a break-in.	No.	No.	As long as the data are encrypted with a state of the art algorithm, backups of the data exist the unique key is not compromised, and the data can be restored in good time, this may not be a reportable breach. However if it is later compromised, notification is required.
ii. A controller maintains an online service. As a result of a cyber attack on that service, personal data of individuals are exfiltrated. The controller has customers in a single Member State.	Yes, report to the supervisory authority if there are likely consequences to individuals.	Yes, report to individuals depending on the nature of the personal data affected and if the severity of the likely consequences to individuals is high.	
iii. A brief power outage lasting several minutes at a controller's call centre meaning customers are unable to call the controller and access their records.	No.	No.	This is not a notifiable breach, but still a recordable incident under Article 33(5). Appropriate records should be maintained by the controller.
iv. A controller suffers a ransomware attack which results in all data being encrypted. No back-ups are available and the data cannot be restored. On investigation, it becomes clear that the ransomware's only	Yes, report to the supervisory authority, if there are likely consequences to individuals as this is a loss of availability.	Yes, report to individuals, depending on the nature of the personal data affected and the possible effect of the lack of availability of the data, as well as other likely	If there was a backup available and data could be restored in good time, this would not need to be reported to the supervisory authority or to individuals as there would have been no permanent loss of availability or

functionality was to encrypt the data, and that there was no other malware present in the system.		consequences.	confidentiality. However, if the supervisory authority became aware of the incident by other means, it may consider an investigation to assess compliance with the broader security requirements of Article 32.
v. An individual phones a bank's call centre to report a data breach. The individual has received a monthly statement for someone else. The controller undertakes a short investigation (i.e. completed within 24 hours) and establishes with a reasonable confidence that a personal data breach has occurred and whether it has a systemic flaw that may mean other individuals are or might be affected.	Yes.	Only the individuals affected are notified if there is high risk and it is clear that others were not affected.	If, after further investigation, it is identified that more individuals are affected, an update to the supervisory authority must be made and the controller takes the additional step of notifying other individuals if there is high risk to them.
vi. A controller operates an online marketplace and has customers in multiple Member States. The marketplace suffers a cyber-attack and usernames, passwords and purchase history are published online by the attacker.	Yes, report to lead supervisory authority if involves cross-border processing.	Yes, as could lead to high risk.	The controller should take action, e.g. by forcing password resets of the affected accounts, as well as other steps to mitigate the risk. The controller should also consider any other notification obligations, e.g. under the NIS Directive as a digital service provider.
vii. A website hosting company acting as a data processor identifies an error in the code which	As the processor, the website hosting company must notify its affected clients (the controllers) without	If there is likely no high risk to the individuals they do not need to be	The website hosting company (processor) must consider any other notification obligations (e.g. under the NIS

controls user authorisation. The effect of the flaw means that any user can access the account details of any other user.	undue delay. Assuming that the website hosting company has conducted its own investigation the affected controllers should be reasonably confident as to whether each has suffered a breach and therefore is likely to be considered as having "become aware" once they have been notified by the hosting company (the processor). The controller then must notify the supervisory authority.	notified.	Directive as a digital service provider). If there is no evidence of this vulnerability being exploited with any of its controllers a notifiable breach may not have occurred but it is likely to be recordable or be a matter of non-compliance under Article 32.
viii. Medical records in a hospital are unavailable for the period of 30 hours due to a cyber-attack.	Yes, the hospital is obliged to notify as high-risk to patient's well-being and privacy may occur.	Yes, report to the affected individuals.	
ix. Personal data of a large number of students are mistakenly sent to the wrong mailing list with 1000+ recipients.	Yes, report to supervisory authority.	Yes, report to individuals depending on the scope and type of personal data involved and the severity of possible consequences.	
x. A direct marketing e-mail is sent to recipients in the "to:" or "cc:" fields, thereby enabling each recipient to see the email address of other recipients.	Yes, notifying the supervisory authority may be obligatory if a large number of individuals are affected, if sensitive data are revealed (e.g. a mailing list of a psychotherapist) or if other factors present high risks (e.g. the mail contains the initial passwords).	Yes, report to individuals depending on the scope and type of personal data involved and the severity of possible consequences.	Notification may not be necessary if no sensitive data is revealed and if only a minor number of email addresses are revealed.