Council of the European Union
General Secretariat

GSC INTERNAL PROCEDURE[1] TO DEAL WITH BREACHES OF PERSONAL DATA (DATA BREACHES)

1. A new obligation: assess all breaches of personal data and in some cases, notify the EDPS and inform persons affected.

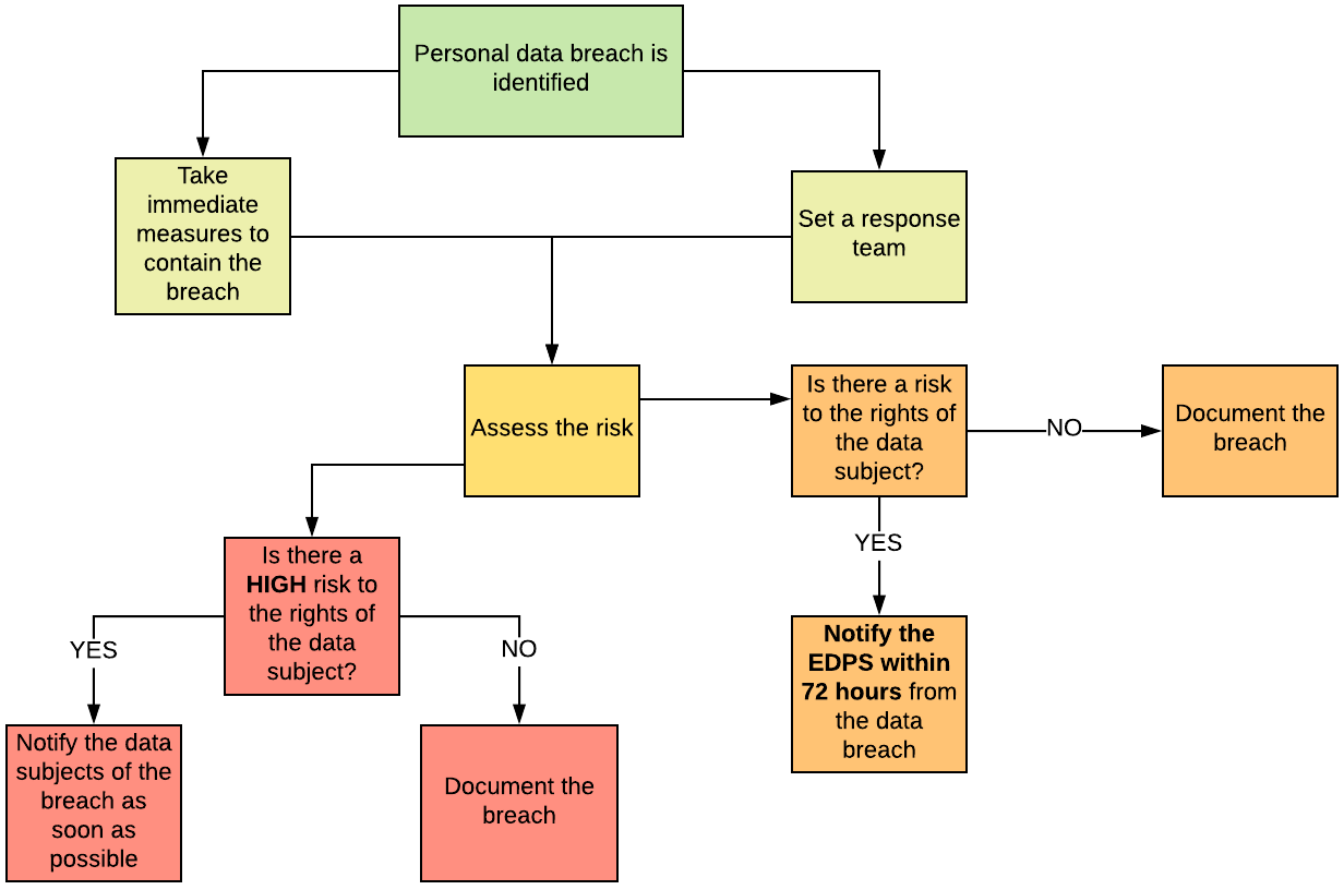
Regulation 2018/1725 (the Regulation) on the protection of personal data by the EU Institutions introduces the **obligation to identify and assess all breaches of personal data** (here in after "breaches"). Under certain circumstances, breaches will have to be notified to the European Data Protection Supervisor (EDPS) and in some cases, communicated to the persons affected.

As deadlines are tight **(72 hours)**, the GSC needs to put in place an internal procedure in place so the necessary assessments and decisions can be swiftly made in order to comply with the Regulation.

Infringements of the obligations related to data breaches may lead to the EDPS to impose an administrative fine to the GSC. The EDPS may also order the GSC to communicate a data breach to data subjects.

[1] This procedure shall be updated whenever deemed necessary and, in any case, every 2 years.

This procedure for dealing with personal data breaches does not replace or supersede any security incident handling process or procedure. This procedure should be integrated with any other incident handling process or procedure, including a business continuity situation.



2. What to do when a data breach happens

STEP 1	Identify a personal data breach. When possible, take an immediate response to contain it.
STEP 2	Set up a response team
STEP 3	Assess impact on the rights and freedoms of the data subjects
STEP 4	Notify the breach to the EDPS when there is a **risk** to the rights and freedoms of the data subjects
STEP 5	Communicate the breach to data subjects when there is a **high risk** to their rights.
STEP 6	Document the breach and include it in the register of data breaches

Diagram 1 . Step by step duty perspective for the controllers

Source: EDPS Guidelines on personal data breach notification. November 2018

STEP 1. Identify a personal data breach

Definition

"A personal data breach" is 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.[2]

- A breach of information security which does not compromise personal data does not fall under this definition.
- Not every information security is a personal data breach, but every personal data breach is an information security incident.
- A personal data breach may occur for a number of reasons, such as negligence, as a result of an accident or due to intentional act by internal or external persons.

The person who becomes aware of a data breach at the GSC should report it immediately to their line manager and to the Data Protection Officer (DPO). Every manager who is informed or becomes aware of a personal data breach will inform their hierachy. The controller can be identified with the help of the DPO or the mapping of records available in the Intranet site of Data Protection.

The procedure has to be launched as soon as the controller "becomes aware" of the breach. The controller is deemed to become aware of a breach when there is a "reasonable degree of certainty that a personal data breach has occurred". The identification of this moment is most relevant because it sets the departure point for the deadlines of 72 hours to notify to the EDPS.

** When the processing of personal data is subcontracted, the contractor, (i.e. processor) has to inform the GSC **without undue delay**. GSC obligation to assess and notify will start from the moment the contractor informs the GSC. The processor does not assess the impact on the rights of data subjects, just notifies the GSC, who has the legal obligation to assess and eventually notify the breach. Requirements on breach reporting must be detailed in the contract between the GSC and the contractor. It is important to know that the GSC retains overall responsibility for the protection of personal data, including data breaches, even if the processing of personal data is done by an external company though a contract (e.g. selection of managers, 360º).

[2] Article 3(16) of Regulation 2018/1725

Act promptly on a breach, contain it and, if possible, recover the compromised data and seek advise from your manager, the DPO and the EDPS.
Never try to hide a data breach or keep it to yourself.

Categories of personal data breaches

There are three types of breaches which follow the three well-known information security principles:

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

A personal data breach may be a breach of confidentiality, availability or integrity or a combination of these.

Examples of personal data breaches

a. staff mistakenly providing personal information to the wrong recipients (e.g. sending email to wrong persons or using wrong distribution list)

b. using unauthorized channels for exchanging personal information

c. staff storing information on unauthorized device

d. contactor accessing personal information (e.g. staff data) without prior authorization or violating technical controls

e. paper records containing personal information stolen or forgotten from insecure recycling or garbage bins

f. staff accessing or disclosing personal information outside their job authorisation

g. databases containing personal information being hacked into or otherwise illegally accessed by third parties outside the controller

h. lost or stolen laptops, mobiles, removable storage devices or paper records containing personal information.

source: EDPS Guidelines on personal data breach notification draft 6 November 2018

Please see more examples in annex 3

Accountability means that the controller shall be responsible for, and be able to demonstrate compliance with the principles relating to processing of personal data. These include "integrity and confidentiality", which are undermined in case of data breaches. Personal data shall be processed in a manner that **ensures protection** against unauthorised or unlawful processing and against its accidental loss, destruction or damage, using the appropriate technical or organisational measures. It needs to be processed in such a way that data breaches can be identified and assessed.

STEP 2 Set up a Response Team

If the breach relates to only one processing operation, the controller responsible for the concerned procedures will establish a response team, coordinate the measures to handle the breach and, if necessary, notify to the EDPS and communicate to the persons affected by the breach.

When the breach affects many processing operations, or concerns IT systems that provide support to multiple processings of personal data, the responsibility of organising the response will escalate to the appropriate level, and a manager in charge will be appointed.

The DPO should be informed as soon as there is an indication that there is a personal data breach. She can advice and guide controllers through the process. The DPO does not take decisions on the notification/communication and cannot notify a data breach on behalf of the Institution.

The Response Team will include:

1. the manager in charge, if appointed
2. the controller of the processing
3. the DPO
4. when necessary, the person in SMART who may better provide information about the nature and impact of the breach identified by [p.m.]
5. when necessary, a representative of Internal communication and/or DG COM, depending on the extent of the breach
6. a representative of any other service deemed relevant for the assessement and subsequent steps.
7. a representative of the SG CAB when justified by the impact of the breach.

The controller or manager in charge shall decide on an immediate response to contain the effects of the personal data breach.

STEP 3 - Assess impact on the rights and freedoms of the data subjects

A breach is assessed through the risks it represents to the rights and freedoms of the data subjects. Severity of breaches will need to be assessed on a case-by-case basis.

Recitals 46 and 47 of the Regulation (below) provide guidance for the risk assessment:

"The risk to the rights and freedoms of natural persons, of varying likelihood and severity, may result from personal data processing which could lead to **physical, material or non-material damage**, in particular:

- where the processing may give rise to discrimination, identity theft or fraud, financial loss, damage to the reputation, loss of confidentiality of personal data protected by professional secrecy, unauthorised reversal of pseudonymisation, or any other significant economic or social disadvantage;
- where data subjects might be deprived of their rights and freedoms or prevented from exercising control over their personal data;
- where personal data are processed which reveal racial or ethnic origin, political opinions, religion or philosophical beliefs, trade union membership, and the processing of genetic data, data concerning health or data concerning sex life or criminal convictions and offences or related security measures;
- where personal aspects are evaluated, in particular analysing or predicting aspects concerning performance at work, economic situation, health, personal preferences or interests, reliability or behaviour, location or movements, in order to create or use personal profiles;
- where personal data of vulnerable natural persons, in particular of children, are processed;
- or where processing involves a large amount of personal data and affects a large number of data subjects."

"The likelihood and severity of the risk to the rights and freedoms of the data subject should be determined by reference to the **nature, scope, context and purposes** of the processing. Risk should be evaluated on the basis of an objective assessment, by which it is established whether data processing operations involve a risk or a high risk."

When assessing a risk, consideration should be given to both the **likelihood and severity** of the adverse effect to the rights and freedoms of data subjects. Then, the risk should be evaluated on the basis of an objective assessment. With an actual breach, the adverse event has already occurred, and so the focus of the assessment is solely on the potential impact of the breach on individuals' rights and freedoms. Some impact may have already happened when the breach was detected, some may only become material at a later time (e.g. if credentials are stolen, some may already have been used, others may be used later).

Factors that can be taken into account are:

1. the type of breach

2. the nature, sensitivity and volume of personal data

3. ease of identification of individuals

4. severity of consequences for individuals

5. special characteristics of the individual

6. special characteristic of data controller

7. number of affected individuals.

Please see Annex 4 for a more detailed explanation as developed by the article 29 Working Party Guidelines on personal data breach notification under GDPR.

All the above factors need to be carefully assessed each one separate or in combination with the others to indicate the level of the risks to the individuals.

The risks identified during a Data Protection Impact Assessment (DPIA) can help the controllers during the process of assessing the risk. It is highly likely that data breaches on processing activities that needed a prior DPIA according to Art.39 of the Regulation, may cause higher risk to the rights and impacts on the individuals. p.m. DPIA will not be needed often at the GSC. EDPS to provide a list of processing operations where DPIAs will be required.

The result of the assessment may conclude that:

a) the personal data breach **does not represent a risk** to the rights of data subjects - This decision should be taken at the appropriate level and should be well documented, in order to enable the EDPS to verify compliance. As described in STEP 6.

b) the data breach **results in a risk to data subjects rights** - the controller notifies to the EDPS without undue delay/72 hours / as described in STEP 4.

c) the data breach **results in a high risk to the rights of data subjects**: the controller notifies to the EDPS and communicates the personal data breach to the data subjects. As described in STEP 5.

The conclusions of the assessment must be communicated to the members of the response Team. These will inform, when appropriate, their hierarchy. In case of severe data breaches, the Secretary general shall be informed.

STEP 4 - Notify the breach to the EDPS when there is a RISK to the rights and freedoms of the data subjects

When to inform:

If the controller or the manager in charge concludes, in view of all elements available, that the breach entails a risk for data subjects, he or she shall notify the personal data breach to the EDPS. This has to be done without undue delay (i.e. asap) and, where feasible, **not later than 72 hours after having become aware of it**.

However:

- Where it is not possible to provide the information at the same time, information may be provided in phases.
- If the deadlines cannot be respected, the controller shall inform the EDPS of the reasons for the delay.

How to inform:

- The EDPS has provided a functional mail box for notifications of personal data breaches: data-breach-notification@edps.europa.eu
- It has also provided for a template for notifications - hyperlink, copy in Annex 1
- It recommends that all communications concerning personal data breaches should be **encrypted**.

What to inform?

The information to be provided includes the nature of the breach, categories of personal data affected and categories of data subjects and approximately number concerned. Contact details of the DPO and any contact point who can provide further information. Finally, the likely consequences and implemented and recommended measures to mitigate the damage for data subjects.

Any personal data breach shall be documented by the controller as it develops, including the facts, its effects and remedial action. The documentation shall be made available to the EDPS to verify compliance with the Regulation.

The EDPS recommends that EU institutions keep a register of data breaches, even those not notified to the EDPS, due to the low level of risk for data subjects. See STEP 6.

The controller should send the notification to the EDPS and keep track of all the facts relating to the personal data breach, its effects and the remedial action taken, with the support of all the other member s of the response team. Any updates, follow/up and further information to be provided to the EDPS or to data subjects will be the responsibility of the controller or manager in charge.

STEP 5 - Communicate the breach to data subjects when there is a HIGH RISK to their rights.

Assessing which data breaches entail a **risk** and which entail a **high risk** is relevant, considering that only in the second case there is the obligation to communicate to data subjects.

When the assessment of the breach concludes that there is a likely **high risk** to the rights of data subjects, the controller or the manager in charge communicates the personal data breach to the data subject without undue delay (i.e. as soon as possible).

Prompt information to the individuals affected will allow them to take all the necessary precautions, and to protect themselves from the effects of a breach.

Communication

Communication to data subjects should be drafted in clear and plain language.

The communication should describe the nature of the personal data breach as well as recommendations for the natural person concerned to mitigate potential adverse effects. Such communications to data subjects should be made as soon as reasonably feasible and in close cooperation with the EDPS, respecting guidance provided by it.
The communication of a breach to affected persons shall include at least:

a) the likely consequences of the breach

b) the measures taken or proposed by the controller to address the breach.

c) the name and contact details of the DPO

The following text can be the basis for the communication to data subjects.

On…there has been a breach of personal data processed by the GSC/or by a concrete entity at the GSC. The breach has been contained / Is in the process of being contained. The damage is limited to …

A notification has been made to the European Data Protection Supervisor.

The Data Protection Officer of the GSC may be contacted at data.protection@consilium.europa.eu

When the personal data breach is considered to have a large impact, due to the number of data subjects affected, the type of data, the reputational risk for the GSC, for the Council or the European Council, DG COMM will decide on a LTT and the breach may be communicated through the web page or a press release.

The relevant breach should be communicated to the affected people directly (email, SMS, direct message, postal communications) unless doing so would involve a disproportionate effort. In these cases, data subjects may be informed by public communication.

Exceptions

There are exceptions to the obligation to communicate to data subjects:

- when the controller has implemented appropriate technical and organisational protection measures, and those measures were applied to the personal data affected by the personal data breach (e.g. encryption); [p.m. this information can only be provided by SMART?]

- when the controller has taken subsequent measures which ensure that the high risk to the rights and freedoms of data subjects is no longer likely to materialise. f [p.m. examples]

If the EDPS determines that the decision not to inform data subjects about a personal data breach is not well founded, it may order the GSC to do so. Failure to comply with such an order may result in the application of enforcement measures and administrative fines.

In accordance with the accountability principle, the GSC will have to be able to demonstrate to the EDPS that one or more of the conditions stated above are met if the GSC decides not to communicate a breach to the affected persons. While communication may initially not be required if there is no risk to people, this may change over time and the risk would have to be re-evaluated.

Examples

See Annex 3 and 5

STEP 6 - Document the breach and include it in the register of data breaches

Article 34(6) of the Regulation sets out that the controller shall document ALL personal data breaches, including the facts relating to the breach, its effects and the remedial action taken. That documentation shall enable the European Data Protection Supervisor to verify compliance with the Regulation and is in line with the principle of accountability of controllers.

Keeping track of data breaches is necessary for the controller to prove its compliance with the obligations laid down in the Regulation. Moreover, the controller would be able to have at its disposal both a repository of best practices to follow in case of data breaches and a list related security incidents that could enable to implement strategies to increase security of data processing.

Keeping the evidence of the data breach is also important to facilitate investigations and decide on corrective actions.

All information collected in the context of the personal data breach procedure or generated by this procedure should be handled on a strict need-to-know basis. Communication on data breaches should not take place on systems / infrastructure that may have been compromised by an event.

GSC Register of personal data breaches

The GSC shall establish an internal breach register of all the facts relating to the personal data breaches, its effects and the remedial action taken. This register could complement the existing IT security incident register.

p.m. The EUI may seek the opinion of its DPO as to the structure, the setting up and the administration of this internal data breach register. The DPO could also be additionally tasked with maintaining such records.

In the case of an investigation, an inspection or any other need for such information, the EDPS expects that the DPO of the EUI is in a position to provide information from the register of breaches and/or provide the EDPS with access to that register.

Further reading

EDPS Guidelines on personal data breach notification for the EU Institutions and bodies.

WP 29 guidelines on personal data breach notification as revised on 6 February 2018 and endorsed by the European Data Protection Board.

ANNEX 1

PERSONAL DATA BREACH NOTIFICATION FORM
(ARTICLE 34 OF THE ...REGULATION)

DATE:

A. TYPE OF NOTIFICATION

A.1 COMPREHENSIVE[21] ☐

A.2 IN PHASES[22]: INITIAL:☐ FOLLOW-UP[23] ☐

CONCLUSIVE[24]☐ Reference Case File[25] :

A.3 REGISTRATION NUMBER[26] OF DATA BREACH IN YOUR

REGISTER: YES ☐ REG.NO: NO☐

B. DATA CONTROLLER EUI :

B.1 NAME OF THE ORGANIZATION (EUI):

B.2 ADDRESS:

B.3 CONTACT PERSON:

B.4 TELEPHONE: B.5 EMAIL:

B.6 DATA PROTECTION OFFICER

B.7 TELEPHONE: B.8 EMAIL:

C. DATA PROCESSOR: (indicate if the data breach was reported by the processor)

C.1 NAME OF THE ORGANIZATION:

C.2 ADDRESS:

C.3 CONTACT PERSON:

C.4 TELEPHONE: C.5 EMAIL:

C.6 DATA PROTECTION OFFICER :

C.7 TELEPHONE: C.8 EMAIL:

---

[21] Select when this is a complete notification.
[22] Select when this is an initial, incomplete, notification, further information to follow (Art.34(4) of the Regulation)
[23] This is a follow-up to initial notification
[24] This is the final information for the incident
[25] In case of a follow-up or conclusive type of notification, please indicate if available the Case File number provided by the EDPS.
[26] Art 34(6) of the Regulation

D. DATA BREACH SECTION

D.1 Briefly explain the incident and how the data breach was detected:Click here to enter text.

D.2 Security criteria affected (tick one or more boxes)

I.CONFIDENTIALITY ☐ (potential) unauthorized disclosure or access

II.INTEGRITY ☐ accidental or unlawful alteration

III. AVAILABILITY ☐ accidental or unlawful destruction or loss

D.3 EXACT DATE OR PERIOD OF THE DATA BREACH:

D.4 DETECTION DATE[27]: TIME :

D.5 NOTIFICATION DATE[28]: TIME :

D.6 If more than 72 hours have passed between detection and notification, explain why you did not notify in time:

D.7 WHO WAS INFORMED/ INVOLVED IN THE INCIDENT[29]:

D.8 CATEGORIES OF PERSONAL DATA AFFECTED[30]

D.9 APPROXIMATE NUMBER OF PERSONAL DATA AFFECTED:

Please Specify the exact number if possible:

D.10 CATEGORIES OF PERSONS AFFECTED[31]:

D.11 APPROXIMATE NUMBER OF PERSONS AFFECTED:

D.12 LIKELY or ACTUAL CONCEQUENCES OF THE DATA BREACH FOR THE DATA SUBJECTS:

D.13 ESTIMATION OF THE RISK TO THE RIGHTS AND FREEDOMS OF NATURAL PERSONS:

RISK ☐ HIGH RISK☐

D.14 Briefly explain how the assessment of the risk to the rights and freedoms of natural persons was done.

D.15 Have you informed the persons affected about the breach? YES[32] ☐ if yes, WHEN:

NO☐, If no, explain why not (yet)

D.16 ACTION MEASURES TO ADDRESS THE RISK AND TO LIMIT ITS IMPACT[33]:

D.17 LAUNCH OF A FORMAL SECURITY INCIDENT PROCESS: YES ☐ NO☐ if no, motivate why not:

D.18 ROOT CAUSE OF THE DATA BREACH[34]

---

[27] Indicate the date when you become aware of the personal data breach.
[28] The notification date should be less than 72 hours after you become aware of the breach. If this is not the case the reasons for the delay shall be presented.
[29] Indicate the persons involved in the handling of the incident (internal and external) of the EU institution
[30] List all elements/fields of data that were compromised e.g. first and last names, date of birth, financial data, health data, etc.
[31] List all the categories of the data subjects affected, e.g. EU staff, , MEPs, European citizens, children, vulnerable groups such as handicapped people etc.
[32] If yes, attach a copy of the communication sent to the data subject
[33] List of security and mitigation measures to address the risk e.g. data was encrypted, redundant system allowed the organisation to have an access to the data for business continuity purposes.
34 Explain the root cause of the security incident that lead to the data breach.

ANNEX 2

Article 3 of Regulation 2018/1725 Definitions

16. 'personal data breach' means a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data transmitted, stored or otherwise processed

Articles 34 and 35

Article 34

Notification of a personal data breach to the European Data Protection Supervisor

1. In the case of a personal data breach, the controller shall without undue delay and, where feasible, not later than 72 hours after having become aware of it, notify the personal data breach to the European Data Protection Supervisor, 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 European Data Protection Supervisor is not made within 72 hours, it shall be accompanied by reasons for the delay.
2. The processor shall notify the controller without undue delay after becoming aware of a personal data breach.
3. The notification referred to in paragraph 1 shall at least:
   (a) describe the nature of the personal data breach including where possible, the categories and approximate number of data subjects concerned and the categories and approximate number of personal data records concerned;
   (b) communicate the name and contact details of the data protection officer;
   (c) describe the likely consequences of the personal data breach;
   (d) describe the measures taken or proposed to be taken by the controller to address the personal data breach, including, where appropriate, measures to mitigate its possible adverse effects.
4. Where, and in so far as, it is not possible to provide the information at the same time, the information may be provided in phases without undue further delay.
5. The controller shall inform the data protection officer about the personal data breach.
6. 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 European Data Protection Supervisor to verify compliance with this Article.

Article 35

Communication of a personal data breach to the data subject

1. When the personal data breach is likely to result in a high risk to the rights and freedoms of natural persons, the controller shall communicate the personal data breach to the data subject without undue delay.
2. The communication to the data subject referred to in paragraph 1 of this Article shall describe in clear and plain language the nature of the personal data breach and contain at least the information and measures referred to in points (b), (c) and (d) of Article 34(3).
3. The communication to the data subject referred to in paragraph 1 shall not be required if any of the following conditions are met:
   (a) the controller has implemented appropriate technical and organisational protection measures, and those measures were applied to the personal data affected by the personal data breach, in particular those that render the personal data unintelligible to any person who is not authorised to access it, such as encryption;
   (b) the controller has taken subsequent measures which ensure that the high risk to the rights and freedoms of data subjects referred to in paragraph 1 is no longer likely to materialise;
   (c) it would involve disproportionate effort. In such a case, there shall instead be a public communication or similar measure whereby the data subjects are informed in an equally effective manner.
4. If the controller has not already communicated the personal data breach to the data subject, the European Data Protection Supervisor, having considered the likelihood of the personal data breach resulting in a high risk, may require it to do so or may decide that any of the conditions referred to in paragraph 3 are met.

Annex 3

Practical Examples [3]

The following examples might assist EUI in determining whether they need to notify the EDPS or communicate to data subjects in different personal data breach scenarios. The list of examples is not exhaustive.

Furthermore, these examples may help to distinguish between risk and high risk to the rights and freedoms of individuals.

Please keep in mind that a breach of information security that does not compromise personal data, does not fall within the scope of this procedure. For instance, if a database containing anonymous data was leaked, this would be a security incident, but not a personal data breach.

In addition, failure of EUI to provide adequate information to data subjects about a processing is not a data breach in the sense of Article 35 of the Regulation.
It is irrelevant whether the breach was intentional or not.

Not every information security incident is a personal data breach, but every personal data breach is an information security incident.

It is important to understand that the criterion for the decisions on notification and communication is **the risk for each of the individuals concerned**, and that it is **not the severity of the incident** as it is normally used as the criterion in security management.

The difference between the two criteria can be illustrated by looking at the elements considered:

The following elements could be used to assess the **severity of the incident**:

 Low severity: compromised data fairly usual given the context of the processing (e.g. only first and last names); security measures in place to limit the impact (e.g. data was lost but is encrypted with strong encryption means), low number of individuals concerned.

 Medium severity: compromised data somewhat comprehensive (e.g. first and last names with date of birth and grade and family allowance and other fields), significant number of data subject affected given the context (e.g. all individuals working for DG XX, most individuals working on a specific sensitive project etc.)

 High severity: sensitive data (e.g. health certificates) and/or very high number of data subjects affected (e.g. all EU staff) and/or political figures affected and/or the data breach was reported in the media (reputational damage for the EUI).

[3] Source: EDPS Guidelines on personal data breach notification for the EUI and bodies

The **risk for the individual** is one of the elements to be taken into account for the severity of the incident, but it depends on specific elements:

 the categories of data concerned, e.g. high risk may be caused by disclosing special categories, financial data, other data elements usually kept confidential,

 the amount of data for an individual, e.g. high risk may be indicated when many records of certain transactions are disclosed, such as a list of phone calls with the connected parties, lists of assignments to tasks, etc., but also when the data concerns many different aspects of an individual, even when no special categories are concerned, such as data about home address, family composition over time, career history, travel records, social media activity, online transactions or any similar combinations of different aspects of life,

 the ease or difficulty of identification of the individuals, e.g. while it may generally be assumed that the risk with pseudonymised data is lower than with data which is fully qualified with identifying attributes, the effectiveness of the pseudonymisation needs to be assessed. It may be the case that the data may allow identification without such attributes (such as a list of job assignments which may be unique among all staff in one organisation and may be accessible through HR tools),

 the characteristics of the individuals concerned, e.g. persons who are already known to be vulnerable, such as victims of harassment or crime, are more likely to suffer high risk than others as consequence of a breach,

 the characteristics of the controller, e.g. the pure fact that an individual was registered in a database of an organisation dealing with family problems may be more risky for the individual than for a database of participants of a technical conference,

 properties of the breach, e.g. if a breach is caused by targeted activities of a malicious actor who has obtained access to confidential data is more likely to create a high risk for the individuals than an accidental disclosure of similar data to a limited group of known recipients.

The number of individuals concerned is an important factor for the severity of an incident, but a higher number does not necessarily increase the level of risk for the individuals concerned, e.g. when a malicious actor obtains access to only a few credit card credentials, the likelihood for each of them to be used illegally may be higher than in a case of a large database being stolen.

For the obligation to notify the breach to the EDPS or to communicate to the data subjects, the level of risk is the decisive criterion. The severity of the incident plays a role for the response of the organisation and for mitigating and corrective action to be taken.

WP29 recommends the assessment should take into account the following criteria:

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 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.

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 5

Example*	Type of Breach	Notify the EDPS	Notify the Data Subject	Explanation
A DG is moving to another building .Movers find locker of HR Archive open and multiple folders missing. Folders contain health data. A digital back-up is available.	Confidentiality Integrity	Yes	Yes	As the folders contain sensitive data there is a high risk for the rights and freedoms of the individuals.
An Agency with a network file system of EU patients with rare diseases is running its own infrastructure. A colleague detects a ransomware after a personal USB stick is used and after a while no one can access data from the file servers.	Availability Confidentiality	Yes	Yes	The sensitive nature of the data present a high risk to the affected individuals.
A high level member of a EUI loses a USB stick containing copies of draft decisions and material from the files, including personal data. The USB stick is encrypted with a state of the art algorithm. Back up of data exists.	Confidentiality	NO	NO	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, there is no need to notify to EDPS and send the communication to the data subject. However, if the USB stick is later compromised, notification to the EDPS and communication to the data subject will be required. This is also the case if later a serious vulnerability in the algorithm used to encrypt the data on the lost USB key is discovered, because that increases the likelihood of the confidentiality data being compromised. This is a case where a personal data breach has to be re-evaluated.
The list of usernames and password to their work account of the staff of a DG has been leaked. The	Confidentiality	NO	NO	As the DG took immediate actions to threat and recover from the negative effects of the

* Source: EDPS Guidelines on personal data breach notification for the EUI and bodies

leak was immediately detected by the IT Security and the institution proceeded straight away with changing the usernames and resetting of the passwords.				personal data breach there is no risk for the individuals.
A member of HR accidentally sends an email to all rejected candidates for recruitment with the email addresses in the cc field instead of the bcc field.	Confidentiality	YES	NO	In this case, notwithstanding the fact that personal e-mail addresses are provided and it is possible to understand who applied for the job, there is risk to the rights and freedoms of individuals who do not want to share this information. No high risk is indicated in this case
An official of a EUI accidentally sends a file containing name, surnames, contact details, office position of an entire DG to staff members in another DG or EU Agency.	Confidentiality	NO	NO	In this case, notification is not required, since the above mentioned information of staff is public already available in interinstitutionally open directories of EUI staff.
A database containing information on whistleblowing procedures in European EUI has been hacked and published on internet. The names of whistle-blowers and persons concerned have been made public.	Confidentiality	YES	YES	In this case, there is a high risk to the rights and freedoms of data subjects. Therefore, EDPS must be notified and a communication should be sent both to whistle-blowers and other persons affected.
An EU Agency suffers a ransom ware attack that results in all personal data of EU citizens registered in a specific funding program being encrypted. No back-ups are available and the data cannot be restored.	Integrity Availability Confidentiality	YES	YES	An integrity, availability and potentially confidentiality data breach. In this case, there is a high risk to the rights and freedoms of data subject. Therefore, EDPS must be notified and a communication should be sent to the individuals.
Health certificates of the employees of a DG have been deleted accidentally or, in the example of securely encrypted data, the decryption key has	Availability Integrity	YES	YES	As there is no backup of the data and data cannot be restored, the loss of health certificates of the employees present a high

been lost. There is no back up of the health certificates data and no physical files.				risk for their rights and freedoms. Therefore, EDPS and the data subjects must be notified
A laptop-containing a copy of a list of employees subject to disciplinary measures was stolen.	Confidentiality	YES	YES	The sensitive nature of data creates a high risk to their rights and freedoms o the employees when accessed by unauthorized individuals.
Thousands of records with personal data are stored unencrypted on the cloud service providers (CSP) platform. The CSP is hacked after one year.	Integrity Confidentiality	YES	YES	Taking into account the big number of affected individuals they should be notified on the incident
Personal Data of high tax payers in the EU is stored encrypted with AES-512 algorithm and the key is on local file system. After one year the LISO informs on a network breach. The encryption key has been accessed.	Integrity Confidentiality	YES	YES	Taking into account the nature of the breach and the potential risk to the affected individuals a notification should be sent.