EUROPEAN DATA PROTECTION SUPERVISOR

Guidelines on personal data breach notification

For the European Union Institutions and Bodies

Draft 21 November 2018

TABLE OF CONTENTS

1. Introduction 4

2. Scope and structure of the Guidelines 6

2.1. SCOPE 6

2.2. STRUCTURE 6

3. Personal Data Breach under the Regulation on processing of personal data by EU Institutions 8

3.1. BACKGROUND 8

3.2. WHAT IS A PERSONAL DATA BREACH 9

4. How to assess a personal data breach (Assessing Risk and High Risk) 12

4.1. ASSESSING RISK AND HIGH RISK 13

5. How to notify a personal data breach to EDPS (Notification to the EDPS) 15

5.1. NOTIFICATION REQUIREMENTS 16

5.2. NOTIFICATION IN PHASES 17

6. How to communicate a personal data breach to the data subject 19

7. How to document a personal data breach (Accountability and documentation requirements) 21

Annex 1. Notification Template Form 22

Annex 2. Practical Examples 25

Annex 3. References and useful readings 30

Annex 4. Glossary 31

Annex 5. In a nutshell 33

EXECUTIVE SUMMARY

The Guidelines aim to provide **practical advice** to the EUI how to comply with the provisions on personal data breaches of articles 34 and 35 of the Regulation on the processing of personal data by EUI.

The Regulation integrates the principles of the General Data Protection Regulation (Regulation (EU) 2016/679, hereafter "GDPR") including those on personal data breaches into the data protection rules for EU institutions.

The Guidelines provide recommendations and indicate best practices to implement accountability for personal data protection by **helping to assess and manage the risks for data protection, privacy and other fundamental rights of individuals in case of a personal data breach**. They collect and consolidate the advice the European Data Protection Supervisor (EDPS) has been giving the EUI in the last years, e.g. regarding the first inter-institutional tenders.

These Guidelines outline the approach that EUI should take to adequately respond to a personal data breach.

The EDPS considers the best practices listed hereafter as **a reference** when assessing compliance with the Regulation. EUI may choose alternative, equally effective, measures other than the ones presented in this paper taking into account their specific needs. In this case they will need to demonstrate how these measures lead to an equivalent protection of personal data.

EUI should regularly perform an assessment of their procedures on personal data breach. The assessment shall show that the EUI can in principle respond effectively to prevent or to mitigate the risk to an acceptable level of a personal data breach.

The Guidelines describe:

- What a personal data breach is

- How to assess a personal data breach

- How to notify a personal data breach to the EDPS

- How to communicate a personal data breach to the data subject

- How to document a personal data breach

Furthermore, the Guidelines provide a template form of notification of a personal data breach to the EDPS by the EU institutions.

1. Introduction

1 These guidelines are intended to provide practical advice to the EUI and bodies (hereinafter "EUI ") to comply with Regulation (EU) 2018/1725 ("the Regulation")[1] which replaced Regulation (EC) No. 45/2001[2] by helping them to respond effectively to personal data breaches. The Regulation introduces the obligation for EUI to notify the EDPS when a personal data breach occurs which presents a risk to the rights and freedoms of the individuals, and to notify the individuals whose data have been affected by the breach in cases of high risk. The Regulation aligns data protection rules for EUI with the General Data Protection Regulation (Regulation (EU) 2016/679, hereafter "GDPR")[3] applicable in EU and EEA member states to private and public sector entities.

2 As the independent supervisory authority competent for the processing of personal data by EUI, the EDPS may among other tasks issue guidelines on specific aspects related to the processing of personal data.

3 These guidelines should be considered by Data Protection Officers (DPOs) and Data Protection Coordinators or Contacts (DPCs),) as well as IT staff and other services concerned with IT security and physical security e.g. Local Information Security Officers (LISO) and Local Security Officers (LSO), and by all persons carrying responsibility for the EUI acting as co-controllers and processors. They will also be useful to senior management in supporting a culture of data protection from the top of the organization and to implement the principle of accountability.

4 The purpose of the guidelines is to make it easier for EUI to fulfil their obligations on personal data breach management. They remain however responsible for compliance with their obligations pursuant to the accountability principle. The measures recommended in these Guidelines allow the EUI to develop or adapt their processes for the management of personal data breaches and to comply with communication obligations towards the EDPS and the individuals. EUI may choose alternative, equally effective measures other than the ones presented in the Guidelines taking into account their specific needs. In this case they will need to demonstrate how they have planned to obtain equivalent protection via these alternative measures.

5 These guidelines will be updated as the EUI and EDPS develop experience and practice with personal data breach notification and communication pursuant to the Regulation. The update will also take account of a common understanding of the severity of personal data breaches

[1] Regulation (EU) 2018/1725 of the European Parliament and of the Council of 23 October 2018 on the protection of natural persons with regard to the processing of personal data by the Union institutions, bodies, offices and agencies and on the free movement of such data, and repealing Regulation (EC) No. 45/2001 and Decision No 1247/2002/EC, OJ L 295 of 21.11.2018, p. 39; available at: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=uriserv:OJ.L_.2018.295.01.0039.01.ENG.

[2] Regulation (EC) No 45/2001 of 18 December 2000 on the protection of individuals with regard to the processing of personal data by the Community institutions and bodies and on the free movement of such data, OJ L 8, 12.01.2001, p. 1.

[3] Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation); OJ L 119, 04.05.2016, p.1, available at: http://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=OJ:L:2016:119:FULL.

and of the risks for the persons whose data has been breached, developed in cooperation with the Member States' Data Protection Authorities (DPAs), as well as ensuring consistency with the practice of the Member States' DPAs in enforcement of the personal data breach provisions of the GDPR.

2. Scope and structure of the Guidelines

2.1. Scope

6 The Regulation specifies the obligations of the controllers within EUI with regard to the processing of personal data under their responsibility and provides individuals with legally enforceable rights to data protection.

7 The processing of personal data in information systems of EUI must fully comply with the Regulation.

8 The guidelines present how to respond to a personal data breach in order to comply with Articles 34 and 35 of the Regulation.

9 The guidelines explain the mandatory notification of personal data breaches and the communication requirements under the Regulation and the basic steps the EUI as controllers and/or as processors shall take to meet these new obligations.

10 The guidelines focus on personal data breach incidents and how the EUI have to be prepared not only to respond effectively and according to their legal obligations, but also to proactively prevent such incidents.

11 Data breach related procedures shall not replace or supersede any security incident handling process or procedure, instead they should be integrated with such an incident handling process or procedure.

2.2. Structure

12 The Guidelines are structured as follows:

- Chapter 1 introduces the purpose of the guidelines.
- Chapter 2 defines the scope and the structure of the document.
- Chapter 3 explains what a personal data breach is.
- Chapter 4 explains how to assess a personal data breach and risks.
- Chapter 5 explains how to notify a personal data breach to the EDPS.
- Chapter 6 explains how to communicate a personal data breach to data subjects.
- Chapter 7 explains how to document a personal data breach.
- Annex 1 presents the notification form.
- Annex 2 describes practical examples.
- Annex 3 provides references to other useful documents (opinions, technical standards, best practices etc.).
- Annex 4 includes a glossary.
- Annex 5 includes a flowchart on data breach notification requirements for EUI and presents a summary of relevant considerations regarding personal data breach.

13 This document does not consider/focus on:

- An exhaustive coverage of relevant IT security measures for the detection and containment of a personal data breach.
- The technical and functional features of the IT infrastructure provided to prevent a personal data breach, such as type of servers, software platforms and applications, network devices, etc.

3. Personal Data Breach under the Regulation on processing of personal data by EU Institutions

3.1. Background

14 Notification of a personal data breach is a new obligation for EUI and reflects a similar obligation introduced with the GDPR. The concept had first been introduced under the ePrivacy Directive. A personal data breach could, if not addressed in an appropriate and timely manner, result in physical, material or non-material damage to natural persons.

15 In all cases, the controller must mitigate the effect of any personal data breach and in particular the impact on data subjects. Controllers must adopt a personal data breach handling procedure which also includes notification to the EDPS and communication to the people affected, where required. The procedure for dealing with personal data breaches does not replace or supersede any other incident handling process or procedure. In fact, controllers would do well to integrate procedures for dealing with personal data breaches in their procedures for information security incident management. Furthermore, the procedure for dealing with personal data breaches should tie into the controller's business continuity plan and the activities carried out by the controller's communication teams where appropriate.

16 In order to achieve compliance with time frames set by the Regulation for the notification and communication of personal data breaches, it is strongly advised that controllers adopt a personal data breach procedure that includes mitigating strategies. This procedure could complement existing IT security procedures/manuals. All staff should be made aware of this obligation and related procedures (e.g. newcomer training, all staff exercise).

17 A personal data breach can potentially have a range of significant adverse effects to the individuals, which may result in physical, material or non-material damage. The GDPR and the Regulation explain that this can include a loss of control over their personal data or limitation of their rights, discrimination, identity theft or fraud, financial loss, unauthorised reversal of pseudonymisation, damage to reputation, loss of confidentiality of personal data protected by professional secrecy or any other significant economic or social disadvantage to those individuals[4].

18 The notification of data breaches to the supervisory authority and communication to data subjects became legal obligations under Art. 33 and 34 of the GDPR and under Art. 34 and 35 of the Regulation. Data breach notifications are measures to empower data subjects, which at the same time reinforce the accountability of data controllers (and processors). Data breach notifications are aimed to ensure more data security in Europe.

19 At the same time, due consideration should be given to the circumstances of that breach, including whether or not personal data had been protected by appropriate technical protection measures, effectively limiting the likelihood of identity fraud or other forms of misuse (Recital 88 GDPR).

[4] Recital 85 GDPR, recital 46 of the Regulation).

20 Although Directive 95/46/EC and Regulation 45/2001 did not address this issue, the concept of notification of data breaches is not new in EU legislation. For instance, providers of publicly available electronic communications services have the duty to notify personal data breaches to competent national authorities and to keep an inventory of data breaches, comprising the facts surrounding the breach, its effects and the remedial action taken (Article 4 ePrivacy Directive)[5].

21 At national level, even before the entry into force of the GDPR, some Member States introduced measures to manage data breaches. The German Federal Data Protection Law introduced an obligation to notify breaches of confidentiality in 2009[6]. In 2011, Ireland set up a Personal Data Security Breach Code of Practice[7]. Between 2014 and 2015, Italy elaborated different templates for notification of data breaches depending on the type of data involved[8].

22 Taking into account the importance of notification and communication of a personal data breach to strengthen the right of data subjects, promote accountability of data controllers (and processors) and foster data security in Europe, the Regulation introduces an obligation on data controllers in case of data breaches occurring in EUI (or at their processors).

3.2. What is a Personal Data Breach

23 **According to the Regulation Article 3, paragraph 16,** a 'personal data breach' means a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data transmitted, stored or otherwise processed under the responsibility of the EUI as a controller.

24 This definition of a personal data breach in the Regulation is aligned with the GDPR[9].

25 If the Regulation is breached in a different way (e.g. no adequate legal basis for a processing operation, inadequate information to data subjects etc.) this does not fall under the obligations related to personal data breach, while it is still a breach of the Regulation. A breach of information security which does not compromise personal data does not fall within the scope of this obligation either. Whether the breach was intentional or not is irrelevant.

---

[5] Directive 2002/58/EC of the European Parliament and of the Council of 12 July 2002 concerning the processing of personal data and the protection of privacy in the electronic communications sector (Directive on privacy and electronic communications); OJ L 201, 31.7.2002, p. 37, as amended by Directive 2009/136 (EC) of 25 November 2009, OJ L 337, 18.12.2009, consolidated text available at: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:02002L0058-20091219.

[6] Gesetz zur Änderung datenschutzrechtlicher Vorschriften vom 14.8.2009, BGBl. 2009 Teil I Nr. 54, p. 2814, available at: http://www.bgbl.de/xaver/bgbl/start.xav?startbk=Bundesanzeiger_BGBl&jumpTo=bgbl109s2814.pdf

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

[8] For health data and biometric data: http://194.242.234.211/documents/10160/0/Linee+guida+in+materia+di+dossier+sanitario+-+Allegato+B.pdf; https://www.garanteprivacy.it/documents/10160/0/All+B+al+Provv.+513+del+12+novembre+2014+Mod.+segnalazione+data+breach.pdf

[9] GDPR, Article 4, paragraph 12

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

27 In its Guidelines which were confirmed by the EDPB, the Article 29 Working Party ("WP29")[10] defined three types of personal data breaches following the three well-known information security principles:

- "Confidentiality breach" – where there is an unauthorised or accidental disclosure of, or access to, personal data, which is about getting knowledge of personal data by an entity not entitled to this knowledge,
- "Availability breach" – where there is an accidental or unauthorised loss of access to, or destruction of, personal data, which is about losing control of access to personal data, or inappropriate deletion of personal data, and
- "Integrity breach" – where there is an unauthorised or accidental alteration of personal data, which is about inappropriate modifications of personal data.

28 A data breach may occur for a number of reasons, such as:

a. Due to negligence,

b. As a result of an accident, or

c. Due to intentional act by internal or external persons.

29 In summary, every personal data breach is a security incident[11] and depending on the circumstances, it can concern a breach of confidentiality, integrity or availability of personal data, as well as any combination of these. Among the causes of data breaches are negligence, accident or technical failure, and intentional acts by internal or external actors.

30 Some examples of data breaches may include[12]:

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

[10] WP29 Guidelines on Personal data breach notification under Regulation 2016/679 adopted on 3 October 2017, as last revised and adopted on 6 February 2018; available at: http://ec.europa.eu/newsroom/article29/item-detail.cfm?item_id=612052. These guidelines were endorsed by the European Data Protection Board

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

[12] Further examples in Annex 2.

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.

31 The procedure for dealing with personal data breaches does not replace or supersede any incident handling process or procedure. In fact, EUI could potentially integrate procedures for dealing with personal data breaches in their procedures for information security incident management. Furthermore, the procedure for dealing with personal data breaches would tie into the controller's security plans and the activities carried out by the controller's communication teams where appropriate.

4. How to assess a personal data breach (Assessing Risk and High Risk)

32 Article 34 of the Regulation follows the risk based approach adopted by the GDPR. The severity of breaches will need to be assessed on a case-by-case basis. The "risk to the rights and freedoms of natural persons" shall be taken as the basis for considerations on the response. The risks identified during a prior data protection impact assessment (DPIA) can serve as a starting point.

33 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.

34 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).

35 As already mentioned, a personal data breach is a security incident. However, not each security incident can be considered as a personal data breach. The necessary requirement to consider a security incident as a personal data breach is that personal data are involved.

36 These guidelines assume that a EUI has a well-established security incident management process including reporting. It is of utmost importance to be able to identify a personal data breach.

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

While assessing each reported incident, it should be detected if personal data is affected.

If personal data is affected, the security incident will be considered a personal data breach

37 As soon as there is an indication that a security incident might affect personal data, the Data Protection Officer (DPO) shall be immediately consulted.

Once the security incident is considered a personal data breach, as the next step, it should be assessed what would be the impact of the incident on individuals; rights and freedoms.

38 Once the security incident is considered a personal data breach, the EUI shall assess the impact of the breach on the rights and freedoms of data subjects. This assessment shall be

as objective as possible. This step is very critical as it will define the notification obligations of the EUI as a controller.

A EUI shall implement its own personal data breach management procedure or set of policies that will focus on the impact assessment of every reported personal data breach and the selection of the adequate notification procedure towards the EDPS and the data subjects. Roles and responsibilities shall be clearly defined.

39 It is of utmost importance the EUI ensures a correct assessment of the risks as a trigger for notification to the EDPS and possible communication to a data subject.

In cases where there is reported evidence that a recorded personal data breach creates no risk to the rights and freedoms of data subjects, the controller will not need to notify the EDPS nor the data subjects. However, this decision should be taken at the appropriate level and should be well documented, in order to enable the EDPS to verify compliance of the EUI also for data breaches which were not notified.

40 EUI shall integrate, in the data breach management procedure or in a separate procedure, a step by step guidance or a methodology that will aim at the objective assessment of the level of risk of a personal data breach.

According to Art. 34 of the Regulation, a EUI should notify a personal data breach not later than 72 **hours** to the European Data Protection Supervisor, unless it is unlikely to result in a **risk** to the rights and freedoms of individuals.

Furthermore, according to Art. 35 (1) of the Regulation, in case the personal data breach result in a "**high risk"** to the rights and freedoms of individual, the EUI should also communicate it to the data subjects.

41 In all cases, the controller must mitigate the effects of any personal data breach and in particular the impact on data subjects.

4.1. Assessing risk and high risk

42 The data breach notification obligation reflects a risk based approach.

Severity of breaches will need to be assessed on a case-by-case basis. The "risk to the rights and freedoms of natural persons" should be taken as a basis for considerations when conducting an assessment. The risks identified during a DPIA can serve as a starting point[13].

43 Assessing which data breaches entail a risk and which entail a high risk is relevant for the notification and communication obligation. In case of a risk which is not high the EUI will only notify the EDPS as the supervisory authority whereas in cases of high risk there is the obligation to communicate also to data subjects.

[13] Art. 39 of the Regulation

44 Recitals 46[14] and 47[15] of the Regulation provide that when assessing a risk, consideration should be given to both the likelihood and severity of the risk to the rights and freedoms of data subjects. Then, the risk should be evaluated on the basis of an objective assessment. With an actual data breach, the event has already occurred, and so the focus of the controller is solely on the impact of the breach on individuals[16].

45 The assessment of the data breach impact on the data subject is important as it will also help the EUI to take the adequate measures to contain and address the breach.

46 As recommended by the WP29 in its guidelines, the factors to be taken into account when assessing the risks are:

1. type of breach
2. 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 characteristics of the data controller
7. the number of affected individuals.

47 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 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.

48 Practical examples of personal data breaches in Annex 2 point out the level of risk. Additional references on assessing risk can be found in Annex 3.

---

[14] "*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.*"

[15] "*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*."

[16] It must be pointed out that this objective assessment in case of data breaches is different from the one in the Data Protection Impact Assessment. The DPIA considers both the risks of the data processing being carried out as planned, and the risks in case of a breach, but at hypothetical level. See also WP29 Guidelines on Personal data breach notification under Regulation 2016/679.

5. How to notify a personal data breach to EDPS (Notification to the EDPS)

EDPS FUNCTIONAL MAILBOX FOR DATA BREACH NOTIFICATIONS

data-breach-notification@edps.europa.eu

ALL COMMUNICATIONS SHOULD BE ENCRYPTED

An EUI should notify a personal data breach not later than 72 hours to the European Data Protection Supervisor, unless it is unlikely to result in a risk to the rights and freedoms of individuals. If the personal data breach result in a "high risk" to the rights and freedoms of individual, an EUI should also communicate it to data subjects.

49 Article 34 of the Regulation sets out the obligation to notify personal data breaches to the EDPS. The controller should notify the EDPS not later than 72 hours after having become aware of the data breach. The controller is considered to become "aware" when there is a reasonable degree of certainty that a personal data breach has occurred

50 The notification procedure to the EDPS involves: on the one hand, the controller (a representative) and; on the other hand, the person in charge of data protection matters e.g. Data Protection Officer (DPO).

51 The processor also plays an important role, since it has the duty to inform the controller about any data breaches

52 The EUI can be both controllers and processors in different data processing activities according to the Regulation. They might also have external, third party processors (e.g. Contractors) that are responsible for some processing activities of personal data.

53 The controller retains overall responsibility for the protection of personal data, the processor might enable the controller to comply with its obligations; this includes breach notification.

54 If a processor becomes aware of a breach of the personal data in processing on behalf of the controller, he must notify the controller "without undue delay" which means as soon as possible. It should be noted that the processor does not need to first assess the risks 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.

As a **controller** it is important to have personal data breach clauses in contracts with any contactors who act as processors, which obliges them to notify you immediately in the event of a personal data breach and provide all necessary information related to the breach.

As a processor you are obliged to immediately notify the responsible controller(s) in case you detect a personal data breach and provide all necessary information on the incident.

55 The representative of 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 case handlers as explained in chapter 7. The controller must

involve the DPO throughout the personal data breach management and notification process (both notification to the EDPS and communication the data subject).

56 When notifying the breach to the EDPS, the controller shall provide the name and contact details of its DPO.

> The controller shall promptly inform the DPO about the occurrence of a personal data breach and ensure that the DPO is involved throughout the breach management and notification process (both to the EDPS and the data subject).

57 The DPO should provide advice, where requested, as regards the necessity for a notification or a communication of personal data breach, and monitor compliance, as well as during a breach (i.e. when notifying), and follow-up as well as during any subsequent investigation by the EDPS.

> The EUI has to put in place the procedures to enable effective communication of the breach from: Data processor to data controller; Data controller to supervisory authority-EDPS; and Data controller to data subject.

5.1. Notification requirements

58 The controller should send the notification not later than 72 hours after having become aware of the data breach.

59 In case the controller do not comply with the time-limit of the 72 hours he shall justify the reasons for the delay with the notification.

60 The obligation to notify depends on the risk level for the person(s) whose data has been breached:

a. In case of unlikely risk, there is no obligation to notify the EDPS, but the controller should inform its DPO and document the breach.

b. When there is a risk, then the controller should notify the breach to the EDPS within 72 hours. An explanation shall be provided in case of delay with complying with the 72 hours' time frame.

c. If there is a high risk, the obligation from Article 35 to communicate a personal data breach to the data subject applies in addition to informing the EDPS.

Diagram 1 . Step by step duty perspective for the controllers

61 The notification of a personal data breach to the EDPS should contain, at least[17]:

1. a description of 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;
2. name and contact details of the DPO
3. a description of the likely consequences of the personal data breach[18]
4. a description of the measures taken[19] or proposed to be taken by the controller to address the personal data breach, including, where appropriate, measures to mitigate its possible adverse effects on individuals.

62 The EDPS in Annex 1 provides a notification form on personal data breach notifications which can be used by the EU institutions[20].

5.2. Notification in phases

63 Depending the nature of the data breach the EUI as a controller may need further information, investigations and time to establish the facts of the data breach. Art34(5) of the Regulation recognizes that and allows that the information might be provided to the EDPS in phases.

---

[17] See also chapter 6

[18] Article 34 of the Regulation refers to likely consequences. The controllers may do well to consider and describe not just likely consequences, but also possible consequences, as the risk of consequences occurring may become more likely over time (e.g. personal data was secured with state-of-the-art encryption at the time of the breach, so there would likely be no consequences, however if later a serious vulnerability in the encryption used is later discovered, then the consequences are more likely). In this regard, see example 1 in Annex 2.

[19] Containment measures may include: Stopping the system if the data breach is caused by system failure ; Changing the users' passwords and system; configurations to control access and use; Consider whether technical advices or assistance be immediately sought internally or from outside to remedy the system loopholes and/or stop the hacking; Ceasing or changing the access rights of individuals suspected to have committed or contributed to the data breach; Notifying the relevant law enforcement agencies if identity theft or other criminal activities were or likely to be committed.

[20] Specific information on how to submit a data breach notification is available on the EDPS website.

64 The controllers will not always have all of the necessary information concerning a personal data breach within the time frame of the 72 hours when they became aware of it, Consequently full and comprehensive details of the incident may not always be available during this initial period

65 This may apply for complex breaches, such as some types of cyber security incidents, where, 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. In such cases the controllers shall have to provide to the EDPS the reasons for the delay of the full reporting.

66 The focus of the notification requirement is to enable the EUI to act promptly on a breach, contain it and, if possible, recover the compromised data and to seek advice from the EDPS.

67 The controller should inform the EDPS if it does not yet have all the required information and will provide more details later on and agree on 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 EDPS.

68 For notification in phases the same notification form of Annex 1 may be used.

6. How to communicate a personal data breach to the data subject

69 Under Article 35 of the Regulation, 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.

70 Therefore, in this case, there is not a defined time limit for sending the communication but it shall be done without undue delay which means as soon as possible. However, considering the high risk, the prompt information will allow the person whose personal data was breached to take all the necessary precautions.

71 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.

72 The relevant breach should be communicated to the affected people directly, unless doing so would involve a disproportionate effort.

73 The communication shall contain the contact details of the DPO and describe in clear and plain language at least:

- the nature of the personal data breach;
- the likely consequences of the personal data breach[21];
- 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 on individuals.

74 The EUI 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.

75 The EUI shall communicate with the affected persons directly unless this would involve disproportionate effort (Art.35(c)). Examples of direct communication methods include email, SMS, direct message, postal communications.

76 There are exceptions to the obligation of the EUI to communicate a personal data breach to the data subject (Some practical examples of cases where communication to the data subject is not required can also be found in Annex 2):

- 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);

[21] Article 35 of the Regulation refers to likely consequences. The controllers may do well to consider not just likely consequences, but also possible consequences. When a data breach does not present a high risk to the data subjects because no consequence is not likely to occur (e.g. sensitive health data was encrypted with state-of-the-art encryption at the time of the breach), there is no need to inform the data subject. However, if the risk of consequences occurring later becomes more likely over time, the data subjects should be informed about the data breach. In this regard, see example 1 in Annex 2.

- 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.

77 In case individual communication would entail a disproportionate effort, (e.g. the contact details have been lost because of the data breach) the controller can inform the data subjects by public communication or similar measure whereby the data subjects are informed in an equally effective manner.

78 In accordance with the accountability principle, controllers have to be able to demonstrate to the EDPS that they meet one or more of the conditions stated above if they decide not to communicate a breach to the affected data subjects. 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.

79 If the EDPS determines that the decision not to inform data subjects about a personal data breach is not well founded, considering the likelihood of the personal data breach resulting in a high risk, it may order the controller to do so. Failure to comply with such an order may result in the application of enforcement measures.

7. How to document a personal data breach (Accountability and documentation requirements)

80 Article 34(6) of the Regulation sets out that the controller shall document all personal data breaches, including 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 the Regulation.

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

82 Accountability means that the controller shall be responsible for, and be able to demonstrate compliance with the other principles relating to processing of personal data. They include also integrity and confidentiality, which are undermined in case of data breaches. In other words, data shall be processed in a manner that ensures protection against unauthorised or unlawful processing and against accidental loss, destruction or damage, using appropriate technical or organisational measures.

The EUI 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.

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.

83 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.

84 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.

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.

Annex 1. Notification Template Form

EUROPEAN DATA PROTECTION SUPERVISOR

PERSONAL DATA BREACH NOTIFICATION FORM

(ARTICLE 34 OF THE REGULATION 2018/1725)

DATE: Click here to enter a date.

A. TYPE OF NOTIFICATION

A.1 COMPREHENSIVE[22] ☐

A.2 IN PHASES[23]: INITIAL:☐ FOLLOW-UP[24] ☐ CONCLUSIVE[25]☐

Reference Case File[26] : Click here to enter text.

A.3 REGISTRATION NUMBER[27] OF DATA BREACH IN YOUR REGISTER:

YES ☐ REG.NO: Click here to enter text.NO☐

B. DATA CONTROLLER EUI :

B.1 NAME OF THE ORGANIZATION (EUI): Click here to enter text.

B.2 ADDRESS: Click here to enter text.

B.3 CONTACT PERSON: Click here to enter text.

B.4 TELEPHONE: Click here to enter text. B.5 EMAIL: Click here to enter text.

B.6 DATA PROTECTION OFFICER Click here to enter text.

B.7 TELEPHONE: Click here to enter text. B.8 EMAIL: Click here to enter text.

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

C.1 NAME OF THE ORGANIZATION: Click here to enter text.

C.2 ADDRESS: Click here to enter text.

C.3 CONTACT PERSON: Click here to enter text.

C.4 TELEPHONE: Click here to enter text. C.5 EMAIL: Click here to enter text.

C.6 DATA PROTECTION OFFICER : Click here to enter text.

C.7 TELEPHONE: Click here to enter text. C.8 EMAIL: Click here to enter text.

---

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

D.4 DETECTION DATE[28]: TIME : Click here to enter text.

D.5 NOTIFICATION DATE[29]: Click here to enter a date. TIME : Click here to enter text.

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

D.7 WHO WAS INFORMED/ INVOLVED IN THE INCIDENT[30]: Click here to enter text.

D.8 CATEGORIES OF PERSONAL DATA AFFECTED[31] Click here to enter text.

D.9 APPROXIMATE NUMBER OF PERSONAL DATA AFFECTED Choose an item.:

Please Specify the exact number if possible: Click here to enter text.

D.10 CATEGORIES OF PERSONS AFFECTED[32]: Click here to enter text.

D.11 APPROXIMATE NUMBER OF PERSONS AFFECTED: Click here to enter text.

D.12 LIKELY or ACTUAL CONCEQUENCES OF THE DATA BREACH FOR THE DATA SUBJECTS: Click here to enter text.

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. Click here to enter text.

D.15 Have you informed the persons affected about the breach? YES[33] ☐ if yes, WHEN: Click here to enter a date.

NO☐, If no, explain why not (yet) Click here to enter text.

D.16 ACTION MEASURES TO ADDRESS THE RISK AND TO LIMIT ITS IMPACT[34]: Click here to enter text.

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

---

[28] Indicate the date when you become aware of the personal data breach.
[29] 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.
[30] Indicate the persons involved in the handling of the incident (internal and external) of the EU institution
[31] List all elements/fields of data that were compromised e.g. first and last names, date of birth, financial data, health data, etc.
[32] List all the categories of the data subjects affected, e.g. EU staff, , MEPs, European citizens, children, vulnerable groups such as handicapped people etc.
[33] If yes, attach a copy of the communication sent to the data subject
[34] 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. .

D.18 ROOT CAUSE OF THE DATA BREACH[35]: Click here to enter text.

[35] Explain the root cause of the security incident that lead to the data breach.

Annex 2. Practical Examples

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).

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.

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

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.

Annex 3. References and useful readings

Policy papers from EDPS, Article 29 Working Party:

1. **Opinion 03/2014 on Personal Data Breach Notification of the Article 29 Working Party**

   http://ec.europa.eu/newsroom/article29/news-overview.cfm

2. **Guidelines on Personal data breach notification under Regulation 2016/679 adopted on 3 October 2017, as last Revised and adopted on 6 February 2018, Article 29 Working Party**

   http://ec.europa.eu/newsroom/article29/item-detail.cfm?item_id=612052

Policy papers from other EU Data Protection Authorities,

1. **Ireland:**

   Personal Data Security Breach Code of Practice, 9 July 2011 https://www.dataprotection.ie/docs/Data_Security_Breach_Code_of_Practice/1082.htm

2. **UK:**

   a. Personal data breach reporting https://ico.org.uk/for-organisations/resources-and-support/getting-ready-for-the-gdpr-resources/pdb/

3. Guidance on data security breach management: https://ico.org.uk/media/for-organisations/documents/1562/guidance_on_data_security_breach_management.pdf **Italy**

   Data breach under GDPR

   http://www.garanteprivacy.it/regolamentoue/approccio-basato-sul-rischio-e-misure-di-accountability-responsabilizzazione-di-titolari-e-responsabili

Papers and references from the European Union Agency for Network and Information Security (ENISA):

4. **Recommendations for a methodology of the assessment of severity of personal data breaches**

   https://www.enisa.europa.eu/publications/dbn-severity

5. **Recommendations for technical implementation of Art.4**

   https://www.enisa.europa.eu/publications/art4_tech

6. **Personal data breach notification tool**

   https://www.enisa.europa.eu/topics/data-protection/personal-data-breaches/personal-data-breach-notification-tool

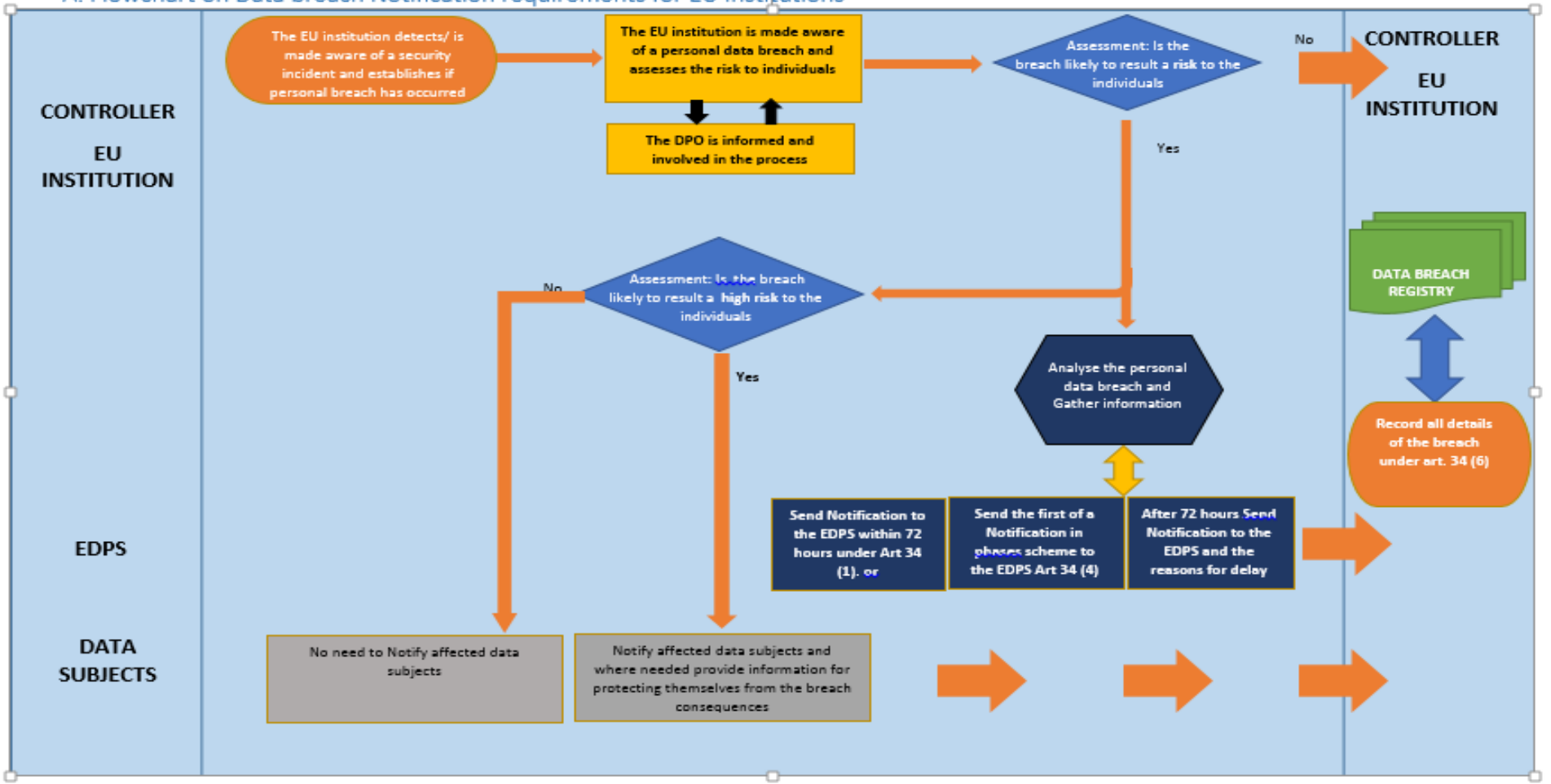
Annex 4. Glossary

Term	Description
Authentication	The process to ensure and confirm the identity of a user or a machine performing an operation (usually via an IT system)
Personal data	Any information relating to an identified or identifiable natural person ('data subject'); an identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person.
Personal data breach	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.
Special categories (of personal data)	Under the current Regulation those data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, trade-union membership, and of data concerning health or sex life. The proposal for a new Regulation adds genetic data and biometric data for the purpose of uniquely identifying a natural person. These categories are subject to specific rules.
Controller	Community institution or body, the Directorate-General, the unit or any other organisational entity which alone or jointly with others determines the purposes and means of the processing of personal data.
Processor	Natural or legal person, public authority, agency or any other body which processes personal data on behalf of the controller.
Sub-processor	Natural or legal person, public authority, agency or any other body which processes personal data on behalf of a processor.
Data Protection Officer (DPO)	Staff member of an organisation tasked with supporting the organisation in ensuring compliance with the applicable data protection law. Appointment, tasks and powers are defined in the Regulation (and the new Regulation). It might be external, or shared among different institutions.
Data subject	Individual whose personal data are processed.
Data Protection Impact Assessment (DPIA)	Assessment of risks to the rights and freedoms of natural persons due to the processing of their personal data. The new Regulation provides mandatory elements and circumstances under which it is obligatory.

	Nonetheless, controllers can carry out this assessment and obtain relevant benefits beyond those circumstances.
Risk	in a privacy context risk can be defined as the impacts of potential events on personal identifiable information principals' privacy and is characterized by its level of impact and its likelihood.
Risk assessment	Overall process of risk identification, risk analysis and risk evaluation
Information Security Risk Management (ISRM)	The risk management process for ensuring that the confidentiality, integrity and availability of an organisation's assets match the organisation's objectives.
Confidentiality	Property that information is not made available or disclosed to unauthorized individuals, entities, or processes
Integrity	Property of accuracy and completeness
Availability	Property of being accessible and usable upon demand by an authorized entity
(personal) Data breach notification	Mandatory notification of (personal) data breaches to the data protection authority
Level of risk	Magnitude of a risk expressed in terms of the combination of consequences and their likelihood

Annex 5. In a nutshell

A. Flowchart on Data breach Notification requirements for EU Institutions



Remember:

EDPS FUNCTIONAL MAILBOX FOR DATA BREACH NOTIFICATIONS

data-breach-notification@edps.europa.eu

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

While assessing each reported incident, it should be detected if personal data is affected.

If personal data is affected, the security incident will be considered as a personal data breach

Once the security incident is considered as a personal data breach, as the next step, it should be assessed what would be the impact of the incident on individuals; rights and freedoms.

An EUI shall introduce in its security incident management process a necessary step for checking in every reported security incident if personal data are involved to identify a personal data breach event that will trigger the data breach management process

An EUI shall implement its own personal data breach management procedure or set of policies that will focus on the impact assessment of every reported personal data breach and the selection of the adequate notification procedure towards the EDPS and the data subjects. Roles and responsibilities shall be clearly defined.

In cases where there is reported evidence that a recorded personal data breach creates no risk to the data subjects the controller will not need to notify the EDPS nor the data subjects. However, this decision should be well documented.

According to Art.34 of the Regulation, an EUI should notify a personal data breach not later than **72 hours** to the European Data Protection Supervisor, unless it is unlikely to result in a **risk** to the rights and freedoms of individuals.

In addition to that in Art.35 (1), in case the personal data breach result in a "**high risk"** to the rights and freedoms of individual, the EUI should also communicate it to the data subjects.

Severity of breaches will need to be assessed on a case-by-case basis. The "risk to the rights and freedoms of natural persons" should be taken as a basis for considerations.

The risks identified during a 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

An EUI should notify a personal data breach not later than 72 hours to the European Data Protection Supervisor, unless it is unlikely to result in a risk to the rights and freedoms of individuals. If the personal data breach result in a "high risk" to the rights and freedoms of individual, an EUI should also communicate it to data subjects.

If there is no backup of the data and services cannot be restored, this could be considered as a personal data breach.

If personal data are already publicly available, a release the same data by others is not going to be a risk to individuals and is not going to be considered as a personal data breach.

The EUI 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.