UNIVERSITÀ DI PARMA

2022

Data Breach Management Procedure

Guidelines for Data Breach Management and Notification under the European Union Regulation (EU) 2016/679 (GDPR)

ANNEX TO THE PRIVACY REGULATION

Automatically translated by DeepL

Summary

1. Purpose of the Document

The purpose of this document is to provide operational guidelines for the management of the Process for the analysis and identification of a possible Data Breach and the management of the possible notification of personal data breaches to the Privacy Guarantor and, if necessary/required, to the data subjects in accordance with the provisions of Regulation (EU) 2016/679 and in particular in accordance with the Guidelines WP250 adopted on 3 October 2017 and drafted by the Working Party of European Data Protection Supervisors, pursuant to the former Article 29 of European Directive 95/46[1].

2. Personal data breach notification under Regulation (EU) 2016/679

2.1 Data Breach and related obligations

Article 4 of Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 (henceforth also "GDPR") on the protection of individuals with regard to the processing of personal data and on the free movement of such data states that a personal data breach ("*Data Breach*") is "***a breach of security leading to accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data transmitted, stored or otherwise processed***".

The European *Data* Protection Supervisors' Working Group, in its WP250 guidelines, has made it clearer that *data breaches* can be classified into three macro-categories:

[1] WP 250 rev.01 - *Guidelines on Personal Data Breach Notification Under* Regulation *2016/679* (Working Party Document Art. 29 adopted on 6 February 2018). In addition, the following documents are suggested reading:

- Guidelines 01/2021 on Examples regarding Data Breach Notification published by the EDPB on 14/01/2021
- WP248. Guidelines concerning data protection impact assessment as well as criteria for determining whether a processing operation "is likely to present a high risk" under Regulation 2016/679 - adopted by the Article 29 Working Party on 4 April 2017
- Guidelines of the Agenzia per l'Italia Digitale - AgID 26 April 2016, *Guidelines for ICT Security of Public Administrations - Minimum ICT Security Measures for Public Administrations (Directive of the President of the Council of Ministers 1 August 2015).*
- European Commission, working party on the protection of individuals with regard to the processing of personal data set up by Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995, *Guidelines on Data Protection Officers ('DPOs') Adopted on 13 December 2016.*

1. *Confidentiality Breach*, when there is accidental or abusive access to Personal Data;
2. *Availability Breach*, when there is an accidental or unauthorised loss or destruction of personal data;
3. *integrity* breach *(Integrity Breach*), when there is an accidental or non authorisation of personal data

Some significant examples of *data breaches* are given that may be of use setting the context

Loss of an unencrypted *device*	Even the simple loss of a smartphone may constitute a valid reason for a *data breach* if it contains Personal Data due to its quantity and quality, and has not been properly encrypted. It can potentially constitute a loss of confidentiality and availability, if no other copies of the data exist.
Incorrect sending of an e-mail containing a file with identification and student contacts.	A potential example of loss of data confidentiality is when personal data is sent by mistake to an unauthorised third party.
Inadvertent deletion or modification of a file (e.g. a spreadsheet containing) large amounts of personal data without a backup or a back-up copy	An example of loss of availability (in the case of deletion) or loss of integrity (inadvertent modification) of data occurs when a piece of personal data is not adequately protected against modification and deletion and there is no regularly updated security copy. In practice, when using non-centralised and inadequately protected tools, one exposes oneself to the risk of data loss or the introduction of incorrect data.

See Section 5 for a more in-depth analysis of possible examples of *data breaches*.

2.2 Types of Data Breach

The events that can cause a *data breach* are thus grouped in Article 4(12) of the GDPR on the basis of the guidelines '*Recommendations for a methodology of the assessment of severity of personal data breaches*', December 2013 of the European Network and Information Security Agency (ENISA):

- *Unauthorised Access*: access to data by persons (internal or external) not entitled to it.
- ***Unavailability****, Loss*: temporary unavailability of data.
- Destruction: irreversible unavailability of data.
- *Transmission*: communication (accidental or intentional) of data to unauthorised third parties.
- *Alteration* or *Modification*: improper modification (accidental or intentional) of data.
- *Disclosure*: improper disclosure of confidential information.

2.3 Notification to the Personal Data Protection Authority (ex art. 33 GDPR)

The GDPR regulations, pursuant Article 33, also stipulated as one of the additional requirements for all organisations processing personal data, the obligation to notify the Personal Data Protection Authority a personal breach; the notification must meet the following requirements:

- describe the nature of the personal data breach including, where possible, the categories and approximate number of Data Subjects concerned;
- provide the name and contact details of the DPO or other contact point where more information can be obtained;
- describe the likely consequences of a personal data breach;
- describe the measures adopted or proposed to be adopted by the Data Controller to remedy the personal data breach and also, where appropriate, to mitigate its possible negative effects.

The notification must be made where possible within 72 hours and without 'undue delay', from when the *Data* Controller became aware of the *Data Breach*. Article 33(3) of the GDPR also clarifies that when it is not possible to provide all the information at the same time, the missing information may be sent at a later stage. Finally, it may also happen that the Data Controller

of the Data Processor notifies the loss of the availability of a particular medium to the Data Protection Authority, which subsequently finds it within its offices without it having been altered. In this case, it is sufficient to notify the Authority that the medium has been found and request that the notification procedure be cancelled.

2.4 Notification of Data Subjects (ex art. 34 GDPR)

In the event that the personal data breach is likely to present a high risk for the fundamental rights and freedoms of Data Subjects, the GDPR obliges the Data Controller to also communicate such breach to each Data Subject in order to enable him/her to take appropriate precautions to minimise the potential harm resulting from the breach of his/her personal data.

Notification of the *Data Breach* to the Data Subject must be made using plain and clear language and must contain an accurate description of the nature of the personal data breach, as well as suggestions and recommendations as to how the potential adverse effects resulting from the breach of his or her personal data may be mitigated. However, notification to the Data Subject may be waived if:

- the Data Controller had put in place appropriate technical and organisational protection measures and those measures had been applied to the Personal Data subject to the breach;
- the Data Controller has subsequently taken measures to prevent the occurrence of a high risk for the rights and freedoms of the Data Subjects;
- such a communication would require disproportionate efforts, in which case, a public communication or similar measure, by which the Data Subjects are informed with similar effectiveness, shall be carried out instead;
- the contents of the hacked communications are fully encrypted.

2.5 *Data Breach* Register

Pursuant to Article 33 of the GDPR, it is mandatory for the Data Controller to keep records of all *Data Breaches* that have occurred. *Data* Controllers are, therefore, required keep a record of *Data Breaches* that must be promptly updated and contain the following information:

- the details of the *Data Breach* (i.e. the cause, the place where it occurred and the type of Personal Data breached);
- the effects and consequences of the breach and the action plan prepared by the Controller. In addition to these aspects, the *Data* Controller should also justify the reason for the decisions taken as a result of the *Data Breach* with particular reference to the following cases:
- the Holder decided not to proceed with the notification;
- the Holder delayed in the notification procedure;
- the *Data* Controller has decided not to notify the *Data Breach* to the *Data* Subjects.

2.6 Key concepts

A **data** breach is a breach of security involving the destruction, loss, modification, unauthorised disclosure of or access to personal data transmitted, stored or otherwise processed	The notification **must be made within 72 hours,** and without 'undue delay', of the Holder becoming aware of the Data Breach. In cases of particular complexity, the Data Controller may provide further details of the Data Breach at a later date. ('prior notification').
In the event that the Data Breach is likely to present a high risk for the fundamental rights and freedoms of Data Subjects, the GDPR obliges **the Data Controller to notify such breach also to each Interested**	Pursuant to Article 33 of the GDPR, it is mandatory for the Data Controller to keep records of all *data breaches* through the **computer incident log**

3. Incident Response

The following describes the composition, competences and duties of the organisational resources that the University has designated for activities related to the identification, management and communication of *data breaches* under the GDPR.

3.1 *Incident Response Team (IRT)*

The team is in charge of managing the entire *data breach* procedure, which consists of the following steps:

1	Preliminary analysis of the event
2	Classification of the event according its scope
3	Entry of the incident in the computer incident register
4	Assessment of the actual risk to the rights and freedoms of natural persons
5	Activation of measures to remedy or mitigate the impact of the breach
6	Drafting of notification to the Data Protection Authority
7	Possible drafting of the notification to interested parties
8	Managing the Remedial Plan

Taking into account the purpose, type of users and organisational set-up, three are identified homogeneous operational areas according to which to classify a *Data Breach*[2]:

- Management and Administration domain: to this domain belong data with main purposes relating to the management and administrative activities of the University.
- Research Area: data with main research purposes belong to this area.
- Didactics Area: to this area belong data aimed at the provision of the university's teaching activities.

3.2 Incident Response Team (IRT) composition

The Incident Response Team (IRT) is composed of members, with differentiated profiles, and its purpose is to manage *data breaches* from an organisational, legal and technical point of view, as well as to identify, manage and communicate in an effective and timely manner any incident that may constitute a *data breach.* This *Team* is usually composed of the following actors, or their delegates:

Data Protection Officer
Privacy Team Coordinator
Legal Privacy Team Member
Privacy Team members identified by the co-ordinator on the basis of of the structures involved

[2] This subdivision is analogous to what is usually implemented, in academic circles, regarding the application of the Minimum Information Security Measures for Public Administrations pursuant to Circular No. 2 of 18 April 2017 of the Agenzia per l'Italia Digitale - AgID.

Digital Transition Manager / ASI Manager[3]
IT Security Service Manager or his delegate

If necessary, *the Incident Response Team* may avail itself of the cooperation of the heads of the Structures, Departments and/or Organisational Units involved in the incident or whose involvement is useful for analysing, identifying and managing the incident. Where the breach has occurred on computer systems managed by third specifically appointed pursuant to Article 28 of the GDPR, the *Team* shall involve such parties to the extent provided by the deed of appointment as external manager entered into with such suppliers.

3.3 Roles and responsibilities

A matrix is adopted to relate resources to the activities for which they are responsible, or to their aggregations. The RACI-type matrix specifies the type of relationship between the resource and the activity. It indicates 'who does what' within an organisation. Resources are distinguished into:

- ***Responsible,* (*Responsible, R*)**: is the one who performs and assigns the activity
- ***Accountable (A*)**: This is the person who has responsibility for the outcome of the activity. Unlike the other 3 roles, he/she must be uniquely assigned for each activity.
- **Collaborator *(Consulted, C*)** is the person who helps and collaborates with the Manager (R) to the execution of the activity.
- Informed **(**Informed***, I*)** is the one who must be informed when the activity is performed.

[3] If the figures do not coincide

ID	Activity Name	RACI				Time of execution	
		R	A	C	I	Start	Term
A1	Preliminary Event Analysis	UP TSI	Dir. ASI	S.IT		Event knowledge	8h
A2	Event Classification	S.IT	S.IT	UP TSI	Responsible concerned	8h	12h
A3	Possible entry of the incident in the register of computer incidents	S.IT	S.IT			12h	20h
A4	Assessment of the actual risk to the rights and freedoms of the natural persons	Privacy Team	DPO		Rector/DG	20h	36h
A5	Activation of measures to remedy or mitigate the impact of the violation	S.IT	Dir. ASI	UP TSI	DG	36h	50h
A6	Possible drafting of the notification to the Garante per la Protezione Personal Data	Privacy Team	Rector	DPO	Rector/DG	50h	60h
A7	Possible transmission of the notification to the Data Protection Authority	Rector or his delegate	Rector or his delegate	DPO	Privacy Team	After the editorial staff	72h
A8	Possible drafting of the notification to interested parties	Privacy Team	Rector	DPO		72h	By 7 days

A9	Managing the Remedial Plan	S.IT	Dir. ASI	UP TSI	DG	After the notification	End of activity
A10	Entry in the databreach register	Privacy Team	Rector		DPO	End of analysis	Closure of the databreach

Legend

Abbreviation	**Acronym**
DPO	Data Protection Officer
Dir. ASI	Information Systems Area Manager
Privacy Team	Group to support the DPO/RPD and liaise with the various branches of the organisation as defined in Article 7 of the Data Protection Regulation (Regulation Privacy).
S.IT	ASI Area - IT Security Organisational Unit
UP	ASI Area - User Support Organisational Unit
TSI	ASI Area - Systems Technology and Infrastructure Organisational Unit

3.4 Key concepts

The *Incident Response Team* is responsible for manage the entire *data breach* procedure	The *Incident Response Team* consists of members with profiles differentiated profiles of type managerial, legal and technical
The RACI matrix has the task of relating resources to the activities for which they are responsible, or to their aggregations	Where the breach has occurred on computer systems operated by third parties specifically appointed pursuant to Article 28 of the GDPR, the *Team* shall involve such parties to the extent provided for in the deed of appointment.

4. *Data Breach* Notification Procedure

A *Data Breach* notification procedure is initiated whenever a Data Controller, a Data Controller, an External Data Processor, a Data Authorised Person, a Data Subject, identifies or is informed of a security breach that may result in the accidental or unlawful destruction, loss, modification, unauthorised disclosure of or access to personal data transmitted, stored or otherwise processed (*Data Breach*).

The procedure must be started without delay and completed as soon as possible. Whenever the procedure is initiated, a record of the event must be made in the University's *Data Breach* Register.

4.1 The *Data Breach* Reporting Form

The report of a potential *Data Breach* incident is normally made by writing to the e-mail boxdatabreach@unipr.it set up by the University for this purpose using the specific form that can be downloaded from the University website at https://www.unipr.it/privacy-databreach. Below are the questions that need to be answered for the correct qualification and quantification of the *Data Breach*:

1	Contact details of the reporting party:
2	When did the violation occur or did you become aware of it?
3	Incident Classification
4	Possible causes of the breach of one's credentials:
5	Did you take any action to limit the damage and if so, what?
6	Type of data involved
7	Categories of data involved
8	Type of data breach

4.2 Assessing the seriousness of the personal data breach

The *Incident Response Team* must promptly assess the level of seriousness of a personal data breach with respect to the rights and freedoms of data . One of the suggested methodologies to make such an assessment is the one proposed by ENISA[4].

The methodology defines quantitative criteria for the owner to arrive at a

overall assessment of the impact of the personal data breach.

In particular, the Controller will apply the methodology on the basis of the information in its possession, gathered during the early stages of the investigation of an incident.

It may be necessary to carry out several assessments at different times, depending on the information gathered during the subsequent phases. Normally at least two assessments will have to be carried out, consistent with the two-step assessment used in breach management and recommended by ENISA, unless the first step already allows for a comprehensive investigation of the incident[5]. The methodology may not cover all possible specific cases: these will have to be treated with particular care and attention.

The main parameters to be taken into account when assessing the impact of a

violation of personal data are as follows:

[4] European Network and Information Security Agency (ENISA), 'Recommendations for a methodology of the assessment of severity personal data breaches', December 2013. https://www.enisa.europa.eu/publications/dbn-severity/at_download/fullReport.

[5] European Network and Information Security Agency (ENISA), 'Recommendations on technical implementation guidelines of Article 4', April 2012. https://www.enisa.europa.eu/publications/art4_tech/at_download/fullReport

- the Data Processing Context **(DPC**): takes into account the nature of the data subject to the breach, together with other factors relating to the general context of the data processing.
- **Ease** of Identification (**EI**): an estimate of how easy it is to identify the data subjects from the breached data.
- the Circumstances of breach (**CB)**: takes into account the specific circumstances of the breach, relating to its type, including the loss data security and any related malicious intent.

The DPC is the key part of the methodology and assesses the criticality of a certain set of data in a specific processing context. To calculate this parameter, it is necessary to identify the types of personal data subject to the breach, classifying them in at least one of the following four categories:

- **Simple**: by way of example, this could be biographical data, contact details, data on educational qualifications and training, information on family life, professional experience **(1 point)**.
- **Behavioural**: data on personal preferences and habits, geolocation data or traffic data **(2 points)**.
- Financial: any type of financial data (e.g. income, financial transactions, bank statements, investments, credit cards, receipts, etc.), including financial information related to social security **(3 points)**.
- **Particulars**: any kind of particular data (e.g. health, political affiliation, sexual life, etc.) **(4 points)**.

The DPC may increase the score according to the possibility of deriving further information from the violated data. Annex 1 of the above-mentioned ENISA document gives more detailed guidance for calculating the score. Just consider that authentication credentials not considered as specific category and must be considered according to the types data processed in the systems to which they give access.

After classifying the data and assigning a score, it is necessary to increase or decrease it according to the value of factors contextual to the data processing. Aggravating factors are: the quantity of the data, special characteristics of the data controller or data subjects. Mitigating factors are: the invalidity or inaccuracy of the data, the public availability of the data prior to the breach, and the nature of the data.

EI is a corrective factor of DPC. The overall criticality of the treatment can be reduced according to the EI value: the lower the EI, the lower the value associated with the overall criticality. For the purposes of this methodology, four levels of EI are defined, with a linear increase in the score:

- Negligible **(0.25 points)**.
- Limited **(0.50 points)**.
- Significant **(0.75 points)**.
- Maximum **(1 point)**.

The lowest score is assigned when the possibility identifying data subjects is negligible, while the highest score is selected when identification is possible directly from the data breached, without any special research or processing being required to discover the identity of the data subjects. When defining the EI value, consideration must be given to all means that are reasonably likely to be used by any person to identify the data subjects, including, for example, information that is publicly available, held or obtained in any way, including information found through the Internet, as well as by cross-referencing data from other sources that may be accessed by the Data Controller or third parties.

The multiplication of the values of EI and DPC provides the initial value of the severity **(SE**) of the violation.

The **CB** value defines specific circumstances of the violation that may or may not be present. Specifically, the factors to be taken into account are:

- **Loss of confidentiality**: occurs when information is accessed by parties who are not authorised or do not have a legitimate reason to access it. The extent of the loss confidentiality may vary depending on the scope of disclosure (e.g. the potential number of subjects who may have illegally accessed the information) **(0 to 0.5 points)**.
- **Loss of integrity**: occurs when the original information has been altered and the replacement of the data may harm the data . The most serious situation occurs when there is a serious possibility that the altered data has been used in such a way as to cause harm to data subjects **(0 to 0.5 points)**.
- **Loss of availability**: occurs when the original data cannot be accessed when needed. It may be either temporary (data can be recovered, but after a period of time that may be detrimental to those concerned) or permanent (data cannot be recovered at all) **(0 to 0.5 points)**.
- **Malicious** behaviour: this element assesses whether the breach was due to an error, human or technical, or whether it was caused by a deliberate action due to malicious behaviour. Malicious behaviour is a factor that may increase the likelihood of data being used with a harmful intent for data subjects, this being the original purpose of the breach **(0 to 0.5 points)**.

With regard to the estimation of the CB value, unlike DPC and EI where the highest score obtained is chosen, the points obtained from each element are added together to obtain the final score, as different circumstances may arise within the same violation.

The value of **CB** is added to the calculated initial value of the severity of the violation, defining the final value of **SE**.

The final value of the **SE** gravity of the violation can be calculated using the following formula:

SE= DPC X EI+ CB

The result will fall into a certain range that corresponds to one of four possible severity levels: **low (if the score is below or equal to 2)**, **medium (if the score is between 2 and 3)**, **high (if the score is between 3 and 4)**, **very high (if the score is above 4)**.

At the end of the calculation, other possible relevant elements will have to be taken into account, such as: (i) a number of persons affected by the infringement exceeding 100 and (ii) the non-decipherability of the data. Obviously in the first case, the score can only increase, whereas in the second case, the score can only decrease based on the specificity of the case under analysis.

4.3 Compilation of the notification

After completing the preliminary analysis on the actual risk for the rights of the interested parties and after starting the entry of the event in the register of computer incidents, where the results of the analysis described in the previous paragraph do not give a score lower than 3, the following procedure of *Data Breach* notification must be started without delay within the timeframe indicated by the legislation (72 hours from the knowledge of the *Breach*) according to the model published on the Authority's website.

Below are the questions that must be answered in order to correctly complete the notification. For each question, brief operational indications will be given and, where present, the guidelines of the Article 29 Working Party and of the Italian Data Protection Authority to which reference should be made in the event of interpretation doubts.

1	**Name of the bank(s) affected by the *data breach* and brief description of the violation of personal data processed therein**
In response to this first question, a brief description of the incident that occurred must be provided, indicating the databases that were breached. It may be that the type of incident has a particularly high degree of complexity. In this regard, please note that pursuant to Article 33(4) of the GDPR, 'if and to the extent that it is not possible to provide the information at the same time, the information may be provided at later stages without further unjustified delay'.	

From an operational point of view, the possibility of involving an IT consultant in certain particularly complex cases, which could also have a criminal relevance, must be carefully assessed in order to ensure the acquisition, in compliance with the *best practices* of the digital *forensics*, suitable digital evidence to prove the data breach occurred.

2	**When did the personal data breach occur?**

The Working Party considers that the controller should be considered to be 'aware' when it is reasonably certain that a security incident has occurred that has led to the compromise of personal data. However, recital 87 of the GDPR makes it clear that the data controller is obliged to take the necessary steps to ensure that it becomes 'aware' of any breach in a timely manner so that it can take appropriate measures. For this reason, if a breach is notified after the prescribed 72 hours, it is important to clarify the reasons why it was not possible to become aware of it earlier.

The Article 29 Party provided four useful examples to understand when the holder of the treatment may be deemed to have become aware of the reported violation:

1. In the event of the loss of a USB key containing unencrypted personal data, it is often not possible to ascertain whether unauthorised persons have had access to the data. However, even if the data controller is unable to establish whether a breach of confidentiality has occurred, such a case must be notified, as there is a reasonable certainty that a breach of availability has occurred; the data controller is deemed to have become 'aware' of the breach at the moment it realised it had lost the USB key.

2. A third party informs the data controller that it has accidentally received the personal data of one of its customers and provides evidence of the unauthorised disclosure. Since the data controller was presented with clear evidence of a breach of confidentiality, there is no doubt that he had 'knowledge' of it.

3. A data controller detects that has been a possible intrusion into its network. It then checks its systems to determine whether any personal data on them have been compromised and obtains confirmation of this. Again, since the data controller has clear evidence of a breach, there can be no doubt that it had 'knowledge' of it.

4. A cybercriminal breaches the data controller's system and contacts him to request a ransom. In that case, after checking his system to ascertain the attack, the owner of the

treatment has clear evidence that a breach has occurred and there is no doubt that it has become aware.	
3	**Where did the data breach occur? (Specify whether it occurred result of lost devices or portable media)**
In some cases, it is particularly complex to determine where the breach occurred. For instance, when there is an accidental or abusive access to personal data (confidentiality *breach*) that occurred on cloud servers, or when it has not been possible to identify how the potential loss of confidentiality of credentials occurred, it becomes difficult to identify the device that was breached. In such cases, it is necessary to crystallise, in accordance with the *best practices* of digital *forensics*, the digital evidence in order to be able to provide all the elements needed to reconstruct what happened, should the Data Protection Authority request further clarification following the violation. In the event of loss of devices or portable media, however, please note that it is necessary to report the fact to the judicial authorities and, where technically possible, to remotely erase the data on the device.	
4	**Modes of risk exposure** ***- Type of Infringement and Device Infringed***
The types of breach can be the following: reading, copying, alteration, deletion, theft. While determining whether there has been a breach of confidentiality or integrity is relatively obvious, it may be less obvious to determine whether there has been a breach of availability. A breach will always be considered a breach of availability if there has been a permanent loss or destruction of personal data. The Article 29 Working Party gives two examples that may be helpful in assessing type of breach. In the first, loss of availability may occur when data are deleted accidentally or by an unauthorised person, or, in the case securely encrypted data, when the decryption key is lost. If the data controller is unable to restore	

access to the data, e.g. by using a backup, the loss of availability will be considered permanent. In the second example, loss of availability may also occur in the event of a significant interruption of an organisations usual service, e.g. a power failure or *denial of service* attack that renders personal data unavailable. Finally, it should be noted that, although a loss of availability of the data controller's systems may only be temporary and may not impact individuals, it is important for the data controller to consider all possible consequences of the breach, as the breach may still need to be reported for other reasons. For instance, a ransomware infection (malicious software that encrypts the data of the data controller until a ransom is paid) might result in a temporary loss of availability if the data can be restored from a backup. However, a network intrusion has still occurred and notification may be required if the incident qualifies as a breach of confidentiality (e.g. if the attacker had access to personal data) and this presents a risk to the rights and freedoms of natural persons. Regarding the indication of the device subject to the breach, the considerations made above regarding location apply. It is not always possible to identify the device that is the object of the breach, but it is certainly appropriate to demonstrate that a breach management system of the efficient and purposeful personal data.	
5	**Brief description of the data processing or storage systems involved, including their location**
This question may generate quite a few problems in the event that the breach is due to a cyber attack on a particularly large number of devices. In such a case, the summary description could be made by categories of processing or storage systems involved. In particularly complex cases, please note the possibility of notification by 'stages' within meaning of Article 33(4) of the GDPR.	
6	**How many people have been affected by the breach of personal data processed within the framework of** **of the database?**

The Article 29 Working Party clarifies that the lack of availability of precise information (e.g. the exact number of data subjects involved) should not be an obstacle to timely notification breaches. The regulation allows for approximations on the number affected individuals and personal data records involved. Care should be taken to address the negative effects of the breach rather than to provide exact figures. Accordingly, when it is clear that there has been a breach but it is not yet known the

scope, a safe way to meet the notification requirements is to notify in 'stages'.

7	**What kind of data are breached?**

Data that could be subject to a breach may be common data or fall under the special categories of data listed in the personal data breach notification form. The GDPR does not define categories of data subjects or personal data records. However, the Article 29 Working Party suggests indicating the categories of personal data records that the data controller may process, such as health data, educational records, social welfare information, financial details, bank account numbers, passport numbers, etc.

Recital 85 makes clear that one of the purposes of notification is to limit harm to individuals. Accordingly, if the types of data subjects or personal data reveal a particular risk of harm as a result of a breach (e.g. identity theft, fraud, financial loss, threat to professional secrecy), it is important that the notification should indicate these categories. In this way, the obligation to describe the categories is linked to the obligation to describe the likely

consequences of the violation.

8	**Level of seriousness of the breach of personal data processed within the database (as assessed by the owner)**

Recitals 75 and 76 of the GDPR well summarise the concept of risk by clarifying that 'risks to the rights and freedoms of natural persons, varying in likelihood and severity, may arise from the processing of personal data that is likely to cause physical, material or immaterial harm, in particular: if the processing is likely to result in discrimination, identity theft usurpation,

financial losses, damage to reputation, loss of confidentiality of protected personal data

by professional secrecy, unauthorised decryption of pseudonymisation, or any other significant economic or social harm; if data subjects are at risk of being deprived of their rights and freedoms or are prevented from exercising control over the personal data concerning them; if personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefstrade union membership, as well as genetic data, data concerning health or data concerning sex life or criminal convictions and offences or related security measures are processed where personal aspects are assessed, in particular by analysing or predicting aspects of a person's professional performance, economic situation, health, personal preferences or interests, reliability or behaviour, location or movements, with a view to creating or using personal profiles; where personal data of vulnerable natural persons, in particular minors, are processed; where the processing involves a substantial amount of personal data and a large number of data subjects'. On the basis of these parameters, it is possible to judge the level of risk as low/negligible, medium, medium-high and high:

- Type of violation
- Nature, sensitivity and volume of personal data
- Easy identification of natural persons
- Severity of consequences for individuals
- Special characteristics of the person concerned
- Special characteristics of the data controller
- Number of natural persons concerned

The WP29 Guidelines on Data Breach make it clear that, in assessing the risk that might result from a breach, the data controller should consider not only the severity of the potential impact on the rights and freedoms of natural persons, but also the likelihood of such impact occurring. Clearly, if the consequences of a breach are more serious, the risk is higher; similarly, if the likelihood of such consequences occurring is greater, so is the risk.

Section 4.2 describes the methodology used by ENISA for risk assessment.

8	**Technical and organisational measures applied to breached data**

This question must be answered listing the technical and organisational measures existing at the time of the violation.

The GDPR clearly requires that, by means of appropriate technical and organisational measures, personal data be processed in a manner that ensures adequate security of personal data, including protection against unauthorised or unlawful processing and accidental loss, destruction or damage.

Accordingly, both the controller and the processor are required to have in place appropriate technical and organisational measures to ensure a level of security appropriate to the risk to which the personal data processed are exposed. These should take into account: the state of the art and the costs of implementation; the nature, subject matter, context and purposes of the processing; the risk of varying degrees of likelihood and severity to the rights and freedoms of natural persons (Art. 33(1)).

9	**Was the breach also communicated to those concerned?**

The controller must bear in mind that notification to the supervisory authority is mandatory unless the rights and freedoms of natural persons are unlikely to be affected by the breach. Moreover, where the breach presents a high risk for the rights and freedoms of natural persons, the latter must also be informed. The threshold for communicating breaches to natural persons is therefore higher than for notifying the supervisory authorities, so not all breaches will have to be communicated to the data subjects, which protects them from unnecessary inconvenience caused by notification.

The regulation states that the communication of a breach to data subjects should take place 'without undue delay', which means as soon as possible. The main objective of the communication to data subjects is to provide them with specific information on the measures they can take to protect themselves. As noted above, depending on the nature of the breach and the risk presented, timely communication will help individuals take steps to protect themselves from any negative consequences of the breach.

It is recalled that the GPDR in Art. 34(3) states that the communication to the data subject referred to in paragraph 1 is not required if one of the following conditions is met:

(a) the data controller has implemented appropriate technical and organisational measures to protection and these measures had been applied to the personal data subject to the breach, in

particularly those designed to make personal data unintelligible to anyone not authorised to access them, such as encryption;

b) the controller has subsequently taken appropriate measures to prevent the occurrence of a high risk for the rights and freedoms of the data subjects referred to in paragraph 1;

c) such communication would require disproportionate efforts. In that case, a public notice or a similar measure, by the persons concerned are informed similar effectiveness, is used instead.

Paragraph 5 of these guidelines provides a non-exhaustive list of examples of cases in which a breach may present a high risk for natural persons and, consequently, in which the

data controller must communicate it to the data subjects.

10	**What is the content of the communication made to the interested parties?**

The data controller must provide in an absolutely simple and clear manner at least the following information:

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

As an example of measures taken to address the breach and mitigate its possible negative effects, the data controller may state that, after notifying the breach to the relevant supervisory authority, it has received advice on managing the breach and mitigating its impact. Where appropriate, the data controller should also provide specific advice to individuals on how to protect themselves from the possible negative consequences of the breach, for example by resetting passwords in case compromised access credentials. Again, the data controller may choose to provide additional information beyond what is required here.

Dedicated messages must be used when communicating a breach to those concerned that do not must be sent together with other information, such as regular updates, newsletters or

standard messages. This contributes to clear and transparent breach communication.

Examples of transparent methods of communication are: direct messaging (e.g. e-mail, SMS, direct message), banners or notifications on prominent websites, postal communications and prominent advertisements in the press. A simple communication within a press release or a corporate blog would not constitute an effective means of communicating a breach to the data subject, except in the residual cases provided for in Article 34(3). The Working Party recommends that the data controller choose a medium that maximises the possibility of properly communicating the information to all data subjects. Depending on the circumstances, this could mean that the data controller should

use several communication methods instead of a single contact channel.

11	**What technological and organisational measures have been taken to contain the data breach and prevent similar future breaches?**

This question is certainly one of the most important and needs an answer that is certainly concise but very effective. It is clear that once a breach has occurred, the so-called 'remedial plan' is essential to ensure the protection of those affected by it. In this respect, we suggest proposing a plan based on three parameters that are well known in the IT security sector: training (*'people'*), procedures and processes (*'process'*) and technology (*'techonology'*). The fact that the implementation of technological measures is placed in third place is no coincidence: in facttechnological security measures may be partially useful if people do not comply with the rules laid down in the procedures or if these rules are not even present. For this reason, knowledge of, compliance with and constant updating of the University's regulations on corporate IT resources is of paramount importance.

Finally, it should be noted that, as part of the notification to the supervisory authority, the data controller may consider it useful to indicate the name of the data controller if the latter is the underlying cause of the breach, in particular if the breach caused an incident to the personal data records of several other data controllers that

have recourse to the same controller.

5. Examples of Data Breach

In order to better contextualise the recognition of *data breaches* in the University, some cases are proposed below as examples but not exhaustive based on those proposed by the Working Party of European Data Protection Supervisors, to former Article 29 of European Directive 95/46:

Data Breach **typology**	**Example**	**Notification required the Privacy Guarantor?**	**Needs Notification to interested?**	**Notes**
Confidentiality Breach	Theft or loss of a USB stick or Notebook or Tablet or Smartphone or Hard Disk on which unencrypted data or data encrypted with algorithms that are not state-of-the-art are stored. of art	SI	YES if the nature of the data and the severity of the theft can have important consequences for the interested	
Confidentiality Breach	Theft or loss of USB stick or Notebook or Tablet or Smartphone or Hard Disk on which encrypted data is stored with state-of-the-art algorithms	NO	NO	It does not have to be notified, but must be entered in the register of Data Breach
Confidentiality Breach	A computer application suffers cyber attack in which attackers have gained access to data personal and there is a reasonable suspicion that have consulted and/or stolen them (examples	SI	YES if the nature of the data and the severity of the theft can have important consequences for the interested	

	of applications: Document Management, Student Career Management*, Ugov Human Resources* Management, Right to Study Management, Library Loan Management, Electronic Mail Service *Office 365*, etc.)			
Availability Breach	Temporary unavailability of a server, application or network connectivity (e.g. due to power failure) electrical, equipment failure)	NO	NO	It does not have to be notified, but must be entered in the register of Data Breach
Confidentiality Breach/ *Availability Breach*	A workstation or server is compromised by ransomware and consequently data is encrypted, there is no data back-up and/or there is reasonable evidence that personal data may have been exfiltrated from the device	SI	YES if the nature of the data and the seriousness of the theft can have important consequences for the data subjects	
Confidentiality Breach/ *Availability Breach*	A workstation or server are compromised by ransomware and consequently the data are encrypted,	NO	NO	does not have to be notified, but must

	there is a BackUp of the data so that they can be restored within a reasonable timeframe and there is reasonable evidence that personal data have not been stolen from the device			entered in Data Breach Register
Confidentiality Breach	A holder of access credentials to computer systems that process personal data reports a loss of confidentiality of his credentials (e.g. by following up a Phishing message), and a quick investigation shows that the credentials have been used to access personal data with unrelated activities to the authorised user	SI	YES if the nature of the data and the seriousness of the theft can have important consequences for the data subjects	
Confidentiality Breach	As a result of a cyber attack, the credentials of users with access privileges to personal data were stolen; these credentials were stored on the server in unencrypted mode or encrypted with algorithms	SI	SI	

	not state-of-the-art or with mechanisms non-reversible encryption (hashing) not at the state of art.			
Confidentiality Breach	As a result of an error in the programming and configuration of a computer system or computer application, personal data were made accessible to persons not authorised to process them or other than Data Subjects, and a quick investigation revealed that access in violation of the above	SI	YES if the nature of the data and the seriousness of the theft can have important consequences for the data subjects	
Confidentiality Breach	Disclosure of personal data to wrong recipient (e.g. by sending to wrong email address)	SI	YES if the nature of the data and the severity of the theft can have important consequences for the interested	
Confidentiality Breach	Sending one or more messages to mailing lists with recipients' email addresses in clear in the 'A' or 'CC' field	YES if the event involves a large number of individuals	It depends on the aim and purpose of the mailing list	