Latest update: 23/12/2012

PROCEDURE FOR HANDLING PERSONAL DATA BREACHES

Abbreviations and acronyms

- *Data breach* = personal data breach
- *DPO* = Data protection officer
- *Privacy Authority* = Italian Personal Data Protection Authority
- *GDPR* = General Data Protection Regulation (EU Regulation 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of individuals with regard to the processing of personal data and on the free movement of such data and repealing Directive 95/46/EC)
- *RTD* = Digital Transition Manager.
- *Response Team* = support group for handling data breach reports, composed of the DPO, the RTD and their staff members previously assigned to monitor the address violazioni.dati@unipd.it and to assessing reports
- *University* = University of Padua

SCOPE AND RECIPIENTS

1. Data breach: definition and characteristics

A personal data breach is defined as "*a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data transmitted, stored or otherwise processed;* (GDPR Article 4(12)).

Accordingly, the breach reporting procedure only applies when a security incident also involves a breach of ***"personal"*** data, i.e. a breach that may compromise the University's ability to ensure compliance with the principles applicable to the processing of personal data, pursuant to Article 5 GDPR ("lawfulness, fairness and transparency", "purpose limitation", "data minimisation", "accuracy", "storage limitation", "integrity and confidentiality").

Three types of personal data breaches can be distinguished:

- **breach of confidentiality**, when there is an unauthorised or accidental disclosure of or access to personal data;
- **breach of integrity**, when an unauthorised or accidental alteration of personal data occurs;
- **breach of availability, even temporarily**, when there is an accidental or unauthorised loss, inaccessibility, or destruction of personal data.

2. Purpose and recipients of the personal data breach management procedure

This procedure is intended to ensure the University's ability to detect and mitigate the effects of a personal data breach in a **timely** manner, assess the risk to individuals, and determine whether it is necessary to notify the breach to the Privacy Authority and communicate it to the individuals concerned, pursuant to Articles 33 and 34 of the GDPR.

Failure to report a breach to an individual or supervisory authority may result in a sanction being imposed on the University under Article 83 of the GDPR.

Failure to comply with this procedure may result in disciplinary action against the offending employees or termination of existing contracts with defaulting third parties, under the relevant laws in force.

2.1. To whom are the reporting procedures addressed?

These procedures are addressed to all persons who, in any capacity, process personal data of which the University is the controller or processor under the GDPR:

a) *Internal recipients*: employees and contractors who for any reason, and therefore regardless of the type of contractual relationship, have access to personal data processed in the course of the services provided *by* or *on behalf of* the University;

b) *External parties:* any party (natural person or legal person) that, by reason of the contractual relationship in place with the University, has access to personal data regarding which the University is the Data Controller and acts as Data Processor (Article 28 GDPR) or as independent Data Controller.

2.2. What types of personal data does this procedure cover?

This procedure applies when the following personal data are breached:

a) personal data processed *by* and on *behalf* of the University, in any format (including paper documents) and by any means;

b) personal data stored or processed by means of any system or software in use at the University.

"Personal data" means: 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 (Art. 4(1) GDPR).

PROCEDURE FOR HANDLING PERSONAL DATA BREACHES

Within 72 hours of becoming aware of a personal data breach that poses a risk to the rights and freedoms of data subjects, the University is obliged to notify the Privacy Authority and, in the event of confirmed high level of risk, to inform the data subjects.

Information about the incident should be collected and transmitted as soon as possible to the address violazioni.dati@unipd.it.

If a detailed description of the incident is not available at the time of detection, it is still essential to **report the incident immediately** for an initial impact assessment, even with incomplete information. The impact assessment will be supplemented with information that is acquired as the investigation continues.

1. Internal procedure for detecting and reporting a potential breach

To ensure compliance with the response time imposed by the GDPR (72 hours), it is necessary to report any breach of personal data processed by the University to the response team (violazioni.dati@unipd.it) **immediately**, and in any case **no later than 8 hours after becoming aware** of a security incident.

If a detailed description of the security incident is not available at the time of detection, it is still essential to **report the incident immediately,** even with incomplete information.

It is advisable to report any type of security incident, even a minor one involving personal data, in order to assess the seriousness and consequences for the data subjects and to update the "Data Breach Log", which allows for a constant risk analysis and the introduction of appropriate prevention measures.

1.1. Detection of a security incident

Who	Anyone who becomes aware of it (authorised persons, staff, contractors, suppliers, data controller, external users, DPO)
To whom	Division Manager (manager, director of department or centre) Privacy Officer (SD [Department Chief Secretary], RTG [Head Technical Manager], office manager, sector manager, research project manager)
When	Immediately
How	By notifying the security incident to the Division Manager and the Privacy Officer, also by quick means (by phone, in person, by e-mail)

Any employee or contractor who, for any reason, has access to personal data processed "by" or "on behalf of" the University, must **immediately** identify any data breach (even if only suspected) which has affected his or her system or office and report it to the head of his or her division and the organisational privacy contact.

Any type of security incident, even a minor one, relating to personal data should be reported so that it can be managed and the seriousness and consequences for the data subjects can be assessed. This will enable the University to maintain an up-to-date incident log, which will allow constant risk analysis and the introduction of appropriate prevention measures.

If your desktop computer, laptop, hard disk, USB stick or other storage media is stolen or lost, you should report the incident immediately.

All incidents that are in any way related to personal data, such as theft of online information, accidental deletion of information, disclosure of information to third parties by mistake, should also be reported. This is the case even if there was no intentional behaviour behind it, but an accidental event.

A successful phishing attack, i.e. the provision or dissemination of credentials and technical data to a third party, should also be regarded as a data breach.

Examples of personal data breaches

In general, a personal data breach is any situation that may lead an unauthorised person to have knowledge or access to personal data. By way of example only, a personal data breach occurs in the following cases:

a) unauthorised disclosure of confidential data to unauthorised persons;
b) public disclosure of confidential data;
c) access or acquisition of data by unauthorised third parties;
d) accidentally sending e-mails containing personal or special data to the wrong recipient;
e) breach of physical security measures such as forcing open doors or windows of particular premises (machine rooms, backup tape stores, premises housing the server, archives, including paper archives, premises containing confidential information);
f) loss or theft of paper documents;
g) theft or loss of a computer or portable device, removable disk, usb pen drive, loss of computer devices containing personal data;
h) viruses or other attacks on the University's computer system or network;
i) deliberate alteration of personal data;
j) inability to access data due to accidental causes or external attacks, viruses, malware;
k) accidental loss or destruction of personal data or due to accident, adverse event, fire or other calamity.

1.2. Assessment of potential consequences and countermeasures

Who	Division Manager (manager, director of department or centre) Privacy Officer (SD [Department Chief Secretary], RTG [Head Technical Manager], office manager, sector manager, research project manager)
When	Immediately after receipt of an alert
How	Coordinating the collection of information, possibly with the support of the division's system administrators

As soon as a report is received, the Division Manager, via the privacy contact persons involved and, if necessary, with the support of the relevant system administrators, must:

a) coordinate the collection of information in the shortest possible time;
b) assess whether a "personal" data breach is involved;
c) order the adoption of countermeasures necessary to remedy the personal data breach and to mitigate its potential negative effects;
d) forward the template for reporting violations to violazioni.dati@unipd.it (see next paragraph).

1.3. Reporting to the Response Team (violazioni.dati@unipd.it)

Who	Division Manager (manager, director of department or centre) Privacy Officer (SD [Department Chief Secretary], RTG [Head Technical Manager], office manager, sector manager, research project manager)
To whom	Response team (DPO, RTD and staff)
When	Immediately and **no later than 8 hours** after learning of the event
How	By sending the "*Personal data breach notification form"* (Annex 1) to violazioni.dati@unipd.it

If the security incident has led to a breach of personal data, the division manager and the organisational privacy contact persons must promptly provide as much detailed information as possible on what has happened, by filling in the special **reporting form** published in the dedicated section of the University portal (**Annex 1**).

The completed form should be sent to the response team **within 8 working hours** of becoming aware of the event at violazioni.dati@unipd.it.

If a detailed description of the security incident is not available at the time of detection, it is still essential to **report the incident immediately,** even with incomplete information.

The most important information is:

A. type of data breached;
B. special (formerly sensitive) data that may have been breached;
C. number of data subjects involved;
D. minors who may be involved;
E. extension of the security incident;
F. time period of the incident;
G. security measures taken;
H. encryption or not of the data breached.

2. Management of the report by the response team

The Director General, upon the proposal of the DPO and the RTD, identifies a support group for the management of reports of data breaches called "response team" and consisting of the DPO, the RTD and their staff previously appointed to monitor the address violazioni.dati@unipd.it.

The response team, in cooperation with the reporting entities and the privacy officers and contact persons of the relevant divisions, proceeds without delay to

1. Assess the impact of the security incident
2. Identify potential countermeasures
3. Notify the Privacy Authority of the breach (if necessary)
4. Notify the data subjects of the breach (if necessary)
5. Update the personal data breach log

2.1. Security incident impact assessment

Who	DPO and response team, in cooperation with the division's privacy officer and contact persons

When	Immediately upon receipt of the alert
How	Assessing the **risk** [= severity *x* likelihood] of the impact of the breach on the rights of the data subjects, based on predetermined parameters

The University, through the DPO and the response team, in cooperation with those reporting and those affected by the security incident, assesses the impact of the personal data breach on the rights and freedoms of individuals, in order to establish the **risk** *[= severity x likelihood]* and the **consequent actions** it must take:

a) taking measures to remedy the personal data breach and mitigate its potential negative effects
b) notifying the breach to the Privacy Authority, unless a risk to the rights and freedoms of natural persons is unlikely;
c) informing data subjects if the risk is high *[severity x likelihood]*[n.]

The following table presents the main factors that should be considered when assessing the impact of a breach on the basis of the information gathered.

FACTORS TO BE CONSIDERED IN ASSESSING THE IMPACT OF THE BREACH	
Severity and likelihood	Assessment of the severity of the potential impact on the rights and freedoms of natural persons and the likelihood of this impact occurring
Type of breach	Disclosure, Destruction and Modification, Loss
Nature, sensitivity and volume of personal data	Special categories of data or combination of personal data, large amounts of personal data relating to many persons involved in the breach
Ease of identifying natural persons	Ease of identifying, directly or indirectly by matching with other information, specific natural persons on the basis of personal data compromised by the breach
Severity of consequences for individuals	Potential harm to natural persons that could result from the breach, including the categories of data subjects and personal data involved and the long-term consequences of the harm (identity theft, physical harm, psychological distress, image/reputation damage)
Special characteristics of the data controller	In the context of its official mission, the University is, in particular, the controller of personal data processed for research purposes
Special characteristics of the data subject	The breach involves in particular personal data of minors or other vulnerable natural persons
Number of natural persons involved	Number of natural persons involved in the breach

2.2. Adoption of countermeasures and corrective actions

Who	DPO and response team
When	At the same time as the impact assessment
How	in cooperation with the division manager, privacy officers and system administrators of the divisions involved

The response team, in cooperation with the manager, the privacy contact persons and system administrators of the divisions involved, identifies the measures that can be taken to remedy the personal data breach and to mitigate its potential negative effects.

The timely adoption of countermeasures **may reduce the risk** to the rights and freedoms of data subjects, making it no longer mandatory to notify the Privacy Authority or to inform data subjects (see next paragraphs).

2.3. Notification of the breach to the Privacy Authority (if necessary)

Who	Director General, after hearing the DPO
To whom	The Italian Personal Data Protection Authority
When	without undue delay → need to state reasons if notification is not made **within 72 hours of knowledge** of the breach
How	By sending the filled-in Data breach notification template to *protocollo@pec.gpdp.it*

If the personal data breach poses a **risk** to the rights and freedoms of natural persons, **the Director General, having consulted the DPO**, must send the completed and digitally signed form to the Privacy Authority by certified email to the address *protocollo@pec.gpdp.it*.

Notification to the Privacy Authority must be made by the data controller without undue delay and, where possible, **within 72 hours of becoming aware** of a breach, in the manner set out in Article 65 of Legislative Decree No. 82 of 7 March 2005 (on the "Digital Administration Code"), by means of the IT systems indicated on the Privacy Authority's official website. The subject of the message must contain the mandatory wording "NOTIFICA VIOLAZIONE DATI PERSONALI" [REPORT OF PERSONAL DATA BREACH] and, optionally, the name of the University.

In case of delay, it is necessary to give **reasons for the delay** that prevented a timely notification.

If a detailed description of the security incident is not available at the time of detection, it is still essential to **report the incident immediately,** even with incomplete information. The documentation will be supplemented at a later stage, in cooperation with the Privacy Authority.

The University shall notify the Privacy Authority of personal data breaches in the manner set out in Article 33 of the Regulation, also with reference to processing carried out for the purposes of prevention, investigation, detection and prosecution of offences or enforcement of criminal sanctions, unless such processing is carried out by the judicial authority in the exercise of its own judicial functions, as well as the judicial functions of the public prosecutor (Articles 26 and 37(6) of Legislative Decree No. 51/2018).

2.4. Communication to affected data subjects (if necessary)

Who	Data Protection Officer (DPO)
To whom	Natural persons whose personal data have been breached (data subjects)
When	Without undue delay
How	Either by contacting the data subjects directly or by communicating the breach and any consequences by means of a publication accessible to the categories of persons

	concerned

If the data breach presents a "**high" risk** to the rights and freedoms of natural persons, notification to the data subjects must be made without delay. Any delay in such notification must be justified.

The communication to the data subjects shall contain:

a) the name and contact details of the Data Protection Officer (DPO);
b) a description of the likely consequences of the personal data breach;
c) a description of the measures taken, or which the University intends to take, to remedy the personal data breach and to mitigate any adverse effects.

If reporting directly to the data subjects requires an effort deemed disproportionate, forms of public communication through the University's official channels may be used, provided that this method does not itself pose a risk to the protection of the personal data of the data subjects.

2.5. Log of personal data breaches

Irrespective of the assessment as to whether a personal data breach needs to be notified, the response team shall document all personal data breaches, pursuant to Article 33(5) GDPR, by noting them in the relevant Log (Annex 2).

The data breach log shall contain at the very least the following information:

1. date and time of the breach;
2. location of the violation (physical or virtual);
3. nature of the breach;
4. categories of data subjects involved;
5. categories of personal data breached;
6. effects of the breach;
7. countermeasures taken;
8. *whether* the breach has been notified to the Privacy Authority;
9. *whether* the breach has been notified to the data subjects;
10. justification of the conduct adopted (impact assessment).

The Data Breach Log is continuously updated by the response team coordinated by the DPO, and is made available to the *Italian Data Protection Authority*, should the latter explicitly request it.