DATA BREACH NOTIFICATION
Art. 33 of Regulation (EU) 679/2016 (GDPR)

FORM FOR INTERNAL REPORTING OF PERSONAL DATA BREACHES

To the response team
c/o General Management
University of Padua
violazioni.dati@unipd.it

Information of any security incident that may lead to the loss, modification, unauthorised disclosure or access to personal data processed by the University of Padua must be collected in this form and reported immediately (and in any case no later than 8 hours after becoming aware of it) to violazioni.dati@unipd.it.

However, it is essential to report the incident immediately for an initial assessment of the risk to the rights and freedoms of the data subjects, even with incomplete information, which will be then supplemented at a later stage.

SECTION A - DATA OF THE REPORTING PARTY

Name and surname of reporting party: ________________________________________________________________
Division or body: ________________________________________________________________________________
Phone: _______________________ Email: _____________________________________

SECTION B - SUMMARY INFORMATION ON THE INCIDENT/BREACH

B.1. Information on incident
Date and time of the incident (even approximate, if not known): _________________________
Date and time the division manager became aware of the incident: _________________________
Place of the incident: ____________________________________________________________________________
Means by which the division manager became aware of the incident:
______________________________________________________________________________________________

B.2. Brief description of the incident:
______________________________________________________________________________________________
______________________________________________________________________________________________

B.3. Scope of data processing involved:
☐ Administration
☐ Communication and marketing
☐ Research
☐ Teaching
☐ Third mission
☐ Other (e.g. medical health activity): ______________________________________________________________

B.4. Type of incident:
☐ Reading (data were accessed but not copied)
☐ Copy (data are still present on the University’s systems but were copied by the infringer)
☐ Alteration (data are present on the data controller's systems but have been altered)
☐ Deletion (data are no longer on the data controller’s systems but are not in the possession of the infringer)
☐ Theft (data are no longer on the data controller's systems but are presumably in the possession of the infringer)
☐ Unavailability (data present on the data controller's systems but unavailable for a certain period of time)
☐ Other: ______________________________________________________________

B.5. Cause of the incident:
☐ Intentional internal action
B.6. Categories of personal data affected by the incident:
- Personal details/tax code
- Contact data (e.g. email address, telephone number)
- Access and identification data (e.g. username, password, other)
- Economic and financial data (e.g. payments, credit card number, current account number)
- Data relating to the provision of electronic communication services (e.g. Internet traffic logs)
- Judicial data
- Profiling data
- Data on identification documents (e.g. identity card, passport, driving licence, National Services Card)
- Location data
- Personal data revealing racial and ethnic origin
- Personal data revealing political opinions
- Personal data revealing religious, philosophical or other beliefs
- Personal data revealing membership of parties, trade unions
- Data concerning sexual life and sexual orientation
- Health data
- Genetic data
- Biometric data
- Other: ____________________________________________________________________

B.7. Volume (even approximate) of personal data involved in the incident:
- Indicate the volume of personal data involved: ______________________________________
- Indicate an estimate of the personal data involved: ____________________________________
- The volume of personal data is not known

B.8. Categories of data subjects involved:
- Teaching and research staff
- Technical-administrative staff
- Students
- Patients
- Minors
- Persons with disabilities
- Vulnerable persons (e.g. victims of violence or abuse, refugees, asylum seekers)
- Other Users: ____________________________________________________________________

B.9. Number (even approximate) of data subjects involved in the incident:
- Indicate the number of data subjects involved: ______________________________________
- Please give an estimate of the number of data subjects involved: _____________________________
- The number is not known

B.10. The incident involves data subjects from other countries:
- Of the EEA\(^1\) (indicate which): ______________________________________________________
- Non-EEA members (indicate which): ____________________________________________________
- NO

SECTION C - DETAILED INFORMATION ON THE INCIDENT/BREACH

C.1 Detailed description of the security incident:

\(^1\) the European Economic Area (EEA) includes all member states of the European Union, as well as Iceland, Liechtenstein and Norway
C.2 Description of the categories of personal data affected by the incident:

______________________________________________________________________________________
______________________________________________________________________________________
______________________________________________________________________________________

C.3 Devices affected by the incident:
- Physical archive (paper document)
- Computer/Laptop
- Server
- Storage
- Network
- Mobile device (smartphone, tablet, etc.)
- File or part of a file
- Backup tool
- Other: ____________________________________________________________________

C.4 Location of equipment involved in the incident:

______________________________________________________________________________________
______________________________________________________________________________________
______________________________________________________________________________________

C.5 Description of the technical and organisational security measures in place at the time of the incident to ensure the security of the data, systems and IT infrastructure involved:

______________________________________________________________________________________
______________________________________________________________________________________
______________________________________________________________________________________

SECTION D - POTENTIAL CONSEQUENCES AND SEVERITY OF THE INCIDENT/BREACH

D.1 Potential consequences of the incident for data subjects:
In case of loss of confidentiality:
- The data have been disclosed outside the scope of the information notice or the relevant regulations
- The data can be correlated, without unreasonable effort, with other information about the data subjects
- The data may be used for purposes other than those intended, or in an unlawful manner
- Other: ____________________________________________________________________

In case of loss of integrity:
- Data have been changed and rendered inconsistent
- Data have been modified while maintaining consistency
- Other: ____________________________________________________________________

In case of loss of availability:
- Lack of access to services
- Malfunctioning and difficulty in using services
- Other: ____________________________________________________________________

D.2 Further considerations on potential consequences:
D.3 Description of the impact of the breach on the rights and freedoms of the data subjects:
- Loss of control of personal data
- Limitation of rights
- Discrimination
- Identity theft or misappropriation
- Fraud
- Financial losses
- Unauthorised decryption of pseudonymisation
- Reputational prejudice
- Loss of confidentiality of personal data protected by professional secrecy
- Knowledge by unauthorised third parties
- Any other significant financial or social damage: ____________________________

SECTION E - MEASURES TAKEN FOLLOWING THE INCIDENT/BREACH

E.1 Technical and organisational measures taken (or proposed to be taken) to remedy the breach and reduce its negative effects on the data subjects:
______________________________________________________________________________________
______________________________________________________________________________________
______________________________________________________________________________________

E.2 Technical and organisational measures taken (or proposed to be taken) to prevent similar future breaches:
______________________________________________________________________________________
______________________________________________________________________________________
______________________________________________________________________________________

SECTION F - FURTHER INFORMATION ON THE INCIDENT/BREACH

F.1 The incident has been notified to other supervisory authorities:
- YES (indicate which): _________________________________________________________
- NO

F.2 The incident has been reported to the judicial or police authorities:
- YES
- NO

F.3 Other information relevant to the assessment and management of the incident/breach:
______________________________________________________________________________________
______________________________________________________________________________________
______________________________________________________________________________________