DATA CLASSIFICATION POLICY

Approval
Date: **03/11/2021**
ASI Manager: **Dr Francesca Pruneti**
Digitally signed pursuant to Legislative Decree No. 82/2005

About the document		
Edited by: *O.U. IT Security* *Legal and Compliance Unit* *O.U. Programming and Management Control*	**Target audience:** *Users of the University of Parma and anyone who has to process data of the University of Parma*	**Document deposit:***www.unipr.it/regolamento- security-EN*

Automatically translated by DeepL

Summary

1. Purpose of the document

The purpose of this document is to provide a method for classifying the data processed by the University of Parma according to their value and criticality for the organisation, with aim of identifying the most appropriate protection measures.

2. Scope of application

The policy described in this document applies to any form of data, including paper documents and digital data stored on any type of medium, that are subject to processing by employees, collaborators of the University and/or persons or companies authorised to process them.

3. Classification of data types

The data processed are divided into:

1. Personal Data
2. Non-personal data

3.1 Personal Data

Personal data means any information that can be uniquely traced back to an identified or identifiable living person.

Different pieces of information that, when collected together, can lead to the identification of a particular person also constitute personal data. For example, an identifier such as a name, an identification number, location data, an online identifier, one or more features of physical, physiological, genetic, mental, economic, cultural or social identity.

Personal data that undergo **de-identification, encryption or pseudonymisation**, but which can be used to re-identify a person, remain personal data

Example of personal data:

- first and last name;
- home address;
- e-mail address as nome.cognome@azienda.com;
- identity card number;
- position data (e.g. the positioning function on a mobile phone);
- IP address;
- Cookie ID
- …

3.1.1 Special categories of personal data

Special categories of personal data are those revealing **racial or ethnic origin**, **political opinions**, **religious or philosophical beliefs**, or **trade union membership**, as well as **genetic data**, **biometric data** intended to uniquely identify a natural person, **data** a person's **health** or sexual life or **sexual orientation.**
Personal data relating **criminal convictions and offences** or related security measures are also to be regarded as special and may only be processed under the control of a public authority or if the processing authorised by Union or Member State law providing appropriate safeguards for the rights and freedoms of data subjects.

3.2 Non-personal data

Non-personal data are data that **do not identify or make a natural person identifiable.**
Examples of data that are not considered personal:

- registration number in the commercial register of a company;
- impersonal e-mail address such as info@azienda.com;
- irreversibly anonymised data;
- statistical data
- aggregated data
- patents
- business plans
- budgets
- …

Starting from these two categories, ten data types have been defined, each with a level of protection appropriate to risk associated with that data. The data types listed below are in order increasing importance in terms of impact in the event of loss of confidentiality, availability and data integrity.

The level of protection associated with each type of data can take one of these five values: low, medium, high, very high, critical. The protection levels, described in a later section, are defined by a set of tools, procedures and control systems appropriate to that level.

Type of data	Description	Level of protection	Example
Non-personal data type 1	These are non-personal data usually intended for public disclosure, especially through own or third-party web applications.	1 - Low	• Announcements, • information on the institution, • aggregated data, • maps, • …
Personal data type 1	This category includes personal data that, as a result of the transparency obligations applicable to the institution, are subject to publication on the University portal and other publicly accessible venues.	1 - Low	• First and last name of assignees o collaborators, • remuneration of senior figures, • …
Non-personal data type 2	This category includes data that are generally not publishable or accessible without a check on the identity of those consulting them. The loss of confidentiality, integrity or availability of this data could have a moderate negative impact on the company's mission in terms of security, reputation or financial viability.	2 - Medium	• Data of business processes, • teaching materials for registered students, • contents educational content for a fee, • …

Personal data type 2	This category includes personal data for which publication is not envisaged.	2 - Medium	• Identity papers, • private home address, • mobile phone number • …
Non-personal data type 3	This category includes data whose protection is required by law or industry regulations. The loss of confidentiality, integrity or availability of data or the system could have a significant negative impact on the company's mission in terms of security, reputation or financial standing.	3 - High	• Search results not yet published, • planning budget planning, • budgets, • corporate strategies, • intellectual property, • …
Special data (excluding those referring to later types)	These are personal data revealing racial and ethnic origin, religious, philosophical or other beliefs, political opinions, membership of parties, trade unions, associations or organisations of a religious, philosophical, political or trade-unionist character, as well as personal data revealing sexual orientation.	3 - High	• Trade union membership, • accession a university organisations, • …
Biometric data	Personal data obtained by specific technical processing relating to the physical, physiological or behavioural characteristics of a natural person that enable or confirm their unambiguous identification, such as facial image data or dactyloscopic data.	4 - Very high	• Face images, • fingerprints, • vocal timbre, • any physical element that can be read and interpreted by programmes automated recognition programmes, • …
Health Data	Personal data relating to the physical or mental health of a natural person, including the provision of health care services, which reveal information about that person's state of health.	4 - Very high	• Body temperature, • previous or ongoing pathologies, • medical reports, • …
Judicial data	Data that may reveal the existence of certain judicial measures subject to entry in the criminal record or the status of defendant or suspect. EU Regulation 2016/679 (Art. 10) includes in this notion data relating to criminal convictions and offences or to	4 - Very high	• Final criminal convictions, • parole, • the prohibition or obligation to stay, alternative measures to detention,

	related security measures. In particular, this category personal data disclosing the measures referred to in Article 3(1)(a) to (o) and (r) to (u) of Presidential Decree no. 313 of 14 November 2002 on criminal records, the register of offence-related administrative sanctions and related charges, or the status of accused person or person under investigation pursuant to Articles 60 and 61 of the Code of Criminal Procedure.		• …
Genetic data	Personal data relating to the hereditary or acquired genetic characteristics of a natural person which provide unambiguous information on the physiology of that natural person, and which result in particular from the analysis of a biological sample of natural person.	5 - Critical	• Genetic test results, • Pre-symptomatic test results o r predictive, • …

4. Levels of data protection

In order to protect data with appropriate security measures, protection levels have been defined in terms of IT tools, procedures and control systems.

Protection level 1 - Low

Tools
IT tools that meet the ICT Minimum Security Measures - minimum level
Web portals and applications without authentication and encryption of information in transit
Mobile media without encryption
Backup to personal devices

Protection level 2 - Medium

In addition to the measures provided for in the previous level of protection, the following measures are taken.

Tools
IT tools that meet the ICT Minimum Security Measures - standard level
Web portals and applications with authentication and encryption of information in transit (OneDrive, Sharepoint etc.)

Mobile media with encryption
Backup to University devices

Protection level 3 - High

In addition to the measures provided for in the previous level of protection, the following measures are taken.

Tools
IT tools that meet the ICT Minimum Security Measures - advanced level
Encrypted Athenaeum file server
Backup to centralised Athenaeum devices

Procedures
Data access only to an identified list of authorised persons

Protection level 4 - Very high

In addition to the measures provided for in the previous level of protection, the following measures are taken.

Tools
Applications with strong encryption algorithms for information in transit and encrypted databases
Operating systems installed and maintained according to CIS guidelines
E-mail systems with message encryption
The software used must have monthly vulnerability analyses and continuous updates

Protection level 5 - Critical

In addition to the measures provided for in the previous level of protection, the following measures are taken.

Tools
Certified ICT systems and applications for genetic data management

5. Data classification procedure

The data controller, or the contact person if one has been appointed (Art. 12 - University Regulation on the processing of personal data), completes a table for each set of data processing he has to manage. In the table, he lists the individual sets of data constituting the processing, labelling each of them with a name, then slashes with an "X" in correspondence with the correct type of data for that set. The level of protection to be applied to the entire processing corresponds to the highest level of protection of the data sets entered. For example, the office in charge of student reception and orientation has to handle a processing with three sets of data: the first is the master data of newly enrolled students with their personal contact details, the second is any cognitive or motor disabilities, and the third is any participation in student organisations of the university. The sets are labelled (Personal Details, Disabilities and Organisations) and then the data type corresponding to each set is chosen. Since the highest level of protection corresponds to the 'Disability' set, processing must be managed with the tools, procedures and control systems contained in protection level 4 - Very High.

Type of data	**Level of protection**	**Set 1: Master data**	**Set 2: Disability**	**Set 3: Organisations -**
Non-personal data - type 1	1 - Low			
Personal data - type 1	1 - Low			
Non-personal data - type 2	2 - Medium			
Personal data - type 2	2 - Medium	X		
Non-personal data - type 3	3 - High			
Special data	3 - High			X
Biometric data	4 - Very high			
Health data	4 - Very high		X	
Judicial data	4 - Very high			
Genetic data	5 - Critical			

6. References

List of documents used and useful resources for understanding or further study.

Name	Contents and addresses
EU Regulation 2016/679 (GDPR)	*https://www.garanteprivacy.it/web/guest/home/docweb/-/docweb-display/docweb/6264597*
"Personal Data Protection Code'. Legislative Decree No 196 of 30 June 2003	*https://www.garanteprivacy.it/web/guest/home/docweb/-/docweb-display/docweb/9042678*

Minimum Security Measures ICT	*https://www.agid.gov.it/it/sicurezza/misure-minime-sicurezza-ict*
University Regulation on processing of personal data	*https://www.unipr.it/node/26898*
Center for Internet Security (CIS)	*https://www.cisecurity.org/*

Document Revisions

Ver.	Description of changes	Author	Date modification
1.0	*Initial version*	*O.U. IT Security*	*10/12/2020*