Maastricht University

Maastricht University
Policy on the Processing of Personal Data

Maastricht University

Date: 29 May 2018

Colophon

This policy on the processing of Personal Data is based on the *Policy on the Processing of Personal Data in Higher Education*, version 2.0, March 2018.

Authors
Raoul Winkens, Data Protection Officer
Bart van den Heuvel, Corporate Information Security Officer

Maastricht University

Contents

1 Introduction

The Processing of Personal Data is necessary for the (business) processes of education and research institutions. Personal Data must be stored and processed with the utmost care because misuse of Personal Data can cause substantial damage, not only to students, staff and other Data Subjects at Maastricht University (hereinafter: UM) but also to UM itself. UM therefore attaches great importance to protection of the Personal Data that are supplied to it and to the way in which Personal Data are processed. The correct processing of Personal Data is the responsibility of UM's board.

Through the measures described in this policy document, UM intends to take its responsibility to optimise the quality of the processing and security of Personal Data and, as a result, to comply with relevant privacy legislation and regulations.

1.1 Definitions

GDPR: General Data Protection Regulation[1]

Administrative Unit: As defined in UM's Administration and Management Regulation, Article 1.1, subparagraph 1 (m.), and Article 6.2.
1. Each faculty forms an administrative unit;
2. The office and the service centres form separate administrative units;
3. Research institutes/research schools, education institutes, schools and graduate schools set up within a faculty or coordinated by a faculty form part of the relevant faculty administrative unit.

Policy: this policy on the processing of Personal Data at UM.

Data Subject: an identified or identifiable individual to whom Personal Data relates.

Special Personal Data: personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade union membership, and the processing of genetic data, biometric data for the purpose of uniquely identifying a natural person, data concerning health or data concerning a natural person's sex life or sexual orientation, as in Article 9 GDPR.

Data breach: a breach of UM's technical and organisational security which leads to a significant risk of serious detrimental consequences or which has serious detrimental consequences for the protection of personal data. In the event of a data breach, Personal Data are exposed to loss or unlawful Processing – in other words, to situations for which the security measures should have provided protection.

Third party: any party other than the Data Subject, the Controller or the Processor or any person who is under the direct authority of the Controller or the Processor and is authorised to process Personal Data.

Data Protection Officer (DPO): the person designated by UM to monitor internal compliance with privacy legislation. This person is registered with the Data Protection Authority and is included in the DPO register maintained by the Data Protection Authority. The statutory duties and powers of the DPO give this officer an independent position within UM.

Data Protection Impact Assessment (DPIA): an assessment of the impact of the planned processing activities on the protection of personal data. One assessment can cover a series of similar processing operations that entail similarly high risks.

Information security: All the technical and organisational measures that are required to guarantee the availability, integrity and confidentiality of (personal) data.

Minor: in the context of privacy legislation in the Netherlands, a minor is anyone under the age of 16.

[1] The General Data Protection Regulation entered into force on 25 May 2016 and will be enforced as of 25 May 2018.

Recipient: a natural or legal person, public authority, agency or another body, to which the personal data are disclosed, whether a third party or not. However, public authorities which may receive personal data in the framework of a particular inquiry in accordance with Union or Member State law shall not be regarded as recipients; the processing of those data by those public authorities shall be in compliance with the applicable data protection rules according to the purposes of the processing.

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.

Privacy by Default: data processing in which the standard settings of products and services are such that the privacy of Data Subjects is guaranteed to the maximum extent. This means, amongst other things, that the minimum of data are requested and processed.

Privacy by Design: management of the entire life cycle of personal data, from collection to processing and removal, in which systematic attention is paid to comprehensive guarantees regarding accuracy, confidentiality, integrity, physical security and removal of the personal data.

Profiling: any form of automated processing of Personal Data consisting of the use of personal data to evaluate certain personal aspects relating to a natural person, in particular to analyse or predict aspects concerning that natural person's performance at work, economic situation, health, personal preferences, interests, reliability, behaviour, location or movements.

Data Subject's consent: any freely given, specific, informed and unambiguous indication of the Data Subject's wishes by which he or she, by a statement or by a clear affirmative action, signifies agreement to the processing of personal data relating to him or her.

Processor: a natural or legal person, public authority, agency or other body which processes Personal Data on behalf of UM.

Processing: any operation or set of operations which is performed on personal data or on sets of personal data, whether or not by automated means, such as collection, recording, organisation, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction.

Controller: the natural or legal person, public authority, agency or other body which, alone or jointly with others, determines the purposes and means of the processing of Personal Data. In this Policy mostly the Executive Board of UM.

1.2 Scope and objective of the Policy

The Policy relates to the processing of Personal Data of all Data Subjects within UM, including, in any event, all staff, students, guests, visitors and external parties (contractors/outsourcing), and to other Data Subjects whose Personal Data are processed by UM.

The Policy focuses on the fully or partially automated/systematic processing of Personal Data that takes place under UM's responsibility and on the documents on which it is based, which are contained in a file. The Policy also applies to non-automated processing of Personal Data which are contained in a file or which are intended to be contained therein.

There is a close relationship and partial overlap with the adjoining Information Security policy area, which deals with the availability, integrity and confidentiality of data, including Personal Data. Attention is paid to this overlap at strategic level, and every effort is made to coordinate both planning and content.

The aim of UM's Policy is to optimise the quality of the Processing and security of Personal Data, whilst ensuring that a good balance is struck between privacy, functionality and security.

The Data Subject's privacy must be respected wherever possible. Data relating to a Data Subject must be protected against unlawful and unauthorised use or misuse in pursuance of the Data Subject's fundamental right to protection of his/her Personal Data. This means, therefore, that the processing of Personal Data must comply with relevant legislation and regulations and that Personal Data held by UM must be secure.

For UM, the objective of the Policy is as follows:

- To provide a framework: the Policy provides a framework for evaluating the (future) Processing of Personal Data against a predefined best practice or standard, and for defining the tasks, powers and responsibilities within the organisation.
- To set standards: the basis for the security of Personal Data is ISO 27001.[2] Measures are taken on the basis of ISO 27002[3] and best practices in higher education. Internally, UM uses the standard and assessment frameworks for Information Security and Privacy developed by SURF's SCIPR community as best practices.
- The Framework of Legal Standards for Cloud Services in Higher Education[4] is used as best practice for cloud services and other outsource contracts.
- To take responsibility: the Executive Board takes responsibility by defining the principles and organisation of the processing of Personal Data for the entire organisation.
- Effective implementation of the policy by the Portfolio holder for the Processing of Personal Data by making clear choices in terms of measures and actively monitoring implementation of the policy measures.
- To comply with Dutch and European legislation.

As well as the specific objectives listed above, a more general aim is to raise awareness of the importance of and need for the protection of Personal Data, partly to avoid risks resulting from failure to comply with the relevant legislation and regulations.

[2] In full: NEN-ISO/IEC 27001: Requirements for Information Security Management Systems
[3] In full: NEN-ISO/IEC 27002: Code of practice for information security controls
[4] https://www.surf.nl/kennisbank/2013/surf-juridisch-normenkader-cloudservices.html

2 Principles of the Policy on the Processing of Personal Data

2.1 Policy principles

The fundamental principle of the Policy is that Personal Data must be Processed in accordance with the relevant legislation and regulations in a fair and responsible way. In this context, a good balance must be struck between the interests of UM in processing Personal Data and the interests of the Data Subject in respecting his privacy making free choices regarding his Personal Data.

In order to fulfil the fundamental policy principle set out above, the following principles will apply:

- The Processing of Personal Data will be based on one of the legal bases set forth in Article 6 of the GDPR (‘lawfulness’).
- Personal Data will only be Processed in a manner that is fair and transparent in respect of the Data Subject. This means that data subjects must be able to find out to what extent and in what way Personal Data are being processed. Any information and communication relating to this must be easily accessible and easy to understand (‘fairness and transparency’).
- Personal Data will only be Processed for specified, explicit and legitimate purposes. In other words, specific, legitimate purposes that have been documented and described before the Processing begins. Personal Data will not be further processed in a manner that is incompatible with the purposes for which they were obtained (‘purpose limitation’).
- When Processing Personal Data, the quantity and type of data will be restricted to the Personal Data that are necessary for the specific purpose. In the context of this purpose, the data must be adequate, relevant and not excessive (‘data minimisation’).
- The processing of Personal Data will be minimal and must be proportionate to the intended purpose (‘data minimisation’).
- Measures will be taken to guarantee as far as possible that the Personal Data to be processed are accurate and up to date (‘accuracy’).
- Personal Data will be adequately protected in accordance with the applicable security standards (‘integrity and confidentiality’).
- Personal Data will not be processed for longer than is necessary for the purposes of the Processing, and the applicable retention and destruction times will be taken into account (‘storage limitation’).
- Every Data Subject will have the right to access, rectify, complete, erase or restrict any Personal Data in the individual Processing operations that relate to him, and the right to object, as set out in Chapter 8 of this Policy.
- For all Processing that is based on the Data Subject’s consent, it will be as easy to withdraw consent as to give it.
- If a specific application does not require Personal Data to be traced back to the individual, wherever possible, the principle of anonymity will be applied.

3 Legislation and regulations

UM complies with relevant legislation and regulations as follows:

3.1 Higher Education and Scientific Research Act (*Wet op het hoger onderwijs en wetenschappelijk onderzoek*)

UM has a quality assurance system which ensures (amongst other things) that student records and academic results are treated with the utmost care. In addition, codes of conduct and ethics for (non-) academic staff are observed and applied.

3.2 General Data Protection Regulation

UM has implemented the statutory requirements (including the lawful and responsible Processing of Personal Data and the taking of suitable technical and organisational measures to prevent loss and unlawful Processing of Personal Data) based on the Policy. In so doing, it also implements the Implementation Act of the General Data Protection Act.

3.3 Public Records Act

UM complies with the provisions of the Public Records Act (Archiefwet) and the Public Records Ordinance (Archiefbesluit) on the management of retention of information that is recorded in (digitalised) documents, information systems, websites etc. This forms part of the annual external auditor's reports.

3.4 Telecommunications Act

The measures that UM has taken to comply with privacy legislation are also sufficient to protect the privacy of users on public networks of UM. The provisions of the Telecommunications Act (Telecommunicatiewet) regarding authorised tapping and data retention have been implemented separately.

4 Roles and responsibilities relating to the Processing of Personal Data

In order to ensure that Personal Data is processed in a structured and coordinated way, UM has identified a number of roles which have been assigned to individuals within the organisation.

4.1 Executive Board

The Executive Board is ultimately responsible for the lawful and responsible Processing of Personal Data within UM and defines policy, measures and procedures in the field of Processing.

4.2 Portfolio holder for the Processing of Personal Data

The Portfolio holder for the Processing of Personal Data is the board member who is responsible for Privacy and Information Security. He has ultimate responsibility for the Processing of Personal Data within UM. In day-to-day operations, the portfolio holder can delegate this to his CIO.

4.3 Data Protection Officer

UM appointed an internal supervisor who will monitor the Processing of Personal Data. This officer is known as a Data Protection Officer (hereinafter: 'DPO'). UM will involve the DPO at an early stage in all matters involving Personal Data. The statutory duties and powers of the DPO give this officer an independent position within UM. UM will register the DPO with the supervisory authority.

The tasks of the DPO will include:

- informing and advising all stakeholders of their obligations under the GDPR;
- monitoring compliance with the GDPR and other relevant privacy legislation;
- monitoring UM's compliance with this privacy policy;
- supervising Data Protection Impact Assessments;
- reporting on compliance with the GDPR at least once a year;
- liaising with the supervisory authority;
- acting as the first point of contact for the supervisory authority.

This has been worked out in the "Regeling Functionaris Gegevensbescherming UM".

4.4 Corporate Information Security Officer

UM has appointed a Corporate Information Security Officer (hereinafter: CISO)at corporate level to advise on and monitor Information Security within UM.

4.5 System owner

The system owner is responsible for ensuring that the application and associated ICT facilities effectively support the process for which they are responsible and comply with the Policy. In other words, the system owner must ensure that, both now and in the future, the application continues to meet the requirements and wishes of users and to comply with legislation and regulations. In the event of non-compliance, the CISO/DPO will advise on applicable measures for use, which will be approved by the CIO/Executive Board.

4.6 Process/Processing owner

The process/processing owner is responsible for ensuring that processes and processing operations comply with the Policy. In other words, the process/processing owner must ensure that, both now and in the future, the process continues to comply with legislation and regulations.

4.7 Line manager

The raising of awareness and compliance with the Policy is part of the line manager's duties. Every line manager must:

- ensure that his staff are aware of the Policy;
- monitor compliance with the Policy by his staff;
- address the issue of privacy from time to time in work meetings;

4.8 Information Manager

In the context of this Policy, the information manager has the following tasks in the field of privacy and Processing of Personal Data:

- Local privacy officer: Within each of the four domains (Education, Research, Operations & Technology)[5], the information manager acts as a local point of contact for privacy and Processing of Personal Data.
- The information manager will liaise with the Data Protection Officer on a regular basis over developments in his domain in the field of privacy and Processing of Personal Data.
- The information manager will contribute annually to the report of the DPO on compliance of UM with the GDPR.

[5] Since UM is still in a transition phase, for the time being, the Information Managers of the Administrative Units will fulfil this role.

5 Implementation of the Policy

UM's Executive Board is responsible for Processing of the Personal data for which it determines the purpose and means of Processing. It is designated as the **Controller** within the meaning of the GDPR. However, the Personal Data are actually processed at all levels of UM. The effective, efficient and responsible management of an organisation is often referred to as governance. This includes in particular the relationship with UM's key stakeholders, such as its, staff, students, other clients and society as a whole. A good governance policy guarantees the rights of all Data Subjects.

5.1 Division of responsibilities

- The responsible processing of Personal Data must be seen as **a line responsibility**: in other words, line managers (heads of department/central support departments) have primary responsibility for the responsible Processing of Personal Data in their department/unit. This also includes the choice of measures and the implementation and enforcement thereof. Line managers' responsibilities also include communicating the Policy to all relevant parties.

- The responsible treatment of Personal Data is also **everyone**'**s responsibility**. Staff and students are expected to behave in an ethical way. It is not acceptable that, intentionally or otherwise, their behaviour gives rise to unsafe situations that cause damage and/or adversely affect the reputation of UM or Data Subjects. It is for this reason that codes of conduct have been drawn up and implemented.

5.2 Inclusion in corporate governance/Coordination with adjoining policy areas

In order to demonstrate the corporate approach to data protection and to coordinate initiatives and activities in the field of Processing of Personal Data within the various units, there must be structured dialogue around privacy at different levels.

At **strategic level**, there are strategic discussions around governance and compliance, and around objectives, scope and ambition in the field of privacy and data protection. The strategic level is fulfilled by the I-Board. Within the parameters set by the Executive Board, the I-Board is responsible for implementation and enforcement of the GDPR.

At **tactical level**, the strategy is translated into plans, standards to be applied and evaluation methods. These plans and tools steer the implementation process. The tactical level is fulfilled by the Information Managers consultation body. As things stand, this is the 14MU consultation body.

At **operational level,** matters relating to day-to-day operations (implementation) are discussed. The operational level is fulfilled by the ICT Consultation Body (DO-ICT).

5.3 Awareness and training

Policy and measures in themselves are not enough to exclude risks in the field of the Processing of Personal Data. Awareness within UM must be raised on an ongoing basis, so knowledge of risks is increased and (safe and responsible) behaviour is encouraged.

Regular awareness-raising campaigns for staff, students and other Data Subjects form part of the Policy. These campaigns are organised centrally by the Executive Board or its mandatories, wherever possible in conjunction with other security campaigns and in connection with national campaigns within higher education.

The Administrative Units themselves are also responsible for the raising of awareness, and are supported in this by the DPO and the Corporate Information Security Officer.

5.4 Audits and compliance

Audits verify the effectiveness of the Policy and the measures taken. The DPO initiates the audit to verify that Personal Data has been processed lawfully and responsibly, together with the Corporate Information Security Officer and the internal auditor.

Any external audits are carried out by independent auditors. This is linked to the annual audit and, wherever possible, is coordinated with the usual Planning & Control cycle. Peer reviews by SURFaudit form part of UM's external audits.

If the data protection and privacy audit reveals serious failings, UM may impose sanctions on the employees involved within the parameters of the collective labour agreement and the statutory provisions.

The processing of Personal Data is a continuous process. Technological and organisational developments both within and outside UM make it necessary to check on a periodical basis that the Policy is still on course.

6 Lawful and responsible Processing of Personal Data

UM processes Personal Data in accordance with the principles set out in Section 2.1 of this Policy. In pursuance of these principles, UM takes the measures outlined in this chapter.

6.1 Basis

UM only processes Personal Data where one of the legal bases listed in Article 6 GDPR applies:

a. The Data Subject has given his consent to the processing.
b. Processing is necessary for the performance of a contract with the Data Subject.
c. Processing is necessary for compliance with a legal obligation to which the Controller is subject.
d. Processing is necessary in order to protect the vital interests of the Data Subject or of another natural person.
e. Processing is necessary for the performance of a task carried out in the public interest or in the exercise of official authority.
f. Processing is necessary for the purposes of the legitimate interests pursued by the Controller or by a third party.

When implementing each Processing operation, UM applies the principles of Privacy by Design and Privacy by Default.

6.2 Privacy statement

UM processes Personal Data in a manner that is fair and transparent for the Data Subject. In other words, UM makes it clear to the Data Subject to what extent and how his Personal Data are being processed. When collecting the Personal Data, UM will notify the Data Subject by means of a privacy notice. The Data Subject will be notified before the Personal Data are processed, unless this is not reasonably possible. See Section 8.1 of this Policy for further details.

6.3 Organisation of Information Security

UM guarantees an adequate level of security and implements suitable technical and organisational measures to protect Personal Data from loss and/or from any form of unlawful Processing. These measures are also designed to prevent unnecessary or unlawful collection and Processing of Personal Data.

A risk analysis of privacy protection and Information Security forms part of UM's internal risk management and control system. In this context, UM uses a pre-defined classification method and a Data Protection Impact Assessment.

6.4 Confidentiality

UM classifies all Personal Data as confidential. Each and every individual must respect the confidentiality of Personal Data and act accordingly.

Even individuals who are not subject to an obligation of confidentiality on account of their position or profession or statutory regulations must treat Personal Data to which they become party as confidential, except insofar as statutory regulations require them to disclose such data or they are required to disclose the data in the course of their work.

6.5 Retention/destruction periods by type of data

Personal Data are not kept for longer than is necessary for the purposes for which they have been collected or are being used, in accordance with UM's retention policy. Once the retention period has expired, Personal Data must[6] be removed from the active records. Once the retention period has expired, UM will destroy the Personal Data or, if the Personal Data are intended for historical, statistical or scientific purposes, will store them in an archive. UM uses the Basic Selection Document for Research Universities (*Basisselectiedocument Wetenschappelijk Onderwijs*) as a starting point for retention and destruction periods.

Where Personal Data is processed on the basis of consent and the Data Subject withdraws his consent, processing of the data will only continue in order to comply with a statutory obligation. Where no such obligation exists, the data will be removed or anonymised.

6.6 Documentation requirements

UM has taken multiple measures to demonstrate that it meets the statutory requirements of the GDPR, including implementation of this Policy.

In addition, any fully or partially automated Processing of Personal Data must be notified to UM's DPO. The DPO assesses the lawfulness of the Processing and the Information Manager ensures that all relevant data are adequately documented.

Also, where (research) projects, infrastructure changes or the procurement of new systems are likely to pose a significant risk to the rights and freedoms of individuals, UM carries out a Data Protection Impact Assessment. If this assessment indicates that the Processing would pose a significant risk if UM failed to take measures to limit the risk, UM will consult the supervisory authority before Processing the data.

6.7 Special Categories of Personal Data

In principle, the processing of Special Personal Data is forbidden, unless one of the statutory exceptions of the GDPR applies, which include, amongst others, the 'explicit consent of the Data Subject' and 'substantial public interest'. Special Personal Data are also subject to more stringent requirements in terms of security. Where the basic level of protection is inadequate, individually adapted additional measures must be taken for each information system.

Two types of Personal Data do not come under the category of Special Personal Data but the Processing and security of such data are still subject to stringent requirements:

a. Personal Data relating to criminal convictions and criminal offences can only be processed under the supervision of the government or under European or national legislation.
b. Under Dutch legislation, a national identification number (BSN or student ID number) can only be processed where laid down by law.

6.8 Transfer of Personal Data

6.8.1 Outsourcing of Processing to a Processor

If UM arranges for Personal Data to be processed by a Processor, execution of the Processing will be regulated in a written contract between UM and the Processor.

6.8.2 Transfer of Personal Data within the European Economic Area (hereinafter: 'EEA')

[6] Retention periods may be laid down by law, as is the case for financial data or formal academic results, but they may also be defined by UM, in a contract between UM and the Data Subjects, for example.

UM only supplies Personal Data to a Recipient (be it Processor, Controller or Third party) that is based within the EEA, if the Processing is based on one of the bases for the Processing of data specified in Article 6 and complies with Article 9 of the GDPR when necessary and if the Recipient meets the statutory requirements of the GDPR.

6.8.3 Transfer of Personal Data outside the EEA

UM only supplies Personal Data to Recipients that are located in a country outside the EEA if one of the following applies:

1. According to the European Commission, the third country, territory or specified sector within a third country, or the international organisation in question offers an adequate level of protection.

UM deems an adequate level of protection to be:
- The general list of countries with an adequate level of protection published by the European Commission[7];
- The Privacy Shield for companies in the United States, published by the European Commission in conjunction with the US Department of Commerce[8].

2. Transfer takes place on the basis of **appropriate safeguards**, as set forth in the GDPR, Articles 46 and 47.
3. Transfer takes place on the basis of one of the **statutory exceptions** set forth in Article 49 of the GDPR.

6.9 Query and complaints procedure

6.9.1 Submission and documentation

Queries or complaints relating to (the processing of) Personal Data may be submitted to privacy@maastrichtuniversity.nl. Queries or complaints with a (potentially) significant impact will be documented.

Queries and complaints may be submitted by anyone, including Data Subjects, Processors or Third Parties.

6.9.2 Weak points in security

Employees and students must document any weak points in systems or services that they identify and report them directly to UM's ICTS service desk. A record will be kept of all reports of weak points in security.

6.9.3 Handling

Queries, complaints and weak points in security will be forwarded to the responsible department or individual and dealt with as quickly as possible in accordance with the predefined procedures.
If the Personal Data of a Data Subject or Data Subjects or the business processes, finances or reputation of UM are seriously at risk, the Executive Board and the DPO and Legal Affairs will be notified accordingly.

6.9.4 Evaluation

It is important to learn from the feedback that is provided through the query and complaints procedure. The documenting of significant queries, complaints and weak points and periodical reporting thereof are

[7] You can find this via the following link https://ec.europa.eu/info/law/law-topic/data-protection/international-dimension-data-protection/adequacy-decisions_en
[8] You can find this via the following link https://www.privacyshield.gov/list.

an essential part of the professional processing of Personal Data. The related reports therefore form a permanent part of the annual reporting of the Executive Board and the DPO.

7 Data Breaches

This chapter describes the policy on reporting, documenting and managing a Data Breach or suspected Data Breach in routine operations and in special circumstances.

7.1 Data Breach

A Data Breach is said to exist if there is a breach of the security of Personal Data that leads to unauthorised Processing of that data. Examples include the theft of a laptop, a USB stick left on a train or an email that has been sent to the wrong person. All Data Breaches must be notified internally. Some Data Breaches must be notified to the supervisory authority within 72 hours of their discovery and, in some cases, also to the Data Subject.

7.2 Reporting and documentation

A Data Breach may occur within UM's own organisation or in that of a Processor that has been appointed by UM. In this context, a distinction must be made between the following situations:

a. *Employee*: if they identify a (potential) Data Breach or suspect that they themselves are part of a Data Breach, employees must contact UM's ICTS service desk preferably using the form "Report possible UM data leak"[9].
b. *Processor:* Data Breaches can also occur on the premises of a Processor appointed by UM. The Processor will report the Data Breach to UM in accordance with the processor agreement concluded in this context.
c. *Other individuals:* if a person other than an employee or a Processor identifies a (potential) Data Breach or is part of a Data Breach themselves, they must contact UM's ICTS service desk via servicedesk-icts@maastrichtuniversity.nl.

(Potential) Data Breaches must be reported as quickly as possible. Whenever a Data Breach is reported, the following details must be recorded:

- Who is reporting the Data Breach?
- What was reported and how did this happen? Provide a summary
- Where did the report come from?
- To what data does it relate? [10]
- Is the data encrypted or secured in any way?
- Which group of people is affected by the incident and how many persons are involved?
- What are the consequences of the incident for the data?
- Which systems are involved/affected by the incident?
- When did the incident take place?
- If the incident was reported by a UM employee: what has been done to resolve the incident/prevent the incident occurring again in the future?

Every Data Breach and how it was managed must be documented.

7.3 Management

Should a Data Breach occur, it will be managed in accordance with the specific provisions on Data Breaches contained in relevant legislation and regulations, as described in the Data Protection Authority's policy guidelines on the duty to notify data breaches[11], so that notification of the Data Breach reaches the right people, and ultimately the supervisory authority and Data Subjects, in good time.

---

[9] https://servicedesk.icts.maastrichtuniversity.nl/tas/public/ssp/

[10] E.g.: Name, Sex, Date of birth and/or age, BSN, Contact data, Access or identification data, Financial data, (Copies of) passports or other identification documents, Location data, Health data, Genetic data, Biometric data.

[11] The Data Protection Authority's policy guidelines on the duty to notify data leaks: https://autoriteitpersoonsgegevens.nl/nl/onderwerpen/beveiliging/meldplicht-datalekken

If the Personal Data of a Data Subject or Data Subjects or the business processes, finances or reputation of UM are seriously at risk, the Executive Board and the DPO and Legal Affairs will be notified accordingly.

7.4 Decision-making

After a (potential) Data Breach has been reported in accordance with the previous paragraphs, the DPO will issue a recommendation regarding the obligation to notify the supervisory authority and the Data Subject. The Executive Board (usually via its mandatories) will be responsible for the decision as to whether or not to notify. If the recommendation of the DPO is not followed by a mandatory, the matter will be escalated immediately to the Executive Board for a final decision.

7.5 Evaluation

It is important to learn from Data Breaches in order to reduce the likelihood of future Data Breaches. The documenting of Data Breaches and periodical reporting thereof are an essential part of the professional processing of Personal Data. Reporting on Data Breaches relating to Personal Data therefore forms a permanent part of the annual reporting of the Executive Board and the DPO.

8 Rights of Data Subjects

The GDPR grants Data Subjects specific rights that enable them to control the Processing of their Personal Data. A written request in order to exercise these rights may be submitted digitally via https://www.maastrichtuniversity.nl/about-um/um-general-privacy-statement/your-rights or in writing to the UM via privacy@maastrichtuniversity.nl or per post to Maastricht University, PO Box 616, 6200 MD Maastricht, attn. the DPO.

The following points apply to all the rights of Data Subjects described in this chapter:

Communication with Data Subjects
UM will ensure that it informs and communicates with Data Subjects in a concise, accessible and intelligible way, using clear and plain language. The language will be adapted to the target audience. UM will answer in Dutch by default and when necessary in English.

Deadline
A written response to a Data Subject's request will be provided as soon as possible and, in any event, within one month of receipt. This response will always advise the Data Subject what action has been taken regarding the request. If the one-month deadline is not reasonably feasible, the Data Subject will be notified in writing that this is the case by the deadline. In that case, UM will deal with the Data Subject's request within two months of expiry of the first deadline.

Identity of Data Subject
When providing the relevant information, UM will check the identity of the requester carefully. UM may request additional information for this purpose.

Minors
A request to exercise one of the rights described in this chapter by a Data Subject who is a Minor or who no longer has mental capacity must be made by his/her legal representative. UM will also send a response to this legal representative.

8.1 Right to be informed

The Data Subject has the right to be informed by UM of certain aspects of the Processing of his Personal Data. UM will provide the Data Subject with information concerning the Processing of his Personal Data free of charge, both where the Personal Data have been collected directly from the Data Subject and where they have been obtained by a different route.

A. Collection directly from the Data Subject
Where the data are collected directly from the Data Subject, UM will provide the Data Subject with a minimum of the following information before collecting the data:

- The identity and contact details of the Controller and, where applicable, of the DPO.
- The specific purposes of the Processing for which the Personal Data are intended as well as the legal basis for the processing.
- Where the Processing is based the legal basis 'legitimate interests', the legitimate interests pursued by the Controller or Third Party.
- Where applicable, the fact that the Controller intends to transfer the Personal Data to a third country,which country this is and on what grounds the Personal Data are being sent to this country.
- The period for which the Personal Data will be stored, or if that is not possible, the criteria used to determine that period.
- The existence of the right to request from the Controller access to and rectification or erasure of Personal Data or restriction of processing concerning the Data Subject or to object to Processing as well as the right to data portability.
- The right to lodge a complaint with the supervisory authority.
- The recipients or categories of recipients of the Personal Data.
- Where the Processing is based on the legal basis of 'consent', the Data Subject's right to withdraw this consent at any time.

- Whether the Personal Data are necessary for the performance of a contract or to comply with a legal obligation.
- Whether the Personal Data are also used for automated decision-making. The Data Subject must also be given information regarding the logic involved, as well as the significance and envisaged consequences of the Processing for the Data Subject.

B. Collection other than from the Data Subject

If the Personal Data are not collected directly from the Data subject himself but rather by a different route, in addition to the aforementioned details, the following information must be supplied to the Data Subject:

- The categories of Personal Data.
- From which source the Personal Data originate.
- This information will be provided as quickly as possible and, in any event, no later than four weeks after the data was obtained, or at the time of the first communication with the Data Subject.

8.2 Right of access

Request

Every Data Subject has the right to be informed as to whether or not his Personal Data are being processed and, if so, to access this Personal Data.

Notification

If data are being processed, the information provided by UM will include a full overview of the requested data, this could be:

- A description of the purposes of the Processing.
- The categories of data to which the Processing relates.
- Categories of recipients.
- Available information on the origin of the data.
- The retention period of data or, if this is not possible, the criteria used to determine that period.
- The Data Subject's right to request from the Controller rectification or erasure of personal data or restriction of processing of personal data concerning the Data Subject or to object to such Processing, as well as the right to data portability.
- The Data Subject's right to lodge a complaint with a supervisory authority.
- Any available information as to the source of the data, where the data are not collected from the Data Subject.
- Whether the Personal Data are also used for automated decision-making. The Data Subject must also be given information regarding the logic involved, as well as the significance and envisaged consequences of the Processing for the Data Subject.
- The appropriate safeguards that were implemented, if the data are transferred to a third country.

Copy

The Data Subject may request a copy of all Personal Data. This copy must be provided in a commonly used electronic form, unless the request was made on paper or the Data Subject explicitly requests a paper copy. The right of access does not standard give access to a copy or transcript of the document that contains the data. The purpose of the right of access is to enable Data Subjects to check the Personal Data being Processed by UM and to check if the data is correct and Processed lawfully by UM.

Charges

A first copy will be provided free of charge. For each additional copy, UM will charge the Data Subject a reasonable fee based on administrative costs.

Rights and freedoms of others

When providing the data, UM will take into account the rights and freedoms of others.

8.3 Right to data portability

Grounds for request
Any Data Subject may submit a request to UM to receive his data (free of charge) in a structured, commonly used and machine-readable format or to have those data transmitted directly to another Controller without hindrance from UM, provided that the following conditions are met:

1. The Processing by UM is based on the principle of 'consent' or 'performance of a contract with the Data Subject'.
2. The Processing in question is fully automated.

Rights and freedoms of others
When providing the data, UM will take into account the rights and freedoms of others.

Erasure of data
If a Data Subject has exercised his right to data portability in the context of Processing for the performance of a contract, UM cannot decide to delete the data. Once the retention period has expired, UM must however delete them.

If the right is exercised in the context of Processing on the basis of consent by the Data Subject, UM may however decide to delete the data once the right has been exercised.

8.4 Right to rectification, completion, erasure or restriction of Processing

Request to rectify, complete, erase or restrict
A Data Subject may request that UM rectify, complete, erase or restrict the Processing of his Personal Data. In the case of the right to restrict processing, the Personal Data will be temporarily restricted and will no longer be processed by UM. The restriction will be clearly specified in the file.

Implementation and Notification
If it appears that Processed Personal Data of the Data Subject are factually incorrect, inadequate for the objective or or purposes of the Processing or not relevant, or that they have otherwise been processed in violation of a legal requirement, the data manager (this can be both the Controller and the Processor) will rectify, erase, complete or restrict these data.

In addition, Third Parties to whom the data was supplied prior to rectification, completion, erasure or restriction will be notified accordingly, unless this is not reasonably possible or, given the circumstances, is not relevant. The requester may request a statement of the parties to whom UM has issued such notification.

8.5 Right to object

Grounds for objection
Data Subjects have two grounds for objecting to Processing:

1. In connection with his or her personal circumstances, a Data Subject may object to Processing by UM, if such Processing takes place on the basis of a) the performance of a task carried out in the public interest or in the exercise of official authority vested in the Controller, or b) the legitimate interests pursued by UM or by a Third Party to which the data have been supplied.

In the event of an objection, UM will in principle stop further Processing of the data. If UM can demonstrate that its compelling legitimate interests override the interests, basic rights and fundamental freedoms of the Data Subject, Processing will continue. If the objection is justified, UM will take the measures that are necessary to stop processing the Personal Data for the relevant purposes (free of charge).

2. Where the purpose of Processing is direct marketing, a Data Subject has the right to object at any time. In the event of an objection, UM will stop Processing of Personal Data for direct marketing purposes immediately (free of charge) and on a permanent basis.

8.6 Automated decision-making

Grounds
Data Subjects have the right not to be subject to a decision based solely on automated Processing which produces legal effects concerning them. A 'decision based on automated Processing' means a decision that is made without human involvement. Amongst other things, this includes Profiling.

UM can only make decisions based on automated Processing in the following three situations:

1. If the decision is necessary for the conclusion or performance of a contract with the Data Subject.
2. If the decision is authorised by a European or national law, provided that this law lays down suitable measures to safeguard the Data Subject's rights and freedoms and legitimate interests.
3. If the decision is based on the Data Subject's explicit consent. This consent may be withdrawn at any time.

In all the above-described situations, UM will implement suitable measures to safeguard the Data Subject's rights and freedoms and legitimate interests. This will include, at minimum, the right to obtain human intervention on the part of UM, to express his or her point of view and to contest the decision. Minors will never be subjected to automated decision-making.

8.7 Legal protection

General complaints
If the Data Subject believes that the statutory provisions concerning privacy protection or the provisions of this Policy have not been correctly enforced in his regard, he may submit a written complaint to UM's Executive Board.

Other means of objection
In addition to the general internal complaints procedure described above, the Data Subject has the following options if he believes that UM has committed a breach of the GDPR that affects him:

A. Objection and appeal

If UM has reached a negative decision regarding a request as described in Sections 8.1 to 8.6 of this Policy, or UM has rejected the Data Subject's request, and UM's decision can be regarded as a decision of an administrative authority within the meaning of Article 6 (4) of the General Administrative Law Act (Awb), the Data Subject may initiate objection proceedings. Objection proceedings must always be initiated within 6 weeks of the announcement of a decision by UM. The decision regarding the objection may be appealed in court.

B. Submission of a claim to the subdistrict court

If UM has reached a negative decision regarding a request as described in Sections 8.1 to 8.6 of this Policy, or UM has rejected the Data Subject's request, the Data Subject may file a claim with the subdistrict court.

The claim must be filed with the subdistrict court within six weeks of receipt of UM's response. If UM fails to respond to the Data Subject's request within the agreed period, the claim must be filed within six weeks of expiry of this period. The claim does not need to be filed by a lawyer.

C. Request for enforcement by supervisory authority

If UM has reached a negative decision regarding a request as described in Sections 8.1 to 8.6 of this Policy, or UM has rejected the Data Subject's request, the Data Subject may submit a complaint to a supervisory authority or allow an interest group to act on his behalf.

9 In conclusion

This policy was adopted by the Executive Board of Maastricht University on 29 May 2018 after receiving approval from University Council.
A review of the policy forms part of UM's annual plan-do-check-act cycle. This also includes an audit of the effectiveness of the measures.

Changes to this policy will be announced via an Institution-wide email and the most recent version will be published at https://www.maastrichtuniversity.nl/privacy

Any queries or comments regarding this policy should be directed to privacy@maastrichtuniversity.nl.

Version overview:

Date:	Version:
29 May 2018	1.0
9 October 2019	1.1