# Privacy code and privacy rules
# Nyenrode Business Universiteit

Version 1.4

July 31, 2017

# Contents

Document creation

This document has been drafted by the Academic Services Center (ASC), following a resolution of the University Board (UB) to appoint the head of ASC as the controller for the protection of personal data. The privacy document of the University of Twente and the Nyenrode policy document, as adopted by the UB on July 31, 2017, have been used, with permission and gratitude, in the drafting of this document.

# 1 NBU privacy statement

Nyenrode Business Universiteit (NBU) respects the privacy of students, participants, alumni, staff, and others. By means of this privacy policy, NBU clearly sets out how the protection of privacy is organized.

Until May 25, 2018, NBU will process personal data in accordance with the Personal Data Protection Act (*Wet bescherming persoonsgegevens*, Wbp). After this date, the General Data Protection Regulation (GDPR) will apply.

NBU processes and provides personal data to third parties solely on the basis of a statutory principle. Besides the principle and purpose limitation, other core themes from the GDPR are elaborated in this document: transparency, data minimization, and security. Information is not stored for longer than is needed for the original purpose for which it was collected (data minimization). Information is not used for purposes that are incompatible with that original purpose (purpose limitation).

Personal data are collected for the administration of education and operational management, including names, e-mail addresses, telephone numbers, residential addresses, details of study programs and previous education, study progress, invoicing, and details relating to other education-related student and personnel matters. In most cases, the data are provided by the data subjects themselves, but can also originate from third-party source systems, such as the Immigration and Naturalization Service (IND) and General Pension Fund for Public Employees (ABP).

Data are collected via the website, mainly for the purpose of student recruitment, including registrations for open days or requests for information.

Data for scientific research are collected in accordance with the scientific research guidelines of the association of universities in the Netherlands (VSNU), where necessary after assessment by the Nyenrode Committee for Scientific Integrity, and, if relevant, are reported to the data protection officer (DPO).

NBU bases the processing of personal data in operational management, research, and the administration of education on the principle of proportionality: personal data processing must be proportional to the intended purpose of the operational management or research. An assessment is made each time to find the correct balance between privacy, operational management, and the research objective.

Personal data are adequately secured and handled as carefully as possible. Attention is paid to information security and privacy within all NBU processes and activities.

# 2 Privacy policy

Privacy is attracting more and more attention in our increasingly digitized society. Staff, students, participants, and others are placing greater emphasis on privacy and the protection of their personal data, partly because of risks to organizations and possible infringements of privacy. A duty to report data leaks was recently added to the Personal Data Protection Act (Wbp) and the General Data Protection Regulation (GDPR) was recently adopted at European level, as the successor of the current regulation on which the Wbp is based.

The use of personal data is necessary for the operating processes of educational and research institutions. This personal data must be stored and processed with the utmost care, because misuse of personal data can cause serious damage to students, staff, and Nyenrode.

The University Board of NBU is legally responsible for the correct processing of personal data. By means of the measures described in this policy document, NBU assumes its responsibility to optimize the quality of personal data processing and security and thus to comply with the relevant privacy legislation.

Definitions and abbreviations are set out in Appendix A.

## 2.1 Scope and objectives of the privacy policy

**The aim of Nyenrode's information security policy is to guarantee the continuity of the operating process, to prevent security incidents or minimize the damage resulting from them, and to at least comply with legislation.**

The privacy policy covers the processing of personal data of all data subjects within NBU, which in any case includes all staff, students, guests, visitors, and external contacts, as well as other data subjects whose personal data are processed by NBU.

The accreditation organizations with which NBU exchanges data to make the quality of education measurable, to guarantee such quality and have it validated externally, are special external contacts. This involves performance data of students and participants (in relation to the quality of assessment, graduation projects, degrees, and lecturers). However, it can also include information on career progression and salaries. If special details apply to the accreditation process, for example managing theses under embargo, in relation to competitively sensitive information, or otherwise highly confidential content, the ASC controls the provision of such documents for internal and external audits.

The privacy policy does not cover personal data processing for personal or domestic use, such as personal work notes or a collection of business cards. The privacy policy covers the full or partial automated and/or systematic processing of personal data, which happens under the responsibility of NBU and in accordance with the underlying documents (electronic or otherwise). The privacy policy also applies to the non-automated processing of personal data, which are included or intended to be included in a database.

The protection of personal data is interpreted broadly at NBU. There is an important relationship and partial overlap with the adjacent policy area of information security, which covers the availability, integrity, and confidentiality of data, including personal data. It is also necessary to manage internal and external data storage, for example to prevent NBU data being stored outside the EU and managed by third parties. The Nyenrode privacy policy pays attention to the common ground with information security and aims for systematic and substantive coordination.

The purpose of the privacy policy is to permanently improve the quality of personal data processing and security and to find the best possible balance between privacy, functionality, and security.

The aim is to respect the privacy of the data subject as far as possible. Based on the fundamental right to protection of his/her personal data, the data relating to a data subject should be protected against unlawful and unauthorized use, loss, and misuse. This implies that personal data processing should comply with relevant legislation and that personal data are secure at NBU.

The privacy policy gives students, staff, and other data subjects insight into how privacy is organized at NBU. It also helps raise awareness of the importance and necessity of protecting personal data.

## 2.2 Main aspects of the privacy policy

- The policy is the starting point for the management system and provides a framework to assess future information security measures against an established standard and to establish roles, including duties, powers, and responsibilities.
- ISO27001/2 has served as inspiration for the design of Nyenrode's information security management. Although formal certification in accordance with ISO27001/2 is not viewed as necessary for Nyenrode, the design of a proper information security process is – this policy is the basis for that purpose.
- Measures are adopted on the basis of legislative amendments, a risk analysis, and audit outcomes.
- Basic principles and the organization of information security functions are explicitly documented, supported by the board, and inferred from that by the institution as a whole.
- Decisive process approach, clear choices in measures, active monitoring of policy measures and their implementation.
- The policy forms the basis for compliance with prevailing legislation.

# 3 Legislation

The relevant legislation is dealt with as follows at NBU.

**Dutch Higher Education and Research Act (*Wet op het hoger onderwijs en wetenschappelijk onderzoek*, WHW)**:
NBU has a quality assurance system, which among other things guarantees the careful handling of data in the student administration and the processing of study results. Integrity codes for scientific research are also applied and observed.

**Personal Data Protection Act (*Wet bescherming persoonsgegevens*, Wbp) / General Data Protection Regulation (GDPR)**:
NBU has implemented the statutory requirements by means of the privacy policy. Personal data are duly processed in accordance with the relevant legislation, with due observance of transparency (Article 5, GDPR), lawfulness (Article 6, GDPR), and security. For this purpose, the best possible balance should be found between NBU's interest in processing personal data and the data subject's interest in making his/her own choices relating to his/her personal data in a free environment.

Chapter 4 of the document entitled *Beleid verwerking persoonsgegevens 'Student' Nyenrode Business Universiteit*' (Policy for the processing of 'Student' personal data at Nyenrode Business University) details the policy principles and the related concepts.

**Public Records Act (*Archiefwet*)**:
NBU draws up the rules for retention periods on the basis of the Public Records Act and the Public Records Decree (*Archiefbesluit*).

**Telecommunications Act (*Telecommunicatiewet*)**:
Among other things, NBU subscribes to the rules with which cookies on websites must comply.

**Copyright Act (*Auteurswet)***:
NBU upholds the portrait right. It does not allow images, photographs, and videos to be published if a reasonable interest of the data subject prevents publication. The GDPR also sets further requirements in relation to processing privacy-sensitive information. See Chapter 6.1.3. of the *Beleid verwerking persoonsgegevens 'Student' Nyenrode Business Universiteit*' (Policy for the processing of 'Student' personal data at Nyenrode Business University) in relation to the use of images.

**Computer Crime Act (*Wet computercriminaliteit*)**:
This Act focuses on problem areas of criminal law relating to computer use. The Act consists of articles that are added to certain parts of the Dutch Criminal Code. These additional articles include:

- Destruction of and making data unusable
- Interception of data
- Denial-of-service attacks
- Computer intrusion
- Purchasing services without payment
- Malicious software (malware)

In principle, if there is an attack on NBU that significantly penetrates that security and falls under the Computer Crime Act, NBU will file a report. The Information Security and Privacy (ISP) steering group advises the board in this regard – only the board can decide to file the report.

# 4 Roles and responsibilities in relation to personal data processing

In order to approach the processing of personal data in a structured and coordinated manner, a number of roles and responsibilities are assigned to officers in the existing organization.

## 4.1 University Board

The University Board (UB) is ultimately responsible for the lawful and careful processing of personal data within NBU and adopts the policy, the measures, and the procedures in the area of processing through this privacy policy and underlying documents.

## 4.2 Privacy portfolio holder

The privacy portfolio holder is the board member who has privacy as part of his/her portfolio. He/she is ultimately responsible for securing personal data within NBU.

## 4.3 IT Security Manager

The IT Security Manager defines the ICT security guidelines for the organization in accordance with the information security strategy and architecture of the organization and organizes and coordinates the ICT security of the organization. The IT Security Manager is the key figure in relation to information security within the organization and is responsible in this capacity for managing the Computer Emergency Response Team (CERT) Nyenrode.

### 4.3.1 CERT-Nyenrode

CERT-Nyenrode is a virtual team that is called together whenever a serious security incident has occurred.

## 4.4 Data Protection Officer

The Data Protection Officer (DPO) oversees the application of and compliance with the Wbp within Nyenrode. In conjunction with the IT Security Manager, the DPO is responsible for settling all security incidents relating to the Wbp/GDPR. In accordance with the GDPR, the DPO has an independent position within the organization.

The DPO advises and informs the entire organization and individual units on the application of privacy legislation. The DPO is responsible for informing staff, students, and managers about the processing of personal data. The DPO facilitates awareness of privacy among staff and students, for example by maintaining a privacy portal on the NBU website. A privacy annual report is drawn up each year.

The DPO is the point of contact and expert for those who have questions on the protection of personal data and he/she manages the register of personal data processing reports.

The DPO has the role of process manager of the privacy incident process. This entails that he/she monitors the organization of the process across the university and is responsible for quality assurance.

## 4.5 Process/system owner

The process owner / system owner is the person who is authorized to determine how a process runs and is responsible for ensuring that the process continues to meet client expectations and business objectives, now and in the future. The security of the related information systems is crucial for this purpose. In the first instance, Nyenrode makes appointments in this role for the most vital strategic operating functions. These are the Customer Relationship Management (CRM) system, Human Resource Management (HRM) system, Financial system, CCTV system, Education system and the Website.

## 4.6 Manager

Complying with the information security policy is part of the overall operational management. Each manager is tasked with:

- ensuring that his/her staff are aware of the security policy;
- overseeing compliance with the security policy by his/her staff;
- periodically raising the topic of information security in work meetings;
- being available as the point of contact for all personnel-related information security matters.
- The manager may be supported in this regard by the DPO.

Appointing a Privacy Contact Person (PCP) is recommended.

## 4.7 User

Each user is deemed to comply with the security guidelines and procedures and to be aware of the privacy policy.

## 4.8 Researcher

Each researcher is responsible for how he/she deals with research data, where applicable in conjunction with a research leader; the professor or chairperson of the research group. This should be detailed further in the NBU data policy.

Privacy sensitivity and ethical implications may have consequences for the research design and for how the research data must be handled. Under the principle of proportionality, the processing of personal data must be proportional to the intended research objective. It is up to the researcher to make this assessment.

## 4.9 Affiliated institutions

Affiliated institutions, foundations, and associations/societies of NBU are each responsible for complying with privacy legislation. NBU will emphasize the importance of this and ask for insight into how compliance is achieved.

Data processing operations of affiliated institutions cannot be reported to the DPO of NBU but, insofar as they do not fall within the scope of the Exemption Decree (*Vrijstellingsbesluit*),[1] should be reported directly to the Dutch Data Protection Authority (*Autoriteit Persoonsgegevens*).

Affiliated institutions can approach the DPO for advice.

[1] Standard processing operations that occur often and are commonly known to take place do not have to be reported under specific conditions. See https://autoriteitpersoonsgegevens.nl/nl/melden/handreiking-vrijstellingsbesluit-wbp.

# 5. Management system for information security

## 5.1 Overview of the management system for information security

Information security is organized as a process. Nyenrode chooses to base its annual planning and control cycle on 'Plan, Do, Check, Act'. The annual planning is made and implemented within these steps. The results are evaluated and then transformed into the new year planning. This planning can generally be found at strategic level in the Nyenrode planning, and in more detail in the ICT annual plans. This ensures a continuous process.

The connection between these steps is as follows:

- Plan: policy formulation and risk analysis
- Do: planning and implementation
- Check: monitoring, evaluation, control, and reporting
- Act: improvement process

The steps are explained below.

## 5.2 Policy formulation

The management system for information security starts with drawing up the information security policy. The objectives and basic principles of Nyenrode's information security are set out in this policy. The policy thus forms the guideline for the other steps of the management system.

## 5.3 Risk analysis

The second step of the management system for information security consists of a risk analysis. The purpose of analyzing risks is to:

- gain insight into the quality and effectiveness of the existing security measures;
- gain insight into the risks that could jeopardize the achievement of the required level of security;
- establish the required level of information security in the form of a classification of operating processes, information systems, and data collection;
- be able to make risk management choices;
- determine priorities for improving the existing situation.

The outcomes of the analysis of the existing information security situation are reported to the ISP steering group.

## 5.4 Planning

An improvement plan is drawn up based on the outcomes of the risk analysis. The improvement activities for achieving the required level of security in a project-based manner are set out in this plan. The information security plan is adopted by the Information Security and Privacy (ISP) steering group.

## 5.5 Implementation

The additional security measures are implemented on the basis of the improvement plan. Among other things, this means drawing up guidelines and procedures for information security, introducing measures to raise security to the required level, and informing and training staff.

## 5.6 Monitoring, evaluating, controlling, and reporting

The last step of the management system for information security consists of monitoring, evaluation, and control. Monitoring means continuously checking the level of information security within Nyenrode. Where threats occur and jeopardize this level, incident management sets in to guarantee the required level of security or restore it as quickly as possible. Once the operating function has been restored, an evaluation is held with all involved. A report is then drawn up for the record and for raising awareness.

### 5.7 Continuous process

The management system for information security is a continuous and cyclic process. This means that based on the outcomes of evaluations and controls or because of new developments (introduction of new operating processes or information systems), there may be a need to reassess the information security policy, carry out a new risk analysis, adopt additional measures, or adapt their implementation. Nyenrode chooses to have an audit and penetration test[2] conducted once every two years, the form of which is considered separately each time.

[2] Audit: a short review of the degree of information security in relation to the information security code and the Wbp/GDPR.
Penetration test: a vulnerability assessment focusing internally/externally on the IT infrastructure to check the security of information.

# 6. Implementation of the privacy policy

## 6.1 Responsibilities

The University Board is responsible for processing the personal data of which it determines the purpose and means of processing (see Chapter 4 above). It is regarded as the *controller* within the meaning of the relevant legislation. However, the actual processing of personal data occurs throughout the university. Good governance ensures that all interested parties are aware of their rights and obligations and act accordingly.

Privacy is *everyone's responsibility*. Staff, students, lecturers, and third parties are expected to act ethically and to deal carefully with personal data. Codes of conduct are formulated and implemented for this reason.

Privacy is *a line responsibility*. This means that managers bear the primary responsibility for the careful processing of personal data within their department/unit. This also includes the choice of measures and their implementation and enforcement. The task of communicating the policy in relation to personal data processing to all relevant parties, within reasonable limits, also falls under line responsibility.

## 6.2 Consultation

In order to properly express the coherence of the information security function within the organization and to coordinate the initiatives and activities in the area of information security within the different units, Nyenrode has a clear meeting structure for discussing the topic of information security at various levels.

At strategic level, there are guiding discussions on governance and compliance, as well as on objectives and ambitions in the area of information security. This takes place in the board, with the IT Security Manager and Data Protection Officer acting in an advisory capacity. This meeting takes place once a year.

At tactical level, the strategy is transformed into plans, standards to be applied, evaluation methods, and reports. These plans and instruments guide the implementation. This tactical meeting is held by the ISP steering group (if necessary, in consultation with process owners). This meeting is held every quarter and more often if needed.

At operational level, matters that affect day-to-day operations in relation to execution and implementation are discussed. This meeting, which is ad-hoc in nature, takes place, for example, when an information security incident occurs. The possible solution is determined, and the different tasks are assigned.

Personal data processing is a continuous process. Technological and organizational developments within NBU necessitate periodic reviews to determine whether NBU is still adequately on course with its policy.

## 6.3 Awareness and training

Policy and measures alone do not suffice to exclude risks in the area of personal data processing. It is necessary to continually heighten the awareness of staff and students in relation to privacy and security, so knowledge of risks increases, and good behavior is encouraged. Good practices can be shared with others within the organization, for example via the privacy portal on the NBU website.

Part of the implementation of privacy policy involves regularly recurring awareness campaigns for staff, students, and third parties. These campaigns may correspond with national campaigns in higher education, if possible in coordination with other security campaigns.

## 6.4 Control and compliance

The DPO oversees compliance with privacy legislation and the privacy policy, including the allocation of responsibilities, awareness, and staff training. In addition to this, audits make it possible to monitor the effectiveness of the privacy policy and the adopted measures.

If there are serious failures in compliance with the protection of privacy and other data, NBU may impose a sanction on the responsible members of staff within statutory limits.

# 7. Lawful and careful processing of personal data

## 7.1 Principle, purpose limitation, and weighing up of interests

The processing of personal data must be based on statutory principles as described in Article 8 Wbp and Article 6 GDPR. The controller describes the purposes for the processing in advance. These purposes are concrete and specifically formulated. Each processing operation is assessed to determine the extent to which the processing of personal data is necessary. Different interests are weighed up for this purpose and efficiency, proportionality, and subsidiarity are taken into account. Personal data are not processed further in a manner that is incompatible with the purposes for which they have been obtained.

NBU adopts the necessary measures to ensure that personal data, given the purposes for which they are collected or subsequently processed, are correct and accurate.

## 7.2 Reporting and documenting of processing operations

Fully or partially automated processing of personal data must be reported to NBU's DPO. The DPO assesses the lawfulness of the registration and ensures adequate documentation.

All processing operations are duly documented and published on media that are accessible to the data subjects, stating the purpose of the registrations and the controllers.

## 7.3 Organization of the security

NBU ensures an adequate level of security and implements suitable technical and organizational measures to secure personal data against loss or any form of unlawful processing. These measures are also aimed at preventing unnecessary or unlawful collection and processing of personal data.

The organization of privacy is taken into account from the start of research and other projects, infrastructure changes, or the purchase of new systems by performing a Privacy Impact Assessment (PIA). The DPO is consulted in relation to such changes. Two principles serve as guidance:

1. During the management of the entire personal data life cycle, from collection to processing and deletion, attention is systematically paid to comprehensive guarantees relating to accuracy, confidentiality, integrity, physical security, and deletion of personal data.
2. If users are given a choice between different options, the standard setting provides the best privacy guarantees.

A risk analysis of privacy protection and information security forms part of NBU's internal risk management and control system.

## 7.4 Confidentiality

All personal data are classified as confidential at NBU. Everyone should be aware of the confidentiality and act accordingly.

Even people who are not subject to a duty of confidentiality by reason of their position, profession, or a statutory rule are obliged to maintain the confidentiality of personal data they become aware of, except insofar as any statutory rule obliges them to disclose such data or the necessity to disclose such data arises from their duties.

## 7.5 Retention periods / destruction deadlines for each type of data

Personal data are not retained any longer than is necessary for the purposes for which they are collected or used. After the expiry of the retention period[3], personal data should be removed from the scope of the active administration. NBU shall arrange for the personal data to be correctly destroyed after the expiry of the retention period or, if the personal data are intended for historical, statistical, or scientific purposes, to be kept in an archive.

## 7.6 Special personal data

The processing of special personal data is prohibited, in principle, unless the processing is based on a statutory principle, the express consent of the data subject is obtained, or there is a compelling public interest. Stricter requirements apply to the protection of these personal data. If the basic protection is insufficient, individually agreed additional measures must be adopted for each information system. See the document *Beleid verwerking persoonsgegevens 'Student' Nyenrode Business Universiteit*' (Policy for the processing of 'Student' personal data at Nyenrode Business University) for the processing of personal data in daily educational administration practice.

## 7.7 Transfer of personal data to third parties

### 7.7.1 Outsourcing processing to a processor

If NBU arranges for a processor to process personal data, the performance of processing operations will be organized in a written agreement between NBU, as the controller, and the processor. If NBU is the processor for an external party, for example when providing personalized learning commissioned by the external party, the processing of personal data is also agreed and recorded contractually.

### 7.7.2 Transfer of personal data within the European Union

NBU provides personal data to third parties within the European Union only if this transfer is based on a statutory principle.

Special personal data are not provided to third parties without the explicit consent of the data subject.

[3] Retention periods may be laid down by law, such as in the case of financial data or formal study results, but can also be defined by NBU, for example in a processing agreement between NBU and the Data Subjects.

### 7.7.3 Transfer of personal data outside the European Union

NBU provides personal data to third parties who are located in a country outside the European Union only if that country as a whole, or the company/institution concerned, specifically *guarantees an adequate level of protection*. For countries with an adequate level of protection, NBU applies the list of countries as published by the European Commission[4].

NBU provides personal data to countries without an adequate level of protection only on the basis of a statutory exception as referred to in Article 77 Wbp or on the basis of recitals 104) and 107) GDPR. One of those exceptions is 'unambiguous consent': the party whose personal data are being transferred must have given unambiguous consent. Another statutory exception is transfer on the basis of a model contract (as drafted by the European Commission). Authorization from the Minister of Security and Justice is required for amendments or additions to the model contract. In all cases where personal data are transferred to a country outside the European Union, this must be reported to the Dutch Data Protection Authority.

Third parties to which NBU transfers personal data include but are not limited to:

- Education Executive Agency (DUO)
- Government institutions
- Municipalities
- Dutch Tax and Customs Administration
- Internship or work placement companies/organizations
- Accreditation organizations
- Study societies
- Student associations

[4] For this list, see: https://autoriteitpersoonsgegevens.nl/nl/onderwerpen/internationaal-gegevensverkeer/doorgifte-binnen-en-buiten-de-eu#wanneer-mag-ik-toch-persoonsgegevens-doorgeven-naar-een-derde-land-zonder-passend-beschermingsniveau-1753.

# 8. Privacy rules

Specific privacy rules are necessary for certain areas. Staff can limit themselves to the privacy rules that are relevant to them. By formally adopting these privacy rules, the implementation of the privacy policy becomes verifiable.

Specific privacy rules have been adopted for the following areas:

1. *Listing of data processing operations*
2. *Website and apps*
3. *Scientific research*
4. *Administration and operational management*
5. *CCTV monitoring*
6. *Confidentiality concerns*

## 8.1 Privacy rules – Listing of data processing operations

**Introduction**

The privacy policy states that specific privacy rules are necessary in certain areas. One of these areas is the listing of data processing operations.

**Responsibility**

1. Data processing operations are reported to the DPO in accordance with Article 27 Wbp and Article 30 GDPR.
2. The process owner is responsible for this report.
3. The DPO is responsible for listing the data processing reports.

**Reports**

Each report contains at least the following details:

- Functional name of the system
- Holder of the system
- External parties involved
- Purpose of the processing
- Which categories of personal data of which categories of data subjects are being recorded
- Retention periods to be observed, which can differ for each type of data
- Which special personal data[5] are being recorded
- Description of the adopted security measures
- List of organizations to which personal data are provided

The statutory principle is also stated along with the purpose of the processing:

- Consent of the data subject
- Performance of an agreement
- A statutory obligation
- To safeguard a vital interest of the data subject
- Performance of a public-law duty
- Legitimate interest of the controller or third party to which the data are provided
- The DPO is responsible for the quality assurance of the reports.
- Information systems that do not use personal data are not reported.

Processing operations that fall under the Exemption Decree[6] are still reported as far as possible to the DPO for the purpose of the summary.

**Transparency**

The DPO publishes a summary of the reports on the website.

[5] Processing of personal data concerning someone's religious or philosophical beliefs, gender identity, race, political opinions, health, sex life, trade union membership, and criminal background is permitted only under certain conditions, Section 2 Wbp, Article 9 GDPR.

[6] Standard processing operations that occur often and are commonly known to take place do not legally have to be reported under specific conditions. The Wbp Exemption Decree, Bulletin of Acts and Decrees 2014, 520 (entry into force: 7 May 2001), see http://wetten.overheid.nl/BWBR0012461. Since NBU wishes to have a summary of all processing operations, an internal report is desirable.

## 8.2 Privacy rules – Website and apps

**Introduction**

The privacy policy states that specific privacy rules are necessary in certain areas. One of these areas is NBU's website and apps.

**Responsibility**

1. Marketing & Communications (M&C) is responsible for implementing the privacy policy for the website and apps.
2. Websites on subdomains fall under the responsibility of the relevant unit or association/society. M&C gives them proactive advice.
3. M&C informs website managers about the relevant privacy rules if they collect personal information with forms.

**Monitoring of visitors**

1. Visitors are monitored only if there is good reason to do so. The proportionality principle is applied for this purpose.
2. The websites and apps clearly state how and for what purpose visitors are monitored.
3. The websites and apps clearly state which data are collected.
4. The websites and apps clearly state how visitors can visit the website or use the app without being monitored.

**Forms**

- Forms on the websites and in apps do not ask for more personal information than is necessary for the purpose for which it is being collected.
- Each form clearly states the purpose or purposes for which the requested information will be used.
- Each form is part of an information system to which the Privacy rules – Listing of data processing operations apply.

**IP addresses**

- IP addresses are not used to monitor visitors.
- IP addresses are logged and can be used to resolve security incidents and/or technical malfunctions.
- IP blocks can be used for statistical analysis.

## 8.3 Privacy rules – Scientific research

**Introduction**

The privacy policy indicates the areas in which specific privacy rules are necessary. One of these areas is scientific research. Researchers like to have a clear summary of the privacy rules that apply to them. This summary follows below. These rules also apply to students who are conducting research.

If a faculty has an ethics committee, it is recommended to include the PCP in the review process.

**Relevant documents**

- Each researcher who works with personal data should become acquainted with the VSNU Code of Conduct for the use of personal data in scientific research[7].
- Each researcher who works with medical data should become acquainted with the Federa Code of Conduct for Health Research[8].

**Commencement of research**

- A data management plan is drawn up in accordance with the Research Data Policy.
- If identifying data of people are used, a report must be made in conjunction with the PCP to the DPO in accordance with the Privacy rules – Listing of data processing operations.
- Consider the anonymization or, if that is not possible, the pseudonymization of the data[9].
- Clear arrangements are made for how personal data will be handled. These arrangements are recorded in the data management plan.

**Data storage**

- If external storage or other cloud services are used, a processing agreement[10] is concluded.
- Bear in mind that personal data cannot simply be stored outside the EU.
- Prevent data leaks by dealing carefully with data storage.
- If confidential information is being transported (e.g. on a USB flash drive or laptop), it must be encrypted.
- If confidential information is being provided to others (for example via a cloud service or e-mail), it must be encrypted.
- The authorization policy is applied for access to a data repository.

[7] See http://www.vsnu.nl/code-pers-gegevens.html.
[8] See https://www.federa.org/code-goed-gedrag.
[9] Article 89(1) GDPR: '... Where those purposes can be fulfilled by further processing which does not permit or no longer permits the identification of data subjects, those purposes shall be fulfilled in that manner.'
[10] ASC can provide support in this regard.

## 8.4 Privacy rules – Administration and operational management

**Introduction**

The privacy policy states that specific privacy rules are necessary in certain areas. One of these areas is administration and operational management. The privacy rules (see Chapter 8.6) apply in full to administration and operational management.

**Responsibility**

The holder or owner of an information system is responsible for complying with the privacy rules.

**Processing**

1. In accordance with the Classification Guideline for Information and Information Systems, a classification is made before or at the start of the project, so the results can also determine the requirements for the information system.
2. SURF's Legal System of Standards for Cloud Services in Higher Education is applied if cloud services are used.
3. A Privacy Impact Assessment (PIA) is carried out if personal data are processed. The results of the PIA are incorporated in the business case for the project. An assessment is made to determine the extent to which the processing of personal data is necessary. The different interests are weighed up for this purpose.
4. The DPO is ideally present/involved during the performance of the PIA. The result is sent to the DPO for assessment in any case.
5. If an external processor is hired, a processing agreement is concluded.

**Implementation**

1. Privacy is taken into account and data minimization is applied from the start of the design process.
2. The holder reports the data processing to the DPO before the system is put into use.
3. Retention periods are defined, so personal data are not kept for longer than necessary.
4. The holder informs the data subjects about the data processing.
5. The holder organizes a process so the right to inspect and the right to improve, supplement, remove, or block data can be promptly complied with, within a period of four weeks.
6. In principle, production data, other than to reproduce identified problems, are not used for testing purposes. If production data are used for an acceptance test, the authorization matrix must coincide with that of the production environment.

## 8.5 Privacy rules – CCTV monitoring

**Introduction**

In addition to the privacy rules, the following rules apply to CCTV monitoring at NBU.

**Responsibility**
As the process and system owner, Facilities Management is responsible for complying with the privacy rules in case of CCTV monitoring at NBU under the ultimate responsibility of the UB.

**Purpose and transparency**
The data are used solely for the following purposes:

- Protecting the health and safety of natural persons
- Securing access to the buildings and grounds*
- Guarding items located in buildings or on the grounds
- Recording incidents

CCTV cameras are mounted in clearly visible places and signs, for example, indicate where they are being used.

**Access**

- Live CCTV footage can only be accessed by staff who are tasked with security and surveillance at NBU.
- Recorded CCTV footage can only be accessed in a specially equipped area.
- Only the head of the responsible department or his/her deputy has access to recorded CCTV footage.
- The staff involved have a duty of confidentiality in relation to data that can be traced to specific individuals.

**Storage**

- Recorded CCTV footage is stored in a way that it cannot be accessed by others.
- Recorded CCTV footage is not kept for longer than two weeks.

**Management of image data**

The UB, Works Council, and Data Protection Officer (DPO) receive a summary of the actual applications of CCTV each year. This summary contains the location of the CCTV cameras, their application, and states which members of staff have access to the monitors and any recorded footage. If CCTV monitoring is to be extended, the application of a camera is to change, or a camera is to be removed, the process and system owner, Facilities Management, must ask the Works Council and the DPO for their prior consent.

*This does not involve the maintenance of public order as stipulated in Article 151c of the Municipalities Act (*Gemeentewet*).

**Incidents**

NBU has a code of conduct in which unauthorized behavior is described. CCTV cameras are not actively used to monitor behavior. However, if it transpires after an incident that relevant footage is available, it may be decided to preserve this footage and keep it as long as is needed for any internal investigation.

Footage is provided to third parties only if required in the interest of NBU and only after the University Board has decided accordingly. The police may obtain the footage only on demand (by commandeering it) or after the public prosecutor or assistant public prosecutor gives consent.

## 8.6 Privacy rules – Confidentiality concerns

The actual generic concerns, which the holders of information systems must interpret for each data processing operation to determine whether or not to introduce additional measures, are set out below.

*Authorization.* It is important to be sure that only those people who need confidential information actually have access to that data. Implementing the authorization policy can ensure this. Pay attention to the use of an account by another person, including during a period of temporary substitution, such as maternity leave.

*Authentication*. Take steps to prevent someone from being able to impersonate another person in order to access confidential information. Prevent staff from sharing or writing down passwords. Consider two-factor authentication.

*Access* from somewhere other than the fixed workplace. Working from home or at another location can lead to additional risks. This can be prevented by filtering by IP address.

*Input* of data. Bear in mind that notes and temporary documents can also include confidential information. Ensure the controlled removal or destruction of such records and files.

*Processing* and consulting data. If a member of staff retrieves or adds information, confidential information, which is not necessary for the operation, can be hidden or placed behind a further button.

*Interrupting* work. Consider using screensavers so as not to leave confidential records visible.

*Exchanging* data with other systems. Do not exchange more data than necessary. If confidential information is provided, ensure that those data also remain confidential. Make clear arrangements in advance.

*Producing* reports. The degree of confidentiality that must apply will be determined for each report. Once it is known that a report is confidential, this can be stated on the report as standard procedure.

*Storing* data. Critically confidential information should be stored encrypted. Where there is centralized storage, it is important to prevent hackers or administrators from having access. Where there is decentralized storage, there is a greater risk of viruses and theft. Documents containing critically confidential information, such as a file, should be stored in a locked cabinet.

*Saving* e-mails. Keeping confidential information on record in the e-mail system means that the information remains accessible for long periods on any device, including a telephone or tablet. Examples include sickness reports, job application letters, and performance reviews. Remove e-mails containing confidential information from the system as soon as possible.

*Archiving* information. Define the retention period and the rules on access and destruction.

*Printing* data. Documents containing critically confidential information may be printed only in the presence of the staff member, may not be left lying around, may not simply be taken elsewhere, and must be removed or destroyed in a controlled manner after their use.

*Carrying* digital data. Information can be carried with you on a USB flash drive, hard drive, laptop, etc. First consider whether the information is necessary; is it not possible to leave out the confidential information? Critically confidential information should be stored encrypted.

*Consulting* information on a mobile device. As described in the memorandum on the use of ‘own’ devices and applications, further security measures may be adopted depending on the classification.

*Working* in public spaces. Other people can be reading from the same screen or document as you. Avoid this happening when consulting confidential information. Examples include corridors, canteens, cafés, restaurants, waiting areas, when traveling on trains or airplanes, etc.

*Discussing* information. Bear in mind that when you are discussing information, including on a telephone, other people can be listening as well.

*Sending* information. Check whether the person involved actually needs this information and try to minimize the information being provided. Check whether we (NBU) are authorized to provide this information to the person involved. If confidential information is sent by e-mail or in another digital form, it should be encrypted.

*Audit trail*. It must be possible to establish via a log file who has had access to confidential information.

*Theft* of information. Which procedures apply if a document containing confidential information or an information carrier (USB flash drive, tablet, etc.) is lost? First, minimize any further damage by changing passwords, etc. The further steps are set out in the Duty to Report Data Leaks procedure.

*Writing* procedures. Include the roles of staff members in procedures and not individual names.

*Expanding* or new designs/purchases of applications. Consider what security aspects play a role beforehand. The Classification Guideline and a PIA can assist in this regard. Extra requirements halfway through a project lead to higher costs.

*Testing* applications. Live data are often used to test an application. This is a realistic approach. However, the critically confidential information can best be left out of most tests. This can be done by overwriting certain fields in a database with other information, or garbling data, and not using any confidential documents.

*Outsourcing* work or using cloud services. Make clear arrangements and if personal data are exchanged, enter into a processing agreement.

# 9 Incidents relating to personal data

Every complaint or report relating to the processing of personal data within NBU is a privacy incident. The best-known form of such an incident is a data leak[11]. This chapter describes the policy relating to the reporting, registration, and handling of incidents, or suspected incidents, during normal business operations and under special circumstances.

## 9.1 Reporting and registration

NBU staff are obliged to report an actual or suspected 'data leak' and other privacy incidents directly to the ICT Help Desk at +31 (0)346-291288 or helpdesk@nyenrode.nl. If the person making the report prefers to do so, a confidential report can also be made to the DPO, who will keep the name of that person confidential. Examples of data leaks are set out in Appendix C.

ICT Services registers every incident and how it is handled. Reports are treated confidentially. The person making the report can rest assured that making a report will have no personal consequences for him/her. As long as the incident is still being handled, the person who made the report must deal with it confidentially and not discuss it with data subjects or other parties.

## 9.2 Handling of reports

Once the report has been received, a thorough analysis takes place to determine the extent and impact of the incident. In case of serious security incidents, the Computer Emergency Response Team (CERT) Nyenrode is activated. In practice, this is a virtual team that consists of the staff members of ICT Services. More information on the progress of the process can be found on Nyenrode's central platform: https://my.nyenrode.nl/organization1/Informatiebeveiliging/Pages/default.aspx.

Incident handling aims to resolve the problem, limit the damage, and comply with legislation. Incidents are handled and discussed in the relevant operational meetings and, if the operating process, finances, or the reputation of NBU are at risk, also in the UB. Immediate action can be taken when alarming trends are discovered, for example by adopting additional measures or running an awareness campaign.

The purpose of CERT-Nyenrode is to prevent information security incidents as far as possible and to tackle them as soon as they arise, so as to support the continuity of Nyenrode and protect its reputation. CERT Nyenrode also deals with security incidents outside Nyenrode if the university's own staff are involved in any role.

The members of CERT-Nyenrode are appointed by the Head of ICT and operate on his/her instructions. CERT Nyenrode can escalate serious incidents via the IT Security Manager to the information security portfolio holder. This structure facilitates direct escalation to the UB and direct contact with other people within Nyenrode who are responsible for contact with the press and for legal matters.

CERT-Nyenrode is entitled to order the temporary isolation of system/network users, computer systems, or network segments to be able to perform its duties.

The IT Security Manager assesses whether there has been any data leak. If there has been a data leak, the DPO is involved in the further handling of the incident. The manager will also often be involved. The DPO is responsible for handling privacy incidents. If the incident involves a data leak, a determination is made under the rules of the Dutch Data Protection Agency (DPA)[12] as to whether a report must be made to the

[11] If personal data fall into the hands of third parties who may not have access to those data, this constitutes a data leak.
[12] 'The duty to report data leaks in the Personal Data Protection Act (Wbp): Policy rules for applying Article 34a Wbp' and Articles 33 and 34 GDPR; Recitals 85-87.
See https://autoriteitpersoonsgegevens.nl/nl/melden/meldplicht-datalekken.

DPA. The report is coordinated with the UB. A report to the DPA must be made within 72 hours of the discovery.

If it is compulsory to notify the data subjects under DPA rules, or otherwise advisable, the communication is dealt with in conjunction with M&C. The person who made the report is informed about the handling of the incident.

## 9.3 Evaluation

It is important to learn from incidents. In addition to drawing up a policy vision, which is subsequently expounded into plans and activities to be able to achieve the defined objectives, the result must be measured. The registration of incidents and periodic reporting are conditions for this purpose. This is not only to measure whether the activities that must ensure the achievement of the result are performed, but also to gain insight into further points for improvement. Reporting on incidents relating to personal data is a permanent feature of the privacy annual report and the plan-do-check-act (PDCA) cycle.

# Appendix A Definitions and abbreviations

CBP: *College Bescherming Persoonsgegevens*, the former name of the Dutch Data Protection Authority.

Controller: the natural person, legal person, or any other party or management body that, alone or jointly with others, determines the purpose and means for the processing of personal data. At NBU, the UB is responsible, but this responsibility has been delegated to the holder of the relevant information system.

Data leak: personal data that fall into the hands of third parties that do not and/or may not have access to those data.

Data subject: an individual and natural person to whom a personal data item relates.

DPA: Dutch Data Protection Authority.

DPO: Data Protection Officer.

GDPR: General Data Protection Regulation. Regulation (EU) 2016/679. The European successor of the Wbp that enters into force as from May 2018.

NBU: Nyenrode Business Universiteit, Universiteit Nyenrode B.V., Nyenrode.

PCP: Privacy Contact Person.

Personal data item: any data item concerning an identified or identifiable natural person.

Privacy Impact Assessment / Data Protection Impact Assessment: a tool that helps to identify privacy risks and provides points of reference for reducing these risks to an acceptable level.

Processing of personal data: any operation or set of operations in relation to personal data, including collection, recording, organization, storage, adaptation, alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, as well as the restriction, erasure or destruction of data.

Processor: the party that processes personal data on behalf of the controller, without being subject to the controller's direct authority.

Third party: any party, other than the data subject, controller, or processor, or any person that falls under the direct authority of the controller or processor and is authorized to process personal data.

UB: University Board.

Wbp: Personal Data Protection Act (*Wet bescherming persoonsgegevens*). Based on Directive 95/46/EC.

# Appendix B Classification

Dealing correctly with information is vital for the proper functioning of operating processes within Nyenrode. Students and staff must be able to trust that information is secure, accessible, available, correct, and complete. Information may moreover only be available to those who are entitled to it. Nyenrode intends to classify all data, to which this information security policy applies, by the quality aspects *Availability*, *Integrity* and *Confidentiality*. This action is included in the information security plan for 2017-2018.

| | |
|---|---|
| A = Availability | Is the information/function present/useful/legible? |
| I = Integrity | Is the information/function reliable/complete/unimpaired? |
| C = Confidentiality | Do only entitled parties have access to the information/function? |

The appropriate level of security measures for a particular information system depends on the classification of the information that the system processes.

The following classes are distinguished in relation to the availability requirements:

| **Classification** | **Definition** |
|---|---|
| Not vital | General loss or unavailability of this information for less than one week does not harm the interests of Nyenrode, its staff, students, or clients. |
| Vital | General loss or unavailability of this information for up to one day does not harm the interests of Nyenrode, its staff, students, or clients. |
| Extremely vital | General loss or unavailability of this information for up to one hour does not harm the interests of Nyenrode, its staff, students, or clients. |

The following classification is used for both Confidentiality and Integrity:

| **Classification** | **Definition** |
|---|---|
| Public | • Anyone may examine the data, such as the general website of Nyenrode.<br>• A selected group may alter these data. |
| Internal | • Anyone who is connected to Nyenrode as a member of staff, student, or third party may examine these data; access can be provided both within and outside Nyenrode (remotely).<br>• A selected group may alter these data. |
| Critical | • The identity of the parties and their specific rights to consult and process these data are explicitly stated and registered. |

The classification should be made by or on behalf of the process/system owner of the relevant information or relevant information system.

# Appendix C Examples of data leaks

Examples of data leaks include:

- a lost or mislaid encrypted USB flash drive with personal data;
- a lost or stolen encrypted telephone/laptop/tablet (private or business) with personal data or access to a Nyenrode account with personal data;
- printed documents containing personal data that are left unattended at a photocopier;
- anonymous survey results that still seem able to be traced back to respondents;
- access to personal data that can be traced back to natural persons to which you should not have any access;
- intrusion in a computer with personal data or access to a Nyenrode account with personal data by a hacker;
- circulation of a list with names, student numbers, and/or study results of students;
- circulation of a list with names, telephone numbers, and/or residential addresses of staff members;
- unauthorized persons who are able to examine CCTV footage.

Examples of other privacy incidents include:

- data collection that is not reported to the DPO;
- unsafe working methods that can lead to data leaks;
- data collection based on a data subject's consent that has not actually been requested or registered;
- sending sensitive personal or other data via an unsecured route or to an incorrect e-mail address (i.e. an unintended recipient);
- intrusion in a computer with personal data or access to a Nyenrode account with personal data by a hacker.