university of groningen

Policy Plan for the Students and Teaching Domain

Policy and guidelines for the careful processing of personal data

Adopted by the Board of the University on 14 January 2020

Preface

The Policy Plan for the students and teaching domain describes how the University of Groningen (UG) protects personal data regarding students and teaching in relation to the General Data Protection Regulation (GDPR). It also contains several guidelines for the processing of students' personal data.

This policy was established on the basis of joint consultation by the privacy and security coordinators for the Teaching domain, who have been appointed at all faculties and a number of university services.
This policy applies to the processing of personal data that takes place within the Students and Teaching domain under the responsibility of the UG.

The policy focuses in particular on all UG staff working in the Students and Teaching domain and on staff of the University Medical Center Groningen (UMCG) working at the medical faculty within the Students and Teaching domain.

The policy plan has been divided into two cycles: Life cycle for students and Life cycle for teaching

Life cycle for students

Recuitment, Admission and Application, Study progress, Degree certificate, Alumni

Life cycle for teaching

More information about the GDPR can be found on the UG website:
https://www.rug.nl/mu/privacy
The privacy portal also contains practical suggestions, elaborations and examples of how the GDPR is being implemented.

Table of contents

1. General information about the processing of personal data

On 25 May 2018, the General Data Protection Regulation came into force.
The essence of the Regulation is that an institution, in this case the UG, has a duty of accountability concerning the protection of personal data.

This means that the following must be documented:

- which personal data are collected and processed
- for what purpose, and
- what organizational and technical measures have been taken to ensure that the processing of personal data is being carried out in accordance with the GDPR.

The Board of the University of Groningen is ultimately responsible for the policy regarding the GDPR and its implementation. To that effect, the Board of the University has prepared a General policy on the protection of personal data.

Within the Students and Teaching domain, the UG deals with the processing of personal data of (prospective) students, course participants and, in the case of research and internships by students, research subjects and third parties involved.

1.1. Basic concepts

The overview below describes a number of basic concepts that are frequently used in the policy plan.
In addition, **Appendix 8.6** includes a list of abbreviations and definitions.

Personal data is understood to mean all information that can identify a natural person or information that can be traced back to this person now or in the future. This may include name and address details, student number or other information that uniquely identifies a person. It can also be a combination of information that, individually, cannot directly be traced back to a person, but which, when combined with other information, may identify a person, e.g. a combination of residence, age and study. This type of data is referred to as indirectly traceable personal data.

The person to whom personal data relate is referred to as the data subject.

Processing is understood to mean the manual or automated collection, recording, ordering, structuring, storage, modification, retrieval, consultation, use, provision, forwarding, distribution or making available, combining, blocking or destroying of data. It concerns both paper files or archives, digital files or personal data in an application or system, including mailboxes, laptops, USB sticks and other data carriers. In other words, everything you do with personal data on any data carrier.

The process manager is responsible for the processing of personal data. This is the person who determines how a process runs, for example, the head of the Education Office, or the head of the Student Information & Administration department.

The process owner must ensure that all staff processing personal data do so in line with the UG's General policy on the protection of personal data.

The controller is the organization, person or group that determines the purpose and means of data processing.

The processor is a person, company or group that processes personal data on behalf of a controller and who/which is not part of the controller's organization.

1.2. The principles and aim of processing

Lawful processing of personal data is only permitted if it is based on one of the following six principles:

Legal duty	Processing is necessary for the execution of a legal obligation.
Execution of an agreement	Processing is based on an agreement to which the data subject is a party.
Task of general interest	Processing is necessary for the performance of a task in the public interest or a task assigned by a government agency (public authority) regulated by law.
Vital interest	Processing is necessary because it affects a person's life, e.g. in the event of a medical emergency.
Legitimate interest	Processing is necessary to protect the legitimate interests of the data controller (UG) and often results from the performance of a legal obligation or a public interest.
Permission	Processing is based on the consent of the data subject. The data subject must be clearly informed in advance about the processing for which they must give their consent actively and voluntary.

In addition, the processing must have a concrete purpose (purpose limitation).

In the context of its teaching activities, the UG processes the personal data of students and prospective students and alumni for the following purposes:

1. Determining the identity of students and prospective students
2. Informing prospective and registered students about degree programmes at the UG
3. Recruiting new students and promoting the University
4. Carrying out administrative activities relating to registration and to the calculation, recording and collection of tuition and examination fees
5. Assessing prior qualifications and operating a ballot system, matching and selection
6. Registering students for course units and registering attendance
7. Recording and showing lectures
8. Collecting and assessing students' assignments
9. Assessing study results and awarding credit points
10. Offering and supplying educational means, IT facilities and restaurant facilities and providing facilities for remote collaboration
11. Supporting students with a physical or intellectual disability
12. Supporting students who have incurred a study delay
13. Measuring and improving the quality of teaching and teaching facilities
14. Early detection of possible study delays or obstacles to study progress
15. Preparing policy decisions in the field of teaching and creating management information for the governing bodies within the University
16. Quality research to prepare policy decisions and management information
17. Offering supplementary teaching, placements, career preparation and other extracurricular activities
18. Executing exchange programmes
19. Organizing and holding elections for consultative participation bodies
20. Recording study results and examination results, and preparing degree certificates
21. Advising and supporting students and assessing special circumstances related to a binding (negative) study advice
22. Dealing with complaints, objections and appeals
23. Registering students for alumni associations
24. Raising funds among alumni and maintaining a bond with alumni
25. Securing the University buildings
26. Securing information and the proper functioning of IT facilities

In addition to determining purpose limitation and lawfulness, several fundamental principles apply:

- *Care, integrity, confidentiality*
  Protect personal data by taking technical and organizational measures against unauthorized or unlawful processing.

- *Availability and accuracy of information*
  Make sure the personal details are correct and update them where necessary.

- *Data minimization*
  Do not process more data than necessary.
  Do not keep personal data longer than necessary for the purpose for which it was collected, or store it in such a way that it cannot be traced back to the person (storage restriction).

- *Transparency, lawfulness, fairness*
  Inform data subjects about the basis on which and the purpose for which personal data are processed; what measures have been taken to protect the data; who has access to the data; what possibilities the data subject has to exercise their rights. Include this in a Privacy Statement.

1.3. Students' rights

Students have several rights with regard to their personal data:

Right to information	The right to be informed about which personal data is being processed
Right of access	The data subject's right to access the personal data collected
Right to rectification	The right to require correction of inaccurate personal data
Right to restriction	The right to restrict the processing of personal data, e.g. pending the outcome of an objection. Restriction means that personal data is flagged, and may not be processed or shared during this period.
Right to erasure of data	The right to request the erasure of personal data
Right to object	The right to indicate that data may not or may no longer be processed

If a data subject wishes to exercise these rights, they can submit a request by email to the privacy desk, privacy@rug.nl
In addition, a student can always submit a complaint, objection or appeal to the Central Portal for the Legal Protection of Student Rights (CLRS): https://www.rug.nl/education/laws-regulations-complaints/

All rights are subject to a balance between the legitimate interest or/and the legal obligation of the institution on the one hand and the rights of the data subjects on the other hand.
https://myuniversity.rug.nl/infonet/medewerkers/faciliteiten-voorzieningen/juridisch-advies/privacy/

1.4. Starting points, principles and recommendations

Derived from the basic principles and rights of students referred to above, the following guidelines and recommendations apply to actions in this policy plan:

- **Only collect data necessary for the purpose of processing**

- **Do not process special categories of personal data**
  Unless the data subject has given their explicit consent. Special categories of personal data include data revealing a person's racial or ethnic origin; political opinions; religion or belief; trade union membership; genetic or biometric data for unique identification; health; sexual behaviour; criminal record. However, there are exceptions to the prohibition of processing special categories of personal data. These exceptions sometimes also apply to teaching.

- **Safe processing**
  Make sure that the data is only accessible to staff who need it by virtue of their duties and regularly check whether the assigned roles and rights giving access to the data still correspond to the work to be carried out.

- **Safe storage**
  An email inbox is not suitable for storing documents; store them on the Y drive, in the Digital Student Dossier (DSD) or in Progress.Net (PN).

- **Retention period**
  Under the GDPR, personal data may not be kept for longer than is necessary to achieve the purpose for which it is collected. This means that it must be deleted at a certain point in time, depending on the nature of the data. Retention periods have also been included in other legislation and regulations; these must of course be complied with. A basic overview is included in the Appendix to provide guidance on how long data should be retained. Make sure that the storage periods are observed. One way to do this is to archive documents by date and type, and to delete them periodically.

- **Safe sharing**
  There are several ways to share information with other stakeholders and interested parties: Unishare, SURFfilesender or via the Y drive.

- **Communication**
  Inform students in advance by means of a Privacy Statement about which data will be processed for which purpose, with whom it will be shared and how long it will be kept. A template for drawing up a Privacy Statement is included in the UG's DOT office.

This translates into the following non-exhaustive list of practical recommendations.

Transparency:
- Students are informed via a privacy statement of the purpose and the basis of the processing, who has access to the data and how long it is kept.
- They are also made aware of their rights and how to exercise them.

Safe storage and transfer:
- Documents attached to an email received must be deleted immediately after the documents have been stored or processed elsewhere.This applies to both sent and received eamils.
- The email message itself will be deleted as soon as it is no longer needed. This is a fixed routine in the workflow. Before the start of a new academic year, all emails relating to, among other things, application, admission, matching, selection, binding (negative) study advice (BSA) from cohort X (= for example three years ago) will be deleted.
- Documents will be shared securely (e.g. via Unishare, SURFfilesender, or Google Drive); if they need to be stored, they will be stored securely on the Y drive or in the DSD or PN. After a set period of time, the documents will be deleted or archived.
- Information storage, such as the mailbox, physical or digital documents or a database containing

personal data must be set up in such a way that a retention period can be linked to the data. After all, on the basis of the GDPR, personal data may not be kept longer than necessary for the purpose for which it was collected or was necessary on the basis of a legal obligation.
- Data may be kept for longer if it is used for historical, academic or statistical purposes or if it serves a public interest.
- Standardization and harmonization of processes in systems promote the control and monitoring of the careful and secure handling of personal data.
- Related to this: it is worthwhile periodically homing in on the processes in order to optimize the quality of data protection. For example, certain documents are unnecessarily copied, retrieved and/or emailed back and forth and stored in different places. This poses a risk to the protection of personal data.
- Periodic checks must be carried out to determine whether staff are still entitled to access personal data. The roles and rights for access to PN and ProgressWWW are determined by the student administration offices of the faculties, in consultation with the functional administrator; these apply throughout the UG. Depending on the sensitivity of the data, this check can be set at 6, 12 or 24 months.
- The inclusion of documents in the DSD contributes greatly to the careful handling of personal data. The central storage of data prevents documents, such as a copy of a passport or of a degree certificate, from having to be submitted more than once.

1.5. Processing of data for, by or with other (educational) organizations or legal entities

The UG provides services in conjunction with or on behalf of other (educational) organizations. Examples are the partnership with Hanze University of Applied Sciences, double/joint degree programmes with (international) universities or the sending of information about the introductory programme by the UG on behalf of the *Kommissie Eerstejaars Introductie* (first-year introduction committee, KEI). In addition, the UG receives much information via *Studielink*, which also includes links with DUO (Dienst Uitvoering Onderwijs, the Education Executive Agency), the BRP (Basisregistratie Persoonsgegevens; municipal personal records database) and the Immigration and Naturalization Service (IND).

Depending on the relationship between the parties and the nature of the services, the terms used are controller and processor or joint controllers.

The controller is the organization, person or group that determines the purpose and means of data processing. e.g. if and when data must be processed, to what purpose or purposes, how long the data must be kept and with whom the data may be shared.

The processor is a person, company or group that processes personal data on behalf of a controller and who/which is not part of the controller's organization. For example, the external legal entity that provides services for the UG (such as the supplier of the student information system PN) is the processor and the UG is the controller. If the UG provides services to another party on behalf of the other institution or legal entity, the UG is the processor and the other party is the controller. In both cases, a data processing agreement must be concluded describing the arrangements for the careful and secure processing of personal data.

Two or more institutions may be jointly responsible. In that case, a cooperation agreement will be concluded, which includes how personal data will be handled by the controllers.

In the case of multiple parties processing personal data, it may be complex to determine who has what role and what needs to be agreed and recorded in concrete terms. Sections 3.9 and 3.10 of the General policy on the protection of personal data provides more details on this. The privacy & security coordinator of the faculty or University Service may also answer questions about it.

Part I: STUDENTS

2. Student application & registration

The application of students or registration of course participants takes place in various ways, depending on the type: via Studielink or via faculty systems. There are the following categories:

- **Prospective Bachelor's and Master's students, including international students**
- **Non-standard registration: Course participants, exchange students, minor students, summer school and winter school students**
- **Postgraduate teaching and PhD students (these are PhD students who are not employed by the UG, but who have been awarded a scholarship by the UG)**

Refer to **Appendix 8.1** of this policy plan for a detailed description of the application and registration process.

2.1. Basis for processing

Pursuant to the Higher Education and Research Act (Wet op het hoger onderwijs en wetenschappelijk onderzoek, WHW) or on the basis of an agreement, personal data may be processed during the registration process.

No special categories of personal data will be recorded during the student application and registration process without their explicit consent. If a student does not give their consent, this should not prevent them from registering.

However, the processing of a copy of the proof of identity and special categories of personal data is permitted for application and registration:

- When the student does not have an EU nationality (for the purpose of applying for a visa with the IND)
- For identification purposes
- In the case of (outgoing) exchange students, the UG provides the foreign institution with a copy of proof of identity in special cases. The student must give their explicit consent for this.

For identification purposes, viewing proof of identity is sufficient and storage is only permitted if this is necessary, for example, for an extra check of personal data; however, the copy must then be masked: the *Burgerservicenummer* (citizen service number, BSN) and photo must be blotted out.
Once the data has been definitively processed, the copy must be deleted.

2.2. Processing and transfer of personal data of students who have applied or registered

If personal data is subsequently used for a purpose associated with the provision of teaching, for example, registration for tutorials, in most cases the basis is still a task carried out in the public interest.
On this basis, staff of faculties and university services are entitled to access personal data of students in, among others, PN and ProgressWWW.

Setting up authorization profiles to ensure that certain staff members have access to certain personal data needed for the performance of their work solely on the basis of their position will ensure that the data is handled securely.

Student and study associations
As already mentioned, the UG does not provide personal data to third parties, except when required by a legal obligation or with the explicit consent of the data subject. Data of newly registered students may not be provided to or shared with the Stichting KEI (for the purpose of the introduction of first-year students), the foundation Academische Centrale voor Lichamelijke Opvoeding (ACLO), study associations and student associations. However, the UG occasionally informs students on behalf of these UG-affiliated organizations of their activities. An example could be to inform prospective students about the KEI introduction programme.

Member lists of student and study associations are also periodically checked for registration as a student. This includes the foundation ACLO. The foundation or association has to inform their members and

participants.

Specific occasions of transfer
The UG supports international students by transferring contact details to the Municipal Health Service (GGD) for tuberculosis control, to the Immigration and Naturalization Service for visa applications, and to the municipality for registration with the municipality.

In order to be able to work at UMCG labs/departments or to follow a clerkship in an affiliate hospital, students must have been vaccinated against hepatitis. The faculty must indicate which students are registered for a degree programme that also uses UMCG labs; these students must demonstrate that they have been vaccinated.

As a service, the UG, with the consent of the student, passes on personal data of international students to the student housing agency Stichting Studenten Huisvesting (SSH).

In order to be eligible for a scholarship, personal data, such as marks and study progress, must in some cases be given to the scholarship provider. This is only allowed if the student has given their explicit consent.

In the case of a joint programme or exchange programmes, the UG transfers personal data to a partner university; the basis for this is the performance of a task of general interest.
Students must be informed in advance that data will be shared and which data that is.
A cooperation agreement must be concluded with the partner university in question, in which the mutual rights and obligations arising from the GPDR are specified.

Information may be requested by a person other than the data subject, e.g. parents requesting a student's contact or study details, or an employer enquiring about a degree certificate. Third-party requests (including parents/carers) for information about students will in principle not be granted unless explicit written consent has been given by the data subject (e.g. if a fiduciary has been appointed).

2.3. Communication with students who have applied or registered

Students request information about their registration or study progress from, for example, the Central Student Administration (CSA) or the Education Office. It is necessary to verify the identity of students in order to prevent information relating to personal data from being disclosed to third parties unintentionally, for example, by:

- Physical identification, for example, by showing the University Card (with photo) or proof of identity
- In the case of a telephone or email reply, the identity can be established by asking a number of verification questions and/or requesting the student to submit the request via their University email account. Of course, it remains difficult to verify anyone's identity over the phone, but questions to ask could include: Could you tell me the correspondence address you gave us? What is your date and place of birth?

2.4. Retention periods

The basic rule for processing personal data is that it may not be kept longer than necessary for the purpose for which it was collected. Therefore, the GDPR does not set unambiguous retention periods. Concrete retention periods are, however, included in several laws. The WHW, the Public Records Act and tax legislation stipulate that certain documents must be kept for a specific period.

If the retention period for personal data has expired, or if the data is no longer needed for the purpose for which it was collected, the data must be destroyed. The data may also not simply be kept for a purpose other than that for which it was collected. An exception to this is the processing of data for scientific or statistical purposes or when the data is kept in the public interest. If personal data is intended for historical, statistical or scientific purposes or if it serves a public interest, it may be stored for a longer period of time. This is subject to the time limits set by the Public Records Act and included in the UG Regulations concerning archives.

Appendix 8.2 contains an explanation of the retention periods.

3. Study progress

After students are registered for a degree programme, they go through several stages in which personal data are also processed. This chapter describes the most important processes and guidelines.

3.1. Attending classes

Various study-related activities are organized during the programme that involve several people, such as seminars, tutorials, examinations, the BSA and the graduation ceremony.

Exchanging personal data (e.g. name, programme, telephone number and email address) is needed for smooth communication and work processes.

The following principles apply:

Data minimization

- Limit the amount of data to a minimum. For example, if data such as date of birth, address, and gender is not necessary to achieve the intended purpose, it should not be retrieved and/or processed.
- Delete the data as soon as the purpose for which it was collected has been achieved or when it is no longer relevant. Consider in particular the data in an email box, on a USB stick or laptop.

Purpose limitation

- Only process data for a specific purpose and make that purpose known in advance.

Transparency

- Inform the student explicitly about the basis on which data is processed, for what purpose and for how long the data will be kept; include this in a privacy statement.

Student rights

- The sharing of information about study results or other sensitive data is not permitted unless the sharing arises from a legal obligation, or is based on a public or legitimate interest. For example, providing study results to the Student Administration Office for the production of a degree certificate, the preparation of a binding (negative) study advice or the sharing of information between study advisors so that they can fulfil their duties arising from the University's duty of care.
- The general rule is that consent is required for the processing of special categories of personal data. However, the basis for making special categories of personal data about a disability available to a study advisor is the general interest. The UG has a legal duty of care towards its students. The data subject must provide proof of the special circumstances in order to be able to make a particular provision. Data will be handled with extreme care.
  Appendix 8.3 contains a description of the procedure for processing personal data of students with a disability.
- The use of a joint app or a mailing list cannot be required. A student has the right not to share certain data with others, as long as there are alternative means of communication. For example, an email to groups of students can be sent using the BCC function, or a message can be posted on Nestor (UG digital learning environment).
- The use of a student's private email address is permitted, provided that the students themselves have made this address available for a specific purpose. As a rule, the UG email address is the default address used to communicate with the student. The same applies to lecturers, who preferably should use their @rug.nl email address.

Safe storage and transfer

- Student assistants or on-call staff have an employment contract with the UG and are therefore bound by the provisions of the collective labour agreement. They are permitted to have access to specific data, provided this is needed for the performance of their job or activities. However, it is expressly advised that they be alerted at the start of their work to the special position they occupy as a student/staff member. When staff change jobs or leave the UG, the authorization must be adjusted immediately.
- If large files containing personal data (e.g. theses, examination results, and shared information regarding students with an external (university) partner) need to be shared, SURFfilesender or Unishare, for example, are safe methods. Both systems are available on the UG My University intranet. This applies to both the sharing of information between staff members (lists of examination results) and to staff members who want to share information with students. The grade centre in

Nestor is another way of sharing examination marks with students. Staff at the Faculty of Medical Sciences use the OWI-OA database to share student and other information.

- Using an app to upload personal data is in most cases an unsafe method; it would be better to use SURFfilesender.
- Google Drive is safe for shared working on a document. The UG has a processing agreement with Google which stipulates that this company must comply with European laws and regulations.
- Relevant student data is shared for the logistical and substantive support of teaching. Examples include personal data for timetabling and seminars, communication between lecturers about students who take part in their teaching, and student administration offices that register examination marks. Part of this information is provided automatically, part of the data transfer is upon request.
- The structure of roles and rights must be set up properly in the registration systems. Lecturers only receive the student number, name and UG email address of their students. In specific situations, they also receive information about, for example, additional facilities related to a functional impairment.

3.1.1 Examinations

Before students actually receive an examination result in their study progress overview, several stages must be completed. Below are the points of attention with regard to the processing of personal data in relation to examinations.

3.1.1.1. Taking examinations

At the time of the examination, students report to the examination location, identify themselves by means of their University card or ID and take the examination. Sometimes a special provision is made because of a functional impairment. This is covered by the guideline for students with a functional impairment, which is included in Appendix 8.3 to this policy plan.

3.1.1.2. Assessment of examinations

The examination is assessed by the examiner, after which a provisional result is announced. Given the nature of this information (i.e. an indicator of the student's competence in a certain field), it is considered sensitive personal data that must be handled with utmost care.

Results may not be shared by the lecturer, for example, by posting a result list in Nestor. The results must be announced individually. Results of group assignments can be shared if the result applies to all group members.

In the case of an individual assessment, the lecturer is not allowed to share this with the other students. Publishing partial marks for multiple students is also not allowed. The student has the right to inspect the work they have done and should have an opportunity to ask questions about the assessment.

3.1.1.3. Determining the final result

Once the final result has been determined, it will be registered in the study progress system (ProgressVolg).

3.1.1.4. Inspection of examinations

The WHW stipulates that the Teaching and Examination Regulations (OER) must lay down how and for how long the student can inspect their assessed examinations. The answers given by the student and any comments made by the examiner must be regarded as personal data and are therefore subject to the provisions of the GDPR. On the basis of the GDPR and the OER, students are entitled to inspect examinations and may request a copy of them.

<u>The following guidelines apply</u>:

- students are entitled to inspect examinations and to receive a copy. However, it is not necessary to provide a copy of the example workings, only the student's work. Students may also inspect (listen to) audio recordings.
- students may also inspect the lecturer's notes on the workings (e.g. feedback).

3.1.1.5. Bachelor's and Master's theses

In most cases, Bachelor's and Master's degree programmes will be concluded with a thesis. These theses are actually a special type of examination. The rules set out in Section 3.1.3 and beyond apply to these as well. However, a thesis has several special features, which are explained below.

A Master's thesis may be published through the UG University Library (UB). The procedure and obligations are described on the UG website and differ per faculty and degree programme. Together with the publication, several personal details are recorded in the library's database, i.e. name, student number, degree programme and the year of graduation. The thesis will be made publicly available online as a full text unless the student objects to this; the thesis will then be kept at the UB but will not be published.

Students may say at any time that their thesis may not be kept (any longer) in the library.

3.1.1.6. Sharing examination results

For some scholarship programmes, the scholarship provider requires access to the study results. Results may also be shared with partner universities at the request of the student if the student is in an exchange programme or if the partner university wishes to receive information about the student's study progress in the form of examination results.

For students with a visa with 'study' as the purpose of stay, the UG issues an annual declaration to the IND if they do not have sufficient study progress to retain their residence permit.

Student data may also be shared with external parties in the context of educational trips or placements.

The general principle is that students themselves are responsible for sharing the information with third parties. In principle, the UG does not provide the data directly to third parties, unless the student has given explicit consent to do so, or if this arises from a legal obligation.

3.2. Study progress supervision

During their study period, students can obtain supervision from a mentor, study advisor, student counsellor, top sports coordinator, student psychologist, and study choice and career counsellors. In addition, training sessions and courses are organized by the Student Service Centre (SSC) and Cultural Student Center USVA.

These forms of supervision are likely to involve special categories of personal data. The processing of special categories of personal data must be particularly safeguarded. These may only be processed with a view to the special supervision of students or to making special provisions in connection with their state of health.

The prohibition on processing special categories of personal data does not apply here if the processing is necessary for the purpose of special assistance or financial compensation due to special circumstances (Graduation Fund) and/or with a view to making special provisions in connection with a person's state of health.

<u>During supervision, the supervisor processes personal data and records them in a secure file that is protected from third parties and to which the following applies:</u>

- only necessary personal data is recorded (data minimization)
- special categories of personal data may be processed if this is necessary for supervision
- in the event of a medical or other emergency, certain information may be provided on the grounds of vital importance
- student psychologists work according to the professional codes of the Individual Health Care Professions Act (BIG) and the Dutch Association of Psychologists (NIP); they have a duty of confidentiality.

The supervision file may only be accessible to the supervisor in question and may only be exchanged with other internal disciplines if the data exchange is necessary for the supervision of the student and/or the provision of study advice. Study advisors can also view the notes of fellow study advisors. This is necessary because students may follow several courses of studies involving different study advisors. The basis for the exchange is that the exercising of a task in the general interest.

Students have the right to inspect the personal data recorded about them in their student file, with the exception of internal notes that contain the personal thoughts of staff members and that are exclusively intended for internal consideration. As soon as internal notes are shared, the notes are no longer covered by this exception and the right of inspection applies.

There may be exceptions due to special legislation (e.g. the Medical Treatment Contract Act).

Student counsellors provide support in the financial compensation procedure via the Education Executive Agency (DUO). The student counsellor, which also includes the BSN, signs and stamps the application form and forwards it to DUO. A copy of this form will be filed. The entire student file kept by the student counsellor and the study advisor must be destroyed 10 years after the end of the student's registration at the UG (related to the DUO degree certificate period).

3.3. Degree certificate ceremony

Once a student has passed their examinations, the degree certificate and the Diploma Supplement will be prepared. These documents contain sensitive personal data, such as examination results and honours.

3.3.1 Determining that the student can be admitted to the final assessment

Sometime before students have completed the examination programme, they must apply for the final assessment, or the Student Administration Office will ascertain that they have completed all examination components and subsequently the application will be made via PN or ProgressWWW.

The study progress will be checked by or on behalf of the Board of Examiners. As soon as all parts of the programme have been obtained, this means that the final assessment of the degree programme has been taken in accordance with the WHW, and honours can be determined. The Student Administration Office of the degree programme and the Central Student Administration will exchange information on behalf of the Board of Examiners. This information will be accessible only to those who, by virtue of their duties, have been granted rights to carry out specific actions. The Board of Examiners and the study advisors may view the history of the application for final assessment and the degree certificate handling.

3.3.2 Preparing the degree certificate and the ceremony

Once a student has passed their final assessment, the degree certificate and the Diploma Supplement will be prepared. These documents contain sensitive personal data, such as examination marks, examination results and honours. These will be included in the Diploma Supplement. At the UG, the Diploma Supplement only contains the pass marks that count towards the final list, the Honours components and any additional courses. Unlike in some other countries, not all course units and examinations taken are listed with the corresponding marks.

Degree certificates will be signed by the chair and secretary of the Board of Examiners. The degree certificates will be kept in a locked room/cabinet at the education office until the ceremony.

<u>Graduate students can obtain their degree certificate and the Diploma Supplement in four ways:</u>

- at a ceremony
- by collecting them from the faculty's education office upon showing proof of identity (ID)
- by having them collected by an authorized representative. An authorization is issued by completing a document signed by the graduate and the authorized representative and which includes a copy of the student's ID
- by having it sent via registered mail.

The two latter options are discouraged; in these cases, the student cannot check the data on the documents nor sign the degree certificate on site.

In the case of collection by an authorized representative and when sending a degree certificate, the instructions point out that the data must be carefully checked and that an unsigned degree certificate is not valid, but there is no conclusive check.

It is not customary to check the identity of the graduate in advance of a degree certificate ceremony.

However, it is customary in Dutch society to address a student with a personal note about their academic careers at the degree certificate ceremony. Such information is sometimes collected from several lecturers. Furthermore, many students have been actively involved in a student or study association during their studies. Sometimes information about this is collected too. The party of whom information is requested has their own responsibility, but restraint must be exercised about what personal information will be divulged during the degree certificate ceremony. In the case of sensitive data, the student must be asked in advance whether they consent to this. The legal basis in this instance is 'legitimate interest'.

3.3.3 Providing information to external parties for the purpose of, for example, degree certificate verification

The UG will never provide information about former students to other persons or organizations without a signed written statement from the student in question.

The examinations and degrees of students who graduated after 1996 are listed in the DUO Diploma Register. Information can be obtained from DUO if desired.

Other requests for verification of a degree certificate will therefore only be dealt with if the students themselves request that information be provided to third parties.

3.4. Alumni

The UG attaches great importance to maintaining contact with its graduates and to ongoing involvement. After students have completed their study with a degree certificate, their personal data is stored so that they can still be contacted as alumni. The following two principles apply:

- alumni must be able to say that they no longer wish to receive information at any time
- they may request the deletion of their data from the alumni file with the proviso that the UG is obliged to retain the basic data relating to their degree programme.

Part II: Teaching

This part contains guidelines for the processing of the student's personal data at the various stages of a degree programme:

- **Development of teaching**
- **Teaching practice**
- **Evaluation**
- **Improvement of teaching**
- **Accreditation**

4. Development of teaching

4.1. Policy frameworks

Management information, such as student analytics (including data on nationality and gender) and learning analytics (including study progress and learning outcomes), is used for the development of teaching, among other things. No special categories of personal data may be registered in this context.

Personal data will be anonymized at the earliest possible stage. Management information only contains anonymized data at an aggregation level that cannot be traced back to individuals.

Case studies used for teaching purposes should also be anonymized.

5. Teaching practice

The starting points, principles and recommendations mentioned in Chapter 1, Section 1.4 also apply to the activities within teaching practice.

5.1. Composition of teaching groups (student timetable)

When making timetables for lectures, the timetablers process the name and availability of the lecturer. To allocate the rooms to a particular course unit, they use an estimate of the expected group size. The Education Support Teams within the faculty put together the teaching groups. This also includes the processing of personal data; students and lecturers can view the tutorials to which they have been assigned.
Higher-year students register for the available seminars themselves.

5.2. Use of case studies, examples and research data in teaching

The teaching may use case studies, examples and research data involving personal data. When personal data needs to be included in the teaching, for example, in examinations or course materials, it should be made anonymous in advance if possible. If the data of the present student population is used, it must always be anonymized. The data used may not be traceable to individual students. If the data can inevitably be traced back to individual students, for example, because the group is small, the data may only be processed if the individual student has given their explicit written consent beforehand. They must also be able to revoke such consent. This means that records must be kept of who has given consent for what and when.

5.3. Student overviews, attendance registers, registration of part-assignments

When a lecturer compiles student overviews, attendance registers, or registrations of part-assignments, they must keep the scope of the data as limited as possible, i.e. only register data that is necessary for the performance of the teaching duties in question. Often these are the name, student number and email address. The processing of sensitive or special categories of personal data is not permitted in this context.

5.4. Audio and video recordings in the context of teaching

In some situations, teaching involves the use of audio and video materials.
Appendix 8.5 (to be added soon) includes these situations and the associated guidelines.

5.4.3 Guidelines for learning analytics regarding video lectures

Inspection of the material is only allowed if it is needed because of the duties to be performed.
The aim of the processing is to be able to inform students at an early stage about their study behaviour in relation to the results obtained.

An extensive step-by-step plan for learning analytics and the careful handling of personal data can be found at: https://www.surf.nl/learning-analytics-in-5-stappen-een-handreiking-voor-de-avg

<u>The analysis may never contain or relate to:</u>

- Other personal data of students
- The duration for which the video lecture was accessed
- IP addresses and providers

6. Evaluation of teaching

The reports made on the basis of the student evaluations and learning analytics are used to further improve teaching and as management information.

6.1. Evaluation of teaching on the basis of student evaluations

The teaching is evaluated by means of student evaluations, among other things. The way in which this is done differs per faculty and degree programme and is carried out using various systems (Blue, Qualtrics, email surveys), usually asking students to complete a questionnaire digitally or on paper.

The evaluation forms must not contain student data; however, in some cases it may be possible to trace the data back to individuals, e.g. in small groups or because of a personal explanation (which can be traced back by a lecturer).

This risk can be reduced by not using handwritten forms and by having the forms anonymized by someone other than the lecturer immediately after they have been collected, and/or by immediately removing personal notes from the forms. If possible, no open questions should be asked.

If students wish to explain their evaluation, an email address may be desired. However, this should not be made compulsory.

The data obtained must be carefully processed. This means that:

- Paper questionnaires containing personal data will be securely archived and destroyed immediately after processing
- Digital forms will be securely stored and deleted or anonymized immediately after processing
- When paper evaluations are collected, it must be ensured that they cannot be traced back to individuals
- The data cannot be traced back to individual students during further processing. Therefore, management information should be aggregated in such a way as to ensure that personal data cannot be traced
- The digital forms in databases or the email and paper questionnaires will only be accessible to staff for whom this is necessary in order to perform their duties (processing into management information)
- Access to them is organized in accordance with the allocation of different roles and rights
- The databases used must comply with security standards.

6.2. Evaluation of teaching on the basis of learning analytics

In addition to student evaluations, learning analytics is used to evaluate the teaching. This involves looking at the effectiveness of the teaching at a higher level of aggregation. It is important that only employees have access to the data at a personal level because of their duties, for example, because they are the ones who have to anonymize the personal data. Further use of data is only possible if it has been anonymized.

An extensive step-by-step plan for learning analytics and the careful handling of personal data can be found at: https://www.surf.nl/learning-analytics-in-5-stappen-een-handreiking-voor-de-avg

6.3. Lecturer evaluations

Lectures are sometimes recorded for the purpose of testing the quality of lecturers within the framework of the University Teaching Qualification (UTQ). The following guidelines apply:

- Lecturers inform students prior to a lecture that it will be recorded. This can be done during an earlier lecture, by publication on Nestor or at the start of the lecture.
- Recordings for the UTQ assessment may only be made on the instruction of or with the consent of the lecturer.
- Wherever possible, care must be taken to ensure that students are not shown. However, this cannot be ruled out completely because of interaction between the lecturer and the class.
- Recordings must be made wherever possible from the back of the room, thus minimizing the risk of recognition.
- Recordings must be deleted after the evaluation is completed.

7. Accreditation of teaching

The University and its various faculties and degree programmes have a legal obligation to provide data within the context of accreditation. The UG or the degree programme must demonstrate that quality assurance is helping to realize its vision of good teaching and sustainably contributes to the development and improvement of teaching.

The UG must make relevant information available to the panel during their visit. This may include student theses, final projects and other tests with the associated grade assessment and information about the assessment procedure. The relevant documents will be placed in a folder in a secure environment (Nestor) and can only be accessed by the panel and staff directly involved in the process. If QANU supervises the process, the theses/final projects and the associated assessment forms will be uploaded to QANU's locked digital environment. Only those directly involved, such as panel members, the QANU secretary and the staff member of the degree programme involved in the accreditation, have access to it.

The following principles apply in the accreditation process:

- The collection and processing of personal data should be limited to what is strictly necessary and should be pseudonymized or anonymized (e.g. by crossing out names, not using student numbers or only using the last three digits of a student number).

- The documents should be stored in a safe and secure place (Nestor, Y drive) in protected folders, or uploaded to QANU's locked digital environment.

- Access to the folders should be limited to those with a direct interest; members of the panel are bound by an obligation of confidentiality with regard to the information entrusted to them.

- They will be given a temporary guest account that grants access to the documents. They may only have the right to access, not to modify. After completion of the visit, access to the folders containing the data must be blocked and the guest account must be deleted.

- Upon receipt of the final accreditation decision, all documents containing personal data must be destroyed; where necessary, the documents will be transferred to the UG archive and kept until after the next accreditation.

- The report of the published development interview may not contain any personal data, unless it relates to a specific position in the accreditation process, or unless the person in question has given their permission. Any visual material used should also be considered.

8. Appendices

Content

8.1 Procedure from application to registration

This document describes the work process of **the application and registration procedure** for various target groups of students, from the perspective of both the Central Student Administration (1) and the faculties (2).

1. Application and registration procedure for Bachelor's (and Master's) degree programmes, exchange students, course participants, minor students and postgraduate programmes from the perspective of the Central Student Administration (CSA)

1.1. Application process for Bachelor's degree programme students with a Dutch preparatory programme VWO or an Hbo-P that gives direct access to a study programme

(please note: the procedure for Master's degree programmes is broadly the same as for Bachelor's degree programmes and has not been further elaborated here.)

Students apply for a Bachelor's degree programme through Studielink. The following information will be filled in and forwarded directly to PN:

- Name-Address-Place of residence/private email address
- prior qualifications; if it can be automatically verified via DUO, the boxes *Vooropleiding* (prior qualifications, VO) will be set to 'positive' and *Centraal Geverifieerd* (centrally verified) will show up green in PN. If the prior qualifications cannot be automatically verified, the student has to send copies of the necessary documents by email or hand them in to the Central Student Administration (CSA)
- person verification: when logged in with DigiD, the identity (and therefore the nationality) will be automatically verified with the BRP. If this fails, the student must hand in a copy of their ID to the CSA. This can be sent by post or email; in the latter case, the copy must clearly state that it is a copy and for what purpose it is provided (specific apps exist for this)
- students with an EU bank account (IBAN) fill in their account number and possibly indicate that a third party will be paying
- they also indicate whether a single or repeated direct debit will be used
- in that case, an authorization form must be filled in, in which the following information is requested: student number, name, address, account number, payment in instalments/one time, date and signature
- the original of the signed form must be sent by post or as a scanned attachment by email or handed in to the CSA
- the authorization form will be kept in a folder, transferred after two years to the central archive and kept there for seven years.

1.2. Application process in the case of foreign prior qualifications

Students apply through Studielink. The following information will be filled in and forwarded directly to PN:

- Personal data/address data/private email address
- Prior qualifications data: if it concerns a foreign preparatory programme or pre-Master's, the data are transferred from PN to OAS (online application system). The student receives a token to log in to OAS and fill in the VO data
- The central Admissions department will deal with the assessment of admission on the basis of previous qualifications
- If the admission is approved (and the Admissions Board or Board of Examiners have issued an admissions decision), the Admissions department will send the admission decision to the CSA by email; it will be archived in PN
- If logged in without a DigiD (foreign students without BRP registration), the identity is not automatically verified and the student must provide a copy of their passport. This will be done by email and it will be forwarded by email from the Admissions department to the CSA. This process will be adjusted as soon as possible
- Students fill in their bank account number. If it concerns an account with an International Bank Account Number (IBAN) from a Single Euro Payment Area (SEPA), students may choose to pay by direct debit
- Students without a SEPA bank account fill in their payment details, but cannot pay by direct debit

If all action boxes have been ticked affirmative, the student will be registered by the CSA.
They will be sent a confirmation of receipt by email.

1.3. Cancellation of application and termination of registration

Students may cancel their application through Studielink or request that their registration be terminated. The data for an application will remain in PN but will be crossed out. Registration data will remain.

The CSA can also cancel the application, for example, if a student does not qualify for admission to a degree programme or has not completed their tuition fee payment, or terminates the application (this rarely happens). Students will be notified about this by email.

The retention periods for cancellation and termination of registration have yet to be set. Currently all data is still stored in PN, except for the Studielink messages, which are periodically deleted.

1.4. Non-standard situations when applying for a Bachelor's degree programme:

- Higher-year Bachelor's phase: Admission decision for final examinations (*Verklaring Toelating Afsluitend Examen*) from the faculty
- Pre-Master's: Admission decision on pre-Master's (*Verklaring Toelating Premaster*) or decision from most faculties
- Special entrance examination (colloquium doctum): form from faculty
- Minor students: minor students form from faculty
- Non-standard starting date: starting date form from faculty
  (for more information, refer to the descriptions of the faculty processes.)

1.5. Application for S&P degree programmes:

- the application must be made before 15 January of the coming academic year
- students send data to the faculty, where a file is created for the selection procedure
- students can fill in a web form if they wish to invoke special circumstances (e.g. late application, inability to take part in selection day)
- selection days are sometimes organized for students to attend
-
  after completion of the selection procedure, the CSA will request the faculty's ranking numbers. These are then placed in PN and sent to Studielink. Studielink sends the ranking numbers to the students (for more information, refer to the descriptions of the faculty processes).
- students send their request for a postponement together with a statement from the institute of secondary/higher education, if the relevant certificate giving access to the degree programme cannot be submitted in time.

1.6. Application process for non-standard students

1.6.1 Participants taking a degree module at a faculty:

1. Students fill in a participants form. The copy of this form goes to the CSA and the CSA enters the data in Progress.Net (PN).

2. At the bottom of the participants form, students tick the authorization box for the direct debit of the amount due. The CSA enters this into PN and the payment runs in the batch for the collection of (tuition) fees (for more information, refer to the descriptions of the faculty processes).

1.6.2 Exchange students:

The faculties enter the data in Progress.Net themselves (for more information, refer to the descriptions of the faculty processes.

1.6.3 PhD students

Besides registration in Hora Finita (the registration system for all PhD students), the Human Resources department registers PhD students in Progress.Net. This provides them with a student number and allows them to make use of the facilities that are available to regular students under the same conditions (e.g. ACLO University Card).

1.6.4 Postgraduate degree programmes

The registration usually takes place via Studielink. Faculties determine admission and payment; once the payment obligation has been met, the registration can be completed.

2. Application and registration procedure from the perspective of the faculties

2.1. Bachelor's degree programme (please note: the procedure for Master's degree programmes is broadly the same as for Bachelor's degree programmes and has not been further elaborated here):

In the case of a regular degree programme without fixed quotas and if the student has a **pre-university education (VWO) with the appropriate profile or has completed an HBO propaedeutic phase** that gives direct access to the programme, there is no faculty involvement and the registration process runs entirely via the Central Student Administration (see 1.1).

2.2. In the case of deficiencies in the profile, students must submit additional documents (e.g. their level of mathematics, English) to the faculty's Student Administration Office. If possible, these documents are added to the digital student file (DSD) or stored in a folder on the Y drive. The retention period for these documents is one year from the date of issue of the admission decision. For some faculties, the process also takes place via the central Admissions Officer.

2.3. In the case of students with foreign prior qualifications, these must be tested for admissibility; the students will receive a link to the Online Application System (OAS) in which relevant documents must be uploaded; this procedure will be handled by the central Admissions Office (see 1.2). The faculty Admissions Board determines whether the admission requirements have been met and issues an admission decision. The decision will be stored in PN and can be deleted three years after the date of registration or date of cancellation of the application.

2.4. The application procedure for the entrance examination varies per faculty.
See the website:
https://www.rug.nl/education/bachelor/nederlandse-studenten/aanmelding-en-inschrijving/colloquium-doctum-

The student applies to the Student Administration Office of the faculty in question.
The Admissions Board determines whether the admission requirements have been met and issues an admission decision which will be archived by the CSA. The retention period is seven years.

2.5. For degree programmes with a fixed quota, the procedure is as follows.

1. The student applies in Studielink by 15 January at the latest. In Studielink, the student will receive a link to the faculty page that contains information about the selection procedure.
2. Faculties use various applications to contact the student and to enable them to provide the correct data and documents (Formdesk, Qualtric) necessary to take part in the selection procedure.
3. Depending on the procedure, students must submit further documentation by a specified date. This information is collected within the faculty department in charge of the selection procedure and (in most cases) stored in Excel lists and folders. These lists and documentation must be stored in a safe place (Y drive or Google Drive) and destroyed at the end of the selection procedure (three months after the start date of the relevant academic year).
4. Once students have provided the correct information, they can take part in the selection procedure, which differs per degree programme.
5. Proof will be requested if a student is prevented from taking part in the selection because of special circumstances.
6. Students will receive their ranking number via Studielink on 15 April. Afterwards, the degree programme will send further details about their ranking position to their private email address.
7. As from 15 April, students who have been placed will be able to complete their registration. SIA will process the registration further.

8. The degree programme sends information to the new students via their UG email address through PN. Depending on the faculty's policy, additional actions will be carried out that are related to the organization of teaching.

2.6. Bachelor's degree programmes miscellaneous: matching

Matching is the last check in choosing a degree programme, after which a student can definitely decide if the programme suits them. All prospective students are entitled to participate in matching activities. The matching procedure differs per faculty. More information can be found on the UG website. Several faculties/studies have compulsory matching.

1. Students apply in Studielink by 1 May at the latest.
2. The degree programme will notify them with an explanation of the matching through PN.
3. How the matching is done differs per faculty and degree programme. It can be done, for example, via the Student Portal (Nestor) or another application. The communication between the student and the faculty takes place via email. The results of the matching must be destroyed two months after the date of commencement of the academic year or must be securely stored so that it can only be used for statistical and scientific purposes. Students must be informed about this (privacy statement) and must be made aware of their rights (removal, objection).
4. After participation, students receive a degree programme advice by email through PN.
5. The degree programme will indicate in PN if the match has been made, after which the registration process continues (see 1.1).

2.7. Non-standard registration

2.7.1 Exchange students

The procedure is as follows:

1. Students are nominated by one of the partner universities
2. The application will be made via 'Mobility Online' (as from the end of 2020). The student adds the relevant document by uploading them to this application system.
3. The faculty's Exchange Office checks the documents. The documents must be stored in a safe place (DSD, or until that time in folders on the Y drive) and periodically deleted (seven years after the end of the academic year in which the exchange took place).
4. The faculty's Student Administration Office creates a student number in PN
    a. The application for a visa, if required, will go through the Immigration Service Desk
    b. Housing for foreign students will be done by MSD/SSH
5. The degree programme sends the student a message about registration for course units
6. The faculty checks via the Learning Agreement to see whether the course unit registration is approved.

2.7.2 Participants taking one or more modules of a degree programme

The students fill in an application form that can be downloaded from the website. The data includes name and address, date and place of birth, bank account number, the course units and a signature. The faculty's Education Office retains the original. A copy is sent to the CSA (for registration/authorization), the financial department of the faculty (for direct debit) and possibly the lecturer. After payment and registration, the Education Office registers the students for the course unit or units in question. The lecturer's copies can be destroyed immediately after the course has ended. The copy at the CSA must be destroyed seven years after the date of commencement of the course year. The original in the faculty's possession can be transferred to the archives one month after the date of commencement of the course and will be destroyed after seven years.

2.7.3 Minor students

(see website https://www.rug.nl/education/bachelor/nederlandse-studenten/aanmelding-en-inschrijving/inschrijfprocedure-bijvakstudent#herinschrijven-bijvakstudent

1. Students apply (as 'Higher Years') via Studielink for the degree programme in which they wish to follow a minor.
   They fill in the form Admission to Bachelor's/Master's minor, which can be downloaded from the website. The following data must be entered:
   - student number
   - year of study
   - last name and initials
   - degree programme
2. To assess the admissibility of students, the following documents must be enclosed and submitted to the Student Administration Office of the faculty in which the course unit will be followed. This means that the physical documents are needed.
   - Copy of propaedeutic certificate (higher education) or copy of university certificate when applying for a Bachelor's degree programme
   - Copy of university certificate when applying for a Master's degree programme
   - Copy of passport or ID
   - Original *Bewijs Betaald Collegegeld* (proof of payment of tuition fees, BBC) from another institution of higher education
3. The faculty's Admissions Board will assess the admissibility of the student. If positive, the student fills in the second part of the form and sends it with the documents to the Student Information & Administration department. The registration process continues.

2.7.4 Summer School

Applications for an UG summer or winter school are made via an application form (Formdesk) on the website. A sample can be found here. The application will be sent to the general email address of the school in question. This is managed by the lecturer who coordinates the school. The coordinator uses the data for the selection and preparation of the official acceptance letter for the visa.

The central summer/winter school office (SSO) creates the application forms in Formdesk, and as such has access to all applications from all schools. The SSO ensures that participants receive an email containing a link to the payment portal (credit card & iDeal). On request, the SSO also makes invoices for participants. All payments are credited to the bank account of the Summer School, after which the FSSC transfers each payment to the project code of the school.

The SSO stores the data for a maximum of one year on Formdesk and on the Y drive. After the school has been completed and the annual report has been drawn up, all data will be deleted. The coordinators often keep a list of their alumni (name, home institution and email address) to reuse in the promotional campaign of the next edition of the school.

Each year, the SSO organizes several practical meetings for all coordinators, with tips on promotional activities, visas, accommodation, etc. The GDPR is another theme: we urge people to share data only via Unishare/SURFfilesender/Google Drive, and to ask permission to use an email address in a mailing list.

2.7.5 Postgraduate degree programmes

1. Students apply in Studielink before 1 May (application runs via SL; students are sometimes registered by the faculty in PN); sometimes the postgraduate programme is offered through a foundation
2. Students apply to the faculty before 1 August
3. The faculty checks the admission requirements. The following data are collected for this purpose: name, address, residence, prior qualification documents, bank account details (or those of the employer), copy of passport or ID
4. The invoicing is done by the faculty's financial administration
5. The faculty informs the CSA when the admission and payment requirements have been met, after which the CSA can proceed with the registration process (1.6.4).

8.2. Retention periods from the selection list Universities and University Medical Centres 2019

An overview and explanation of retention periods will be drawn up, based on the Selection List Universities and University Medical Centers 2020. This selection list was compiled in consultation with the joint Universities and Medical Centers. The document describes the processes within teaching and academic research, and defines the corresponding legal retention periods. As soon as the selection list has been published in the Government Gazette, it will be placed on the UG intranet and the overview will be added to this policy plan.

In addition, we refer to the digital system **I-Navigator** that is available within the UG, which describes all processes within the University, with the corresponding retention periods. The **I-Navigator** application is managed by the OSI department within the CIT and is, among other things, the tool to fill and support the Digital Student Dossier. I-Navigator describes in detail which sub-process is involved.

Any changes relating to legal retention periods are implemented directly in this application, so that it is up to date at all times. I-Navigator can be consulted after access has been granted.

8.3. Guideline for sharing data of students with a functional impairment

Processing special categories of personal data at the UG

The UG has a duty of care towards its students. Students may be hindered in their studies by special circumstances. These can be incidental or temporary conditions such as illness, pregnancy or family circumstances, as well as long-term circumstances such as a functional impairment or the responsibility of informal care.

Depending on the situation, students can be helped in their efforts to continue studying. This may include individual adjustments to the study programme, e.g. by postponing deadlines, or by adjusting the form and duration of examinations. This can prevent a student from suffering a (further) study delay.

In order to come to a decision for adequate support, the student must provide information and supporting evidence about the nature of the impediment to the student counsellor, study advisor, or the Board of Examiners. The 'evidence' usually consists of a statement from an attending physician or another expert.

This information contains at least sensitive and/or special categories of personal data (such as race, ethnicity, religion, health, sexual preference, biometric data); the processing of special categories of personal data is not permitted unless the student gives their consent.

Although in principle it is forbidden for an organization to process special categories of personal data, exceptions do apply, as mentioned in Article 9.2.g of the GDPR in conjunction with Article 30.2.a of the Dutch Implementation Act GDPR (UAVG):
'schools (i.e. educational institutions) may specifically process data relating to health, insofar as the processing is necessary for the special supervision of pupils or the provision of special services relating to their state of health'.

In addition, the UG has several legal obligations towards students with a functional impairment under the Higher Education and Research Act, the Equal Treatment Act, and under the UN Convention on the Rights of Persons with Disabilities. The basis for processing is the exercising of a task in the general interest. In short, the UG must ensure an inclusive education system and offer reasonable accommodation to persons with a functional impairment so that they can be educated on an equal footing with other students.

The UG will exercise caution in the processing of special categories of personal data. An official statement is needed to make provisions, but it is not necessary to keep it after a study advisor or student counsellor has established that an officially recognized diagnosis has been made. A note about this in a secure environment within Progress.Net or ProgressWWW will suffice. This complies with the principle of data minimization.

Student psychologists and student counsellors store their documents in the Stuf! application. The Board of Examiners stores its documents in the DSD.

What conditions apply to the processing of special categories of personal data?

Additional obligations apply to the processing of health data:

- 'the data shall only be processed by persons who are bound by an obligation of secrecy by virtue of their office, profession or statutory regulations or by an agreement on confidentiality' (Article 30.4 UAVG in conjunction with Article 9.2.g GDPR).
- the organization shall take 'appropriate technical and organizational measures to ensure a level of security related to the risk'. Because the processing of special categories of personal data involves more risks, the security requirements will also be stricter.

How should the UG handle the processing of special categories of personal data?

Each faculty has its own internal procedures and responsibilities towards students with a functional impairment. Therefore, it is not always possible to have a leading approach that applies to all faculties. It is, however, possible to adhere to a number of principles that every processing action must comply with. Below is a concrete elaboration of the principles of the GDPR:

GDPR principle	**Concrete elaboration**
Legitimacy Personal data may only be processed if there is a legal basis for this.	The primary basis for the UG is a task of general interest.
Transparency The data subject must be aware that their personal data is being processed and must be informed of their rights.	Students will be informed about the processing of (special categories of) personal data through a special privacy statement given by a study advisor, student psychologist or student counsellor.
Fairness The data subject must, as much as possible, be in control of the processing of their data.	The student is responsible for providing the statement or diagnosis to the correct staff member or service. No data will be shared with third parties without the data subject's explicit consent.
Purpose limitation A data subject's personal data may only be used for specific and legitimate purposes and may not automatically be processed for other purposes.	The purpose of the processing of special categories of personal data is to be able to assess which adjustments to the teaching or examination are appropriate and fair. Special categories of personal data will only be requested if it serves a particular purpose.
Data minimization No more personal data may be processed than is required to achieve the legitimate purposes of the entity processing it.	Staff who organize the facilities (e.g. lecturers and/or invigilators) will only be told which facilities are necessary and not the reasons. Name, student number and facility will suffice.
Data quality Personal data that is processed must be correct and up to date.	The student provides a relevant current statement or diagnosis from a medical or paramedical professional. Administrative systems such as ProgressVolg and ProgressWWW will be used. The data in these systems will be automatically updated if the student adjusts their data.
Storage limitation Personal data may be stored no longer than is necessary to achieve the legitimate purposes of the entity processing it. Considering the duration of retention periods is essential.	Statements or diagnoses will not be stored unnecessarily. Showing them is sufficient for awarding the facility or to give advice. Notes on the functional impairment are stored in Progress.net in the memorandum function, which only staff with the same rights can view. Where possible, documents will be removed from the mailbox and if applicable from the download folder on the X drive.
Security Technical and organizational measures must be taken to protect personal data and prevent its loss or unlawful processing.	To avoid the risk of invasion of privacy, only the UG systems will be used. Information about the student is saved in Progress.net, Stuf!, Corsa or on the Y drive. Sensitive information will not be sent by email, but via SURFfilesender or Unishare. The UG exercises restraint regarding the storage of paper documents.

Confidentiality Personal data must in principle be confidential.	A provision is granted exclusively by staff who are authorized to do so by virtue of their position. Medical or paramedical statements or diagnoses will only be processed by UG staff who are obliged to maintain confidentiality by virtue of their profession. These are primarily student counsellors, study advisors, student psychologists, or staff who have signed a confidentiality agreement.
Responsibility The UG must be able to demonstrate to the data subject and the supervisory authorities that the above principles have been applied.	The UG adheres to the principles of the GDPR and can explain any deviations.

The exact steps in the process of allocating facilities differ per faculty. The order may also differ in practice, as may the specific actors and the specific faculty processes. From a data protection point of view, the following general 'ideal scenario' could be adopted:

1. Any student who wants to make use of (examination) facilities fills in an information tool on the external website to find out what precise steps have to be taken to apply for facilities.
2. If a student indicates that they have dyslexia and/or dyscalculia, they can request the examination facilities online. This application includes a mandatory upload of the diagnostic report on the functional impairment.
3. The application will be processed by a student counsellor who will write a recommendation letter for the study advisor and the Board of Examiners of the degree programme in question and give it to the student.
4. In other cases, the student will talk to a student counsellor. The student counsellor writes a recommendation letter for the study advisor and the Board of Examiners of the degree programme in question. Arrangements, notes and facilities are stored by the student counsellor in Stuf!
5. The student makes an appointment with the study advisor of the degree programme in question. The student takes along a statement/diagnosis and the recommendation letter from the student counsellor. Arrangements, notes and facilities are stored by the study advisor in Progress.net.
6. If necessary, the study advisor makes a scan of the supporting documents for storage in Corsa. The original documents will be handed back to the student.
7. The Board of Examiners, or the student counsellor if authorized, grants the facility to the student and communicates this decision to the student and to the department or staff who organize the facilities. It is not necessary to mention the background of the student, only which facilities are required.
8. The teaching staff or department organizes the facilities. For each examination, they will inform the lecturer and/or the invigilators in a secure manner (via the Y drive, SURFfilesender or Unishare) about which facility has been assigned to which participating student.
9. In the case of study delay, or the threat of study delay, as a result of the special circumstance, the student will in any case report this to the study advisor, and to the student counsellor (if the student will suffer a delay if 15 ECTS or more or has been referred to the student counsellor by the study advisor).
10. The study advisor or student counsellor will complete a digital registration form on the basis of the study delay circumstances. This form also includes the agreements made. The student must tick this digital form for approval via the website.
11. If a student invokes an exception to the binding (negative) study advice (BSA), and further file creation occurs (motivation letter, proof of circumstances, adjusted study plan and any decisions), the Y drive is a suitable place for storage, provided access rights are properly secured. Unishare is suitable for communication with the BSA Committee.
12. If a student also wishes to apply for a contribution from the Graduation Fund, they can submit a digital application after the end of the academic year via a special portal on My University.

8.4. Guideline for dealing with fraud committed by students

Student fraud guideline

This guideline describes the process within a faculty in the event of possible examination fraud or cheating by a student in accordance with the requirements set by the GDPR. Minor variations of the exact procedure may occur per faculty. In particular, this guideline helps members and secretarial support to the Board of Examiners as this Board deals with reports of possible fraud.

Duties and powers of the Board of Examiners

The Board of Examiners has an important task within the educational organization. It is responsible for ensuring the quality of examinations and final assessments. It is the Board's responsibility to determine in an independent and expert way whether each individual student has satisfied the requirements set by the degree programme for being awarded the relevant degree. As such, it is responsible for the quality of the diplomas.

The legislator has therefore assigned several powers and duties to the Board of Examiners.
One of these is assuring the quality of the organization and the procedures relating to examinations and final assessments (Art. 7.12b.1.e WHW). The Board of Examiners of a degree programme also lays down rules that relate to the handling of (suspected) fraud by a student and the measures that it can take.

Examination fraud and the GDPR

Sometimes irregularities are observed in examinations or written assignments, such as cheating or plagiarism. The model Rules and Regulations (for the Boards of Examiners) contains a definition of fraud. Generally speaking, cheating or fraud is an act or omission by the examinee designed to partly or wholly hinder the accurate assessment of their or someone else's knowledge, understanding and skills.

'Fraud' or 'cheating' is defined as a behaviour. When a Board of Examiners receives a report of possible fraud committed by a student (see 'Process description' below), it collects data about someone's behaviour. The GDPR does not consider information about (undesirable) behaviour as a special category of personal data.

However, it may harm the interests of the student concerned if data on examination fraud is revealed inappropriately. It could lead not only to emotional and reputation damage, but also to a reduced chance of becoming a student assistant or being eligible for a participation council. It is therefore recommended that data on examination fraud be treated on principle as sensitive information and that appropriate measures be taken to optimally protect the interests of the students concerned.

Process description

1. The examiner of the course unit suspects fraud or cheating.
2. The examiner submits a written report on the suspected fraud to the Board of Examiners (BE). The report describes at least the alleged manner of fraud as well as the reasons why the examiner classifies the acts or omissions as fraud or cheating.
3. If someone other than the examiner of the course unit reports suspicion of fraud, the BE investigates whether it is a case of alleged fraud and makes a written report.
4. In principle, the personal data of the person reporting the suspected fraud (other than the examiner) will not be shared with the student, unless this is necessary the investigation.
5. The student in question will be informed immediately in writing of the suspicion of fraud and possibly invited for an interview to investigate the matter.
6. Before the BE decides to impose further sanctions as referred to in the Rules and Regulations (for the Boards of Examiners), it will give the student the opportunity to respond to the allegation. This can be done in writing or in an interview.
7. The BE subsequently assesses whether or not fraud has been committed and, if it considers fraud to be proven, decides on the sanction to be imposed.
8. The student, the examiner and the faculty's Student Administration Office will be informed in writing of the decision and the sanction.

9. If an assignment was made as a group, all members of the group are accountable in the case of fraud. The BE may make an exception to this rule in individual cases.
10. The student may lodge an appeal with the Board of Appeal for Examinations (CBE) within six weeks after the decision of the Board of Examiners, and in the second instance with the Appeals Tribunal for Higher Education (CBHO).
11. The decision and the accompanying correspondence will be archived and kept in accordance with the prevailing retention periods in the DSD.

Impact and level of impact

The data in this process must be considered as sensitive and critical. The probability of an incident is estimated to be low, but the impact on someone's privacy may be considerable. The risks are therefore estimated to be medium.

Risk of breach of privacy

Based on the assessment of the risk, the UG makes the following recommendations:

- Restrict the communication as much as possible to email and share sensitive information via, for example, Google Drive or Unishare, or similar systems used, for example, by the UMCG.
- It is preferable not to print documents, but if this is necessary, ensure that they are taken back and destroyed after use.
- Save documents and correspondence only on the Y drive and the Digital Student Dossier and not on any other data carriers such as laptops and USB sticks.
- If minutes are taken on a laptop, or if the documents are consulted via your own device, work directly via the UWP (the standard workplace for students and staff).
- Destroy the data in good time in accordance with the set retention period, including the data in the email (e.g. messages sent) and on drives.
- If students are invited for an interview, make sure that the privacy of students is respected as much as possible by preventing students from meeting each other during interviews.

How should the UG deal with the processing of data relating to fraud?

Each faculty has its own internal procedures and responsibilities regarding suspicions of fraud or cheating committed by students. Therefore, it is not always possible to have a leading approach that applies to all faculties. It is, however, possible to adhere to a number of principles that every processing action must comply with. Below is a concrete elaboration of the principles of the GDPR:

GDPR principle	Concrete elaboration
Legitimacy – personal data may only be processed if there is a legal basis for this.	The primary basis for the UG is a task of general interest.
Transparency – the data subject must be aware that their personal data is being processed and must be informed of their rights.	The UG informs the student about the nature of the suspicions, their rights, the procedure and where data about fraud is stored and for how long. The UG can explain how to handle the student's privacy rights. In addition, the General Privacy Statement of the UG applies.
Fairness – the data subject must, as much as possible, be in control of the processing of their data.	The student will be offered the option to respond to the allegations.
Purpose limitation – personal data may only be used for specific and legitimate purposes and may not automatically be processed for other purposes.	The purpose of the processing of personal data is to be able to assess whether fraud has been committed, to impose or implement any sanctions and to register these.

Data minimization – no more personal data may be processed than is required to achieve the legitimate purposes of the entity processing it.	The UG only request data to support the assessment of suspicions of fraud. This includes at least the current registration data such as name, student number and the degree programme. It is also possible to request details of any fraud committed previously.
Data quality – personal data that is processed must be correct and up to date.	The student will be given the opportunity to correct factual inaccuracies. Administrative systems such as Progress Volg and Progresswww will be used. The data in these systems will be automatically updated if the student adjusts their data.
Storage limitation – personal data may be stored no longer than is necessary to achieve the legitimate purposes of the entity processing it. Considering the duration of retention periods is essential.	Decisions and the related documents will not be kept longer than the retention periods specified for that purpose. The Board of Examiners is responsible for timely destruction. Decisions will be kept in the Digital Student Dossier. In addition, supporting documents will be kept on the Y drive. Documents in the mailbox and possibly in the download folder will be saved in a secure place and either saved or deleted.
Security – technical and organizational measures must be taken to protect personal data and prevent its loss or unlawful processing.	To avoid the risk of invasion of privacy, no system other than UG systems will be used. Information about the student is in ProgressVolg, Corsa and on the Y drive. Any notes on the fraud will be saved in a protected part of ProgressVolg. Sensitive information will not be sent by email, but via SURFfilesender or Unishare. The UG exercises restraint regarding the storage of paper documents.
Confidentiality – personal data must in principle be confidential.	Investigations of cases of fraud and the sharing of supporting documentation may only be carried out by staff members for whom it is necessary because of their duties. Case studies will only be introduced and discussed anonymously.
Responsibility – the UG must be able to demonstrate to the person in question and the supervisory authority that the above principles have been applied.	The UG adheres to the principles of the GDPR and can explain any deviations.

8.5 Guideline for audio and video recordings in the context of teaching

On several occasions, the teaching involves the use of audio and video materials.
These situations and the associated guidelines will be added soon.

8.6. Abbreviations and definitions

Abbreviations and definitions for the Policy and guidelines for the careful processing of personal data in the domain of teaching.

ABJZ	Department of General Administrative and Legal Affairs of the Office
ACLO	Academic central of physical education
BBC	Proof of tuition fees paid
BIG	Individual Healthcare Professions
BKO	University Teaching Qualification
BRP	Persons Database
BSA	Binding (negative) study advice
BSN	Citizen Service Number
CAO	Collective Labour Agreement
CSA	UG Central Student Administration
CvB	Board of the University of Groningen
DSD	Digital Student Dossier
DUO	Education Executive Agency
GDPR	General Data Protection Regulation
GGD	Municipal or Joint Health Service
ID	Proof of identity
IND	Immigration and Naturalization Service
KEI	First-year introduction committee
Nestor	UG Electronic Learning Environment
NIP	Dutch Association of Psychologists
OER	Teaching and Examination Regulations
OAS	Online Application System
PhD students	PhD students who receive a scholarship from the UG
PN	Progress.Net
ProgressWWW	Registration system for student results
QANU	Quality Assurance Netherlands Universities
SIA	Student Information and Administration Office
S&P	Selection & Placement
UB	University library
UG	University of Groningen
UMCG	University Medical Center Groningen
WHW	Higher Education and Research Act

Definitions

Personal data: all information that can identify a **natural person** or information that can be traced back to that person now or in the future. This may include the name and address details, the student number or other information that uniquely identifies a person.

It can also be a combination of data that cannot directly be traced back to a person, but which, when combined with other data, may identify a person, e.g. a combination of residence, age and study. This type of data is referred to as indirectly traceable personal data.

Data subject: the person to whom personal data relate

Basis: the legal basis for processing

Purpose limitation: the well-defined, particular purpose of processing relating to the basis

Basic principles: conditions under which processing may take place

Privacy statement: this explains, among other things, what data is collected from data subjects; for what purpose; how long it is kept; where the data is stored; and which appropriate security measures have been taken. It also describes the rights that the data subject can exercise.

Processing: collecting, recording, organizing, structuring, storing, changing, retrieving, consulting, using,

providing, forwarding, distributing or making available, combining, blocking or destroying data, automated or otherwise. It concerns both paper files or archives, digital files or personal data in an application or system, including mailboxes, laptops, USB sticks and other data carriers. In other words, everything you do with personal data on any data carrier.

The controller: the organization, person or group that determines the purpose and means of data processing

The processor: a person, company or group that processes personal data on behalf of a controller and who/which is not part of the controller's organization

The process manager: the person responsible for processing the personal data

The process owner: the person who must ensure that all staff processing personal data do so in line with the UG's General policy on the protection of personal data.