



**UNIVERSITY**  
.....  
**OF APPLIED SCIENCES**

# **HZ Privacy Regulations Students**

Processing and protection of personal data of students at HZ University of Applied Sciences  
Rev.280619.

HZ University of Applied Sciences  
Data Protection Officer  
PO Box 364  
4382 NW Vlissingen

**Table of contents**

PARAGRAPH 1 DEFINITIONS.....	3
Article 1    Definitions .....	3
PARAGRAPH 2 SCOPE AND GOAL OF REGULATIONS .....	4
Article 2 Scope.....	4
Article 3 Goal of regulations.....	4
Article 4 Goal of the data processing .....	5
Article 5 Grounds for lawful Processing of personal data.....	5
Article 6 Notification obligation .....	5
PARAGRAPH 3 PERSONS CONCERNED: THE PERSONS ABOUT WHOM PERSONAL DATA IS.....	6
BEING PROCESSED .....	6
Article 7 Categories of persons .....	6
PARAGRAPH 4 TYPES OF DATA: THE PERSONAL DATA WHICH IS PROCESSED .....	6
Article 8 Types of data.....	6
Article 9 Special data .....	7
Article 10 The way in which personal data is acquired .....	7
PARAGRAPH 5 DATA PROVISION: TO WHOM THE PERSONAL DATA IS PROVIDED .....	8
Article 11 Provision of data .....	8
PARAGRAPH 6 RIGHTS OF PERSON CONCERNED.....	9
Article 12 Rights of person concerned: right to inspect, request correction or deletion, complaints.....	9
PARAGRAPH 7 ACCESS TO FILES, MANAGEMENT AND SECURITY .....	9
Article 13 Direct access to the personal data.....	9
Article 14 Controller .....	10
Article 15 Confidentiality and security .....	10
Article 16 Storage, anonymization and deletion of data.....	10
PARAGRAPH 8 DATA LEAK NOTIFICATION REQUIREMENT .....	10
Article 17 Notification Personal Data Authority.....	10
PARAGRAPH 9 FINAL AND IMPLEMENTATION PROVISIONS.....	11
Article 18 Transitional and final provisions .....	11
Article 19 Commencement and title .....	11
Article 20 Consultation of the regulations .....	11

## **Privacy Regulations processing and protection of personal data of HZ University of Applied Sciences students**

These regulations were, in compliance with the European Privacy decree (General Data Protection Regulation), recorded by the Executive Board on 03-04-2018.

### **PARAGRAPH 1 DEFINITIONS**

#### **Article 1 Definitions**

The following definitions are used in this regulation:

- a. Personal data: any information regarding an identified or identifiable natural person;
- b. Processing of personal data: every act or body of actions relating to personal data, including in any case collecting, recording, organising, storing, updating, modifying, retrieving, consulting, using, providing by means of forwarding, distribution or any other form provision, bringing together, relating to each other, as well as the protection, erasure or destruction of data;
- c. File: any structured set of personal data, regardless of whether this set of data is centralized or distributed in a functionally or geographically determined manner, which is accessible according to certain criteria and relates to different persons;
- d. Controller: the natural person, legal person or any other person or any other party who, alone or jointly with others, determines the purpose of and the means of processing of personal data, in this case the competent authority of HZ;
- e. Processor: the person who processes personal data on behalf of the controller without being subject to his direct authority;
- f. Administrator: the officer responsible for the processing of personal data by order of the controller, in this case the competent authority of HZ University of Applied Sciences;
- g. System administrator; the person who administrates the technical part of the files;
- h. Person concerned: the person to whom a piece of personal data relates;
- i. Third party: anyone, not being the data subject, the controller, the processor or any person authorised under direct authority of the controller or the processor to process personal data;
- j. Receiver: the party receiving the personal data;
- k. Collection of personal data: the acquisition of personal data;
- l. Provision of personal data: the disclosure or provision of personal data, insofar as they are wholly or largely derived from data included in a file, or which have been obtained by processing thereof, whether or not in connection with other data;

- m. Consent of the person concerned: every free, specific and informative expression of will by which the person concerned accepts that personal data relating to him will be processed;
- n. Data Protection Authority. Supervisory authority as referred to in Chapter 4 art 37 of the Privacy Regulation (GDPR);
- o. GDPR: General Data Protection Regulation. Directive 95/46/EC of the European Parliament and the council;
- p. WHW: Higher Education and Academic Research Act (Government Gazette 1992, 593 and later modifications and additions);
- q. DUO: Education Executive Agency, organisation in which the IB-Groep and the CFI are merged;
- r. HZ: HZ University of Applied Sciences, the competent authority of the university;
- s. Institution: the operational unit within HZ, in which the core competencies of the HZ especially are organised and which carries out the primary process. Is, if applicable, externally referred to as HZ University of Applied Sciences.
- t. Support service: the operational unit within HZ, which executes the business processes that support the primary process.
- u. Competent authority: the HZ University of Applied Sciences Executive Board;
- v. Data Protection Officer: the officer as referred to in Section 4 art 37 ff. General Data Protection Regulation (Regulation: GDPR);
- w. Data leak: loss of personal data to third parties who should not have access to that data as a result of a security issue;
- x. Regulation/GDPR: General Data Protection Regulation/European Privacy Regulation<sup>1</sup>.

## **PARAGRAPH 2 SCOPE AND GOAL OF REGULATIONS**

### **Article 2 Scope**

1. These regulations apply to all personal data of data subjects, as stated in Article 7, at HZ, which are processed by the controller or on his instructions, insofar as the data can easily be traced back to individual persons.
2. Insofar as data is provided to third parties, this can only be done with the express consent of the student in question, or on the basis of a power or duty included in a statutory regulation or these regulations.

### **Article 3 Goal of regulations**

1. These regulations are intended:

---

<sup>1</sup> <sup>1</sup> The General Data Protection Regulation (REGULATION (EU) 2016/679 OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL of 27 April 2016 on the protection of individuals with regard to the processing of personal data and on the free movement of such data and repealing Directive 95/46/EC (General data protection regulation/GDPR) comes into direct effect in the EU Member States. The GDPR enters into effect on 25 May 2018. This regulation takes into account the applicable provisions of the GDPR.

- a. To protect the privacy of any person whose personal data is processed from the misuse of that data and against the processing of incorrect data;
- b. To prevent personal data from being processed for a different goal than that for which they were collected;
- c. To secure of the rights of the persons concerned.

#### **Article 4 Goal of the data processing**

1. The goal of the data processing is:
  - a. To have access to information for the purpose of operating the university of applied sciences and providing a safe environment for employees and students, or the execution of statutory duties.
  - b. Being able to adequately supply data to persons or institutions with a public law task.

#### **Article 5 Grounds for lawful Processing of personal data**

1. HZ University Of Applied Sciences only processes personal data if one or more of the legal bases are met as described in Article 6 of the AVG:
  - a. Consent: the person concerned has given clear consent to process their personal data for a specific purpose.
  - b. Contract: the processing is necessary for a contract with the person concerned, or because the person asked to take specific steps before entering into a contract.
  - c. Legal obligation: the processing is necessary in order to comply with the law (not including contractual obligations).
  - d. Public task: the processing is necessary to perform a task in the public interest or official functions, and the task or function has a clear basis in law.
  - e. Vital interests: the processing is necessary to save someone's life.
  - f. Legitimate interest: the processing is necessary for the legitimate interest of the processor or the legitimate interest of a third party, unless these legitimate interests do not outweigh the interests of the person concerned.

#### **Article 6 Notification obligation**

1. A fully or partially automated processing of personal data, which is intended for the realisation of a purpose or of various related purposes, is reported by the Controller to the Data Protection Officer.
2. The Data Protection Officer keeps a register of the notifications.
3. Following from what has been stated in the previous paragraphs, every administrator and every employee who creates a new data processing is obliged to report this to the Data Protection Officer, stating the purpose of that file and the name(s) of the processor(s).
4. Persons concerned can acquire information from the Data Processing Officer regarding the registered processing of personal data.
5. If the Controller intends to record data on the basis of the targeted collection of information by means of his/her own research without informing the person concerned, the Controller must report this to the Data Protection Officer prior to the start of the investigation.

### **PARAGRAPH 3 PERSONS CONCERNED: THE PERSONS ABOUT WHOM PERSONAL DATA IS BEING PROCESSED**

#### **Article 7 Categories of persons**

The categories of persons whose data is being processed:

1. Applicant (potential students)
2. Students
3. External minor's students
4. External students
5. Contract students
6. Course participants

### **PARAGRAPH 4 TYPES OF DATA: THE PERSONAL DATA WHICH IS PROCESSED**

#### **Article 8 Types of data**

The following types of personal data can be processed:

- a. Name and address details, date of birth, for communication with the student and for formal documents.
- b. Student number, correspondence number OC&W, BSN and copy of identity card for identification of the students who cannot be verified via the GBA, digitised passport photo for the identification and communication with the student.
- c. Nationality and place of birth to be able to guide students of a certain ethnic or cultural minority in a more targeted way prior to and during their studies.
- d. Data necessary for health and well-being with the aim of giving students in special circumstances, insofar as necessary, special guidance or to be able to make specific provisions prior to and during their studies.
- e. Data such as insurance company and policy number only in case of a student's stay abroad for support in emergency situations.
- f. Study data and study progress data.
- g. Data related to the calculation, recording and collection of registration fees, school and course fees and contributions for fees for educational and extracurricular activities, as well as bank account number.
- h. Other legally required data.
- i. Diploma of prior education to evaluate the admissibility to Higher Professional Education and the desired programme.
- j. School of origin for the provision of study progress data to schools of origin of students, after explicit permission from students, this in the context of improving the connection between the prior and higher education.
- k. Digitised documents with regards to registration for the validity of enrolment, such as diploma for previous education (in case this cannot be verified at DUO), bank guarantee for foreign students, residence permit for foreign students, health insurance coverage of students/health insurance policy.

- l. Information about motivation for the study programme for advice on a good match between student and study programme in the context of the study choice check.
- m. Data collected via a camera, in the broadest sense of the word, which is visible or of which the presence has been made known (promotional activities, graduation, recording lectures, etc.).
- n. Other data, collected with the aid of a hidden camera, if there is a suspicion of a criminal offense or wrongful act and the use of a hidden camera can be regarded as proportionate.

#### **Article 9 Special data**

- 1. The processing of personal data concerning a person's religion or belief, race, political opinion, health, sexual life, as well as personal data concerning the membership of a trade union is prohibited, subject to the provisions of paragraph 2. The same applies to personal data regarding criminal law and personal data about unlawful or troublesome behaviour in connection with a prohibition following that behaviour.
- 2. The prohibition on processing personal data relating to criminal law does not apply to the controller who processes this data on his own behalf in order to:
  - a. assess a request from the person concerned to make a decision about him or to deliver a performance to him or
  - b. protection of his interests insofar as it concerns criminal offenses which are or are expected to be committed on the basis of facts and circumstances against him or against persons who are in his service.
- 3. The prohibition on processing personal data on someone's race does not apply if the processing takes place:
  - a. with the goal of identifying the person concerned and only insofar as this is unavoidable for this goal;
  - b. with the aim of granting a privileged position to persons of a particular ethnic or cultural minority group in order to eliminate or reduce actual inequalities only if:
    - i. this is necessary for that purpose; ii. the data only relate to the country of birth of the persons concerned, of his parents or grandparents, or to other criteria laid down by law, on the basis of which it can objectively be established whether someone belongs to a minority group as referred to in the preamble of section b,
    - iii. and the person involved has not objected to this in writing.

#### **Article 10 The way in which personal data is acquired**

- 1. The data listed under article 8 is provided by the person concerned during registration or application as much as possible, or collected by the Student Facility Service, Financial Service, Marketing Service or AV service, and recorded in the file and kept up-to-date. In addition, the student is responsible for the timely delivery and verification of the correct data for the registration of the correct name, address and residence details of both the residential address and the correspondence address by the student administration.
- 2. The data, as referred to in Article 8 sub n are obtained through the use of a camera that is visible or of which its presence has been made known.

3. The data referred to in article 8, sub o, are obtained through the use of a hidden camera, if there is a suspicion of criminal or unlawful actions committed by students, in which the proportionality and subsidiarity principle is respected.

## **PARAGRAPH 5 DATA PROVISION: TO WHOM THE PERSONAL DATA IS PROVIDED**

### **Article 11 Provision of data**

1. With the exception of the cases referred to in paragraphs 2, 3, 4 and 5 of this article, no registered personal data is provided to third parties, either in writing or orally, by or on behalf of the controller without the written consent of the data subject.
2. Personal data which can be traced back to individuals is provided to:
  - a. The Ministry of Education, Culture and Science;
  - b. The Higher Education Inspection;
  - c. The Education Executive Agency;
  - d. other third parties insofar as provision arises from the purpose of the data processing, is required as a result of a statutory requirement or is necessary for the performance of an agreement to which the person concerned is a party;
  - e. Planbureau|Zeeuwse bibliotheek for access to collections and knowledge services;
  - f. other institutions exclusively with the permission of the person concerned.
3. Apart from the cases in which this is required pursuant to a statutory requirement, the registered personal data, consisting only of: name, address, postcode and place of residence, e-mail address, can be provided to third parties insofar as this is necessary for the guidance of those involved, making payments, placing claims in the hands of third parties, dealing with disputes, and carrying out audits.
4. In addition to the provisions under paragraphs 3, personal data as referred to in paragraph 3 may be provided in further specification to third parties if this is deemed to be in the interest of the persons concerned. This will be only undertaken after the intention has been made known to the persons concerned or their legal representatives in a proper manner and they have for a reasonable period of time been given the opportunity to submit a request to omit this provision of information.
5. Furthermore, data as referred to in Article 8 can be provided to investigating officers if the information so requires. If the data referred to in Article 8 sub n and o presents reason to do so, HZ may provide this information to third parties for further investigation.
6. If personal data is made anonymous in such a way that it can not be traced directly to individual persons, the responsible party can decide to provide this for the purposes of scientific research or statistics in so far as:
  - a. the study serves a general interest;
  - b. the processing is necessary for the study or statistic in question;
  - c. asking for explicit permission is impossible or requires a disproportionate effort; d. the execution ensures that the privacy of the person concerned is not disproportionately harmed.
7. For the purposes of student studies, such as the National Student Survey (NSE), the organisation that carries out the study may be provided with personal data that are necessary

for carrying out the study. This then concerns personal data which is necessary to be able to approach the students and programme and study progress data. Reporting takes place in an anonymous manner.

8. Contact details of students (email address and potentially mailbox at the institution) are accessible to fellow students, unless the student objects to this.
9. If the data processing is outsourced to a third party, a processor's agreement is concluded with the processor on the basis of which the processor accepts the obligations arising from the GDPR, including with regards to security and confidentiality and the reporting of a data breach with regards to the processing of the personal data.

## **PARAGRAPH 6 RIGHTS OF PERSON CONCERNED**

### **Article 12 Rights of person concerned: right to inspect, request correction or deletion, complaints**

1. Each person concerned has the right to gain access to and determine the source of the personal data which is processed about them.
2. A request for inspection must be made to the controller, who will grant this request within a week of receipt. This request can be addressed to [privacy@hz.nl](mailto:privacy@hz.nl).
3. If the party concerned proves to the controller that some of his/her data is incorrect or incomplete or is not relevant considering the purpose of the system, or conflicts with these regulations, the administrator must within a month after the person concerned has demonstrated the incorrectness or incompleteness take care of improvement, addition or deletion.
4. If the administrator is in doubt as to the identity of the applicant, the applicant will be asked for further written information regarding his identity or to submit a valid identity document. Because of this request, the term is postponed until the time that the requested evidence has been delivered.
5. The person concerned can direct complaints regarding the implementation of the privacy regulations to the Data Protection Officer via [privacy@hz.nl](mailto:privacy@hz.nl), in accordance with article 5.15.9 of the HZ Student Statute<sup>1</sup>.

## **PARAGRAPH 7 ACCESS TO FILES, MANAGEMENT AND SECURITY**

### **Article 13 Direct access to the personal data**

1. The following parties have access to the personal data of the students:
  - The controller;
  - The administrators;
  - The officers appointed by HZ, who need the data for performing the activities in the framework of the performance of their function;
  - The system administrators
2. The system administrator will with an encryption and password protection give the various officers as referred to in paragraph 1 access to certain parts of the personal data or to all personal data depending on whether their activities require this.

---

<sup>1</sup> <https://hz.nl/over-de-hz/regelingen-documenten/onderwijs-en-examenregelingen>

## **Article 14 Controller**

The competent authority of the HZ is controller of the personal data. The competent authority takes care of enforcement of the regulations as well as the correctness of the collected data.

## **Article 15 Confidentiality and security**

1. The controller ensures suitable technical and organisational measures to prevent loss or wrongful processing of personal data. These measures guarantee, taking into account the state of the art and the costs of implementation, an appropriate level of security, paying attention to the risks involved in the processing and the nature of the data to be protected.
2. The controller can demonstrate with documentation that the correct organisational and technical measures have been taken to comply with the Regulation.
3. The controller carries out a Privacy Impact Assessment (PIA).
4. The administrator, system administrator and processor have the same duty.
5. Officers who become aware of personal data as a result of their duties are prohibited from using this information other than for the performance of their duties and not to inform unauthorised persons, in accordance with the provisions of the CLA-HBO.

## **Article 16 Storage, anonymization and deletion of data**

1. In any case, the personal data will not be deleted during the course of the studies on the basis of which the processing takes place and will be stored or filed after the end thereof in accordance with the decision drawn up for this purpose, Determination of the documents to be archived (V720150429), as determined by the Executive Board.
2. If the relevant data has been processed in such a way that it cannot be traced back to individual persons, it can be kept in an anonymous form.
3. Personal data of aspiring students who are not registered with the university of applied sciences are deleted from the final two years after the beginning of the new academic year at the latest.
4. Personal data as referred to in Article 8 shall not be kept for longer than is necessary for the purpose for which they were collected. The data will be destroyed within 14 days of recording, or after handling of the identified incidents. If the data relating to a particular incident has been transferred to an investigating officer, a copy of this data for internal use can be stored for a maximum period of 6 months, insofar as there is a presumption of risk of recurrence of the incident.

## **PARAGRAPH 8 DATA LEAK NOTIFICATION REQUIREMENT**

### **Article 17 Notification Data Protection Authority**

1. HZ will immediately report to the Dutch Data Protection Authority in the event of a breach of security that leads to the considerable chance of serious adverse consequences or has serious adverse consequences for the protection of personal data, i.e. a data breach, where personal data of a sensitive nature are leaked or there is a significant risk of adverse consequences for the protection of the processed personal data or unlawful processing of the personal data cannot reasonably be excluded.
2. HZ will report a data leak to the person(s) concerned whose personal data have been released, if the data leak has adverse consequences for the privacy of the person(s) concerned.

3. Personal data of a sensitive nature include special personal data, information about the financial or economic situation of the data subject, data that can lead to stigmatization or exclusion of the data subject, user names, passwords and other login data and data that can be misused for (identity) fraud.
4. Reporting a data leak takes place no later than 72 hours after its discovery.

## **PARAGRAPH 9 FINAL AND IMPLEMENTATION PROVISIONS**

### **Article 18 Transitional and final provisions**

1. Without prejudice to any statutory requirements, these regulations are in force for the entire duration of the processing of the personal data.
2. In case of transfer or transition of the files to a different controller, the person concerned must be informed of this, so that an objection can be made against transfer or transition of personal data relating to them.
3. In case of transfer or transition of the files to another controller, the Data Protection Officer must be informed of this, so that the processing register remains up-to-date.

### **Article 19 Commencement and title**

These regulations were recorded by the Executive Board on 03-04-2018. A revision has been recorded in July 2019. These regulations can be requested as HZ Privacy Regulations Students.

### **Article 20 Consultation of the regulations**

1. The controller will communicate the existence of this document through a general notification.
2. These regulations can be consulted by anyone whose personal data could be processed. The regulations can also be consulted via the HZ website.