



UNIVERSITY
.....
OF APPLIED SCIENCES

Privacy Regulations HZ Employees

Processing and protection of personal data of HZ University of Applied Sciences employees
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 personal 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 personal 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	11
Article 17 Notification Personal Data Authority.....	11
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	12

Privacy Regulations processing and protection of personal data of HZ University of Applied Sciences employees

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 administrative body who, alone or jointly with others, determines the purpose of and the means for the 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 official 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. DPA: Data Protection Authority. Supervisory authority as referred to Section 4 Article 37 ff of the General Data Protection Regulation (Regulation: GDPR);
- o. C.L.A.: Collective Labour Agreement for Higher Professional Education;
- p. HZ: HZ University of Applied Sciences, the competent authority of the university.
- q. 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.
- r. Support service: the operational unit within HZ, which executes the business processes that support the primary process.
- s. Competent authority: HZ management or the HZ Executive Board.
- t. DPO: Data Protection Officer: the officer as referred to in Section 4 art 37 ff. General Data Protection Regulation;
- u. Data leak: loss of personal data to third parties who should not have access to that data;
- v. (Privacy) Regulation/GDPR: General Data Protection Regulation/European Privacy Regulation.¹

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.

Article 3 Goal of regulations

1. These regulations intended to:
 1. protect the privacy of any person whose personal data is processed from the misuse of that data and against the processing of incorrect data;
 2. prevent personal data from being processed for a different goal than that for which it was collected;
 3. secure the rights of the persons concerned.

¹ 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 regards 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.

Article 4 Goal of the data processing

1. The goal of the data processing is:
 - a. To have access to legitimately acquired information for the benefit of the operations of the institution, the supporting service, or carrying out legal obligations;
 - 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 processing.
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 or application and the name(s) of the processor(s).
4. Persons concerned can acquire information regarding the registered processing of personal data from the Data Processing Officer.

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

Article 7 Categories of persons

The following categories of persons employed or working for HZ or who were employed or working for HZ can be processed:

- a. Persons employed by or (temporarily or otherwise) working for the controller, including temporary workers, seconded staff, trainees, guest lecturers, applicants and other third parties.
- b. Former employees. Persons as referred to in sub a, who no longer work for HZ.

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

Article 8 Types of data

The following types of data can be processed:

- a. Name and address details, passport photo, date of birth, potential date of death for communication with the employee and for formal documents;
- b. Personnel number to identify the employee;
- c. Nationality and place of birth;
- d. Information regarding training, knowledge and skills, competencies and behavior and training data with regards to performance for the purpose of organising a staff assessment and being able to perform career guidance for the employee. The data is known to the persons concerned;
- e. Information and correspondence concerning the appointment (duration, nature, content, salary data, labour history and times of service) for the handling of personnel matters;
- f. Attendance and absence registration related to leave, illness, etc. for the administration of leave and absenteeism for another law. The nature of the illness is not registered. Data regarding health is only processed to the extent allowed under Article 9, paragraph 2, under b, of the GDPR;
- g. Data on working conditions for the benefit of the people concerned with regards to specific working conditions. Data regarding health is only processed to the extent allowed under Article 9, paragraph 2, under b, of the GDPR;
- h. Specific data, also regarding (previous) family members. This information is only recorded insofar as is necessary with regards to an agreed upon employment condition, especially the CLA or for contact details in emergencies;
- i. Other legally required data for the purpose of implementing or applying the law;
- j. Documents for the personnel file for the handling of personnel affairs;
- k. Data collected by a visible camera or of which the presence is known;
- l. Other data, collected with the aid of a hidden camera, if there is a suspicion of a criminal offense or wrongful act.

Article 9 Special personal data

The processing of personal data concerning a person's religion or belief, race, political opinion, health, sexual life, citizen service number (BSN), as well as personal data concerning the membership of a trade union is prohibited. The same applies to personal data regarding criminal law and personal data about unlawful or troublesome behavior in connection with a prohibition following that behavior.

1. The prohibition on processing data regarding the membership of a trade union does not apply to the controller who processes this data on his own behalf for the reimbursement of the contribution in accordance with Annex IV/Trade Union contribution regulation which is part of the applicable collective labour agreement for higher professional education.
2. The prohibition on processing health data does not apply to the controller who processes this data on his own behalf to settle Wajong and labour participation registrations.
3. The prohibition on processing personal data regarding criminal law does not apply to the controller who processes this data on his own behalf to:
 - a. evaluate a request from a person concerned to make a decision about him or to deliver a performance to him or
 - b. protection of his interests insofar as this concerns criminal offenses which are or are expected to be committed against him or against persons who are in his service on the basis of facts and circumstances.
4. 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 goal:
 - 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, and
 - iii) the person concerned has not objected to this in writing.

Article 10 The way in which personal data is acquired

1. The data referred to in Article 8 shall be provided by the person concerned during the application or commencement of employment as much as possible, or collected by the Personnel and Organisation Department, the payroll administration and the personnel administrations of the institutions and services or collected by the supervisor of the person concerned, recorded in the file and kept completely confidential and up-to-date.
2. The data, as referred to in Article 8 sub k, is obtained through the use of a camera that is visible or of which presence has been made known.

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

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

Article 11 Provision of personal data

1. Within the organisation of the controller, personal data from the files is provided to officers insofar as this is necessary for the performance of their duties, including for the handling of disputes.
2. In addition to the cases in which this is required pursuant to a statutory regulation, personal data will be provided to third parties from the files insofar as this is necessary with a view to:
 - a. an employment condition applicable to the person concerned;
 - b. the salary administration;
 - c. the administration regarding claims to payments related to the termination of employment;
 - d. the administration of the staff association;
 - e. training;
 - f. the in-house emergency services (BHV);
 - g. company security;
 - h. the transfer of the person concerned to or his temporary employment with another part of the group with which the controller is affiliated;
 - i. the possibility of dismissal;
 - j. placing claims in the hands of third parties;
 - k. handling disputes;
 - l. having an audit carried out by an accountant or the tax authority.
3. Furthermore, information can be provided by or on behalf of the controller to governmental and semi-governmental bodies within the framework of the implementation of laws and regulations and to organisations whose activities arise from a statutory regulation. 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 k and l presents reason to do so, HZ may provide this information to third parties for further investigation.
4. In addition to the provisions in paragraphs 2 and 3, personal data as specified in paragraphs 2 and 3 may be provided to third parties if this is deemed to be in the interest of the employees. This will be only undertaken after the intention has been made known to the parties 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 such provision of information.

5. If personal data is made anonymous in such a way that it cannot 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 statistics in question;
 - c. asking for explicit permission is impossible or requires a disproportionate amount of effort and
 - d. the execution ensures that the privacy of the person concerned is not disproportionately harmed.
6. If employees work from home at their own request with the permission of their supervisor, they must be reachable. Contact details of employees (email address and/or private telephone number at the choice of the employee in question) are available to this end.
7. 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 sent to 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 goal of the data processing, 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. In that case, any costs paid are reimbursed.
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 produced.
5. The person concerned can direct complaints regarding the implementation of the privacy regulations to the Data Protection Officer via privacy@hz.nl.

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 employees:

- 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 duties; - The system administrators.
 - System administrators
2. The system administrator will with an encryption and password protection in the system 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. The administrator is mandated to do so by the Executive Board.

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. Employees 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 from informing unauthorised persons.
4. If necessary (in accordance with the guidelines of the GDPR), a Privacy Impact Assessment (PIA) is carried out.

Article 16 Storage, anonymization and deletion of data

1. The personal and financial data are deleted from the files in accordance with the legally applicable term after the employment or the activities of the person concerned for the controller have been terminated, unless a longer term is deemed purposeful.
2. When the storage term of ten years has passed, the data in question is deleted and destroyed within a year.
3. 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.
4. Personal data of persons with whom an employment contract is not concluded after an application procedure shall be removed from the file at the request of the person concerned, but in any case, no later than four weeks after the application procedure has ended, unless the personal data is stored for one year after the end of the application procedure with the permission of the person concerned.

5. Personal data of persons who have submitted an open application will be removed from the file after six months, unless the person concerned himself requests an extension of this retention period.
6. Personal data of camera images as referred to in Article 8 shall not be kept for longer than necessary for the purpose for which they were collected. The data will be destroyed within 30 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 a 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 is 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.

Article 19 Commencement and title

These regulations were recorded by the Executive Board on the third of April 2018. A revision has been recorded in July 2019. These regulations can be requested as HZ Privacy Regulations Employees.

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.

