

## **Privacy Rules**

### **Processing and protection of personal data of Fontys Students**

**Fontys University of Applied Sciences  
Service Organisation Education and Research  
Legal Affairs  
Postbus 347  
5600 AH Eindhoven**

## Contents

<b>SECTION 1</b>	<b>DEFINITIONS OF TERMS</b>
Article 1	Definitions of terms
<b>SECTION 2</b>	<b>SCOPE AND OBJECTIVE OF THESE RULES</b>
Article 2	Scope of these Rules
Article 3	Objective of these Rules
Article 4	Purpose of the data processing
Article 5	Notification obligation
<b>SECTION 3</b>	<b>DATA SUBJECTS: WHOSE PERSONAL DATA ARE PROCESSED</b>
Article 6	Categories of data subjects
<b>SECTION 4</b>	<b>TYPES OF DATA: WHICH PERSONAL DATA ARE PROCESSED</b>
Article 7	Types of data
Article 8	Special personal data
Article 9	The manner in which data are obtained
<b>SECTION 5</b>	<b>DISCLOSURE OF DATA: TO WHOM ARE PERSONAL DATA DISCLOSED</b>
Article 10	Disclosure of data
<b>SECTION 6</b>	<b>DATA SUBJECT'S RIGHTS</b>
Article 11	Data subject's rights: access, request to correct or delete, complaints
<b>SECTION 7</b>	<b>ACCESS TO FILES, MANAGEMENT AND PROTECTION</b>
Article 12	Direct access to the personal data
Article 13	Control responsibility
Article 14	Confidentiality and protection
Article 15	Retention and destruction of data
<b>SECTION 8</b>	<b>MANDATORY NOTIFICATION OF DATA LEAKS</b>
Article 16	Notification to Dutch Data Protection Authority (Dutch DPA)
<b>SECTION 9</b>	<b>FINAL PROVISIONS AND IMPLEMENTATION PROVISIONS</b>
Article 17	Transitional and final provisions
Article 18	Entry into force and official title
Article 19	Availability of Rules for inspection

## Privacy Rules on the processing and protection of personal data of Fontys Students

These Rules were adopted by the Executive Board on 24 January 2003 after consent was issued by the Central Participation Council (CMR) on 23 January 2003, in implementation of the Dutch Personal Data Protection Act (Bulletin of Acts and Decrees 2001, 302, Act of 6 July 2000, effective from 1 September 2001).

These Rules were amended and adopted by the Executive Board on 13 December 2011. The Central Participation Council (CMR) issued consent on 16 March 2012.

With due regard for and in anticipation of the General Data Protection Regulation (GDPR), these Rules were amended and adopted by the Executive Board on 14 February 2017.

The Central Participation Council (CMR) issued consent on 30 March 2017.

### SECTION 1 DEFINITIONS OF TERMS

#### Article 1 Definitions of terms

In these Rules, the following definitions apply:

- a. Personal data: any information relating to an identified or identifiable natural person;
- b. Processing of personal data: any operation or set of operations which is/are performed upon personal data, including in any case the collection, recording, organisation, storage, adaptation, alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, blocking, erasure or destruction of data;
- c. Filing system: any structured set of personal data, whether centralised or dispersed on a functional or geographical basis, which is accessible according to specific criteria and relates to different persons;
- d. Controller: the natural or legal person or any other party who or the administrative body which, alone or jointly with others, determines the purposes and means of the processing of personal data, in this case the competent authority of Stichting Fontys;
- e. Processor: the person who processes personal data on behalf of the controller without being subject to his direct authority;
- f. Administrator: the official who on the instructions of the controller, in this case the competent authority of Stichting Fontys, is responsible for the processing of the personal data;
- g. System administrator: the person administering the technical part of the filing systems;
- h. Data subject: the person to whom the personal data relate;
- i. Third party: any person other than the data subject, the controller, the processor or any person who, under the direct authority of the controller or the processor, is authorised to process the personal data;
- j. Recipient: the party to whom personal data are disclosed;
- k. (Data) Controller: the natural or legal person or any other party who or the administrative body which, alone or jointly with others, determines the purposes and means of the processing of personal data;
- l. Collection of personal data: obtaining personal data;
- m. Disclosure of personal data: the publication or making available of personal data, in so far as these are entirely or largely drawn from data recorded in a filing system, or which have been obtained through processing of such data, whether or not in combination with other data;
- n. The data subject's consent: any freely given specific and informed indication of his wishes by which the data subject signifies his agreement to personal data relating to him being processed;
- o. Data Protection Authority (as from 1 January 2016 the Dutch Data Protection Authority (Dutch DPA): the Authority referred to in Section 51 of the Personal Data Protection Act (*Wet Bescherming Persoonsgegevens*);
- p. WBP: the Dutch Personal Data Protection Act (Bulletin of Acts and Decrees 2002, 302, including later amendments and additions);
- q. WHW: the Dutch Higher Education and Research Act (Bulletin of Acts and Decrees 1992, 593, including later amendments and additions);
- r. DUO: the Education Executive Agency of the Ministry of Education (*Dienst Uitvoering Onderwijs*), which is a combination of the IB Group and CFI;
- s. Fontys: Stichting Fontys (Fontys Foundation), the competent authority of the Fontys universities of applied sciences;
- t. Institute: the operational unit of organisation for Fontys' core competencies which is responsible for the execution of the primary process. Where applicable, it is referred to externally as Fontys University of Applied Sciences.
- u. Services organisation: the Fontys operational unit which is responsible for the execution of the business process and provision of technical support to the primary process.
- v. Competent authority: the board of Stichting Fontys or the Executive Board of Stichting Fontys;

- w. Exemption decree: the Decree of 7 May 2001, concerning the processing of personal data that are exempted from the notification referred to in Section 27 of the Dutch Personal Data Protection Act (Bulletin of Acts and Decrees 2001, 250, including later amendments and additions);
- x. Data Protection Official: the official referred to in Section 62 of the Dutch Personal Data Protection Act and Section 4, article 37 et seq. of the General Data Protection Regulation (Regulation/GDPR);
- y. Data leak: a loss of personal data to a third party who should not be able to access those data due to a security problem;
- z. Regulation/GDPR: the General Data Protection Regulation.<sup>1</sup>

## SECTION 2 SCOPE AND OBJECTIVE OF THESE RULES

### Article 2 Scope

1. These Rules apply to all personal data of data subjects, as referred to in Article 6, affiliated with Fontys, which are processed by or on the instructions of the controller, insofar as the data are easily traceable to individual persons.
2. These Rules do not apply to personal data contained in the files of student counsellors and psychologists, confidential advisers, the Fontys University of Applied Sciences Commission for Complaints about Undesirable Behaviour, the Fontys Examination Appeals Board and the Executive Board Advisory Committee for Objections and Complaints.
3. The personal data contained in the files referred to in paragraph 2 above are, in principle, confidential and should be treated as such.
4. Insofar as data from the files referred to in paragraphs 2 and 3 above are disclosed to third parties, this may only take place with the consent of the student concerned, or pursuant to an authority or obligation provided in a statutory regulation or in these Rules.

### Article 3 Objective of these Rules

The purpose of these Rules is:

1. to protect the privacy of anyone whose personal data are processed against misuse of those data and against the processing of inaccurate personal data;
2. to prevent personal data from being processed for any purpose other than the purpose for which they were collected;
3. to safeguard the rights of data subjects.

### Article 4 Purpose of the data processing

1. The purpose of data processing is:
  - a. to enable access to information in the interest of the operations of the university of applied sciences and to ensure a safe learning and working environment for staff and students, or to implement statutory tasks and duties in accordance with the provisions in Article 19(2) of the Exemption Decree;
  - b. to comply adequately with a request for the disclosure of data to persons or administrative bodies with a public law task.

The processing will be undertaken among other things for the purposes laid down in the 'Notifications required under the Dutch Personal Data Protection Act'

(<https://connect.fontys.nl/fontysbreed/privacy/Paginas/persoonsgegevens.aspx>).

### Article 5 Notification obligation

1. The controller will notify the Data Protection Officer of the processing of personal data wholly or partly by automatic means, which is intended to serve a single purpose or several related purposes.
2. The Data Protection Officer will keep a register of notifications.
3. In accordance with the above provisions, each administrator and each employee engaging in new data processing is subject to an obligation to report such processing to the Data Protection Officer, stating the purpose of that filing system and the name(s) of the processor(s).
4. Data subjects can obtain information on the notified processing of personal data from the Data Protection Officer.
5. If the controller intends to record data based on the targeted collection of information by carrying out his own investigation without informing the data subject of this, the controller will report this to the Dutch Data Protection Authority (Dutch DPA) prior to commencing the investigation.

---

<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 natural persons 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) has direct effect in the EU Member States. The GDPR is effective from 25 May 2018. These Rules take into account the applicable provisions from the GDPR.

## SECTION 3 DATA SUBJECTS WHOSE PERSONAL DATA ARE PROCESSED

### Article 6 Categories of persons

The categories of persons whose data are processed:

1. Registering (prospective) students
2. Students
3. External minor students
4. External candidates
5. Contract students
6. Course participants

## SECTION 4 TYPES OF DATA: WHICH PERSONAL DATA ARE PROCESSED?

### Article 7 Types of data

1. The following types of personal data can be processed:
  - a. Name and address details, date of birth, date of decease, where applicable, for the purpose of communication with the student as well as formal documents;
  - b. Student ID number, Ministry of Education, Culture and Science correspondence number, BSN (citizen service number) and copy of identity document for the purpose of identifying the student for students whose identity cannot be verified through the Municipal Personal Records Database (GBA), digitised passport photo for the purpose of verifying the identity and communicating with the student;
  - c. Nationality and place of birth in order to provide students of a certain ethnic or cultural minority group with more targeted support prior to and during their course of studies;
  - d. Data that are necessary with regard to health and welfare in order to provide students with special needs, to the extent necessary, with special assistance or make targeted provisions prior to and during their studies;
  - e. Data including name of insurance company and policy number solely in case of a stay abroad by the student, in order to provide support in emergency situations;
  - f. Study data and data on study progress;
  - g. Data relating to the calculation, recording and collection of enrolment fees, school and tuition fees and contributions toward allowances for teaching materials and extracurricular activities, as well as bank or giro account number;
  - h. Other data required by law;
  - i. Prior education certificate to enable assessment of admissibility to the HBO and the desired study programme;
  - j. Originating school to allow the provision of data on study progress to students' former schools, with students' express consent, to improve contact and ensure a continuing educational line;
  - k. Digitised documents on enrolment to allow verification of the validity of the enrolment, such as prior education certificate (in the event this cannot be verified with DUO), bank guarantee and residence permit in the case of foreign students;
  - l. Details of motivation for the study programme to enable advice to be given on a good match between student and study programme as part of the Study Check;
  - m. Data gathered via a camera that is visible or whose presence has been made known;
  - n. Other data, gathered via a hidden camera, in cases where there is a suspicion of a criminal offence or unlawful act and the use of a hidden camera may be considered proportional.

### Article 8 Special data

1. The processing of personal data relating to a person's religion or belief, race, political affinity, health, sex life and trade union membership is prohibited, subject to the provisions in paragraph 2 below. The same applies to personal data concerning criminal law matters and personal data on unlawful or objectionable conduct in connection with a prohibition imposed in response to such conduct.
2. The prohibition on processing personal data relating to criminal law matters does not apply to a controller who processes these data for his own purposes in order to:
  - a) assess a request from the data subject to take a decision on him or to provide a service to him, or
  - b) protect his interests in cases of criminal offences committed against him or which, on the basis of facts and circumstances, can be expected to be committed against him or persons employed by him.
3. The prohibition on processing personal data relating to a person's race does not apply if the processing is carried out:
  - a) to identify the data subjects and only in so far as this is unavoidable for that purpose;
  - b) with the purpose of conferring a preferential position on persons of a certain ethnic or cultural minority group in order to eliminate or reduce *de facto* inequalities connected with race, and only if:
    - l. this is necessary for that purpose;

- II. the data relate solely to the country of birth of the data subject, his parents or grandparents, or to other criteria set by law on the basis of which it can be objectively determined whether a person belongs to a minority group as referred to in the opening lines of (b), and
- III. the data subject has not objected to this in writing.

#### **Article 9 The manner in which data are obtained**

1. The data referred to in Article 7 will be provided by the data subject in so far as possible on registration or enrolment, or will be collected by the Student Facilities department or the Finance department (from third parties), and will be filed and kept up-to-date. The student is additionally responsible for providing in good time and checking the correct information to enable registration of the correct name and address details for both home and correspondence address by the Student Administration Office.
2. The data referred to in Article 7(m) will be obtained from a camera that is visible or whose presence has been made known.
3. The data referred to in Article 7(n) will be obtained from a hidden camera, in cases where there is suspicion of a criminal offence or unlawful act committed by students, with due regard for the principles of proportionality and subsidiarity.

### **SECTION 5 DISCLOSURE OF DATA: TO WHOM ARE PERSONAL DATA DISCLOSED**

#### **Article 10 Disclosure 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 will be disclosed to any third party, in writing or orally, by or on the instructions of the controller without the written consent of the data subject.
2. Personal data that are traceable to individual persons may be disclosed to:
  - the Ministry of Education, Culture and Science;
  - the Higher Education Inspectorate;
  - the Education Executive Agency;
  - other third parties, in so far as disclosure is inherent in the purpose of the data processing, is required pursuant to a statutory provision or is necessary for the implementation of an agreement to which the data subject is a party;
  - other institutions, solely with the consent of the data subject.
3. Apart from cases in which there is requirement under a statutory provision, registered personal data, consisting solely of name, address, postal code and place of residence and email address, may be disclosed to third parties in so far as necessary with a view to assisting data subjects, making remittances, passing on claims for collection, handling disputes as well as for the performance of audits.
4. Supplementary to the provisions in paragraph 3 above, personal data referred to in paragraph 3 may be disclosed to third parties on further specified conditions where the controller believes that to be in the data subjects' interest. This will not be done before the data subjects or their legal representatives have been properly informed of that intention and they have had the opportunity during a reasonable period to request that no such disclosure of data take place.
5. Data referred to in Article 7 can furthermore be disclosed to investigating officers if the nature of the data gives cause to do so. If the data referred to in Article 7 (m) and (n) provide cause to do so, such data can be disclosed to third parties for further investigation.
6. If personal data have been anonymised in such a way that they are not directly traceable to individual persons, the controller may decide to disclose them for purposes of scientific research or statistics, in so far as:
  - a) the research serves a public interest;
  - b) the processing is necessary for the research or statistics concerned;
  - c) it proves impossible or would involve a disproportionate effort to request express consent, and
  - d) safeguards have been put in place for the processing such that the data subject's privacy is not disproportionately compromised.

Personal data may be disclosed to an organisation carrying out student surveys, such as the National Student Survey, provided that such data are needed to carry out the survey. The personal data concerned are data that enable the students to be contacted as well as educational data and data on study progress. Reporting is conducted in anonymised form.

7. Contact details of students (email address and mailbox/pigeon hole at the institute, where applicable) are available to fellow students, unless the student makes an objection.
8. If data processing is outsourced to a third party, a data processor's agreement will be concluded with the processor under which the processor accepts the obligations arising from the Personal Data Protection Act (and from 25 May 2018 the GDPR), with regard to, among other things, protection and confidentiality and the notification of a data leak, in relation to the processing of the personal data.

## SECTION 6 DATA SUBJECT'S RIGHTS

### Article 11 Data subject's rights: access, request to correct or delete, complaints

1. Every data subject has the right to access and learn the origin of the personal data that are being processed in relation to him/her.
2. A request for access must be made to the controller, who will comply with the request within a week of receiving it. This request can be sent to the administrator concerned.
3. If the data subject demonstrates to the controller that certain recorded data concerning him/her are incorrect or incomplete, or are irrelevant given the objective of the system, or are contrary to these Rules, the administrator will ensure those data are corrected, supplemented or removed within one month of the data subject demonstrating the incorrectness or incompleteness of the data. In that case any costs that have been paid will be reimbursed.
4. If the administrator has doubts about the identity of the applicant, he will request the applicant as soon as possible to provide further details in writing concerning his identity or to submit a valid identity document. This request by the administrator will have the effect of suspending the above-mentioned period until such time as the requested proof is furnished.
  - a. The data subject may lodge complaints about the application of the Privacy Rules with the Data Protection Officer, in accordance with the procedure set out in Article 47 of the Fontys Students Charter (see website).<sup>2</sup>

## SECTION 7 ACCESS TO FILES, MANAGEMENT AND PROTECTION

### Article 12 Direct access to the personal data

1. The personal data of students may be accessed by:
  - the controller;
  - the administrators;
  - the officials who require data in order to carry out the work in connection with the performance of their duties;
  - the system administrators.
2. The system administrator will deploy coding and password protection to grant the various officials referred to in paragraph 1 above access to certain parts of the personal data or to all the personal data, as required by their work.

### Article 13 Control responsibility

The competent authority of Stichting Fontys is the controller of the personal data. The competent authority will ensure compliance with the Rules as well as the accuracy of the collected data.

### Article 14 Confidentiality and protection

1. The controller will ensure appropriate technical and organisational measures to protect personal data against loss or any unlawful forms of processing. Such measures will guarantee a level of security appropriate to the risks represented by the processing and the nature of the data to be protected, with due regard to the state of the art and the cost of their implementation.
2. The controller can provide documentary evidence to demonstrate that the correct organisational and technical measures have been taken for compliance with the Regulation.
3. The controller will carry out a Privacy Impact Assessment (PIA).
4. The administrator, system administrator and processor are subject to a similar obligation.
5. Officials who have access to personal data held in a filing system by virtue of their position are obliged to use such data only as required for the performance of their duties and not to disclose the data to unauthorised persons, in accordance with the relevant provisions in the collective labour agreement for higher professional education (CAO-HBO).

### Article 15 Retention, anonymization and destruction of data

1. The personal data will in any event not be removed for the duration of the study programme on the basis of which the processing takes place, and on the expiry of the study programme will be stored or archived in accordance with the policy on retention periods for student and education-related documents, as adopted by the Executive Board.
2. Provided that the data concerned have been edited in such a way as to ensure they cannot reasonably be traced back to individual persons, they may be retained in anonymised form.
3. Personal data of prospective students who are not registered with the university of applied sciences will be deleted no more than two years after the start of the new academic year.

---

<sup>2</sup> <https://connect.fontys.nl/fontysbreed/privacy/Paginas/home.aspx>

4. Personal data referred to in Article 7 will not be retained for longer than is necessary for the purpose for which they were collected. The data will be destroyed not more than 14 days after recording, or after the incidents to which the recordings relate have been dealt with. In the event the data relating to a particular incident have been handed over to an investigating officer, a copy of such data may be retained for internal use for a maximum period of 6 months in so far as there is a suspicion that the incident may be repeated.
5. Personal data referred to in Article 7 will not be retained for longer than is necessary for the purpose for which they were collected.

## **SECTION 8 MANDATORY NOTIFICATION OF DATA LEAKS**

### **Article 16 Notification to Dutch Data Protection Authority (Dutch DPA)**

1. Stichting Fontys will, without delay, notify the Dutch DPA of a breach of security which results in a substantial probability of serious adverse consequences or which has adverse consequences for the protection of personal data, constituting a data leak whereby sensitive personal data have been leaked, or there is a substantial probability of adverse consequences for the protection of the processed personal data, or the possibility of unlawful processing of the personal data cannot reasonably be excluded.
2. Stichting Fontys will notify the data subject(s) whose personal data have been disclosed of a data leak, if that leak has adverse consequences for the data subject's/data subjects' privacy.
3. Sensitive personal data are special personal data, data on the data subject's financial or economic situation, data that can lead to stigmatisation or exclusion of the data subject, user names, passwords and other login details and details that can be misused for the purpose of (identity) fraud.
4. A data leak will be reported within 72 hours of its discovery.

## **SECTION 9 FINAL PROVISIONS AND IMPLEMENTATION PROVISIONS**

### **Article 17 Transitional and final provisions**

1. Without prejudice to any statutory provisions, these Rules will remain in force throughout the duration of the processing of the personal data.
2. The data subject must be informed of any transfer or transmission of the filing systems to another controller in order to enable him to make an objection to the transfer or transmission of data relating to his person.

### **Article 18 Entry into force and official title**

These Rules will enter into force on 1 September 2002 and may be cited as Privacy Rules pertaining to Personal Data of Fontys Students.

These amended Rules were adopted by the Executive Board on 14 February 2017.

The Central Participation Council (CMR) issued consent on 30 March 2017.

These Rules will enter into force with effect from 1 April 2017.

### **Article 19 Availability of Rules for inspection**

1. The controller will notify the existence of these Rules by means of a general notification.
2. These Rules are available for inspection by anyone whose personal data might be processed. The Rules are also available on the Fontys website ([www.fontys.nl/regelingen](http://www.fontys.nl/regelingen)).