

EMPLOYEE PERSONAL DATA PROCESSING REGULATIONS VRIJE UNIVERSITEIT AMSTERDAM

Regulations for processing personal data of Vrije University Amsterdam employees

This document is a translation. In the event of any ambiguity or uncertainty arising from the translation, the original Dutch version shall take precedence and govern the interpretation and understanding of the content.

Contents

Introduction	3
Article 1. Terms	4
Article 2. Scope of application.....	5
Article 3. Purposes of Processing	6
Article 4. Personal data	7
Article 5. Special Personal Data.....	7
Article 6. Basis for Processing.....	9
Article 7. Transparent information and communication	9
Article 8. Duty to inform.....	10
Article 9. Access to Personal Data	11
Article 10. Provision of Personal Data to Third Parties	11
Article 11. Quality of Personal Data	11
Article 12. Retention periods and deletion of Personal Data	11
Article 13. Confidentiality.....	12
Article 14. Security	12
Article 15. Data protection by design and by default ('Privacy by Design' and 'Privacy by Default').....	12
Article 16. Register of processing activities.....	12
Article 17. International transfer.....	12
Article 18. Data protection officer (DPO) and internal responsibility Processing	13
Article 19. Rights of Data Subjects	13
Article 20. Complaints	14
Article 21. Final provisions	14

Introduction

As an employer, the Stichting VU (hereinafter **VU**) processes personal data of various data subjects. Upon entering employment, employees provide various personal data, such as name, address, date of birth, citizen service number (BSN) and information about education and work experience. The VU also collects and processes employees' personal data during their careers, for example with regard to the content of the employment, training courses taken or to be taken, and assessments. These personal data are accessed and processed by authorised VU employees. Examples include a manager or an employee of the VU payroll administration department.

The VU values the careful handling of its employees' personal data. Compliance with laws and regulations on the protection of personal data and privacy is of great importance to the VU.

These Regulations (hereinafter: **Regulations**) describe tasks, responsibilities and procedures and describe how data subjects can exercise their rights when their personal data are processed by the VU. These Regulations apply not only to the processing of personal data of employees of the VU, but also to the processing of personal data of persons working for the VU without an employment contract with the VU (such as temporary employees, secondees, self-employed workers, interns and guest lecturers), (pre)retired persons and family members of (former) employees.

The purpose of these Regulations is to promote and ensure that:

- the VU complies with applicable laws and regulations regarding the protection of personal data;
- VU employees have a framework of standards for handling personal data within their jobs;
- employees and other data subjects are adequately informed about how the VU processes their personal data.

These Regulations outline the data processing of employees. More detailed information on data processing can be found on VU.nl. Here you can also find more information on the rules and guidelines that apply to employees, such as the Regulations on ICT facilities for employees.

Article 1. Terms

The terms in these Regulations have the meanings ascribed to them by the General Data Protection Regulation and related laws and regulations (hereinafter: the **Act**), unless expressly stated otherwise.

- a. **File:** any structured set of Personal Data accessible according to certain criteria, regardless of whether this set is centralised, decentralised or distributed on functional or geographical grounds.
- b. **Data Subject:** the person to whom a Personal Data relates. In the context of these Regulations, this includes at least: a (former) Staff Member, a person working at the VU without an employment contract with the VU (such as a temporary employee, seconded person, self-employed person, trainee or guest lecturer), a (pre)pensioner and a family member of a (former) Staff Member.
- c. **Authorised Officer:** the person authorised by the VU to have access to (certain) Personal Data. In addition to Employees, this may also include those working at the VU without employment with the VU, such as a temporary employee, seconded employee, self-employed person, trainee or guest lecturer.
- d. **Special Personal Data:** Personal data relating to racial or ethnic origin, political opinions, religious or philosophical beliefs, trade union membership, genetic data, biometric data for the purpose of uniquely identifying a person, health data and data relating to a person's sexual behaviour or sexual orientation.
- e. **Executive Board:** The Executive Board (CvB) of VU University Amsterdam.
- f. **Third Party:** a natural or legal person, a public authority, a department or another body, other than the Data Subject, the VU, a Processor or the persons authorised under the direct authority of the VU or a Processor to process the Personal Data.
- g. **Third country:** all countries outside the European Economic Area.
- h. **VU Data Protection Officer (DPO):** an internal officer as referred to in Article 37 et seq. of the General Data Protection Regulation. The DPO independently monitors compliance with laws and regulations relating to data protection and VU's policy on the protection of Personal Data.
- i. **ICT facilities:** all (digital) facilities that the VU uses and makes available as part of its information and communication processes. These facilities may be made available directly by the VU or via third parties with whom the VU has an agreement. They include: networks, internet, computers, programmes and applications, printers, copying and scanning equipment, information carriers, storage space, e-mail, (mobile) phones and other means of communication.
- j. **Employee:** the person who has an employment relationship with the Stichting VU.
- k. **Personal Data:** any information relating to an identified or identifiable natural, living person (the Data Subject). The term Personal Data is a broad concept that includes almost all data related to a natural person. It includes both objective and subjective data, regardless of whether the information is accurate. It concerns information about a person, such as name, date of birth and contact details. It also involves value judgements, such as an Employee's rating. Only in exceptional cases is information that concerns a natural person not Personal Data.

- l. **Processor** : a natural or legal person, a public authority, a service or another body which processes Personal Data on behalf of and under the responsibility of the VU. The VU instructs the Processor and determines the purpose and means for which the Personal Data are processed. The Processor may only process Personal Data on behalf of the VU. If the VU outsources any Processing to a Processor then additional legal rules apply, such as the obligation to draw up a Processor Agreement. A VU Employee falls under the VU hierarchy (internal management) and is not considered a Processor for the VU.
- m. **Processor Agreement**: the Controller and Processor are required by law to regulate a proposed Processing in an agreement or other legal act. A Processor Agreement is the usual instrument for this purpose. In a Processor Agreement it is agreed in any case that: the Processor provides adequate guarantees regarding the application of appropriate technical and organisational security measures, the Processor only processes the Personal Data on the basis of written instructions from the VU, and the Processor ensures that the persons authorised to process the Personal Data are obliged to maintain confidentiality. In addition, agreements are made about, among other things: the subject and duration of the Processing, the nature and purpose of the Processing, the type of Personal Data and the categories of data subjects and the rights and obligations of the Controller and Processor.
- n. **Controller**: a natural or legal person, public authority, agency or other body which, alone or jointly with others, determines the purpose and means of Processing Personal Data. In the context of these Regulations, this is the VU. VU has formal legal authority to determine the purpose and means of Processing. The various faculties and departments are themselves responsible for ensuring that their processes remain within the boundaries of the standards framework of these Regulations.
- o. **Processing**: any operation or set of operations involving Personal Data or a set of Personal Data, whether or not carried out by automated means, such as collection, recording, organisation, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, blocking, erasure or destruction of data.

Article 2. Scope of application

- 2.1 These Regulations apply to the Processing of Personal Data of Employees of the VU.
- 2.2 These Regulations also apply, where relevant, to the Processing of Personal Data of other Data Subjects, such as a former Employee, a person working under the authority and responsibility of the VU without employment (such as a temporary employee, seconded employee, self-employed person, trainee), a (pre)pensioner and a family member of a (former) Employee.
- 2.3 These Regulations do not apply to the processing of data of deceased persons. The VU processes such data carefully in compliance with applicable laws and regulations.
- 2.4 These Regulations apply to the fully or partially automated Processing of Personal Data (via a computer or electronic system such as the digital personnel file) and to the Processing of Personal Data included (manually) in a File or intended to be included therein.
- 2.5 These Regulations apply in full to the Processing of Personal Data by all organisational units of the VU, with the exception of the Health & Safety & Environment Department of the HRM/AMD service (hereinafter: **Health & Safety Service**). The Processing of Personal Data by the Health & Safety Service is subject to the 'Regulations for the Processing of Personal Data by the Health & Safety Service Vrije Universiteit Amsterdam' insofar as it concerns the assessment of incapacity for work, absenteeism counselling and reintegration of employees as well as in the context of consultations or individual advice provided by the Health & Safety Service to Employees. All other processing by the Occupational Health and Safety Service is subject to these Regulations.

Article 3. Purposes of Processing

- 3.1 The VU collects Personal Data only for specified, explicit and legitimate purposes ("purpose limitation") and processes Personal Data only for these purposes and the purposes compatible therewith. The purposes for which Personal Data are collected by the VU are determined prior to the Processing.
- 3.2 The VU collects and processes Personal Data for the following purposes:
- a. performing the work of Employees;
 - b. Record/implement the agreements made regarding terms and conditions of employment;
 - c. Determine and pay salary and other financial entitlements;
 - d. recording leave and absence;
 - e. identify, assess and promote performance and career development;
 - f. recruitment and selection of Employees and other Relevant Persons, including the assessment of candidates' suitability for a position (internal and external applicants);
 - g. (internal) disclosure, including information on ancillary activities;
 - h. policy-making;
 - i. Providing knowledge and training opportunities, as well as registering training courses;
 - j. Implementing legal regulations;
 - k. Maintaining, testing and securing VU ICT facilities;
 - l. security and access to buildings or other VU facilities;
 - m. identification.
- 3.3 If Processing for a purpose other than that for which the Personal Data were collected is not based on the Data Subject's consent, the VU shall take into account when assessing whether further Processing is compatible with the purposes for which the Personal Data were obtained:
- a. any relationship between the purposes for which the Personal Data were collected and the purposes of the intended further processing. The more the purposes are related, the sooner the Processing is compatible with the original purpose;
 - b. the context in which the Personal Data were collected. If the Personal Data was obtained from the Data Subject itself, compatible use is more likely than if the Personal Data was obtained outside the Data Subject;
 - c. the nature of the Personal Data, in particular whether Special Personal Data are processed. In general, if the Personal Data is more sensitive in nature, compatible use is less likely to occur;
 - d. the possible effects of the intended Processing on the Data Subject. Where further Processing has the effect of making a particular decision about the Data Subject, the Processing is more likely to be incompatible than if the Personal Data is used for research;
 - e. to what extent appropriate safeguards have been taken vis-à-vis the Data Subject, which may include encryption or pseudonymisation. Which measures are appropriate will be assessed on a case-by-case basis.
- 3.4 Further processing of Personal Data for historical, statistical or scientific purposes, shall not be considered incompatible, if the VU has made the necessary provisions to ensure that the further Processing is done solely for these specific purposes. Where possible, Personal Data shall be pseudonymised and encrypted.

Article 4. Personal data

- 4.1 The VU processes the following (categories of) Personal Data for the purposes stated above and only to the extent necessary:
- a. name, address, place of residence, telephone number and e-mail address of the Data Subject;
 - b. gender, date of birth, marital status, citizen service number (BSN) of the Data Subject;
 - c. data on degrees obtained;
 - d. employment history and acquired work experience of the Complainant;
 - e. function, department, type of employment of the Data Subject;
 - f. date in service, date out of service of the Data Subject;
 - g. data on primary and secondary conditions of employment of the Data Subject;
 - h. data on training, (career) development and performance of the Data Subject;
 - i. data regarding skills, expertise, preferences and interests of the Data Subject;
 - j. data on and arising from the Data Subject's activities;
 - k. data for the (internal) provision of information, including information on ancillary activities of the Complainant;
 - l. data on attendance and absence of the Data Subject at the VU;
 - m. data associated with or resulting from the use of ICT facilities, such as usernames, IP addresses, video and audio recordings and login attempts;
- (other) data about the Data Subject necessary for the implementation of legal requirements.

Article 5. Special Personal Data

- 5.1 Special Personal Data provide sensitive information about a person. Processing Special Personal Data can be a major invasion of the Data Subject's privacy. Therefore, stricter rules apply to the processing of Special Personal Data.
- 5.2 The processing of Special Personal Data within the VU is prohibited unless the Data Subject has previously given express, informed and specific consent to the Processing or the Law provides another exemption ground for such Processing.

- 5.3 The VU processes, to the extent necessary, the following Special Personal Data:
- a. Personal data on health. For example, the VU processes:
 - data on the presence and absence of Employees due to illness and pregnancy;
 - data for determining and implementing benefits that depend on the Employee's health status;
 - data for adapting the workplace to an Employee's health condition;
 - data on reintegration activities and absence management of an Employee.
 - b. Personal data on racial or ethnic origin. For example, the VU processes: - data on the country of origin of Employees for the purpose of its diversity policy.
 - c. Biometric data for the purpose of uniquely identifying an individual. For example, the VU processes:
 - photographs of Employees and other Data Subjects for access passes to VU buildings, rooms and facilities. Biometric data results from specific processing of physical, physiological or behavioural characteristics that allow unambiguous identification, such as a photograph of an Employee.
 - d. Personal data on union membership. The VU processes these, for example:
 - when an Employee applies for provisions from the Collective Labour Agreement, such as an allowance for union dues or the granting of union leave.
 - e. Personal data religion or belief. The VU processes these, for example:
 - in that a photograph for the access card may reveal an Employee's religion or belief.
 - f. Personal data on sexual orientation. For example, the VU processes:
 - data of Employees' partners, for example in connection with pension insurance or because an Employee requests special leave in connection with caring for his partner or marriage. Employees' sexual orientation can often be inferred indirectly from this data.
- 5.4 For the Processing of the citizen service number (BSN), the VU may only process it to the extent required by law. For example, the VU is legally obliged to process the BSN in the payroll administration and also pass it on to the Tax Office. If the use of BSN is not prescribed by law, the VU may not use BSN. Not even if the Data Subject were to give permission to do so.
- 5.5 The processing of Personal Data relating to criminal convictions and offences or related security measures shall only be processed to the extent specifically provided for in the Act.

Article 6. Basis for Processing

- 6.1 A Processing must always have a lawful basis. Without a basis, a Processing is not permitted. The bases on the basis of which VU processes Personal Data are:
- a. the Processing is necessary for the performance of the (employment) agreement with the Employee or necessary in response to a request from the Data Subject to take pre-contractual measures;
 - b. the Processing is necessary to serve the legitimate interest of the VU, or of a Third Party to whom the Personal Data are provided, unless the interest or fundamental rights and freedoms of the Data Subject, in particular the right to privacy, prevail. Here, the VU must always weigh up whether it or the Third Party to whom the Personal Data is provided actually has a legitimate interest. The Processing must be necessary to realise this interest. In addition, the VU must weigh up whether the interests of the Data Subject not to process the Personal Data outweigh and/or the Data Subject's right to privacy must prevail. In doing so, the VU must at least take into account the sensitivity of the Personal Data and, insofar as Processing takes place, ensure safeguards for careful use of the Personal Data;
 - c. the Processing is necessary to fulfil a legal obligation to which the VU is subject;
 - d. the Processing is necessary to prevent or combat a serious health threat to the Data Subject;
 - e. the Processing is necessary for the performance of a task carried out in the public interest or in the exercise of public authority vested in the VU; or
 - f. the Data Subject has previously given specific, unambiguous and informed consent to the Processing. The Data Subject must have freely expressed this will. That is, the Data Subject must not have consented under pressure of circumstances. If the Data Subject does not consent to the Processing, this must not have negative consequences for the Data Subject. Moreover, consent must always relate to (a) particular Processing(s). The Data Subject must have been informed prior to the Processing such that the Data Subject understands what consent is being given for.
- 6.2 The Data Subject may withdraw the consent referred to in Article 6.1 under f at any time without giving reasons. Such withdrawal shall not affect any Data Processing that took place before the time of withdrawal. If the basis for the Processing is consent and the Data Subject withdraws the consent, the Processing must be discontinued.

Article 7. Transparent information and communication

- 7.1 The VU takes appropriate measures to provide transparent, easily accessible and easily understandable information and communication regarding the Processing of Personal Data. Data subjects must be able to find out easily that their Personal Data are being processed and why, for example through privacy statements and FAQs.
- 7.2 Information shall be provided in writing, or by other means such as electronic means. If requested by the Data Subject, the VU may also communicate information orally, provided that the identity of the Data Subject is proved.

Article 8. Duty to inform

- 8.1 When the VU collects Personal Data from the Data Subject, the VU provides the following information to ensure proper and transparent Processing:
- a. its contact details and, where appropriate, those of a contact person ;
 - b. the contact details of the Data Protection Officer;
 - c. the processing purposes for which the Personal Data are intended and the legal basis for the Processing;
 - d. the legitimate interests of the VU or of a third party, where this is the legal basis for the Processing;
 - e. where applicable, the recipients or categories of recipients of the Personal Data;
 - f. where appropriate, that VU intends to transfer the Personal Data to a Third Country or an international organisation and what appropriate or suitable safeguards are in place (to the extent that there is no adequacy decision by the European Commission), how a copy of it can be obtained or where it can be accessed;
 - g. the period for which the Personal Data will be stored, or if that is not possible, the criteria for determining that period;
 - h. that the Data Subject has the right to request the VU to inspect and rectify or erase the Personal Data or restrict the Processing in question, as well as the right to object to the Processing and the right to data portability, as stated in Article 18 of these Regulations;
 - i. that the Data Subject has the right to withdraw consent at any time, where this is the legal basis for the Processing;
 - j. that the data subject has the right to lodge a complaint with the Personal Data Authority, as stated in Article 19.2 of these Regulations;
 - k. whether the provision of Personal Data is a legal or contractual obligation or a necessary condition to conclude an agreement, and whether the Data Subject is obliged to provide the Personal Data and what the possible consequences are if such Personal Data is not provided;
 - l. the existence of automated decision-making and, where relevant, useful information on the underlying logic, as well as the significance and expected consequences of the Processing for the Data Subject.
- 8.2 Where the VU does not obtain Personal Data from the Data Subject, the VU shall provide the following information in addition to the information set out in Article 8.1 of these Regulations:
- a. the categories of Personal Data concerned;
 - b. the source from which the personal data originate and, where appropriate, whether they come from public sources.
- 8.3 If the VU intends to further process the Personal Data for a purpose other than that for which the Personal Data were collected, the VU shall, prior to such further Processing, provide the Data Subject with information about that other purpose and all relevant further information as referred to in Article 8.1 and, where relevant, Article 8.2.
- 8.4 The obligation to inform as referred to in Article 8.1 does not apply if the Data Subject already has the information.

- 8.5 The obligation to provide information referred to in article 8.2 does not apply when:
- a. the Data Subject already has the information;
 - b. the provision of such information proves impossible or would require disproportionate effort, in particular in the case of Processing for archiving in the public interest, scientific or historical research or statistical purposes;
 - c. obtaining or providing the Personal Data is expressly required by Union or national law applicable to the VU and that law provides for appropriate measures to protect the legitimate interests of the Data Subject;
 - d. the Personal Data must remain confidential by virtue of professional secrecy.

Article 9. Access to Personal Data

- 9.1 The Personal Data processed by the VU is accessible on a 'need to know basis' to:
- a. Authorised officers who, because of their specific work, necessarily need access to Personal Data; and
 - b. Processors engaged by the VU;
- 9.2 Each Employee has access to their own digital personnel file.
- 9.3 A Processor Agreement shall be concluded with all Processors who process Personal Data on behalf of and under the responsibility of VU, which shall include adequate safeguards to guarantee the security and confidentiality of the Processing and to ensure that all other requirements under the Act are also met.

Article 10. Provision of Personal Data to Third Parties

- 10.1 The VU only provides Personal Data to Third Parties insofar as this fits within the purposes as stated in Article 3 and the Act provides a basis for this. For example, the VU may provide Personal Data to the pension fund, the Tax Authorities or the Employee Insurance Administration Agency (UWV).

Article 11. Quality of Personal Data

- 11.1 The VU will always endeavour to ensure that the Personal Data processed are correct and accurate. In addition, the VU will always process as little Personal Data as possible. This means in any case that the Processing must be discontinued or designed differently if the purpose of the Processing can also be achieved without or with less Personal Data.
- 11.2 Personal data of Employees will be processed in a digital personnel file. VU will endeavour to keep these files complete and up to date. Employees themselves shall ensure that, where possible, they make changes to their file in good time or notify the VU HRM department. The digital file is leading. No shadow files are kept in departments.

Article 12. Retention periods and deletion of Personal Data

- 12.1 Personal Data of Data Subjects shall not be kept longer than necessary for the purposes for which it was collected or is further processed.
- 12.2 The VU observes the statutory retention period for Processing. Insofar as there is no statutory retention period, the VU has formulated a retention period.
- 12.3 The VU has established records management for Personal Data with archival purpose.

Article 13. Confidentiality

- 13.1 All Authorised Officers are obliged to maintain confidentiality. They may only share, disclose or otherwise process Personal Data insofar as this is necessary for the performance of their work for the VU or insofar as any legal requirement obliges them to do so.

Article 14. Security

- 14.1 The VU processes various Personal Data. Some of these processing operations, such as the Processing of Special Personal Data or the processing of financial data, have a high degree of sensitivity.
- 14.2 The VU takes technical and organisational measures to protect Personal Data against destruction, loss, alteration, unauthorised disclosure of or unauthorised access to data transmitted, stored or otherwise processed, whether accidentally or unlawfully.
- 14.3 When determining the security measures, the VU shall take into account the state of the art, implementation costs, the nature, scope, context, processing purposes and the likelihood and severity of the risks. The VU will ensure that security is adequate at all times.
- 14.4 If there is unauthorised Processing, loss of Personal Data or any other form of unlawful Processing, whether or not due to a breach of security, action will be taken in accordance with the VU's 'Protocol Obligatory Data Breach Reporting'.

Article 15. Data protection by design and by default ('Privacy by Design' and 'Privacy by Default')

- 15.1 The VU shall ensure that the mechanisms used for Processing are designed to take into account, as far as possible, the protection of the Personal Data of Data Subjects and the requirements under the Act ('Privacy by Design').
- 15.2 The VU shall ensure that the default settings in a Processing are chosen in such a way that the protection of Personal Data of Data Subjects is maximally guaranteed ('Privacy by Default').

Article 16. Register of processing activities

- 16.1 All processing activities of the VU are kept in the Register of Processing Activities of the VU (hereinafter: **Register**). The Register is set up in accordance with Article 30 of the General Data Protection Regulation.

Article 17. International transfer

- 17.1 When processing Personal Data by the VU, Personal Data may be transferred to countries outside the European Economic Area (EEA) or international organisations.
- 17.2 Transfer to countries outside the EEA or international organisations only takes place when an adequate level of protection is guaranteed and the requirements of the GDPR, in particular Chapter 5, are met.

Article 18. Data protection officer (DPO) and internal responsibility Processing

- 18.1 The DPO of the VU is charged with supervising compliance with these Regulations. The VU's DPO is enabled by the VU to perform this supervisory task independently and properly. This means that the DPO cannot receive any instructions from (the Executive Board of) the VU with regard to the performance of this function and that the DPO is not disadvantaged in the performance of this function. The DPO of the VU has an advisory role towards the Executive Board.
- 18.2 All Authorised Officers are obliged to provide the DPO with all cooperation that the DPO may reasonably request in the exercise of these powers, unless a legal duty of confidentiality prevents this.
- 18.3 Faculties and departments are responsible for compliance with these Regulations with regard to the Processing of Personal Data within their departments.

Article 19. Rights of Data Subjects

- 19.1 The Data Subject has the following rights:
- a. Right of access and information. Data Subjects have the right to access their Personal Data. Data Subjects may also inquire about the purposes of processing, the categories of Personal Data, who are the recipients of the Personal Data and the period for which the Personal Data is expected to be stored or, if that is not possible, the criteria for determining that period. When Personal Data are not collected from the Data Subject, information on the available information on the source of the Personal Data may also be inquired. When Personal Data is transferred to a Third Country, the Data Subject has the right to be informed of the appropriate safeguards regarding the transfer. Inspection may be refused, for example if it is necessary in the interests of prevention, detection and prosecution of criminal offences or to protect the rights and freedoms of others.
 - b. Right to rectification. Data Subjects have the right to obtain from the VU without undue delay rectification of inaccurate Personal Data concerning them. Subject to the purposes of the Processing, Data Subjects also have the right to supplement their Personal Data, including by providing a supplementary statement. Only objectively inaccurate Personal Data are subject to correction. The Personal Data must therefore be manifestly incorrect. For example, a name that is misspelled. Data subjects can request supplementation if Personal Data is subjectively incorrect, i.e. if there is a difference of opinion whether the Personal Data is correct or incorrect. This could be, for example, an interview report or an assessment.
 - c. Right to data erasure. Data subjects have the right to have their Personal Data erased by the VU when:
 - the Personal Data are no longer necessary for the purposes for which they were collected;
 - the Processing is based on consent and the Data Subject withdraws his consent and there is no other legal basis for the processing;
 - when the Data Subject objects to the Processing of their Personal Data in accordance with Article 19.1(d) and such objection is upheld; or
 - Personal data are not processed lawfully.
 - d. Right of Objection. Under circumstances, Data Subjects have the right to object to the Processing of their Personal Data by the VU. If this objection is justified, the Processing will be terminated immediately.

e. Right to data portability. Data Subjects have the right to obtain and transfer Personal Data that they have provided to the VU and that are processed pursuant to consent or pursuant to the employment contract in a structured, common and machine-readable form to a Controller other than the VU. Employees may have access to data relating to their employment contract via the digital personnel file.

19.2 The rights referred to under a to e of Article 19.1 as well as any other right to which the Data Subject is entitled under the Act may be exercised by making this known to the DPO. The DPO will, on behalf of the VU, respond within 4 weeks. Data Subjects always have the option to discuss the matter (first) with their supervisor or another contact person.

Article 20. Complaints

20.1 The Data Subject may at any time submit a complaint to the CvB about the Processing of Personal Data, without prejudice to the rights described in Article 19. The Executive Board will deal with complaints as soon as possible and aim to respond substantively within 4 weeks. The VU DPO advises the CvB in assessing and handling the complaint.

20.2 The Data Subject may at any time lodge a complaint with the Personal Data Authority about the Processing of Personal Data.

20.3 The Data Subject may at any time apply to the competent court in relation to the manner in which Personal Data are processed by the VU.

Article 21. Final provisions

21.1 In cases not covered by these Regulations, the Executive Board decides.

21.2 These Regulations are published on the VU website and intranet.

These Regulations were adopted by the Executive Board, after approval of the Works Council on 13 June 2023 and came into force on 1 July 2023.
