Adopted with the consent of the
Participation Council on 13-3-2018
Executive Board decision no. 2017/1243

The HAN University of Applied Sciences Privacy Regulations

Preamble

The business processes of HAN University of Applied Sciences require the collection, processing and storage of personal data. Naturally, this should be done with the utmost care. HAN is responsible for complying with the General Data Protection Regulation (GDPR) and attaches great value to the protection of personal data that are disclosed to the organisation and the way in which personal data are processed. These regulations cover, among other things, which personal data are processed at HAN, to whom these personal data may potentially be disclosed, and the rights of the persons whose personal data are processed.

***I** General provisions*

Article 1 Terms and definitions

The following definitions will apply in these regulations, in line with and supplementary to the General Data Protection Regulation:[1]

- **a.** administrator: the person who is responsible on behalf of the controller for the day-to-day processing of personal data and the accuracy of the entered data, as well as for storing, deleting and disclosing data. The appendix contains an overview of the administrators. In cases where it is unclear who the administrator is, the director of the Services Department will act as the administrator;
- **b.** application manager: the person who ensures that the application works properly within HAN;
- **c.** controller / HAN: the Stichting Hogeschool van Arnhem en Nijmegen (foundation of HAN University of Applied Sciences), represented in this matter by the Executive Board.
- **d.** data subject: the person to whom the personal data relate;
- **e.** disclosure of personal data: publishing personal data or otherwise making data available;
- **f.** file: any structured set of personal data, whether this set of data is centralised or dispersed on a functional or geographical basis, that is accessible in accordance with certain criteria;
- **g.** GDPR: General Data Protection Regulation;
- **h.** infringement of personal data: an infringement of data protection that accidentally or in an unlawful manner leads to the destruction, modification or unlawful disclosure of or unlawful access to forwarded, stored or otherwise processed data;
- **i.** officer: the personal data protection officer who monitors the implementation of and compliance with the GDPR at HAN;
- **j.** personal data: all data relating to an identified or identifiable natural person. By identifiable is meant a natural person who can be identified, directly or indirectly, particularly on the basis of an identifier such as a name, an identification number, location data, an online identifier or from one or more elements that are characteristic of the physical, physiological, genetic, psychological, economic, cultural or social identity of this natural person;
- **k.** processing personal data: any operation or set of operations performed upon personal data, including in any event the collection, recording, organisation, storage, adaptation, alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, as well as blocking, erasure or destruction of data;
- **l.** processor: the person who processes data for the controller;

[1] Regulation (EU) 2016/679 of the European Parliament and 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.

m. profiling: any form of automatised processing of personal data whereby on the basis of personal data, certain personal aspects of a natural person are evaluated, particularly with the intention of analysing or predicting his or her professional performance, economic situation, health, personal preferences, interests, reliability, behaviour, location or movements.
n. special categories of personal data: personal data as referred to in Article 9 of the GDPR, such as race or ethnic origin, religious or ideological convictions (photos, etc.) or data about health, such as disability, chronic illness;
o. staff: persons employed by or working for the controller;
p. technical work activities: work activities relating to the maintenance, repair and protection of hardware and software;
q. the Authority: The Data Protection Authority, the supervisory authority as defined in article 51, paragraph 1 of the GDPR;
r. user: the person entitled, on behalf of the administrator, to enter, modify and/or delete personal data, or to seek information about the data being processed;

II Purpose and Scope

Article 2 Purpose of the regulations

The purpose of these regulations is:
a) to allow personal data to be processed in accordance with the GDPR;
b) to protect the personal privacy of the data subject whose personal data are processed in one or more files against the misuse of these data and against the processing of erroneous data;
c) to inform the data subject about what HAN will do with their personal data; and
d) to guarantee the rights of the data subjects.

Article 3 Scope of the regulations

These regulations apply to the processing of the personal data of data subjects within HAN, including, in any case, all staff, students and external contacts (temporary employees/outsourcing), as well as to other data subjects whose personal data are processed by HAN.

These regulations apply to personal data that are processed wholly or partly by automatic means; it also applies to personal data that are processed otherwise than by automatic means if these data are included or intended to be included in a filing system.

III Data management

Article 4 Mandate from controller

The director of the Services Department assumes responsibility on behalf of the controller for the processing of personal data.

Article 5 Documentation of data processing

HAN maintains a register of all processing of personal data. This register of processing activities contains the following data:
a) the name and contact details of the controller;
b) the purpose of the processing activity;
c) a description of the categories of data subjects and categories of personal data;
d) the categories of receivers to whom the personal data were or are being disclosed;
e) if applicable, the transmission of personal data to a third country or organisation;
f) the intended periods within which the different categories of data must be erased;
g) a general description of technical and organisational security measures.

The whole or partial automatised processing of personal data must be reported to the data protection officer. How this should be reported is indicated on the HAN Intranet. The officer performs random checks on the

legality of the registration and is responsible for ensuring adequate documentation.

IV Data collection and processing

Article 6 Purpose limitation and data minimisation

Personal data must be gathered in a transparent manner for well-defined, specifically described and legal purposes, and may not subsequently be processed in a manner that is incompatible with these purposes. In addition, personal data must be adequate, relevant and limited to what is required for the purposes for which they are processed ('minimal data processing').

Article 7 Lawful processing

The processing of personal data is based on one of the legal bases defined in article 6 of the GDPR. In accordance with article 6 of the GDPR, the processing of the personal data of data subjects can be required to:

a) implement an agreement to which the data subject is party;
b) comply with a legal obligation resting upon the controller;
c) protect the vital interests of the data subject;
d) fulfil a task that is in the public interest or a task that forms part of the exercise of the public authority invested in the controller;
e) serve the legitimate interests of the controller or a third party, except when these interests are outweighed by the interests or fundamental rights and fundamental freedoms of the data subject that require the protection of personal data, especially when the data subject is a child.

The processing of personal data can also be based on consent given by the data subject themselves. The controller must then be able to show that the data subject has consented to the processing of their personal data. If the data subject is a minor, in some cases it is also compulsory to obtain the consent of the parent/legal guardian. In further regulations, it will be specified in which cases this is and is not required.

In specific - yet to be determined - cases, HAN can ask a subject to consent to the processing of their personal data, by means of a permission form (for example).

Article 8 Procedure for applying for disclosure of data

An application for the disclosure of data submitted to a HAN staff member or organisational unit must in any event be submitted to the ICT service unit if:

a) an external party is involved in any way in the application for the disclosure of data;
b) the request for personal data does not form part of the regular task/job of the HAN staff member or of the regular work performed by the organisational unit;
c) the application for data is not in keeping with the purposes as defined in the register of processing activities (article 5 of these regulations); or
d) there is doubt as to whether the GDPR will be infringed.

V Data protection, duty to report data leaks and confidentiality

Article 9 Data protection and duty to report data leaks

1. The controller must provide the necessary technical and organisational measures for protection against the loss or any form of unlawful processing of personal data.
2. The measures are partly aimed at preventing the unnecessary collection and further processing of personal data.
3. Every infringement in relation to personal data as defined in Article 1, paragraph j of these regulations will be documented. The Authority will be informed of the infringement without unreasonable delay, and if possible within 72 hours of becoming aware of the incident, unless there is no likelihood that the infringement involves a risk to the rights and freedoms of natural persons. If the Authority is not informed within 72 hours, the report should be accompanied by reasons for the delay. If it is likely that the infringement entails a high risk to the rights and freedoms of natural persons, then the data subject(s) involved should also be informed of the infringement without delay.

4. The notification of the Authority and the data subjects should cover, in every case:
   a) the nature of the infringement;
   b) the contact details of the officer or another contact point where more information about the infringement can be obtained;
   c) the likely consequences of the infringement; and
   d) the recommended measures for dealing with the infringement of personal data, including, as the occasion arises, measures to limit the potential negative consequences of the infringement.
5. The notification of the data subject, as defined in paragraph 3, is not required if:
   a) the data affected by the infringement are incomprehensible to unauthorised persons, for example due to encryption;
   b) subsequent measures have been taken to the effect that the high risk defined in paragraph 3 has been obviated;
   c) the notification requires disproportionate efforts. In that case, a public notification should instead be made or a similar measure taken, whereby data subjects are informed in a manner that is equally effective.
6. The person who discovers an infringement of personal data as defined in paragraph 3 should report the infringement to the Service Desk within one working day. The Service Desk should immediately report the infringement to the officer, who should inform the controller and make the notifications defined in paragraph 3.
7. The officer maintains a register of every infringement of personal data. This register should contain, in every case, the facts and data relating to the nature of the infringement, as defined in paragraph 3, as well as the text of the announcement to the data subject, as applicable.

Article 10 Confidentiality

1. Employees are obliged to uphold the confidentially of the knowledge that they acquire on account of their job, insofar as this obligation follows from the nature of the case, or is imposed expressly in writing. This obligation also applies after the termination of the employment contract.
2. Without prejudice to legal provisions, the employer is obliged to uphold the confidentiality of the personal data of the employee, unless the employee has given written consent for the disclosure of data relating to his or her person.

VI Processor(s) (agreement)

Article 11 Processor

1. If the controller has assigned the processing of a certain set of data to a processor, an agreement must be drawn up by the controller and the processer that must be observed by the processor with regard to protecting the personal data in question. Among other things, this agreement should describe the subject and the duration of the processing, the nature and the purpose of the processing, the type of personal data and the categories of data subjects, and the rights and obligations of the controller. In addition, the controller should ensure that (in this agreement) the processor offers sufficient guarantees with regard to technical and organisational security measures relating to the processing to be undertaken and with regard to notification in the case of an infringement of personal data.
2. The contract owner should include a copy of this agreement in Proquro. A format for this processor agreement is available on the HAN Intranet.

VII Notification

Article 12 Information provided to data subjects

1. When obtaining data from the data subject, the controller should provide the data subject with the following information:
   a) their identity and contact details;
   b) the contact details of the officer;
   c)the purposes of the data processing and its legal basis;
   d) the legitimate interests (if the processing is based on article 9, paragraph 1, section f of the

GDPR);

e) the receivers or categories of receivers of the personal data;
f) guarantees in the case of the transfer of personal data to a third country or international organisation;
g) retention periods;
h) the rights of the data subject (including the existence of the right to request that the controller inspect personal data and to demand the amendment or erasing of personal data, as well as the right to object and the right to data transferability);
i) whether disclosure by the data subject is obligatory;
j) the right to submit a complaint to the Authority;
k)information about profiling.

The above is not applicable if and insofar as the data subject already possesses this information.

2. The information contained in paragraph 1 will be provided by way of a general announcement on the HAN website addressed to data subjects, mainly containing information about the existence of the data processing and of these regulations, the manner in which data may be inspected, and about the manner in which data subjects can obtain more information.
3. If the personal data are obtained by means other than those defined in paragraph 1 (i.e., if the personal data are not obtained from the data subject themselves, but from a third party), the announcement described in paragraph 2 will be made:
   a) within a reasonable period of time, but no later than within one month of obtaining the personal data; or
   b) on the first communication with the data subject; or
   c) no later than the time of the first disclosure to a third party.

   The announcement will be made by way of a general announcement on the HAN website.
4. The announcement described in paragraph 3 will not be made if it is not possible to notify the data subject or if this requires disproportionate efforts, the data subject already has the information, it is a legal obligation, or if the personal data must be kept confidential for reasons of professional confidentiality. In this case, the controller will record the origins of the data.
5. The data subject will not be notified if the data processing is prescribed by a statutory provision.

Article 13 Opt-in/Opt-out[2]

Prior permission must be requested (opt-in) for the unsolicited sending of email messages for commercial, non-profit or charitable purposes. In addition, the receiver must always have the option of being able to deregister (opt-out). It is not necessary to request prior permission if the email message does not have any commercial, non-profit or charitable purposes, the data subject has provided their email address for these purposes, or in the case that the email address is obtained in the context of the sale of a product or service and the email address is used for one's own similar products or services. The email message should nevertheless contain an opt-out option.

VIII Data storage

Article 14 Data retention and periods

Personal data must be stored in a form that makes it possible to identify the data subjects for no longer than for the purposes for which the personal data are being processed. Personal data may be retained for longer periods purely with a view to archiving data in the public interest, scientific or historical research or statistical purposes, or on the grounds of a statutory provision, provided that appropriate technical and organisational measures are taken to protect the rights and freedoms of the data subject. Retention periods have been adopted for the retention of personal data. Retention periods can be determined in law, but can also be adopted by HAN. See the HAN-Bestandsoverzicht.[3]

IX Right of information, inspection, copies, correction, deletion, transfer and objection

Article 15 General

---

[2]In accordance with article 11.7 of the Telecommunications Act
[3]This overview is available from the HAN Service Desk.

1. In relation to their personal data, the data subject will have the right to submit a request to the administrator to:
   a. obtain information;
   b. inspect and correct (amend, add to, delete and/or protect) and transfer data.
2. No costs will be involved for the data subject in exercising these rights.
3. The data subject may be assisted in exercising those rights, at their own expense.
4. The administrator advises the data subject about the possibilities of legal protection and monitoring and the Authority's role in this.

Article 16 Right to object

1. If the lawful basis for a particular data processing activity:
   a. is required for properly fulfilling a duty under public law; or
   b. is required for the legitimate interest of the controller, the data subject may lodge an objection with the administrator at any time against the processing of their data based on special personal circumstances.
2. The data subject shall have the right not to be subjected to a decision based exclusively on automated processing, including profiling, which has legal consequences for them or which otherwise affects them to a considerable degree. The data subject may lodge an objection to this with the administrator. This does not apply if the decision is required for the conclusion or execution of an agreement between the data subject and controller, or if this is permitted under the law that provides for appropriate measures.
3. The controller will assess whether the objection is justified within four weeks of receipt of the objection.
4. If the data are processed in connection with the creation or maintenance of a direct relationship between the controller or a third party and the data subject with a view to soliciting for commercial or charitable purposes (direct marketing), the data subject may lodge an objection with the controller at any time against the processing of data.
5. When the data subject objects to data processing for the purposes of direct marketing, the personal data will no longer be processed for these purposes.
6. An objection lodged against processing for commercial or charitable purposes is justified at all times.
7. The administrator must terminate the data processing immediately if the controller considers the objection to be justified.

X Legal protection and monitoring

Article 17 Complaints procedure

1. The data subject is entitled to submit a complaint to the officer:
   a. against a decision on a request, as defined in Article 15;
   b. against a decision on an objection lodged by the data subject, as referred to in Article 16;
   c. against the manner in which the controller, administrator or processor implements the rules contained in these regulations.

   Every data subject has the right to lodge a complaint with the Authority.
2. The officer must respond to the complainant in writing and with reasons stated as soon as possible, but within six weeks of receipt at the latest.
3. Data subjects may be assisted in the submission and handling of their complaints.
4. The officer may obtain advice from the Authority.
5. The officer may arrive at the opinion that the complaint is unjustified or fully or partially justified.
6. If the officer decides not to allow the complaint or to allow it only partially, the data subject may submit a complaint to the Authority. The controller informs the data subject whose complaint he or she has decided not or only partially to allow about the option of lodging a complaint with the Authority and of the Authority's address.
7. If the officer is of the opinion that the complaint is wholly or partially justified, they will decide to:
   a. fully or partially honour the data subject's request, if the complaint is directed against a decision as defined in paragraph 1 under a;
   b. honour the data subject's objection, if the complaint is directed against a decision as defined in paragraph 1 under b;
   c. still implement the rules contained in these privacy regulations, if the complaint is directed against the

manner of implementation as defined in paragraph 1 under c.

8. The officer must inform the data subject of their decision in writing.

XI Data protection officer

Article 20 Data protection officer

1. The data protection officer is appointed by the controller.
2. The data protection officer may not receive instructions from the controller regarding the performance of their duties.
3. The data protection officer will have the same powers as the supervisor referred to in Title 5.2 of the Dutch General Administrative Law Act (*Algemene wet bestuursrecht*).
4. All HAN employees must provide the information and cooperate with what is required of them pursuant to the previous paragraph.
5. The officer is obliged to:
   a. produce an annual report on their work duties and findings as part of HAN's annual report;
   b. pursue a comprehensive policy in relation to privacy.
6. The data protection officer is responsible for:
   a. monitoring compliance with privacy legislation;
   b. monitoring their internal policy, including awareness-raising and training;
   c. providing information and advice on privacy issues;
   d. collaborating with the Authority;
   e. acting as a contact point for the Authority;
   f. handling complaints from data subjects;
   g. handling requests from data subjects if the wishes of the requester are not fully met;
   h. making notifications to the Authority and data subject(s), as described in article 9, paragraph 3, and informing the controller about this;
   i. keeping a register, as described in article 9, paragraph 7 of these privacy regulations.
7. The data protection officer only has access to personal data in that capacity and only uses the personal data that they obtain in their capacity as data protection officer if these data concern the performance of their duties as an officer.
8. The officer can make recommendations to the controller for the purpose of better protection of the data that are processed.
9. The controller must ensure that the officer is provided with the full cooperation that they require to perform their job.
10. The officer is bound to confidentiality.

Article 19 Monitoring compliance

The Authority is authorised under the GDPR to monitor compliance with the provisions contained in these privacy regulations pursuant to the GDPR.

XII Other provisions

Article 20 Training

The controller must provide regular training for the administrators and users to ensure that they understand the processes involved in processing data, the applicable rules and their own role within this.

Article 21 Unforeseen

Circumstances that are not provided for in these privacy regulations will be decided upon by the controller, after taking advice from the officer.

Article 22 Publication and inspection

These privacy regulations will be placed on the HAN Intranet and on www.han.nl.

Article 23 Changes and additions

1. Changes to the purpose of data processing and to the type of content, use and manner of obtaining personal data may lead to revisions of these privacy regulations.
2. Changes and additions to the privacy regulations require the consent of the Participation Council.

Article 24 Entry into effect and official title

1. These privacy regulations will come into effect on 13 March 2018.
2. These privacy regulations may be referenced as 'The HAN University of Applied Sciences Privacy Regulations.'