HAN_UNIVERSITY OF APPLIED SCIENCES

PRIVACY REGULATIONS

of HAN University of Applied Sciences

Subject	*Privacy Regulations*
Executive Board decision no.	*2020/1691*
Participation Council consent	*10-7-2020*
Adopted on	*10-7-2020*

Preamble

The business processes of HAN require the collection, processing and storage of personal data. Naturally, this must be done with the utmost care. HAN is responsible for compliance with the General Data Protection Regulation (GDPR) and attaches great value to the protection of the personal data disclosed to its organisation and to the way in which personal data is processed. These regulations cover various matters such as which personal data are processed at HAN, who these personal data may be disclosed to, and the rights of the people whose personal data are processed.

I General provisions

Article 1 Terms and definitions

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

a. the Authority: The Data Protection Authority, the supervisory authority as defined in article 51 paragraph 1 of the GDPR;

b. application manager: the person who ensures the application works properly at HAN;
c. GDPR: General Data Protection Regulation;
d. administrator: the person who is responsible on behalf of the controller for the day-to-day processing of personal data, for 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 acts as the administrator;
e. filing system: any structured set of personal data, whether centralised, decentralised or dispersed on a functional or geographical basis, which is accessible according to specific criteria;
f. data subject: the person to whom the personal data relate;
g. special categories of personal data: personal data as referred to in article 9 of the GDPR, which reveal racial or ethnic origin, religious or philosophical beliefs (photos, etc.) or data about health, such as disability or chronic illness;
h. officer: the personal data protection officer who monitors the application of and compliance with the GDPR at HAN;
i. user: the person authorised on behalf of the administrator, to enter, change and/or delete personal data, or to seek information about the data being processed;
j. personal data breach: a breach of security leading to the accidental or unlawful destruction, alteration, unauthorised disclosure of, or unauthorised access to personal data transmitted, stored or otherwise processed;
k. employee: persons employed by or working for the controller;
l. personal data: all data relating to an identified or identifiable natural person. An identifiable natural person is a person who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, psychological, economic, cultural or social identity of that natural person;

[1]Regulation (EU) 2016/679 of the European Parliament and the Council of 27 April 2016 that covers the protection of natural persons in relation to the processing of personal data and the free movement of those data.

m. profiling: any form of automated processing of personal data which uses personal data to evaluate certain personal aspects of a natural person, in particular with a view to analysing or predicting aspects concerning that natural person's work performance, economic situation, health, personal preferences, interests, reliability, behaviour, location or movements;
n. technical work: work relating to the maintenance, repair and protection of hardware and software;
o. disclosure of personal data: the disclosure of personal data or otherwise making data available;
p. processor: the person who processes data for the controller;
q. processing of personal data: any operation or set of operations related to personal data, including in any case collection, recording, organisation, storage, adaptation, alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, as well as restriction, erasure or destruction;
r. controller / HAN: HAN, represented in this matter by the Executive Board.

II Purpose and scope

Article 2 Objectives

The objectives of these regulations:

a) allow personal data to be processed in accordance with the GDPR;
b) protect the privacy of the data subject whose personal data are processed in one or more filing systems, against misuse of those data and against processing of incorrect data;
c) inform the data subject about what HAN does with their personal data;
d) guarantee the rights of the data subjects.

Article 3 Applicability

These regulations apply to the processing of the personal data of data subjects at HAN, including in any case all employees, students and external contacts (temporary employees/outsourcing), as well as other data subjects whose personal data are processed by HAN. These regulations apply to the fully or partially automated processing of personal data; as well as to the processing of personal data (non-automated) that are stored or intended to be stored in a filing system.

III Data management

Article 4 Mandate

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

Article 5 Documentation of processing

HAN maintains a register of all its 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 of categories of personal data;
d) the categories of recipients to whom the personal data have been or will be disclosed;
e) if applicable, the transfer of personal data to a third-party country or organisation;
f) the intended periods within which the different categories of data must be deleted;
g) a general description of technical and organisational security measures.

Any fully or partially automated processing of personal data must be reported to the data protection officer. How this should be reported is specified on the HAN Intranet. The officer performs random checks on the legal validity 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 collected in a transparent manner for specified, explicit and legitimate purposes,

and may not be further processed in a manner that is incompatible with those purposes. In addition, personal data must be adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed ('minimal data processing').

Article 7 Lawfulness of processing

The processing of personal data is based on one of the legal principles as described in article 6 of the GDPR. In accordance with article 6 of the GDPR, the processing of personal data of data subjects may be necessary for:

a) performance of a contract to which the data subject is party;
b) compliance with a legal obligation to which the controller is subject;
c) protection of the vital interests of the data subject;
d) performance of a task carried out in the public interest or in exercising public authority assigned to the controller;
e) protection of the legitimate interests of the controller or a third party, except when the interests or fundamental rights and freedoms of the data subject which require protection of personal data, in particular where the data subject is a child, weigh more heavily.

The processing of personal data may also be based on consent given by the data subject themselves. The controller must then be able to demonstrate that the data subject has consented to the processing of their personal data. If the data subject is a minor, it is also compulsory in some cases to obtain the consent of the parent/legal guardian. In specific – yet to be determined – cases, HAN can ask a data subject to consent to the processing of their personal data by means of (for example) a signed consent form.

Article 8 Procedure for requesting data

Requests submitted to a HAN employee or organisational unit of HAN for the provision of data must always be submitted to the ICT Service Unit if:

– an external party is in any way involved in the request for provision of data;
– the request for personal data does not belong to the regular task/job of the HAN employee or does not belong to the regular activities performed by the organisational unit;
– the request for data is not in keeping with the purposes as defined in the register of processing activities (article 5 of these regulations); or
– there is any doubt about whether the request is an infringement under the GDPR.

V Security, duty to report data leaks and confidentiality

Article 9 Security and duty to report data leaks

1. The controller must ensure that appropriate technical and organisational measures are taken to protect 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. Any breach relating to personal data as described in article 1 paragraph j of these regulations must be documented by the officer in the manner described in paragraph 7. The Authority must be notified of the breach without undue delay, and where possible within 72 hours of becoming aware of the incident, unless the breach is not likely to result in a risk to the rights and freedoms of natural persons. If the Authority is not informed within 72 hours, the report should include the reasons for the delay. If the data breach is likely to result in a high risk to the rights and freedoms of natural persons, the data subject(s) concerned must also be notified of the breach without delay.
4. The notification of the Authority and the data subjects should cover, at least:
   a) the nature of the data breach;
   b) contact details of the officer or another point of contact where more information can be obtained about the data breach;
   c) the likely consequences of the data breach;
   d) the recommended measures to address the personal data breach, including, where appropriate, measures to mitigate the possible negative consequences of the data breach.
5. Notification of the data subject, as defined in paragraph 3, is not required if:
   a) the data affected by the breach are incomprehensible to any unauthorised persons, for example due to encryption;
   b) subsequent measures have been taken to ensure the high risk defined in paragraph 3 will not

recur; or

c) the notification would require disproportionate effort. In such a case, a public notification should be made instead or a similar measure taken to ensure the data subjects are informed in an equally effective manner.

6. Anyone who discovers a personal data breach as defined in paragraph 3 should report the breach to the Service Desk as soon as possible, but in any case within one working day. The Service Desk will immediately report the data breach to the officer, who will inform the controller and make the notifications as defined in paragraph 3.
7. The officer maintains a record of every personal data breach. This record should at least contain the facts and information relating to the nature of the breach, as defined in paragraph 3, and where applicable also the notification text used to inform the data subject.

Article 10 Confidentiality

1. Employees are obliged to uphold the confidentiality of the knowledge they acquire on account of their job, insofar as this obligation follows from the nature of the case or is expressly imposed in writing. This obligation also applies after termination of the employment contract.
2. Without prejudice to legal provisions, HAN is obliged to uphold the confidentiality of the personal data of the employee with respect to third parties, unless the employee gives written consent to disclose data relating to his or her person.

VI Processor (agreement)

Article 11 Processor

1. If the controller has assigned a particular set of data processing operations to a processor, an agreement must be drawn up by the controller and the processer covering the processor's obligations regarding the protection of the personal data concerned. Among other matters, 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 this agreement offers the processor sufficient safeguards with regard to technical and organisational security measures for the processing activities and for reporting personal data breaches.
2. The contract owner must 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 to data subjects

1. When obtaining data from a data subject, at the same time the controller provides the data subject with the following information:
   a) the identity and the contact details of the controller;
   b) the contact details of the officer;
   c) the purposes and the legal basis for the data processing;
   d) the legitimate interests (if the processing is based on article 9, paragraph 1, section f of the GDPR);
   e) the recipients or categories of recipients of the personal data;
   f) safeguards in the case of the transfer of personal data to a third-party country or international organisation;
   g) retention periods;
   h) the rights of the data subject (including the existence of the right to request from the controller access to, rectification of or erasure of personal data, as well as the right to object to data processing and the right to data portability);
   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 does not apply if and insofar as the data subject already has this information.

2. The information as described in paragraph 1 will be posted as a general notification on the HAN website addressed to the data subjects concerned. It will contain in particular information about the

existence of the data processing operations and this set of privacy regulations, where these regulations can be accessed, and how further information can be obtained.

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 data subject will be notified as described in paragraph 2:
   a) within a reasonable period, but at least within one month of obtaining the personal data;
   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 notification will be posted as a general announcement on the HAN website.

4. The data subject will not be notified as described in paragraph 3 if that is not possible or if this would require disproportionate effort, if the data subject already has the information, if it is required by law and that law has its own regulations for protecting the interests of the data subjects concerned, or if the personal data must remain confidential for reasons of professional confidentiality. In these cases, the controller will record the origins of the data.
5. The data subject will not be notified if the data processing is prescribed by law.

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

Prior consent must be requested (opt-in) for sending unsolicited email messages for commercial, non-profit or charitable purposes. In addition, the recipient must always have the option to opt out. Prior consent is not required if the email message has no commercial, non-profit or charitable purposes, the data subject has provided their email address for those purposes, or the email address was obtained in connection with the sale of a product or service and is used to market similar products or services from the same organisation. 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 is necessary for the purposes for which the personal data are processed. Personal data may be retained for longer periods purely with a view to archiving in the public interest, scientific or historical research or statistical purposes, or on the basis of a legal provision, provided that appropriate technical and organisational measures are taken to protect the rights and freedoms of the data subject. Retention periods have been set for the retention of personal data. Retention periods can be determined by law, but can also be set by HAN. See the HAN-Bestandsoverzicht.[3]

IX Right to information, access, copies, rectification, deletion, transfer and objection

Article 15 General

1. In relation to their personal data, every data subject has the right to submit a request to the administrator to:
   a. obtain information; or
   b. access, correct (rectify, add, delete and/or restrict) and transfer data.
2. No costs are 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 to the administrator at any time against the processing of their data based on special personal circumstances.

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

2. The data subject has the right not to be subject to a decision based solely on automated processing, including profiling, which would have legal consequences for him or her or significantly affect him or her in any other way. In that case the data subject may lodge an objection with the administrator. This does not apply if the decision is required for the realisation 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 receiving the objection.
4. If the data are processed in connection with the establishment 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 at any time lodge an objection with the controller against the processing of this data.
5. If the data subject objects to data processing for direct marketing purposes, personal data will no longer be processed for these purposes.
6. Objections lodged against processing for commercial or charitable purposes are always justified.
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 referred to 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 seek advice from the Authority.
5. The officer may conclude 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 considers the complaint fully or partly justified, they will decide to:
   a. fully or partly allow the data subject's request, if the complaint is directed against a decision as defined in paragraph 1 under a;
   b. allow the data subject's objection, if the complaint is directed against a decision as defined in paragraph 1 under b;
   c. implement the rules in these privacy regulations if the complaint is directed against the manner of implementation as defined in paragraph 1 under c.
8. The officer will inform the data subject of their decision in writing.

XI Data protection officer

Article 18 Data protection officer

1. The data protection officer is appointed by the controller.
2. The officer may not receive instructions from the controller regarding the performance of their duties.
3. The officer has 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 cooperation required of them pursuant to the previous paragraph.
5. The officer is obliged to:
   a. report annually on their work activities 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. cooperating with the Authority;
   e. acting as a point of contact 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. notifying the Authority and data subject(s), as described in article 9 paragraph 3, and informing the director of the Services Department about this;
   i. keeping an overview, as described in article 9 paragraph 7 of these privacy regulations.
7. The data protection officer only has access to personal data in their capacity as data protection officer and only uses the personal data they obtain in their capacity as data protection officer for performing their duties as an officer.
8. The officer can make recommendations to the controller with a view to improving the protection of the data that is processed.
9. The controller must ensure that the officer is provided with the full cooperation they require to perform their duties.
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 regulations pursuant to the GDPR.

XII Objection procedure concerning the use of portraits by HAN on the Internet

Article 20 General Provisions

1. A portrait means any visible representation in which a person is recognisably depicted (photo, painting, drawing, film or video images).
2. The articles mentioned in these regulations only concern portraits not requested by the student.
3. HAN may use a portrait depicting a student in an educational setting on the Internet if HAN is regarded as the creator of the material in accordance with the Copyright Act and the portrait is used in the interest of education for the purpose of informing, educating, or exchanging information with other educational institutions. HAN may do this without the student's prior consent, unless the student has a reasonable interest that opposes publication on the Internet.
4. HAN excludes any liability for damages resulting from the use of portraits on the Internet by HAN, unless the portrait was not immediately removed by HAN after proven reasonable interest by the student.

Article 21 Objection procedure

1. If the student has a reasonable interest based on the provisions of article 1 paragraph 3 of these regulations, the student may report this in writing to the Marketing, Communication and Public Relations director.
2. A student may also object in advance to the use of their portrait on the Internet. This objection must also be submitted to the Marketing, Communication and Public Relations director.
3. The objection should be signed by the submitter and contain:
a. the name, address and telephone number of the submitter;
b. the date: the date on which the objection is submitted;
c. a clear description of the portrait in question and the date on which the portrait was made;
d. motivation of the student's reasonable interest against publication of the portrait.
4. If an objection does not or does not entirely meet the requirements, the Marketing, Communication and Public Relations director will inform the submitter and give them the opportunity to rectify this omission within a term to be set by the director.

Article 22 Decision, term, content

1. The Marketing, Communication and Public Relations director will decide within ten working days after receipt of the objection. The decision must be based on sound reasons, which must be provided when

the decision is given.
2. The Marketing, Communication and Public Relations director may decide that the objection is inadmissible, wrongful or wholly or partly justified.
3. In the event of a (partly) justified objection, the portrait in question will not be used by HAN on the Internet and portraits already posted on the Internet will be removed by HAN without delay.

Article 23 Unforeseen circumstances

In cases not provided for by these regulations, the objection will be submitted to the Executive Board of HAN. The Executive Board will decide on the objection based on the documents submitted.

XII Other provisions

Article 24 Training

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

Article 25 Unforeseen

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

Article 26 Publication and access

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

Article 27 Changes and additions

1. Changes in the purpose of the processing and in the type of content, use and manner in which personal data is obtained may lead to changes to these regulations.
2. Changes and additions to these regulations require the consent of the Participation Council.

Article 28 Entry into effect and official title

1. These regulations enter into effect on 13 March 2018.
2. These regulations can be cited as ‘HAN Privacy Regulations’ (or ‘Privacyregeling HAN’ in Dutch)