Privacy Policy Plan
NHL Stenden

Emmen, November 2019
Version number: 1.1

Colophon

Model for a Processing Personal Data policy

SURF
PO Box 19035
NL-3501 DA Utrecht
T +31 88 787 30 00

info@surf.nl
www.surf.nl

This version is based on the Joint product of the SURF Project Group 'Preparation for Implementation of the General Data Protection Regulation' and SURFibo (now SCIPR). The following persons worked on the original version: Frans Pingen (Wageningen University), Bart van den Heuvel (Maastricht University), Sedat Capkin (SURFsara), Ronja Meijer (Wageningen University), Jaap Gall (Arnhem Nijmegen University of Applied Sciences) and Chloë Baartmans (SURFnet).
This version has been edited, adapted and supplemented for NHL Stenden University of Applied Sciences by Willem Bakker, Data Protection Officer.

Version 2.0 March 2018

SURF is the ICT cooperation organisation of Dutch higher education and research.
This publication is available digitally via the SURF website: www.surf.nl/publicaties

NHL STENDEN hogeschool

Table of contents

1. Introduction

In a data-driven society in which technology provides almost unlimited possibilities to collect, store, analyse and distribute data, the protection of personal data is of the utmost importance. Privacy is a fundamental right[1] that now more than ever deserves protection in our society. This is the background of the General Data Protection Regulation which has been applied all across Europe since 25 May 2018.

Personal data protection is a top priority for a knowledge institution such as NHL Stenden. A university of applied sciences is indeed a real 'data factory'. Knowledge, information and personal data are our operating capital.

Apart from the large material and immaterial risks[2] associated with careless processing of personal data, NHL Stenden places a very high priority on the protection of the personal data of students, staff and other data subjects. The correct processing of personal data by the university of applied sciences, also according to law, is ultimately the responsibility of the Executive Board.

With the measures as described in this policy document, NHL Stenden University of Applied Sciences gives substance to this responsibility. This policy is aimed at the quality of the processing and optimizing the protection of personal data. With this policy and its correct implementation, NHL Stenden complies with the privacy legislation.

1.1. Definitions

GDPR: General Data Protection Regulation[3].

Policy: this policy with regard to the processing of personal data by NHL Stenden.

Data subject: an individual and natural person to whom personal data is related. NHL Stenden distinguishes the following categories of data subjects: permanent employees, temporary employees, students, course participants, leads, alumni, external relations, guests of the Stenden Hotel and research subjects.

Controller: the Executive Board of NHL Stenden that determines the purpose and resources for processing personal data.

Personal data: all information about an identified or identifiable natural person.

Processor: a (third) party engaged by NHL Stenden to process personal data on behalf of NHL Stenden and on the basis of written instructions.

Processing: any operation or set of operations with regard to personal data, including collecting, recording, organising, storing, consulting, updating, restriction, deleting or destroying data.

Third party: everyone else - not being the data subject, the controller or the processor, or any person who falls under the direct authority of the controller or the processor, who is authorised to process personal data.

[1] See Article 9 of the Constitution and Article 12 of the Universal Declaration on Human Rights.
[2] As is appropriate to the nature of the offence the maximum penalties are 10 or 20 million euros or, if this is greater, respectively 2 or 4% of the annual turnover. However, it is expected that reputational damage due to a scandal of any magnitude for an Institute for Higher Education, for which the financing is dependent on the student intake, is possibly even worse.
[3] The General Data Protection Regulation entered into force on 25 May 2016 and came into effect on 25 May 2018.

Data breach: a breach of security of personal data, which leads to any improper processing thereof. This includes both intentional as well as unintentional data breaches.

Privacy by Default: data processing for which the standard settings of products and services are set up so that the privacy of data subjects is as far as possible guaranteed. This means, among other things, that as little data as possible is requested and processed.

Privacy by Design: The management of the complete lifecycle of personal data, from the collection through to the processing and deletion, for which mechanisms are designed so that as far as possible they observe the privacy of data subjects. Systematic attention is given to all-embracing guarantees with regard to accuracy, confidentiality, integrity, physical security and deletion of the personal data.

Data Protection Impact Assessment: An assessment which helps to identify privacy risks and provides the tools to reduce these risks to an acceptable level.

Profiling: every form of automated processing of personal data for which, on the basis of personal data, specific personal aspects about a natural person are evaluated, in particular with the intention of analysing or predicting their professional performance, economic situation, health, personal preferences, interests, reliability, behaviour, location or movements.

Minors: every person who is younger than 16 years of age.

1.2. Scope and purpose of the Policy

The policy concerns the processing of personal data of all data subjects within NHL Stenden, which at least includes all employees (including hired and outsourced staff), students, guests, visitors and external relations, as well as other data subjects of whom NHL Stenden processes personal data.

This policy puts the emphasis on the fully or partially automated/systematic processing of personal data that takes place under the responsibility of NHL Stenden as well as on the underlying documents that are contained in a file. The policy is also applicable to the non-automated processing of personal data that is included in a file or that is intended to be included therein.

NHL Stenden adopts a broad interpretation of the protection of personal data. There is an important relationship and partial overlap with the related policy area of information security, which concerns the availability, integrity and the confidentiality of data, including personal data. On a strategic level attention is given to these overlapping areas and both planned as well as substantive coordination is sought.
NHL Stenden's policy aims to optimize the quality of processing and the protection of personal data ensuring a good balance between privacy, functionality and security.

The intention is to respect as far as possible the personal privacy of the data subject. The data which is related to a data subject needs to be protected against unlawful and unauthorised use, or misuse on the basis of the fundamental right to protection of their personal data. This entails that the processing of personal data must comply with relevant legislation and that the personal data is secure at NHL Stenden.

This Policy has the following objectives:

- Provision of a framework: the Policy provides a framework to monitor the (future) processing of personal data against a specified ‘best practice’ or standard; and to organise the tasks, powers and responsibilities within the organisation.
- Setting standards: the basis for the protection of personal data is ISO 27001[2]. Measures are taken on the basis of ‘best practices’ in higher education and on the basis of ISO 27002[3]. The data registers (see § 6.5) provide the standard for the question of which personal data may be processed by whom.

- The SURF Framework of Legal Standards (Cloud) Services[4] is adhered to as best practice for cloud services and other outsourcing contracts.
- Taking responsibility: the Executive Board herewith establishes the basic principles and the organisation of the processing of personal data for the entire organisation/ NHL Stenden University of Applied Sciences.
- Decisive implementation of the policy by making clear choices in measures and applying active monitoring on the execution of the policy measures.
- Compliance with Dutch and European legislation.

Along with the above specific objectives this policy paper also wishes to contribute to awareness with regard to privacy. Compliance with the law will only succeed if everybody in the organisation is aware of the necessity of careful processing and a good protection of personal data.

[2]In full: NEN-ISO/IEC 27001: Requirements for Management systems for information security
[3]In full: NEN-ISO/IEC 27002: Code of practice for information security controls
[4]SURF Framework of Legal Standards (Cloud) Services, determined by the board of Platform for ICT & Business Operations 3 April 2014 and updated in 2016, which can be found at https://www.surf.nl/kennisbank/2013/surf-juridisch-normenkader-cloudservices.html.

2. Policy principles for Processing personal data

2.1. Policy principles

The general policy principle is that personal data is processed in a fair and careful manner in accordance with the relevant legislation. In this regard, it is required to find the right balance between the interests of NHL Stenden to process personal data and the interests of the data subject, who has a right that their personal privacy is respected and who must, as far as possible, have control of their own personal data.

The following principles apply to satisfy the above policy principle:

- Processing of personal data is based on one of the legal grounds as stated in article 6 of the GDPR (“legitimacy”).
- Personal data is only processed in a manner which is fair and transparent with regard to the Data Subject. This means that the extent to which and in which way personal data is processed should be clear for the data subjects. Information about this must be easily accessible and understandable (“fair and transparent”).
- Personal data is only processed for well-defined, explicitly described and justified purposes. It concerns specific and justified purposes, which are specified and described prior to commencement of the processing. Personal data is not further processed in a manner which is incompatible with the purposes for which it is obtained (“purpose limitation”).
- During the processing of personal data, the amount and the type of data remains restricted to the personal data that is necessary for the specific purpose. With a view to that purpose, the data must be adequate, relevant and not excessive (“data minimisation”).
- Processing of personal data takes place in the least intrusive manner and should be proportional to the intended purpose (“data minimisation”).
- Measures will be taken to guarantee as far as possible that the personal data to be processed is accurate and up to date (“accuracy”).
- Personal data is adequately secured according to current security standards (“integrity and confidentiality”).
- Personal data is not stored for longer than is necessary for the purposes of the processing. The applicable retention and deletion periods are observed for this purpose (“storage limitation”).

3. Legislation

NHL Stenden has the following approach to deal with the relevant legislation.

3.1. Higher Education and Scientific Research Act

NHL Stenden has a quality assurance system that guarantees (among other things) the careful processing of data in the student administration and the study results. In addition, behaviour and integrity codes for (non-)scientific staff are observed and applied.

3.2. General Data Protection Regulation

With this Policy, NHL Stenden has implemented the necessary mechanisms to comply with the legal requirements. This includes the lawful and careful processing of personal data and the implementation of suitable technical and organisational measures against loss and the unlawful processing of data or personal data.

3.3. Public Records Act

NHL Stenden adheres to the provisions of the Public Records Act and the Public Records Decree on how to process information recorded in (digitized) documents, information systems, websites, etc. This is part of the annual external audit.

4. Roles and responsibilities with regard to Processing personal data

To handle the processing of personal data in a structured and coordinated fashion, NHL Stenden applies the following division of roles.

4.1. Executive Board

The Executive Board is the controller and therefore has the final responsibility for the lawful and careful processing of personal data within NHL Stenden. The EB determines the policy, the measures and the procedures.

4.2. Portfolio holder for protection of personal data

The portfolio holder for protection of personal data is the board member that has privacy in their portfolio. He is ultimately responsible for the protection of personal data within NHL Stenden.

4.3. Data Protection Officer

In accordance with Article 37 of the GDPR, NHL Stenden has appointed a 'Data Protection Officer' (hereafter: DPO). The DPO is registered with the Data Protection Authority. NHL Stenden will engage the DPO in a timely manner in all matters involving personal data. The DPO provides information and advice with regard to compliance with the privacy legislation and ensures this compliance[4]. The DPO has an independent position within the university of applied sciences.

The DPO has the following tasks. He:

- informs and advises all the involved parties about their obligations under the GDPR;
- ensures compliance with the GDPR and other relevant privacy legislation;
- ensures compliance with this privacy policy by NHL Stenden;
- ensures the execution of Data Protection Impact Assessments (DPIAs);
- cooperates with the Data Protection Authority and is the first point of contact within the organisation.

4.4. System owner

Every application has a system owner who is responsible for ensuring that the system does what it should do and that this takes place within the frameworks of this Policy. The system owner ensures that the application, both now and in the future, continues to fulfil on the one hand the requirements and wishes of the users and on the other hand the legislation.

4.5. Director

The director is responsible for compliance with this policy within his Academy, Service or Liaison Unit. He supports and facilitates the Data Protection Counsellor (see § 4.6). The director has the task to:

- ensure that his employees are aware of the Policy;
- ensure compliance with the Policy by his employees;
- periodically discuss the topic of privacy during work meetings.

[4] Article 39 of the GDPR explicitly mentions both roles: Providing information and advice on the one hand and ensuring compliance on the other.

4.6. Data Protection Counsellor

The Data Protection Council at NHL Stenden is a consultative and advisory body with regard to policies on privacy (protection of personal data) and security (information security). The DPC is composed of representatives from all Academies, Liaison Units and departments. The members of the Information Security Steering Group are officially part of the DPC. The members of the DPC are called Data Protection Counsellors.
The executive committee of the DPC is composed of the Data Protection Officer and the Security Officer, both of whom form a part of the Executive Staff. The meetings are led by the DPO.

Profile of the Data Protection Counsellor

The Data Protection Counsellor

- has knowledge of the priority areas privacy and security[5];
- is part of the management team of the Academy, department or unit which he/she represents (hereafter referred to as 'department') or has the position to exercise direct influence on the execution of the policy in this area;
- is a permanent employee of NHL Stenden;
- supports the execution of this policy within the department, particularly but not exclusively where it concerns compliance with the data registers, entering into the Controller-Processer Agreements, organising Data Protection Impact Assessments, contributing to the awareness of privacy and security within the department, executing specific work instructions within the department and facilitating the rights of those involved;
- is the first point of contact within the department in matters concerning privacy and security;
- identifies points of attention in matters concerning privacy and security within the department: in this respect, the Data Protection Counsellor has an obligation to report to the DPO;
- within the DPC, indicates what the bottlenecks, requirements and suggestions are from the department in matters concerning privacy and security;
- does his/her utmost to attend all meetings of the DPC; in exceptional circumstances he/she may send a replacement.

An annual joint training session is part of the activities of the Data Protection Council.

4.7. Privacy Officer

De Privacy Officer supports the Academies, departements and units in the execution of this privacy policy. He does so as a member of the Star team.

4.8. Employees and students

Employees and students are not the only ones for whom personal data is processed and who as such have certain rights, but as an employee and as a student they also have their obligations where it concerns the processing of personal data within the framework of their work or study. Both employees and students must comply with this Policy. In all cases, they need to process personal data with care and are obliged to immediately report possible data breaches or vulnerabilities via the data breaches hotline or to the Data Protection Officer.

If required, there are protocols and work instructions available for employees within their Academy, Liaison Unit or department. Students are informed by NHL Stenden of their rights and obligations, among other things via the Students' Charter.

[5] An annual joint training session is part of the activities of the Data Protection Council.

A sanction can be imposed by the EB on employees, due to their culpable behaviour in relation to the processing of the personal data of colleagues, students or other data subjects.

The sanctions that can be imposed on students due to culpable behaviour in relation to the processing of personal data of other students, staff or data subjects at NHL Stenden, are described in the Students' Charter.

Paragraph 1.1 describes which other data subjects NHL Stenden distinguishes.

5. Implementation Policy

The NHL Stenden Executive Board is responsible for processing personal data for which the Executive Board determines the purpose and the resources. The EB is therefore the **Controller** in terms of the GDPR. The actual processing of personal data is, however, performed at all levels at NHL Stenden.
A good governance structure ensures that the university of applied sciences makes compliance with the privacy legislation possible and that those involved know that their personal data is processed carefully and within the frameworks of the law. This structure also makes it possible that those involved can exercise their rights (see § 8).

5.1. Distribution of responsibilities

- The careful processing of personal data needs to be regarded as **a line responsibility**. This means that directors of Academies, Services and Liaison Units bear the primary responsibility for the careful processing of personal data within their department. They do this within the frameworks agreed to within this Policy. The line responsibility also has the task of communicating the policy with regard to the processing of personal data to all relevant parties.

- The careful processing of personal data is **everyone's responsibility**. It is expected from employees and students that they behave with integrity. It is not acceptable that due to behaviour, even if not intentional, unsafe situations arise that could result in damage and/or have a negative impact on NHL Stenden's reputation or on that of individuals. It is for this reason that codes of conduct are formulated and implemented. Taking this responsibility is also the task of the result-responsible teams.

5.2. Incorporation in the institutional governance/ Coordination with related policy areas

To clearly demonstrate the coherence within the organisation with regard to data protection and coordinate the initiatives and activities with regard to the processing of personal data within the various departments, it is important to have structured discussions on the topic of privacy at different levels.

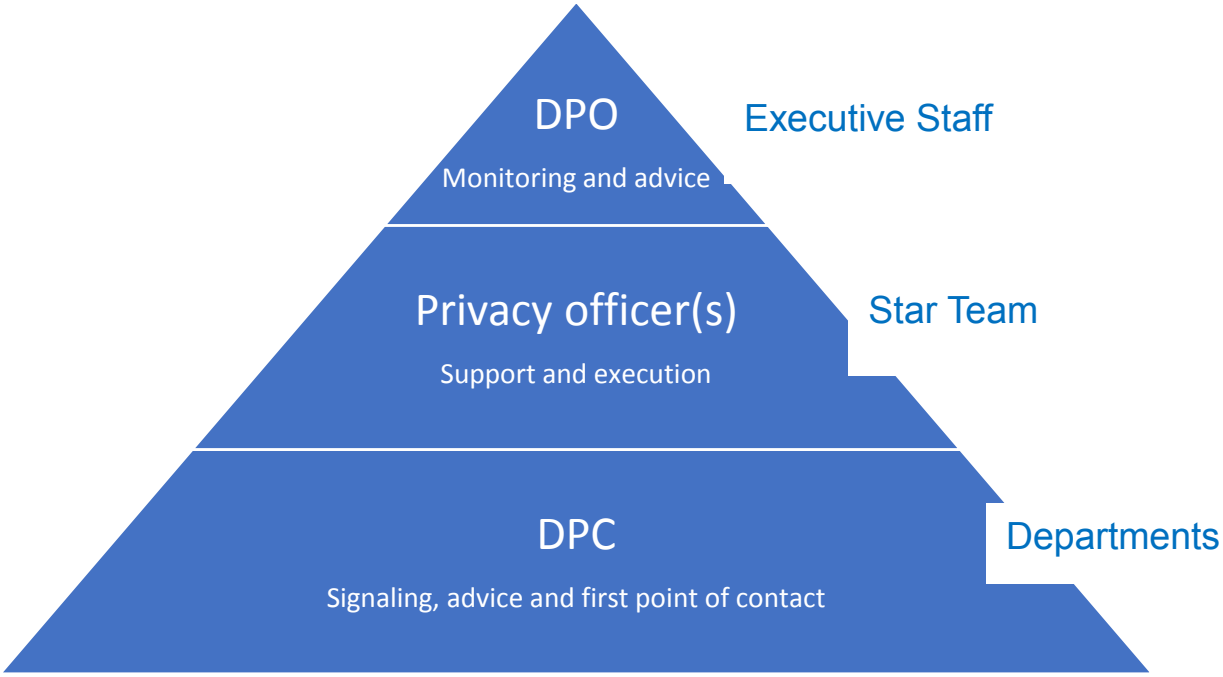
At a **strategic level** this involves providing guidance with regard to governance and compliance, and also with regard to the objectives, scope and ambition concerning privacy. The Executive Board and the university consultation provide substance at the strategic level.

At the **tactical level** the strategy is translated into plans, the standards to be applied, and methods of evaluation. These plans and instruments are a guideline for the execution. The Data Protection Council (see § 4.6) and the management teams of the Academies, Services and Liaison Units provide substance at the tactical level.

Matters which concern the daily business operations (execution) are discussed at the **operational level**. The Information Security Steering Group (coordination between the execution of privacy and information security) and all result-responsible teams provide substance at the operational level.

The Executive Staff advises at the strategic level, oversees the tactical level (by means of audits) and provides information upon request at the operational level.

Focused on activities which have to been performed in the domain of privacy, three levels can be distinguished.



5.3. Awareness and training

Policy and measures are not sufficient to eliminate all risks with regard to processing personal data. It is necessary to continuously raise awareness at NHL Stenden in order to increase the knowledge of risks and to encourage safe and responsible behaviour. A part of the policy are the regularly held awareness campaigns for employees, students and guests. These campaigns are in line with national campaigns in higher education, if possible, in coordination with other data protection campaigns. Increasing awareness is a joint responsibility of the Data Protection Officer and the Security Officer.

5.4. Monitoring and compliance

Audits make it possible to monitor the policy and the measures taken for effectiveness. From the Executive Staff, the DPO and the Security Officer initiate monitoring the lawful and careful processing of personal data.

Any external checks are carried out by independent accountants. This is linked to the annual audit and as far as possible is integrated into the normal Planning & Control cycle. Peer reviews within the framework of the SURFaudit form part of the external audits of NHL Stenden.

If compliance with the regulations on protection of data and privacy details falls seriously short, NHL Stenden may impose a sanction on the responsible employees, within the frameworks of the Collective Labour Agreement and the legal possibilities.

The processing of personal data is a continuous process. Technological and organisational developments inside and outside NHL Stenden make it necessary to periodically check whether the Policy is still sufficiently on the right track.

6. Lawful and precise processing of personal data

NHL Stenden processes personal data in accordance with the principles as explained in paragraph 2.1 of this Policy. To implement these principles, NHL Stenden takes the measures as mentioned in this chapter.

6.1. Lawfulness

NHL Stenden only processes personal data if there are legal grounds as described in article 6 of the GDPR:

a. *Consent of the Data Subject.*
b. *Necessary for the performance of a contract with the Data Subject.*
c. *Necessary for compliance with a legal obligation to which the controller is subject*
d. Necessary to protect the vital interests of the Data Subject or another natural person.
e. Necessary for the performance of a task carried out in the public interest or within the framework of exercising public authority.
f. Necessary for the protection of the legitimate interests pursued by the controller or by a third party.

In practice it usually concerns one of the principles written in italics, for which it should be pointed out that 'consent' in interdependencies (such as that between an employer and an employee, or between a university of applied sciences and a student;) is generally not a valid principle[6]. The principles for the various processing operations are stated in the data registers (see § 6.5).

6.2. Privacy statement

NHL Stenden processes personal data in a way that is fair and transparent with regard to the Data Subject. This means that NHL Stenden provides the Data Subject with insight into the extent and manner in which their personal data is processed. When collecting personal data, NHL Stenden will inform the Data Subject by means of a privacy statement. Information will take place prior to the processing, unless in all reasonableness this is not possible. The data registers for the various categories include a privacy statement which is concentrated on that category. The NHL Stenden websites contain an overarching privacy statement. See also paragraph 8.1 of this Policy.

6.3. Retention periods

Personal data will not be kept longer than necessary for the purposes for which it was collected or for which it is used, in accordance with the detailed retention policy of NHL Stenden. NHL Stenden will destroy the personal data after the expiration of the retention period or store it in an archive if the personal data is intended for historical, statistical or scientific purposes. The retention periods are stated in the data registers.

6.4. Suitable data protection measures:

NHL Stenden is responsible for an adequate level of data protection and implements appropriate technical and organisational measures to protect personal data against loss or against any form of unlawful processing. These measures are partly focused on avoiding unnecessary or unlawful collection and processing of personal data. NHL Stenden has implemented an internal data protection policy outlining the measures that NHL Stenden employees must adhere to.

[6] Permission must be given completely freely, you need to know exactly what you are giving permission for and the permission needs to be explicit.

A risk assessment on the protection of privacy and information security forms part of the internal risk management and monitoring system of NHL Stenden.

6.5. Obligation of documentation

NHL Stenden has taken various measures to demonstrably comply with the legal requirements of the GDPR, including the implementation of this Policy.

In accordance with Article 30 of the GDPR, NHL Stenden maintains a 'record of processing activities'. NHL Stenden gives substance to this with integral, well-organised 'data registers' for the various categories of data subjects (Cuijpers method). There are data registers for:

- students
- course participants
- permanent employees
- temporary employees
- leads
- alumni
- external relations
- hotel guests (of the Stenden University Hotel).

An amended form of the obligation of documentation has been designed for the last category 'research subjects' (persons who are interviewed within the framework of research, varying from the bachelor thesis to the research of a Professor of Applied Sciences). The DPO is involved in drawing up the data registers and they monitor compliance to them. For every 'data register' there is one director who has mandated responsibility (see appendix 10.1 for an overview).

NHL Stenden also structurally performs Data Protection Impact Assessments (DIPAs), at least in the case of (larger research) projects, infrastructural changes within the information architecture or the purchase of new systems that are likely to pose a high risk to the rights and freedoms of natural persons. If it appears from these assessments that the processing would entail a high risk if NHL Stenden does not take measures to limit the risk, NHL Stenden will consult the supervisory authority prior to processing.

The DPIAs referred to above are, where applicable, repeated after three years.

A 'quick DPIA' is also carried out as standard procedure prior to the introduction of new apps within, for example, an Academy.

The DPO and the Security Officer give advice on the question of whether a DPIA is mandatory, recommended or is not required.

6.6. Privacy by Design and Privacy by Default

NHL Stenden applies the principles of "Privacy by Design" and "Privacy by Default" for the implementation of each Processing activity.

Due to the considerable material risks, the risk analysis on protection of privacy and information security is the subject of the audit and an annual discussion during the meeting of the Supervisory Board.

6.7. Confidentiality

NHL Stenden classifies all personal data as confidential. Everyone should be aware of the confidentiality of personal data and act accordingly.

Persons who are not bound by a confidentiality obligation by virtue of office, profession or statutory regulations, are also obliged to maintain the confidentiality of the personal data of which they are aware, except to the extent that any statutory regulation obliges them to disclosure or the necessity for disclosure arises from their duties.

6.8. Special Personal Data

The processing of special personal data is in principle prohibited, unless one of the legal exceptions of the GDPR applies, such as 'explicit consent from the Data Subject' or 'substantial public interest'. Moreover, these special types of personal data are subject to stricter security requirements. In cases where basic protection is not sufficient, additional, individually tailored measures must be taken for each information system.

Special personal data includes the following data:

- data relating to race or ethnic origin;
- data revealing political opinions;
- religious or philosophical beliefs;
- data revealing a membership of a trade union;
- genetic data with the purpose of the unique identification of a person;
- biometric data with the purpose of the unique identification of a person;
- data concerning health;
- data concerning a person's sex life or sexual orientation.

For two types of personal data it applies that they do not fall under the category of special personal data, but that the Processing and protection thereof is however subject to comparable similar strict requirements:

a) Processing of personal data relating to criminal convictions and criminal offences is only permitted under the supervision of the government or requires a lawful basis under European or national legislation.

b) Under Dutch law, the processing of a national citizen service number (Dutch BSN or the individual education number) requires a lawful basis.

6.9. Transfer of personal data

6.9.1. Outsourcing of Processing to a Processor

If NHL Stenden engages a *Processor* to process personal data, the execution of the Processing shall be governed by a Controller-Processor Agreement, between NHL Stenden, the Controller, and the Processor in question.

6.9.2. Transfer of personal data within the European Economic Area (hereinafter 'EEA')

NHL Stenden only provides personal data to a Processor domiciled within the EEA, if the processing is based on one of the principles for data processing of Articles 6 or 9 of the GDPR and if the Processor meets the legal requirements of the GDPR.

6.9.3. Transfer of personal data outside the EEA

NHL Stenden only provides personal data to Processors established in a country outside the EEA, if one of the following conditions is met:

1. The third country, territory, specific sector in a third country or the international organisation in question offers an adequate level of protection according to the European Commission.

   NHL Stenden applies the following appropriate level of protection:
   - The general list of countries with an adequate level of protection, published by the European Commission[7];

- The Privacy Shield for companies in the United States, published by the European Commission in cooperation with the US Department of Commerce[8].

2. Transfer takes place subject to **appropriate safeguards** referred to in Articles 46 and 47 of the GDPR. Transfer of personal data to the International Branch Campuses of NHL Stenden takes place based on Standard European Contractual Clauses ('Model Clauses'). These model clauses have been signed by all four IBCs.

3. Transfer takes place subject to one of the **legal exceptions** of Article 49 of the GDPR. Pursuant to Article 30, paragraph 2a of the (Dutch) General Data Protection Regulation Implementation Act of 16 May 2018, NHL Stenden only transfers medical data, such as information on allergies or medication, of students who are going on a Grand Tour ™, this with regard to their own safety, with their knowledge and only if necessary.

6.10. Questions and complaints procedure

6.10.1. Notification and registration

Questions or complaints regarding (the processing of) personal data can be reported to the Data Protection Officer. A record will be kept of questions or complaints with a (potential) significant impact.

All data subjects, all processors of NHL Stenden and all third parties may submit a complaint or a question.

6.10.2. Security vulnerabilities

Employees are obliged to report any potential data breaches immediately to the Data Breach hotline for personal data (https://datalekken.nhlstenden.com). This may, for instance, concern the loss or theft of data carriers or mobile devices, weaknesses observed in systems or services, suspicions of security breaches or indications that personal data is in the wrong place. A record is kept of all notifications regarding security vulnerabilities.

6.10.3. Processing

Questions, complaints and security vulnerabilities are transferred to the responsible department or person and consequently dealt with as quickly as possible in accordance with the relevant procedures. If the personal data of Data Subject(s) or the business processes, the finances or the reputation of NHL Stenden are seriously threatened, at a minimum the Executive Board and the DPO will be informed.

6.10.4. Evaluation

It is important to learn from the feedback obtained through the question and complaints procedure. Registration of significant questions, complaints and vulnerabilities and a periodic report thereof are part of a professional manner of processing personal data. The relevant reports are therefore an integral part of the annual report of the Executive Board and the DPO.

---

[6] Retention periods may be imposed by law as is the case with financial data or formal study results, but they may also be established by NHL Stenden, for instance in an agreement between NHL Stenden and the Data Subject.
[7] You can find these via the following link http://ec.europa.eu/justice/data-protection/international-transfers/adequacy/index_en.htm.
[8] You can find these via the following link https://www.privacyshield.gov/list.

7. Data Breaches

This chapter describes the policy with regard to the notification, registration and processing of a Data Breach or a suspected Data Breach in normal business operations and in special circumstances.

7.1. Data breach

A Data Breach is a breach of security of personal data leading to any unauthorised Processing thereof. This may concern the theft of a laptop, a USB stick left on a train or an email sent to the wrong person. Data Breaches must be reported to the Data Protection Authority within 72 hours after discovery and in some cases also to the Data Subject, i.e. the person whose personal data has been leaked.

7.2. Notification and registration

A Data Breach may occur within the organisation of NHL Stenden, but also at a Processor, engaged by NHL Stenden. In this regard, the following situations should be distinguished:

a. *Employee*: employees, if they detect a (potential) Data Breach or if they suspect to be involved in a Data Breach, must notify the data breaches hotline via https://datalekken.nhlstenden.com or, in exceptional cases to a confidential advisor or the Data Protection Officer of NHL Stenden.
b. *Processor:* it is also possible that a Data Breach occurs at the Processor engaged by NHL Stenden. The Processor will report the Data Breach to NHL Stenden as agreed in the Controller-Processor Agreement.
c. *Other persons:* if anyone other than an employee or a Processor detects a (potential) Data Breach or is involved in a Data Breach, they must immediately notify the data breaches hotline via https://datalekken.nhlstenden.com or the Data Protection Officer.

7.3. Processing

A suspicion of a data breach must be reported immediately using the appropriate online reporting form. This reporting form will state, among other things:

- The person reporting the incident;
- How the incident manifested itself;
- Whether personal data is involved and if so, what kind of data and how many people it concerns.

After such a report, a team of specialists (the 'triage team') will be immediately notified by email that there is a potential data breach. The triage team processes the notification as quickly as possible and based on the Instructions of the Data Protection Authority, they determine whether or not it concerns a data breach (or a simple security incident) and whether the data breach must be reported to the Data Protection Authority (as this is not required in all cases) and finally they determine whether the data subject(s) must also be notified of the data breach. These considerations are recorded in the online registration system. Any notification to the Data Protection Authority and the data subjects is made by the Executive Board, assisted by the Data Protection Officer. In accordance with the law, notification must be made within 72 hours of discovery. Data subjects are notified by the Academy, department or Liaison Unit where the data breach occurred with the assistance of Corporate Communication and the DPO.

The triage team consists of two representatives of the Digital Learning and Working Environment (Operational Security Officer and Information Architect) and two representatives of the Executive Staff (Security Officer and DPO). In this way, the DPO has knowledge of all the (potential) data breaches. If necessary, the triage team may seek assistance from a colleague from the Legal Affairs Department.

The EB is informed about all data breaches identified as such, including the data breaches that have not been reported to the Data Protection Authority.

7.4. Decision making

The triage team *advises* on whether or not a data breach must be reported to the Data Protection Authority and possibly also to the data subject. The *decision* as to whether or not to make a notification is taken by the EB. The notification itself is officially made by the EB. If, contrary to the advice of the triage team, the EB decides not to report the data breach, the DPO will include this decision with the underlying considerations in his annual report.

7.5. Evaluation

It is important to learn from Data Breaches in order to reduce the likelihood of Data Breaches in the future. The registration of Data Breaches and a periodic report thereof are part of the professional manner in which personal data is processed. The reports on Data Breaches with regard to personal data are therefore an integral part of the annual reports of the Executive Board and of the DPO.

[10] Policy Rules on Data Breach Notification Obligation of the Data Protection Authority: https://autoriteitpersoonsgegevens.nl/sites/default/files/atoms/files/richtsnoeren_meldplicht_datalekken_0.pdf.
[11] Comparable to the CSIRT team: Computer Security Incident Response Team.

8. Rights of Data Subjects

Under the GDPR, Data Subjects have certain rights with which they can exercise control over the Processing of their personal data. A request can be submitted to the appropriate desk <link>.

The following points apply to all rights of Data Subjects as described in this chapter:

- **Notification to Data Subject**

NHL Stenden will ensure that information and communication are provided to the Data Subject in a concise and accessible manner and in clear and simple language. The language will be attuned to the target group. NHL Stenden has set up a data register for each target group (category of data subjects) in which is recorded which personal data is processed for which reason, purpose and on which legal grounds. Each data register contains a privacy statement geared towards the category in question.

- **Period**

A Data Subject request must be replied to in writing as soon as possible and at least within four weeks from receipt of the request. The Data Subject must in any event be informed of the actions taken in response to the request. If the period of four weeks is not reasonably feasible, the Data Subject must be notified accordingly within this period. In this case, NHL Stenden will comply with the Data Subject Request within two months after expiry of the first period.

- **Identity of the Data Subject**

When providing the relevant information, NHL Stenden must ensure that the identity of the Data Subject is properly verified. For this purpose, NHL Stenden may request additional information.

- **Minors**

A request to exercise one of the rights as described in this chapter by a Data Subject, being a Minor, placed under guardianship or legal custody, must be submitted by their legal representative. A response by NHL Stenden will be sent to the legal representative in question.

8.1. Right to be informed

The Data Subject has the right to be provided by NHL Stenden with information about certain aspects of the Processing of their personal data. NHL Stenden shall inform the Data Subject free of charge of the Processing of their personal data, both in the case of personal data that has been collected directly from the Data Subject and in the case where the data has been obtained by other means.

A. Personal data collected directly from the Data Subject.

If the personal data is collected directly from the Data Subject, NHL Stenden provides the Data Subject with at least the following information prior to the collection of the data:

- The identity and contact details of the Controller and where appropriate of the DPO.
- The specific purpose of the Processing for which the personal data is intended as well as the legal grounds for the processing.
- The legitimate interests of the Controller or Third Party if legal grounds for the Processing is a 'legitimate interest'.
- Where appropriate, the intention of the Controller to transfer personal data to a third country, which country it concerns and on which grounds the personal data is to be transferred.
- The retention period of personal data, or if this is not possible, the criteria used to determine the retention period.
- The existence of the right to request the Controller to inspect, rectify or delete personal data, limit the processing of personal data related to the data subject, as well as the right to object to the Processing and the right to data portability.
- The right to complain to the supervisory authority.
- The recipients or categories of recipients of the personal data.

- If the Processing is based on ‘consent’, the Data Subject has the right to withdraw this consent at any time.
- Whether the personal data is necessary for the performance of a contract or to comply with a legal obligation.
- Whether the personal data is also used for automated decision making. The underlying logic, as well as the importance and the expected consequences of the Processing for the Data Subject must also be reported.

B. Personal data collected from another source than the Data Subject

If the personal data is not collected directly from the Data Subject but from another source, the Data Subject shall be provided with the following information in addition to the above-mentioned points:
- The categories of personal data.
- The source from which the personal data is obtained.

The above information is recorded at NHL Stenden in the data registers and insofar it concerns research, in the SmartPIA package.

The data registers are accessible to all categories of data subjects from the first contact with NHL Stenden. Students, course participants and staff members are actively informed of the data registers at the beginning of their study or at the commencement of their employment contract.

8.2. Right of access

- *Request*

Every Data Subject has the right to request information as to whether their personal data is being processed and if that is the case, the Data Subject has the right to access their personal data.

- *Notification*

When providing access to the data register, NHL Stenden provides the data subject with the following information:
- A description of the purposes of the Processing.
- The categories of data to which Processing is related.
- Categories of recipients.
- Available information about the origin of the personal data.
- The retention period for personal data or, if that is not possible, the criteria used to determine this period.
- The Data Subject's right to request the Controller for rectification or erasure of personal data, the right to restrict or object to the Processing as well as the right to data portability.
- The Data Subject's right to make a complaint to a supervisory authority.
- All available information about the source of the data, if the data is not collected from the Data Subject.
- The appropriate safeguards put in place, if the personal data is transferred to a third country.

- *Copy*

The Data Subject can request a copy of all the personal data. This copy must be provided in a standard electronic format, unless the request is made on paper or if the Data Subject explicitly requests a paper copy.

- *Costs*

Every first copy can be requested free of charge. However, for any additional copy NHL Stenden will charge the Data Subject €15 for administrative costs.

- *Rights and freedoms of others*

When providing the personal data, NHL Stenden will take into account the rights and freedoms of others.

8.3. Right to data portability

- *Grounds for request*

Any Data Subject may submit a request to NHL Stenden to obtain (free of charge) their personal data in a structured, commonly used and machine-readable format or to enable them to easily transfer their personal data to another Controller (data portability), without being hindered by NHL Stenden, provided the following conditions are met:

1. The Processing by NHL Stenden is based on 'consent' or 'execution of a contract with the Data Subject'.
2. The Processing in question is fully automated.

- *Rights and freedoms of others*

When providing the personal data, NHL Stenden will take into account the rights and freedoms of others.

- *Erasure of personal data*

If a Data Subject has exercised their right of data portability in the context of a Processing activity for the execution of a contract, NHL Stenden may not decide to erase the data. However, after expiry of the retention period, NHL Stenden must then erase the data.

If the right is exercised within the context of Processing based on the consent of the Data Subject, NHL Stenden may decide to erase the data after the right has been exercised.

8.4. Right to rectification, completion, erasure or restriction of the Processing.

- *Request for rectification, completion, erasure or restriction*

Every Data Subject may request that personal data stored at NHL Stenden is rectified, supplemented, deleted or that the Processing is restricted. In the event of the right to restriction, the personal data is temporarily restricted and is no longer processed by NHL Stenden. The restriction will be clearly indicated in the file.

- *Notification*

If it appears that the recorded personal data of the Data Subject is factually incorrect, that it is incomplete or irrelevant for the purposes of the Processing or has otherwise been processed contrary to statutory regulations, the data manager (the functional data manager or the Processor) will correct, permanently delete, supplement or limit this data.

Moreover, Third Parties who have been provided with data prior to the rectification, supplementation, erasure or restriction, are notified unless this is reasonably impossible or given the circumstances irrelevant. The Data Subject may request NHL Stenden to provide information as to whom NHL Stenden has made this notification.

- *Execution period*

The data manager ensures that a decision to correct, supplement, erase or restrict is executed as soon as possible. The execution of this will take place without any charge to the Data Subject.

8.5. Right to object

- *Grounds for objection*

There are two grounds for the Data Subject to object to Processing:

1. In relation to their private circumstances, any Data Subject may object to Processing by NHL Stenden if this Processing takes place on the basis of promoting the legitimate interest of NHL Stenden or a Third Party to whom the data is provided. See paragraph 6.1 for a description of the grounds.

   In the event of objection, NHL Stenden will, in principle, cease the Processing. If NHL Stenden can prove that its compelling legitimate interests outweigh the interests or the fundamental right and freedoms of the Data Subject, the Processing will continue. If the objection is justified, NHL Stenden will (free of charge) take the necessary measures to cease processing the personal data for the purposes in question.

2. With regard to Processing for 'direct marketing' purposes, the data subject has the right to object at any time. In case of an objection, NHL Stenden will immediately cease the processing for direct marketing purposes (free of charge) and not resume the processing.

8.6. Automated decision-making

Grounds
Data subjects have the right not be subjected to a decision solely based on automated Processing, which may have legal consequences for them. A 'decision based on an automated Processing' means a decision made without human intervention. This includes Profiling.

NHL Stenden never takes decisions about individuals solely based on automated processing of personal data.

8.7. Legal protection

- *General complaints*

If the Data Subject is of the opinion that the legal provisions relating to the protection of privacy or the provisions of this regulation are not enforced correctly, they may complain in writing to the Data Protection Officer: fg@nhlstenden.com. A complaint about the Data Protection Officer can be submitted to the confidential counsellor or to the Data Protection Authority.

- *Other provisions for appeal*

In addition to the general internal complaints procedure as described above, the Data Subject has the following possibilities if they feel that NHL Stenden has committed a violation of the GDPR that affects them.

A. *Appeals procedure at the Subdistrict Court*

If NHL Stenden has taken a negative decision on a request as described in paragraphs 8.1 to 8.6 of this Policy, or if NHL Stenden has rejected the request of the Data Subject, the Data Subject has the option to start an appeals procedure at the Subdistrict Court.

The appeal must be submitted to the Subdistrict Court within six weeks after receipt of the reply from NHL Stenden. If NHL Stenden has not replied to the Data Subject's request within the stipulated period, the appeal must be submitted within six weeks of expiry of this period. The appeal does not need to be submitted by a lawyer.

B. *Objection and appeal*

If NHL Stenden has made a negative decision with regard to a request as described in paragraphs 8.1 to 8.6 of this Policy, or if NHL Stenden has rejected the request of the Data Subject, and the decision of NHL Stenden can be considered to be a decision by an administrative body within the meaning of Article 6 paragraph 4 of the General Administrative Law Act, the Data Subject has the option to start an objection procedure. An objection procedure must always be started within 6 weeks of the publication of a decision from NHL Stenden. An appeal may be lodged with the court against a decision on objection.

C. Request for enforcement to a supervisory authority

If NHL Stenden has made a negative decision with regard to a request as described in paragraphs 8.1 to 8.6 of this Policy, or if NHL Stenden has rejected the request of the Data Subject, the Data Subject has the option to lodge a complaint with a supervisory authority or to have an organisation representing their interests act on their behalf.

9. Finally

This policy has come about following advice from

- The executive staff, in particular the Legal Affairs department
- The Data Protection Council of NHL Stenden
- The university consultation.

It was adopted by the EB of NHL Stenden dated 1 October 2019, following agreement of the participation body on 24 September 2019.

A review of the policy forms part of the two-yearly plan-do-check-act cycle of NHL Stenden. This also includes a check on the effectiveness of the measures.

Amendments to this policy are announced via intranet. The most recent version is published on one of the institution's Internet pages.

Please contact the DPO for questions or comments with regard to this policy.

10. Appendices

10.1. The data registers: which personal data, where and why?

Article 30 of the GDPR obliges us to draw up and maintain a 'register of processing activities'. This enables an organisation to demonstrate which personal data is processed under its responsibility. NHL Stenden provides substance to this obligation with a data register[7] for each target group (in the terms of the GDPR: 'category of data subjects').

NHL Stenden has drawn up data registers for the following groups. The mandated responsible directors are shown between parentheses (situation as of November 2018).

- Students (Angela Schat)
- Course participants (Soon Hee Santema)
- Leads (Rob Koning)
- Alumni (Rob Koning)
- Permanent employees (Alette Hospers)
- Temporary employees (Alette Hospers)
- External relations (Rob Koning)
- Guests of the Stenden University Hotel (Thulani Xhali)

The EB has appointed a mandated responsible person for each data register, a director who is responsible for compliance and maintenance of the data register. Their names are given above between parentheses[8].

The data register is essentially a matrix in which an exhaustive list of the processed personal data is set off against the locations where this personal data 'resides': at external controllers, such as the Tax Authorities, at processors such as Youforce Raet and at the various organisational units of NHL Stenden.

The compliance of the data registers is part of the privacy audit carried out by the Executive Staff, which takes place twice a year. Furthermore, the data registers are an express subject of debate in the reporting discussions with all directors.

Within their Academy, Service or Liaison Unit, the members of the Data Protection Council have a monitoring and informing task where it concerns the data registers.

All data registers can be found via https://privacy.nhlstenden.com/

10.2. Procedure 'How can data subjects exercise their rights?'

Data subjects who want to exercise their rights can apply to an online desk for this purpose[9]. If it concerns a request for inspection, they will receive the data register applicable to them by return. If the data subject wants to know more than *which* of their data is processed and with other requests, a meeting will take place within two weeks with a representative of the Data Protection Council[10]. The data subject must be able to identify themselves during this conversation. The purpose of the conversation is two-fold: de-escalation and specification. If it is then clear what the data subject exactly wants, the request (for example a request for inspection) is sent to the mandated person responsible for the data register in question. They ensure that the data subject is able to exercise their

[7] The instrument is developed under the direction of Ludo Cuijpers of Leeuwenborg Opleidingen and is also used, among others, at Fontys University of Applied Sciences and the Open University. The Data Protection Authority has praised the instrument.
[8] Situation on 1 September 2018.
[9] As long as that desk has not been set up, the requests are sent directly to the Executive Board.
[10] Action: appoint someone at each location who will do this.

rights within four weeks and, in this example, are able to inspect their data. See Chapter 8 for the rights of the data subject.

Requests for erasure of leads and alumni are granted without further investigation on the basis of a check of the e-mail address.

All requests and also their settlement are documented and stored for a period of two years in a central register.

Data subjects who are not satisfied about the manner in which their request is dealt with, can contact the DPO. The DPO monitors the existence, the organisation and the operation of this procedure.

10.3. Procedure Data Protection Impact Assessments

A Data Protection Impact Assessment is a systematic assessment of the necessity and the risks of the (intended) processing of personal data. The GDPR requires the DPIA particularly if it concerns:

a) *a systematic and extensive evaluation of personal aspects relating to natural persons which is based on automated processing (…)*

b) processing on a large scale of special categories of data (…)

c) a systematic monitoring of a publicly accessible area on a large scale.[11]

The requirements of the Data Protection Authority appear to imply a broader use of the DPIA. A DPIA is always recommendable and provides useful information for the data register, for any Controller-Processor Agreement that needs to be entered into and for the required level of information security.

The DPIA is therefore carried out within NHL Stenden

- for all large, essential processing of personal data (repeated every three years)
- for all new systems or processes
- for all apps and other digital applications deployed at an Academy or at a departmental level
- for research projects in which personal data is processed, a DPIA will be carried out if one or more of the following criteria are applicable.
    - international;
    - cooperation with other institutions;
    - processing of special personal data;
    - processing data of more than 1000 respondents;
    - master or PhD research.

The initiative for a DPIA is taken by the system owner and/or manager and/or main researcher. The execution takes place under the direction of the Security Officer. The results are documented, just as following-up on the resulting recommendations.

Monitoring the compliance of the execution of a DPIA forms part of the privacy audit that is carried out twice a year. The topic is put on the agenda in the report discussions which the directors hold with the EB. Within the Academy, Service or Liaison Unit the members of the DPC have a monitoring and informing role where it concerns the DPIAs. The reporting about the execution of the DPIAs is part of the annual report of the DPO.

Each year, a general information meeting is held with regard to the instrument of the DPIA.

[11] GDPR, Article 35, section 3a.

10.4. Procedure Privacy by design

'Data protection by design (*privacy by design*) implies that the mechanisms used for processing are so designed that they take into account as far as possible the privacy of the data subjects and the requirements from the GDPR. A system that satisfies this could therefore, for example, have buttons incorporated with which data subjects could inspect their personal data. This includes other measures focused, for example, on minimising the amount of personal data and pseudonymising personal data as soon as possible'[12].

Privacy by Design for NHL Stenden is a design requirement for systems and processes and a precondition during procurement and tendering.

Privacy by Design automatically precludes certain information or data, only selects relevant persons and data, removes (partial) information that is no longer required and deletes personal data as soon as it is no longer required[13].

Specific examples of privacy by design are :

- A button 'My details'
- A good authorisation structure
- The possibility to delete data automatically and in a differentiated manner (for example, at the end of the retention period)
- Possibility for detailed logging
- The correct information on the correct screen (if for example the BSN number *must* be used in the system, it is hidden deep and is only visible for those users for whom it must be visible)

The DLWE service ensures technical development of the design requirements which result from Privacy by Design and for an annual update thereof.

The Purchasing department is responsible for including the requirement of privacy by design in the purchasing and tendering process.

Within the Academy, Service or Liaison Unit the members of the DPC have a monitoring and informing role where it concerns the Privacy by Design.

Each year, the DPO and the SO hold an information meeting about Privacy by Design.

Privacy by Default (data protection through standard settings) is an associated concept: by default, the possibilities for choice must be set up in the most privacy-friendly manner. Within NHL Stenden, this is a point of attention within the Office365 environment.

The DLWE service is responsible for the privacy-friendly set-up of the systems used within the university of applied sciences and for the information about them.

10.5. Controller-Processor Agreement Procedure [14]

In accordance with Article 28 paragraph 3 of the GDPR, NHL Stenden enters into Controller-Processor Agreements with processors, parties which process personal data for us.

[12] Engelfriet, Meij and Kager (2017), p. 119.
[13] Taken from a presentation of Dr. Jaap-Henk Hoepman at Stenden University of Applied Sciences on 15 February 2017.
[14] Mandating and procedure had not been determined yet at the time of submission of this plan.

The responsibility for entering into and the management of the Controller-Processor Agreements lies with the Purchasing department or, with contracts under €50,000, with the budget holder.

In principle, NHL Stenden applies the model agreement which has been developed by SURF. Small deviations, desired by the supplier, are submitted to the DPO for assessment. Substantial deviations are submitted to the legal counsel on privacy of the Executive Staff. The Controller-Processor Agreements are signed by the EB or, for contracts under €50,000, by the budget holder.

Monitoring the compliance with the obligation to enter into Controller-Processor Agreements is part of the privacy audit which is carried out twice a year by the Executive Staff. This monitoring takes place on the basis of the overviews from the data registers.

Each year, in cooperation with the legal counsel on privacy, the DPO organises an information session about Controller-Processor Agreements.

The Controller-Processor Agreements are emphatically addressed in the report discussions of the director of Finance, Procurement & Control with the EB.

10.6. Increasing awareness

The protection of personal data is included in information systems, which are designed according to requirements of Privacy by Design, in procedures and mechanisms such as described, for example, in the data registers, but primarily in human actions. If employees and other data subjects are insufficiently aware of the importance of privacy, then drawing up a privacy policy is fighting a losing battle.

The awareness site http://datacare.nhlstenden.com was launched in the run up to the merger. In the first half of 2018 the SO and the DPO have jointly given more than twenty workshops and information meetings. This is now included in the programme of the Professionalisation Academy. Training takes place on three levels:

- Open registration for both teaching and support staff
- Training for teams
- Training members of the Data Protection Council. This training will have an impact on the Academies, Services and Liaison Units that they represent. An important task of the members of the DPC is to propagate the importance of and to provide information about the careful processing of personal data.

Under the responsibility of HRM, a module ‘privacy and security in a data-driven society’ will be included in the management development projects. Attention to the protection of personal data is pre-eminently an issue to be discussed during the report meetings with all directors and the EB.

At least once a month for the next two years, special attention will be paid to the topic of privacy.

The awareness campaign focuses on all categories of data subjects, whereby the staff members and students will be addressed first.

This campaign is supported by the Marketing and Communication service.

10.7. Privacy and internationalisation

The privacy legislation imposes strict requirements on the transfer of personal data to countries outside the European Economic Area.

The GDPR applies to all European students and employees of NHL Stenden, wherever they may be. The GDPR also applies to students from outside the EEA, who are studying in the Netherlands, such as the so-called ’60 ECs students’.

In accordance with Article 46, paragraph 2c, NHL Stenden bases the transfer of personal data to the countries in which our International Branch Campuses are located on ‘appropriate safeguards’, in particular on the ‘standard data protection clauses adopted by the (European) Commission’. NHL Stenden has concluded these so-called model contracts or ‘model clauses’ with all four IBCs. This means that the transfer of personal data within the framework of the Grand Tour™ has a legal basis[15].

The transfer of personal data to countries outside the EEA within the framework of placements or exchanges is based on compliance with a contract entered into in the interest of the data subject (Article 49, paragraph 1).

The transfer of the data of registered international students to agents outside the EEA is based on the permission that the students in question have given for this purpose.

Although the International Branch Campuses legally have their own responsibility and must comply with the legislation applicable to them, it stands to reason to handle personal data globally in the same way within the 'NHL Stenden Group', regardless of the different responsibilities and the different legal regimes. NHL Stenden has a Privacy Guideline for this purpose, as an internal code of conduct with regard to processing personal data at the various locations and the transfer of personal data between the locations. (see appendix 10.9).

The EB is responsible for compliance with the European model contracts. This responsibility has been mandated to the Director of International Affairs.

The responsibility for compliance with the Privacy Guideline lies with the General Managers of the IBCs.

The DPO monitors the alignment of the Privacy Guideline with the GDPR and promotes awareness at the International Branch Campuses.

10.8. Privacy and research

A lot of research is done within an institute for higher education, such as NHL Stenden. In many cases, personal data of the research subjects is processed in the context of such research. Because every research is different, the category of research subjects does not lend itself for a data register as set up for the other target groups. The SmartPIA tool is used to identify the personal data processed within the framework of the various research projects.

NHL Stenden will develop a privacy toolbox for research as soon as possible, using good examples from elsewhere.

This toolbox should ideally contain the following tools.

- A concise privacy protocol for the various types of researchers, from Bachelor students to PhD students.
- An ethics committee, possibly in cooperation with one or more other educational institutions.
- A safe tool, provided by NHL Stenden to perform online research.
- A repository for research data, possibly in cooperation with one or more other educational institutions.
- A platform for launching and participating in internal research among students and staff.

[15] This is based on a detailed advice from among others Duthler Associates *Transfer of personal data to third countries* from 17 August 2017.

The responsibility for compliance with the privacy rules for research lies with the Director of R&D Education and Research.

The development of the privacy toolbox has been assigned to the Research and Privacy committee specially set up for this purpose.

10.9. International Privacy guideline NHL Stenden

Privacy guideline NHL Stenden University of Applied Sciences

Purpose
By issuing this guideline NHL Stenden shows how it acts in accordance with the legal requirements and protects the personal data of members of staff, students and third parties. The guideline describes the approach we take to privacy and is based on Dutch law.

Scope
The guideline covers the processing of all personal data by or on behalf of NHL Stenden (all locations).

Definitions
Personal data: all data concerning an identified or identifiable natural person.

Processing of personal data: all actions or series of actions related to personal data, including in all cases the collection, registration, classification, storage, editing, amendment, retrieval, viewing, usage, issue by means of forwarding, distribution or any other form of provision, uniting, placing in mutual relation, as well as the protection, exchange or destruction of data.

Controller: the natural person, legal person or any other person who or administrative body that, acting alone or in association with others, lays down the purpose and the means of processing personal data.

Processor: the person who processes the personal data for the controller, without being subject to the controller's direct authority.

Data subject: the person to whom the personal data relates.

Data protection officer (DPO): The position of the DPO is laid down by law. He oversees the processing of personal data and can make recommendations to improve how the personal data is processed.

Data Protection Council: The Data Protection Council at NHL Stenden is a consultative and advisory body with regard to policies on privacy (protection of personal data) and security (information security). The DPC is composed of representatives from all Academies, Liaison Units and departments. The members of the Information Security Steering Group are officially part of the DPC. The members of the DPC are called Data Protection Counsellors.

Privacy governance
Data processing carried out by or on behalf of NHL Stenden is reported to the Data Protection Officer and published on the intranet.

The adopted NHL Stenden policy forms the framework for this. The key terms are transparency and purpose limitation. We say what we do and we do only what is necessary. Privacy issues are communicated via the privacy portal accessible via the Start Menu.

How do we obtain the data?
Data is only collected:
- directly or indirectly (via Studielink, agents, social media) from the data subject through the channels provided for by law.

What do we do with the data?
Personal data is processed exclusively:
- if necessary for education or research, in particular to facilitate education for students;
- if necessary for the purpose of the employer-employee relationship;
- if it has been given to the DPO (stating the legal grounds);
- if the data subject has given explicit consent for this to be done;
- if the vital interests of the data subject are at stake.

What are our general principles?
The personal data processed by NHL Stenden is correct and relevant and is legitimately and legally processed.
NHL Stenden does not collect any more data than what is necessary (data minimisation).
Employees of NHL Stenden are asked to provide a copy of their passport when they join the organisation; on no occasions other than that.
NHL Stenden does not keep data for longer than necessary. This is based on the Selection List for Universities of Applied Sciences (*Selectielijst hogescholen*).
NHL Stenden collects data only for a precisely defined purpose that is related to the institution's social mandate (purpose limitation);
NHL Stenden never passes on data to third parties unless:
- it is legally obliged to do so;
- the data subject has given explicit consent for this to be done.

A supporting document or copy of the diploma is only issued to or on the request of the data subject, for example. Email details of students or members of staff are issued to the research agencies for quality surveys (National Student Survey (NSE), staff satisfaction survey).
To the extent that NHL Stenden has personal data processed by third parties (processors), a processor's agreement is entered into with the processors laying down responsibility for data breaches.
NHL Stenden never sells personal data and does not make it available for commercial purposes in any way whatsoever.
NHL Stenden effectively protects the personal data in accordance with the current state of technology. Personal data is encrypted where necessary and possible.

Special categories of personal data
NHL Stenden does not process any special personal data other than
- nationality (in connection with the internationalisation policy);
- religion (exclusively for the Education in Primary Schools programme in connection with assigning the placements by denomination);
- medical data (if necessary for assistance in the context of the Study and Disability scheme and for the safety of students during the Grand Tour™.

Forwarding of data to third countries
NHL Stenden Netherlands does not exchange personal data with the international branch campuses unless:
- this is necessary for educational purposes;
- there is no alternative owing to the obligations under the employment contract;
- the vital interests of the data subject are at stake.

Rights and obligations of data subjects
Data subjects have the right to view and correct their data. They can also object to the registration of certain data.
For matters concerning the protection of their personal data they can lodge a complaint with the DPO. Students can also lodge a complaint via ELF (single point of contact facility).
All persons at NHL Stenden are obliged to report possible personal data protection breaches to the DPO (responsible disclosure).
Managerial staff and members of the Data Protection Council are obliged to report the processing of personal data to the DPO.

To conclude
If in doubt, the DPO should be consulted.
The Data Protection Officer of NHL Stenden University of Applied Sciences is Willem Bakker.
willem.bakker@nhlstenden.com | □□+31 6 15 31 95 03

10.10. Phasing and implementation