Privacy Regulations Personal Data Students Saxion University of Applied Sciences

Explanation

Statutory frameworks

On 1 September 2001 the Personal Data Protection Act (*Wet bescherming persoonsgegevens*; Wbp) came into effect. This Act replaces the Data Protection Act (*Wet persoonsregistraties*) effective from 1989. The Wbp is required to implement the European Directive (no. 95/46/EC).

In the Wbp the *processing of personal data* is the starting point. *Personal data* is broadly defined as each piece of data that is traceable to and can provide information on a natural, identifiable, person. *Processing* includes each imaginable activity with regard to data: from collecting and processing, via distributing, storing, consulting, up to and including destroying data.

The Wbp prescribes that each processing of personal data must meet a number of conditions: the processing must for example be legitimate, careful, not excessive, the objectives for which processing takes place are to be clearly defined and recorded in writing, and the persons involved must have the right of perusal and correction with regard to the data.

Furthermore the law takes as starting point that each automated processing should in principle be reported to the Dutch Data Protection Authority (*College Bescherming Persoonsgegevens*; CBP), unless the processing falls under one of the provisions of the WBP Exemption Decree and also meets the conditions mentioned in that decree. The Board of Directors has decided not to try to meet too strictly all the conditions stated by the Exemption Decree in order to be exempted from the notification requirement; several of these conditions are difficult or undesirable for Saxion to satisfy. Therefore, before 1 September 2002, the following processed personal data were reported to the CBP: Staff administration, salary administration, student administration, alumni/graduates administration, study progress administration, accounts payable and accounts receivable administration, network systems, computer systems, other internal administration, video camera surveillance and administrative archives.

The law requires Saxion to bring existing data and newly processed data in line with the Wbp and allows Saxion to appoint its own ‘officer’ in the context of protection of personal data. This officer will independently monitor the application and compliance of the Wbp within the organisation. Reports can be made to this officer instead of to the

CBP. Saxion has chosen to appoint a staff member as Data Protection Officer.

Choice of regulations

To implement the Personal Data Protection Act (Bulletin of Acts and Decrees 2000, 302, Act of 6 July 2000, effective since 1 September 2001), the Board of Directors of Saxion adopted the Privacy Regulations Personal Data Students Saxion University of Applied Sciences on 25 March 2003. On 2 April 2003 the Central Participation Council endorsed this.

Although the Wbp does not require any regulations to be in place, there are obligations with regard to the clear recording of the objectives that the party responsible (Board of Directors) has for processing personal data. To address this properly, Saxion needs to include largely the same type of data as in the previous regulations: the objectives, the relevant data, the extent to which third parties may obtain data, the rights of the persons involved, etc. Based on the above Saxion has opted for drawing up privacy regulations for students. The present document provides for this.

A review of the regulations took place in September 2009.

Privacy Regulations Personal Data Students Saxion University of Applied Sciences

Definitions

In these regulations the following terms have the following meaning:

a. **administrator:** the person who manages the day-to-day activities regarding the processing of the personal data, in this case: the heads of the Schools/Service Departments;
b. **processing of personal data**: each act or set of acts regarding personal data, including at any rate the collecting, recording, ordering, saving, updating, changing, retrieving, consulting, using, providing via forwarding, distributing or any other form of provision, combining, connecting, protecting, erasing or destroying of data;
c. **database:** each structured set of personal data, irrespective of whether this set of data is centralised or is functionally of geographically distributed, which is accessible in accordance with certain criteria and involves different persons;
d. **Dutch Data Protection Authority:** the authority referred to Section 51 of the Personal Data Protection Act;
e. **Saxion:** Saxion University of Applied Sciences;
f. **party responsible:** Board of Directors of Saxion;
g. **processor:** the person who processes personal data on behalf of the party responsible, without being directly subjected to its authority;
h. **person involved:** the person to whom a piece of personal data pertains;
i. **permission of the person involved:** each free, specific expression of will based on information by which the person involved accepts that personal data concerning him/her are processed;
j. **recipient:** the person or body to whom or to which the personal data are provided;
k. **officer:** the person who has been authorised by the Board of Directors to make reports to the Dutch Data Protection Authority;
l. **piece of personal data:** each piece of personal data concerning an identified or identifiable natural person;
m. **system administrator:** the person who manages the technical part of the databases;
n. **provision of personal data**: disclosing or making available of personal data, to the extent these originate entirely or largely from data stored in the database, or which have been obtained through processing of these, whether or not in connection with other data;
o. **provision of personal data to a third party:** provision of data from a database to anyone, not being the person involved, the party responsible, the processor or any person who under the direct authority of the party responsible or the processor is authorised to process personal data;
p. **collection of personal data:** obtaining personal data;
q. **Wbp:** Personal Data Protection Act;

r. **Exemption Decree:** Decree of 7 May 2001, (Bulletin of Acts and Decrees 2001, 250), containing instructions for processing of personal data that are exempted from the report referred to in Section 27 Wbp;
s. **WHW:** Higher Education and Research Act;
t. **CAO:** Collective Labour Agreement for Higher Professional Education.

Section 2 Scope of the regulations

1. These regulations apply to all personal data of persons involved, as mentioned in Section 6, within Saxion, which are processed by the party responsible or on its behalf, to the extent that these data from this registration can easily be traced back to individual persons.
2. These regulations do not apply to personal data processed in databases of student counsellors, confidential counsellors, the various complaints committees and appeals and objections committees – with the exception of the registration of the decision – of Saxion.
3. All personal data stored in the databases mentioned in paragraph 2 are in principle confidential and must therefore be treated confidentially.
4. To the extent data from the databases mentioned in paragraph 2 are provided to third parties, this can only take place with the permission of the person involved, or in accordance with a power or obligation laid down in statutory provisions or the relevant school regulations.

Section 3 Objective

The objective of these regulations is:

1. To protect the personal privacy of each person whose data have been processed in one or more databases against abuse of these data and against processing of inaccurate data;
2. To prevent personal data processed in a database from being used for another purpose than for which that database is intended;
3. To safeguard the rights of the persons involved.

Section 4 Purpose of the processing of personal data

The purpose of data processing is:

1. To be able to dispose of information for Saxion's business operations, and the implementation of its statutory tasks, in accordance with the provisions laid down in Section 19 paragraph 2 Exemption Decree;
2. To adequately meet the request for the provision of data to persons or bodies with a public-law duty, to the extent this obligation arises from legislation and to the extent they need these data for the performance of their duties and the personal privacy of the persons involved is not disproportionally compromised.

Section 5 Obligation to report databases

1. Prior to the start of any processing, a fully or partially automated registration of personal data (see Section 7) destined for the effectuation of a purpose or of several related purposes, must be reported to the data protection officer.

2. The party responsible completes a 'processing personal data notification form' for the person obliged to notify, after which the data are sent to the Dutch Data Protection Authority. The party responsible can mandate the power of notification to the data protection officer.
3. Following from the foregoing paragraphs, each staff member who manages or creates a database is obliged to notify this to the party responsible, stating the objective of the database and the name (names) of the administrator and processors, if any.

Section 6 Categories of persons involved

Data can be processed in the databases with regard to the following categories of persons:

- Students;
- *Extranei* (persons who take exams and examinations but do not attend lectures);
- Course members;
- Contract students;
- Alumni;
- Prospective students;
- Visitors of conferences and seminars.

Section 7 Categories of data

The following types of data can be processed in the databases:

1. Personal data such as:
a. family name, initials, prefixes, first names, name by which one is known;
b. name spouse for married women (if stated);
c. date of birth, place of birth, country of birth;
d. nationality, nationality parents, country of birth parents;
e. passport photo, whether or not digitalised;
f. gender;
g. student number;
h. correspondence number OC&W/IBG;
i. bank/giro number;
2. Addresses:
a. most recently known address, postal code, place of residence, country, telephone number;
b. address, postal code, place of residence, country, telephone number and other similar data useful for communication on application;
3. Application / enrolment data:
a. degree programme, study mode, form of registration, phase, year, funding, date of enrolment/application;
b. date and reason for deregistration;
4. Prior education:
a. (type of) prior education enjoyed including subjects and marks obtained;
b. year in which the diploma for the prior education was obtained;
c. name of the school where prior education was enjoyed;

5. School history:
a. first year of enrolment higher education;
b. first year of enrolment institution;
6. Study progress:
a. date of obtaining propaedeutic certificate;
b. date obtaining final certificate;
c. marks and credits obtained;
d. performance-based student grant and progress-based student grant data regarding whether or not the standard has been achieved[1];
e. binding recommendation regarding continuation of studies[2];
7. Financial data:
a. invoicing and payment tuition fee;
b. invoicing and payment other costs;
c. granting of social fund;
d. granting of graduation fund[3];
e. granting of top-class sport fund;
f. granting of facilities fund;
8. Alumni data:
a. career data;
b. email address;
c. participation alumni activities;
9. Other data, collected via a camera that is visible or the presence of which has been made known;
10. Other data, collected via a hidden camera, if there is a suspicion of punishable or unlawful conduct by persons involved, whereby the principles of proportionality and subsidiarity are taken into account;
11. The list of data in paragraph 1 is not a limitative list. Changes may occur as a result of, among other things, changes in the (educational) organisation or in legislation.

Section 8 Special data

1. It is prohibited to process personal data concerning a person's religion or personal beliefs, race, political inclination, health, sexual life, as well as personal data concerning the membership of a trade association, except for the provision in paragraph 2 of this Section. The same applies to personal data pertaining to criminal law and personal data on unlawful or irritating behaviour in connection with a ban imposed in connection with that behaviour.
2. The prohibition to process a person's religion or personal beliefs as referred to in paragraph 1, does not apply if the processing takes place with a view to Saxion's objective and this processing is important for achieving its principles and the data have been obtained with the express permission of the person involved.
3. The prohibition to process personal data concerning a person's race as referred to in paragraph 1, does not apply if the processing takes place with the purpose of

[1] Section 7.9b and 7.9a WHW
[2] Section 7.8b WHW
[3] Section 7.51 WHW

granting a preferential position to persons of a certain ethnical or cultural minority group in order to undo or reduce a factual inequality, but only if this is necessary for that purpose and the data only concern the person involved's country of birth, his/her parents or grandparents, or are based on other criteria set by law, based on which it can be established objectively whether a person involved belongs to a certain ethnical or cultural minority group and provided he/she has not objected to this in writing.

Section 9 The way in which personal data are obtained

1. The data mentioned in Section 7 are provided by the person involved as much as possible on application or enrolment, or collected, entered into the database and updated by the departments within Saxion for which the collection of these data is necessary.
2. The data as referred to in Section 7 paragraph 9 are obtained by using a camera that is visible or the presence of which has been communicated.
3. The data referred to in Section 7 paragraph 10 are obtained by using a hidden camera, if there is a suspicion of punishable or unlawful behaviour by the persons involved, whereby the principles of proportionality and subsidiarity are taken into account. A hidden camera can only be used following a decision to that end of the Board of Directors, with due observance of the protocol attached in annexe 2.

Section 10 Retention period

1. No later than two years[4] after termination of the enrolment all personal data of the person involved are deleted from the database, unless a longer period, for example in the context of inspections or contacts afterwards, is considered to be efficient[5] or is necessary pursuant to a statutory obligation.
2. Retention periods of certificates and study results obtained can be found in the Saxion selection list.
3. Personal data of prospective students who are not enrolled to the university of applied sciences after admission, will be deleted from the database no later than after 1 year.

Section 11 Direct access to database

1. The following persons have access to the database:

a. the party responsible;
b. the administrator;
c. the staff members designated by the administrator with regard to the personal data relating to the persons involved who work in their field;
d. the processor;
e. the system administrator.

[4] Article 19 Exemption Decree
[5] Section 7 in conjunction with Section 9 paragraph 1 Wbp

2. The system administrator will give the staff members designated by the administrator access to certain parts of the personal data or to all personal data via authentication and authorisation, according to the requirements of their tasks.
3. The authorisation of persons who no longer need access to the data in connection with their function, will be revoked forthwith.

Section 12 Categories of persons or bodies to whom or to which personal data from the database may be provided.

1. Except to the persons who have access to the database, personal data from the database are provided by the administrator to:

a. the person involved: only his/her own data;
b. study career counsellors and other officers, only with regard to the personal and enrolment data of the persons falling under them and to the extent this is needed in the context of the tasks and powers;
c. educational secretariats, only with regard to the personal and enrolment data of the persons falling under them and to the extent this is needed in the context of the tasks and powers;
d. other departments, only to the extent this is needed in the context of the tasks and powers of the department;
e. student counselling centre and confidential counsellors, to the extent this is needed in the context of the tasks and powers;
f. Examination Boards and Appeals Board, to the extent this is needed in the context of the tasks and powers;
g. Admission Board, to the extent this is needed in the context of the tasks and powers;
h. Facilities Committee and funds administrator, to the extent this is needed in the context of the tasks and powers;
i. Election Committees participation bodies;
j. schools for senior general secondary education (havo), pre-university education (vwo) and vocational and adult education delivering students as far as the progress of former students is involved.

2. Data traceable to identifiable persons from the database can be provided to:

a. the Ministry of Education, Culture and Science;
b. the Information Management Group (*Informatie Beheer Groep;* IBG);
c. the Higher Education Inspectorate;
d. other institutions in so far as there exists a statutory basis for this;
e. other institutions only with permission from the person involved.

3. Once personal data have been anonymised such that they are not traceable to individual persons, the party responsible can decide to provide these for academic research or statistics to the extent that:
   a. the research serves a general interest;
   b. the processing for the research or the statistics in question in necessary;
   c. asking of explicit permission is not possible or takes a disproportionate amount of effort and the execution is surrounded by such guarantees that the person involved's personal privacy will not be disproportionately compromised.

4. The categories of data that can be provided to the authorities mentioned in paragraph 2 are those data that the party responsible is required to provide by law or by contract.
5. Other data will only be provided with the permission of the person involved.

Section 13 Inspection

These regulations are included in the Saxion University of Applied Sciences Student Students' Charter and can be consulted via MijnSaxion. It is also open for inspection at the student information centre and at the education and degree programme desks for anyone whose personal data may be or become included in the database.

Section 14 Rights of persons involved

1. Each person involved may request:

a. to peruse the personal data processed with regard to him/her and to be informed of their origin via a written overview;
b. if the data from the overview are factually incorrect, insufficient or irrelevant for the purpose of the registration or in violation of a statutory provision, to improve, supplement or remove these data;
c. to be informed whether any data concerning him/her have been provided from the system to third parties in the previous year;
d. a statement containing certain personal data from the database, which the person involved can prove he/she needs these to provide to third parties.

2. A request is to be made to the administrator in writing; the administrator shall comply with the request as referred to under 1a, c and d within one month after receiving the request in writing and will state within two months after receipt whether or to what extent the request under 1b will be complied with.
3. If the administrator has doubts about the identity of the person making the request, he/she will ask the person making the request as soon as possible to provide further data concerning his/her identity or, in the event of a request as referred to under 1a or d, whether he/she can collect the overview in person and submit proof of identity. As a result of this request of the administrator the period is suspended until the moment the proof requested is provided.

Section 15 Complaints

The person involved may submit a written complaint concerning the application of these regulations to the party responsible via the Reporting Centre for Complaints and Disputes (*Meldpunt Klacht & Geschil*). The person involved will receive a letter containing the decision on the complaint submitted within two months.
If the complaint has not been settled satisfactorily, the person involved may submit the complaint to the Dutch Data Protection Authority.[6]

[6] Section 47 Wbp

Section 16 Secrecy and security

1. Staff members who in connection with their function take cognisance of personal data from the database, are required to use these data in no other way than is necessary for the performance of their tasks and not to share these with persons who are not authorised to take cognisance of these, in accordance with the provisions laid down in the Collective Labour Agreement.
2. The party responsible, as well as the administrator, processor and system administrator, ensure that fitting technical and organisational measures are put in place to prevent the loss of unlawful processing of personal data. These measures guarantee – taking into account the state of the art and the costs of execution – a fitting safety level in view of the risks involved in the processing and the nature of the data to be protected.

Section 17 Compliance check

1. The party responsible checks compliance with the provisions laid down in these regulations.
2. This check comprises checking whether the set-up of the organisation, including the procedures, is in accordance with the provisions in these regulations and checking, at random points in time, whether these regulations and the procedures are complied with by the relevant staff members. This check also involves the security measures against burglary and theft.
3. The party responsible may instruct a Saxion officer in accordance with Section 62, 63 and 64 Wbp to perform actual checks regarding the protection of personal data.

Section 18 Transitional and final provisions

1. Without prejudice to any statutory provisions these regulations are in force during the entire period of the processing of personal data.
2. In the event of a transfer or transition of the processing of personal data to another party responsible, the person involved is to be informed of this, in order to allow objections to be made against the transfer or transition of the data relating to such person.
3. These regulations shall replace the previous Registration of Personal Data Scheme adopted by Saxion (or its legal predecessor).
4. The party responsible sees to it that these regulations are evaluated regularly.
5. Evaluation takes place at least once every five years.
6. In all cases not provided for by these regulations, the party responsible shall decide in accordance with the law.
7. If there exists lack of clarity or if there are any questions relating to the implementation of the WBP, these will be presented to the CBP via the Data Protection Officer who will state how to proceed. This lack of clarity/these questions and their answers will be registered by the data administrator.

Section 19 Effective date and short title

After the Central Participation Council had given its approval, these regulations were adopted by the Board of Directors on 6 October 2009, and have become effective from this moment. These regulations can be cited as Privacy Regulations Students Saxion University of Applied Sciences.

Annexe 2: Protocol for use of hidden cameras (see Section 9 paragraph 3)

1. The use of a hidden camera is only permitted after a decision taken to that end by the Board of Directors;
2. This involves situations in which the safety of humans, property and/or the organisation is at stake and where no other options are open;
3. The decision is taken on the proposal of a head and on the advice of the Data Protection Officer;
4. The Chairman of the Central Participation Council (CMR) will be informed confidentially;
5. After the incident, it will be evaluated and accounted for to the CMR.