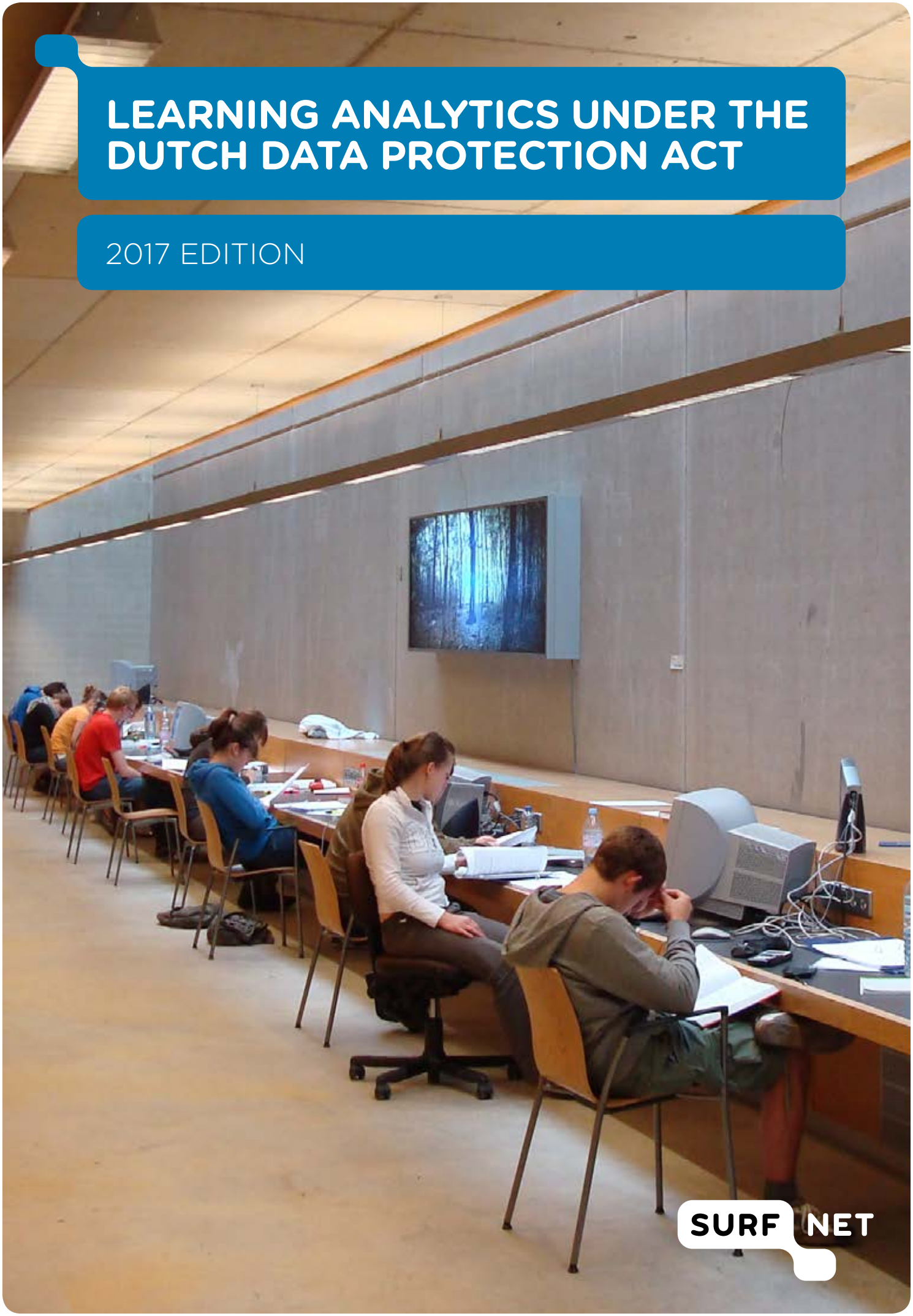
LEARNING ANALYTICS UNDER THE DUTCH DATA PROTECTION ACT

2017 EDITION



SURF NET

TABLE OF CONTENTS

1. LEARNING ANALYTICS AND PRIVACY

Learning analytics is the collection and analysis of data from learning environments in order to improve students' learning process. This information is then made available to various stakeholders, such as the students themselves, lecturers or degree programme managers. This enables you to better understand and improve the learning process. However, the collection and analysis of data involves the processing of personal data: data that directly or indirectly tells us something about the students involved. When an education institution processes personal data, it is subject to the Dutch Data Protection Act (Wet bescherming persoonsgegevens, or Wbp). So what does the Wbp have to say about learning analytics?

This guide tells you what you should look out for when collecting student data in order to improve the learning process. Firstly, we will clarify what is meant by personal data and what you are permitted to do with it. We will then address the requirements that you must comply with in order to collect personal data. We will examine the preconditions for data processing and your obligations, for instance in the area of security and disclosure requirements. Furthermore, the guide informs you of the issues you must take into account when using the services of third parties. The requirements relating to data storage are also addressed. The guide concludes with a step-by-step plan.

It is important to be aware that the use of learning analytics is legally complex. It is not simply a case of asking permission once and including a privacy statement on the website. The Wbp sets stringent requirements for the use of learning analytics and information provision: it must be customised to suit the students in view of the tools that you wish to implement within your education institution.

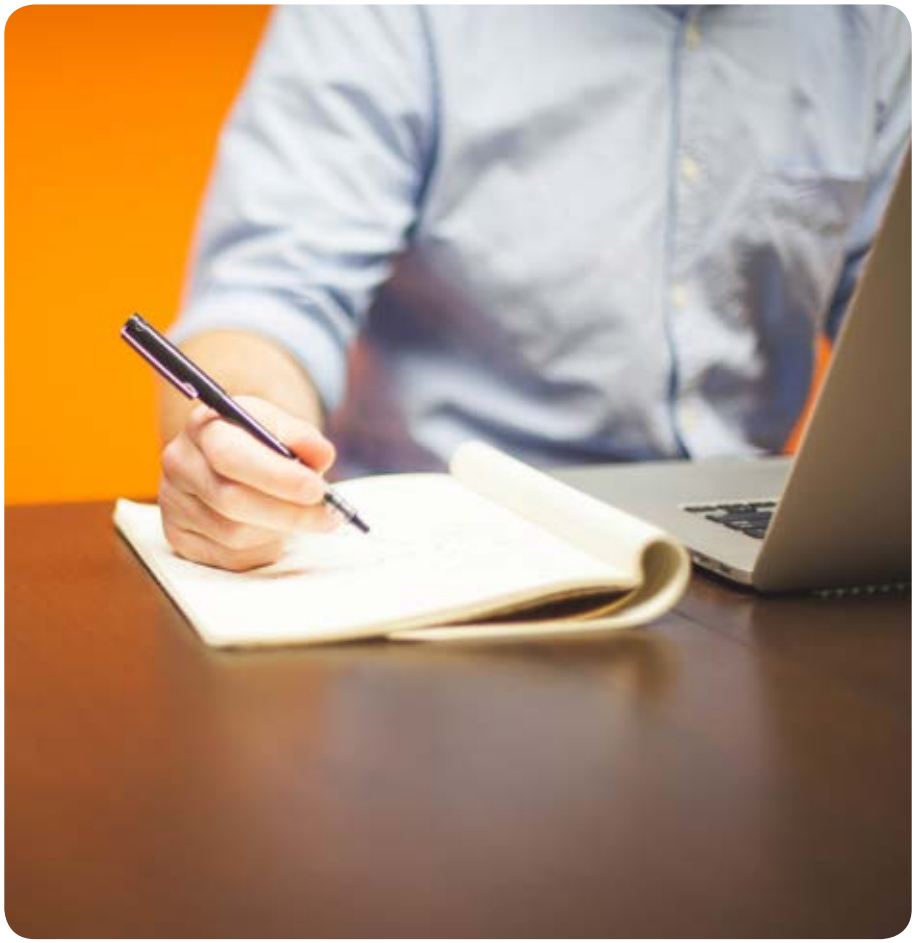
2. WHAT IS PERSONAL DATA?

Under the Wbp, personal data includes all data that can be traced to an individual, either directly or indirectly. A name or address is classified as personal data, but so is data on behaviour. Recording a person's actions within a learning environment, therefore, is a form of personal data collection

Directly or indirectly traceable

All data that can be traced - directly or indirectly - to a particular person is classified as personal data. Personal data covers more, therefore, than just names and contact details. For example, a student ID number is also personal data, as it can be linked to a particular person. The data can only be classified as non-personal if it is not reasonably possible to trace the data to the person concerned (for example, if random numbers are allocated to the data, and the list linking the random numbers to the names is then destroyed).

However, people can often be traced via other data. For example, each student's grade history is unique to that student as no two students achieve exactly the same grades for exactly the same combination of courses. The grade history forms a set of personal data, even if the student's name is not included.



Specific personal data

Specific personal data includes data about matters like the person's health, ethnic background, sexual preference, political views or religious beliefs. Normally, you are not permitted to collect or use this kind of data. This is only permitted with the express permission of the person concerned, or if usage is permitted by law. Express permission entails that you must ask each person for this data, explain why you need it and give them the opportunity to decline permission.

For example, a student church is permitted to record who attends services, although this is effectively a record of people's religious beliefs. However, in a questionnaire intended to get to know students better, you cannot ask about the students' religious beliefs, even if you include the option 'I do not wish to respond' as an answer to the question. You are permitted to ask about a person's disability if it is relevant to their studies. An example of such a disability would be dyslexia, as it requires extra time for examinations.

The Citizen Service Number (BSN number) is also a specific type of personal data: you are only allowed to use this data if the law permits it for the intended purpose. For example, when making copies of ID documents, the Citizen Service Number must be rendered illegible. Also note that you may sometimes be asking for specific personal data without intending to. For example, if you ask students to take a test on Sunday, then some of them may say no for religious reasons.

When is data no longer personal data?

Data loses its status as personal data when it is aggregated, i.e. combined into statements expressing the opinions of multiple people. For example, '80% of the students failed this test' is non-personal data. The law places no demands on this kind of aggregated statistical data.

When does personal data become aggregated data? There are no fixed rules for this. A frequently used rule of thumb is that the data of at least five people must be combined for the data to become non-personal. Other sources, such as the Central Bureau of Statistics in the Netherlands, use a minimum of 12 people. The universal principle is that no data must be traceable to any individual. For example, if all five students are male first-year physics students, then this remains personal data even after aggregation. If an aggregated statistic relates to 0% or 100% of the surveyed population, then this is still classified as personal data.

You can do whatever you wish with aggregated data. However, the source data is personal data to which the Wbp applies. An operation in which aggregated data is the end result is therefore subject to the Wbp. The Wbp is only inapplicable to edits and analyses in which the data is aggregated from the start. For example, a legal basis is required if a lecturer wishes to measure how fast the students are processingthe course content. This remains the case even the lecturer only wishes to formulate statistical conclusions from the data.

3. WHEN ARE YOU PERMITTED TO PROCESS PERSONAL DATA?

The Wbp defines all usage of personal data as 'processing'. You are only permitted to process personal data if you comply with one or more requirements in this act, known as principles. The principles that are of importance to learning analytics are:

- permission
- execution of contract
- legal obligation
- execution of a government task
- legitimate interest

3.1 Permission

A frequently used principle is the permission of the person(s) whose data you are collecting. If you wish to use the data, you must first explain what you are going to do with it and why. Only then are you permitted to ask the students in question for their permission. For more information, see Section Duty of disclosure.

Permission must be freely granted. Students must be able to say no. For example, if they decline permission, then this must not result in their exclusion from a compulsory course or examination. If you wish to use an online tool for learning analytics as part of a particular course, you should ask permission for this before registration. If the students have already registered, then refusal is no longer realistic.

Ensure that the permission is specifically formulated. For example, 'I consent to the use of learning analytics' is not specific. Make it clear who will be conducting the monitoring, what data will be collected and what will happen to it. One example: 'I give permission for the tracking and registration of my study performance for the purposes of customised study advice. The study advisor will be given access to this data in order to proactively address any risks of study delay.'

You can ask for permission for multiple courses, for a whole academic year or even for an entire degree programme in one go. You therefore do not have to ask permission for each separate course. However, extensive permission such as this must also include extensive information. To what courses does the permission relate, to what extent is monitoring conducted for each of the courses and what are the consequences for each course? This places stringent demands in terms of the duty of disclosure. Students cannot give permission until adequate information has been provided. You can also give a brief explanation (in a few sentences) that includes a link to the privacy statement, in which more information can be found. It is not enough to only include a sentence referring to the permission provisions included in the conditions of use, the general terms and conditions or the privacy statements, although you can refer to these documents for explanatory purposes. For more information, see Section Duty of disclosure.

Permission can be withdrawn. As of the moment of withdrawal, no more processing of the data is permitted. Permission can be withdrawn at any time and without giving reasons.

3.2 Execution of contract

If two parties have agreed to a contract, they can process each other's personal data if it is necessary for the proper execution of the contract. They therefore do not have to ask permission separately. For example, a web shop is permitted to give a customer's personal details to a courier to enable delivery of the order. However, permission is required if, for example, the web shop wishes to send newsletters to the customer. This is because the newsletter is not essential to the processing of the order. This principle applies from the moment that the parties begin negotiation of the contract.

In general, education institutions do not enter into contracts with the student. Some regard the student's enrolment at the institution as a contract, but from a strictly legal perspective this is incorrect. Of course, you can conclude contracts with students in which learning analytics are included, for example, a final thesis or work placement.

The data must be essential for the execution of the contract. 'Essential' is a stricter term than 'desirable' or 'useful'. The term 'essential' means that the contract cannot reasonably be executed without using this personal data. The education institution must demonstrate the necessity of learning analytics. As learning analytics is a new instrument, it may easily be viewed as non-essential. The view in such cases is that teaching is perfectly possible without learning analytics. This is a chicken-and-egg problem: you can only present learning analytics as essential once it becomes evident that the teaching is of lesser quality without it. However, this will only be possible once learning analytics has demonstrated its value over a period of several years.

3.3 Legal obligation

The third principle referred to by the Wbp is the legal obligation. Data processing is permitted if it is required by law. Education institutions can argue that they are obliged to provide the best possible education. In order to do so, they need good insight into study performance, and learning analytics is a tool to gain such insight. This argument could be used in order to justify use of the tool.

However, this does involve the same caveats as for Section Execution of contract. You must be able to substantiate why this new tool is truly essential and that a feasible alternative is not/no longer available.

3.4 Execution of government task

Higher-education institutions can be viewed as government institutions. Within the meaning of the Wbp, the provision of education could therefore be classified as a government task. In this case, personal data required for the purposes of that government task can be collected and used. Again, high standards apply regarding the definition of the term 'essential', for which substantiation is required.

3.5 Legitimate interest

The final principle referred to by the Wbp is that of 'legitimate interest'. This principle governs situations in which no permission is asked, the processing of the data is necessary and privacy considerations are taken into account to the maximum possible extent.

The use of this principle is subject to high standards. Camera surveillance is a good example: it is practically impossible to ask every person who enters a building to give their permission, but the need for surveillance and security measures is evident. In such cases, a warning sign and regulations that specify what is done with the footage is sufficient. Furthermore, no camera surveillance is permitted in areas in which privacy is a major consideration (e.g. toilets).

For learning analytics, a case can be made based on this principle. Educational institutions could argue their significant interest in the introduction of learning analytics when no other – less privacy-invasive – solutions are available. However, educational institutions must carefully consider whether serving this interest really outweighs the breach of privacy. Many learning analytics tools go to very great lengths to collect and combine data, which can be viewed as a major breach of privacy. This makes it difficult to demonstrate that the importance of applying the tool outweighs the privacy concerns. An opt-out arrangement for students can be considered a significant mitigating circumstance in this regard.

Scientific and statistical research is not a legal principle

The processing of personal data for scientific or statistical research is not as such justified under the Wbp. You can only collect and process data based on one of the aforementioned five principles. However, subsequently, this data can also be used for scientific and statistical research. Further data processing for statistical or scientific purposes is not considered incompatible with the purpose if the educational institutions have taken the necessary measures to ensure that any further processing only serves these specific purposes.

For example:

A lecturer uses a monitoring tool in order to measure any differences in performance between students resitting examinations and students making their first attempt. Permission is required in order to do this. The results can then be processed for statistical analysis into success factors for that examination. This counts as further processing for research purposes.

4. WHAT PRECONDITIONS APPLY?

The Wbp sets a number of preconditions for all kinds of data processing. The goal of these preconditions is to ensure that the processing of data is fair, transparent and understandable. The most important preconditions are:

- Purpose limitation: You are only permitted to use data for the original purpose.
- Compatibility: You are only permitted to use the data for other purposes if these are compatible with the original purpose.
- Care: You must use personal data with care and be able to substantiate the use.
- Justifiability: You must be able to explain the use of personal data in detail.

Purpose limitation and compatibility

Purpose limitation means that you can only use data for the purpose for which it was collected. If you receive an email address from a person asking a question, then you can send an answer to the question but you cannot send newsletters to the email address, since this is a different purpose than the one for which the email address was provided. Other purposes are permitted if they are compatible with the original goal. For example, you can send a questionnaire about the quality of the helpdesk's service to a person who has made use of the helpdesk.

The purpose must be specific and clearly described, and must clarify what is going to happen. A general purpose description such as 'quality purposes' is not sufficient for the recording of telephone calls. This is because it does not describe what it entails and how the data will be used. A correct formulation would be: 'This conversation is being recorded in order to document exactly what was said in the event of disputes.'

You cannot use data for a purpose that was not stated prior to collection of the data. This makes purpose limitation a difficult requirement for learning analytics to comply with. After all, the idea of learning analytics is to generate new insights, to be able to pose new questions, and to look at the data from new angles. By definition, then, there is no 'specific objective'. For this reason, we advise stating as many purposes as possible in the information provided and to regularly review this information.

Care

Personal data must be processed in compliance with the law and in a careful and proper manner. It is therefore not permitted to collect and process data on people without informing them. 'Secret' analytics are not permitted.

Justifiability

You are only permitted to collect personal data for clearly determined, specifically described and substantiated purposes. Amongst other matters, this entails that you must be able to explain all usage of personal data in detail. Furthermore, the explanation must be available for inspection (see also the information below regarding the duty of disclosure). A legitimate purpose is required for every type of use. Finally, the purpose for which the data is being collected must be known before collection of the data commences.

5. WHAT OBLIGATIONS MUST YOU COMPLY WITH?

When recording students' data in order to improve their learning process, you must comply with certain obligations. You must also take into account the students' rights. This chapter provides more information on these obligations.

5.1 Duty of disclosure

Anyone who processes personal data must clearly inform the person(s) to whom the data applies about what is done with the data and why. The student must receive this information prior to or at the moment that he or she gives permission to process his or her data. Internet services often provide this information by means of a privacy statement. A privacy statement alone is not sufficient: it must be integrated. A privacy statement serves as a supplement to the request for permission or as an explanation if you invoke a principle other than permission, such as execution of contract or inherent urgent necessity.

Content of a privacy statement

In a privacy statement, you explain to students what happens to their personal data. The manner in which you use the data can be divided into categories. In a privacy statement, you should describe (for each category):

- what personal data you will be collecting;
- the way in which you will be collecting this data;
- which institution(s) will have access to it;
- for which purposes the data will be used;
- how this usage will be conducted in practice.

Automated processing

If you will be processing the data automatically, describe in the privacy statement the logic that will be used when processing the data. In the privacy statement, you must also provide the student with explanation of exactly what learning analytics is, what data you will be using for this purpose and in what way the tool will reach its conclusions. For instance: 'We are monitoring how long it takes you to complete the online exercises. If this is significantly longer than average, then you will be given extra explanation and exercises to do before you can complete this module.'

Inspection and agreement

It is important that students have easy access to the privacy statement before their data is processed. Inspection of the information is not mandatory and you do not have to force students to read the privacy statement. It is sufficient to simply provide a link to the privacy statement on the home page, although many institutions include a link to the privacy statement in the footer of every web page.

It is not necessary to make students declare that they agree to the privacy statement (e.g. by ticking a box). If you invoke permission as a principle, then students can give permission by placing a tick beside a sentence. This sentence must clearly state what the student is permitting. For example, it must say something like 'I agree to share my data with the lecturer' and not simply refer to the privacy statement.

5.2 Security obligation

When storing personal data, you must ensure sufficient security measures. This means that you must secure – to a reasonable extent – all stored personal data against unauthorised and unlawful access or usage. You must secure not only all data that you requested, but also any personal data that was unintentionally and unlawful received. We recommend that you establish a policy for security and data leaks.

'To a reasonable extent' means that security does not have to be perfect. Even when you are in full compliance with the law, it is still possible that personal data is abused or appropriated. Naturally, in the event that this happens, you will have to provide an explanation. As of 1 January 2016, it is required by law that any breach of security be reported to the supervisory authority if this breach could result in serious adverse effects to the parties involved. You can find more information on this matter in the section entitled 'Duty of disclosure in the event of data leaks'.

As yet, no generally applicable standard is in place specifically for security of personal data. Specific standards apply within certain sectors (such as NEN 7510 in the healthcare sector). SURF has prepared an information security standards and testing framework based on NEN 27001. See: SURFaudit.

The Dutch privacy watchdog has published guidelines on how organisations and institutions can comply with the security obligation. These guidelines indicate that security must be an integral part of the development and improvement of your services and that you must regularly test (Plan-Do-Check-Act) whether the security is still adequate. You can find more information about the Dutch DPA on Autoriteitengegevens.nl

Liability

When you use the software or services of third parties, the institution itself remains responsible and liable for their security. This also applies in the event that the supplier has limited their liability. In the latter case, it is therefore advisable to refuse this limitation of liability or to extend it to cases in which damage or loss is caused by a breach of privacy. You can find more information on this matter in the section entitled 'Enforcement of the law'.

Data leaks

As of 1 January 2016, the Wbp will include additional provisions with regard to data leaks. Any breach of security or loss of personal data is referred to as a data leak. The term therefore not only applies to large-scale theft of personal data by external hackers: unauthorised access to data is also classified as a data leak.

Duty of disclosure in the event of data leaks

If a data leak occurs, then the institution must report this. However, there is no duty of disclosure in the event that the leaked personal data has been made technically incomprehensible or inaccessible to the hacker. This is the case if the personal data has been secured by means of encryption. However, for this to apply, the encryption must be indecipherable at the moment of the breach. Naturally, in the future, it may become possible to decipher a previously indecipherable encryption, but the law does not require you to take this possibility into account.

In the event of a data leak, you must fulfil two obligations:

1. **Report the leak to the supervisory authority**. Data leaks must be reported to the supervisory authority in the event that serious adverse consequences to the parties concerned are certain or quite likely. In principle, reports to the super visory authority are confidential, although they can be made public if there is cause to do so.

2. **Report the leak to the parties concerned.** You must inform the parties concerned of any data leaks if the leak is likely to have adverse consequences on their personal life.

The supervisory authority's policy on the duty of disclosure in the event of data leaks helps organisations to determine whether there is a data leak they need to report to the supervisory authority and possibly to the parties concerned.

The form made available by the supervisory authority must be used to report a data leak to the supervisory authority. Always notify the party concerned of:

- what kind of a leak it is;
- where the party concerned can obtain more information on the data leak;
- the consequences of the data leak;
- your advice on how to limit the data leak's negative consequences;
- what you have done (and will do) to resolve the leak and restrict its consequences.

5.3 Students' rights

Students have the right to know what personal data their education institution is processing. Students also have the right to have their data corrected or removed, if the data is found to contain factual inaccuracies or is out of date. You can read more about these rights below.

Right of inspection

Students are entitled to submit inspection requests if they wish to know what data an institution has collected about them. In response to such a request, the institution is obliged to provide the complete dossier and all registered data. In principle, the right of inspection also applies to notes and recorded data that are not published online. There is only one situation in which an institution can refuse a request for inspection, which is when a student submits an excessively large number of requests for inspection within a short period. The institution may not refuse inspection based on trade secrets or copyrights of the supplier of the tool, or in the event that it is unclear what the student wishes to do with the data. The institution is entitled to charge a maximum of €5 per request for inspection. It is difficult to satisfy an inspection request if no inspection functionality has been incorporated into the learning analytics tool. We therefore recommend that you ask the provider of your tool to include this functionality.

Right to correction

Students are entitled to request that the institution corrects their personal data in the event of inaccuracies. The right to correction applies only to obvious inaccuracies, such as a spelling mistake in the student's name, an incorrect date of birth or an out-of-date registration. The right to correction also applies to data collected in error or contrary to the law. When students request a correction, they must provide the correct data themselves.

If students are able to correct the data themselves, then they are not entitled to requestthat the institution corrects it for them. Students also cannot compel the institution tocorrect or remove data if it is difficult for the institution to verify the data or if extensive research into the accuracy of the data is required. Other data to which the right to correction is not applicable includes ideas, opinions, research results and conclusions contained in reports, statements or assessments. For example, a student cannot request adjustment of an examination grade by claiming that the assessment was incorrect. The right to correction is rarely exercised with regard to learning analytics. This data is generally indisputable: the student took 23 minutes and 12 seconds to complete the test, the student did/did not read the extra

information, the student watched three of the five videos etc. This more usually relates to the conclusions drawn from the data, but the right to correction does not apply in such cases.

Right of removal

The right of removal applies to all data that is no longer relevant or necessary for the purposes for which it was collected. If aggregated combinations of personal data have been made, then these combinations do not need to be removed following a request for removal. After all, the data contained in these combinations is not classified as personal data. If the personal data is contained in source files for scientific research, then storage of this data is permitted, but only for verification of the research (not for any other research, including any follow-up research to the research in question). If it is technically impossible to remove the data, then the student has the right to protect it so that the data it can no longer be used for any other purpose. For example, this is the case if the data is included in external back-ups. Following the request for removal, your institution is no longer permitted to use the data on such back-ups. The removal of source data for learning analytics is mandatory once the data is no longer processed. Once a course has ended, the data on the students' progress is no longer necessary and storage of the data is no longer permitted. This means that the data must be analysed as soon as possible upon completion of the course. The law does not specify any time frames for this. We do recommend however that in the information you provide prior to data collection or in the privacy statement, you specify the storage periods that your education institution considers reasonable.

6. AUTOMATED DECISION-MAKING

The Wbp prohibits fully automated decision-making or sanctions based on a personality profile. This relates not only to legally binding decisions or legal consequences such as the exclusion of a student; it also relates to every decision that affects the person involved 'to a significant degree'. For example, if you force a student to complete extra assignments based on a personality profile, then this is contrary to the Wbp despite the fact that extra assignments such as these are not legally binding decisions as referred to in the Wbp.

Decision-making within learning analytics

Learning analytics involves automated decision-making from a very early stage. Examples of this include analyses that indicate a student is performing poorly or that students with similar backgrounds rarely complete a particular course at the first attempt. Forcing students to take preparatory courses based on this kind of analysis constitutes a violation of the Wbp.

Requirement of human intervention

Learning analytics software is permitted to draw conclusions and make recommendations based on constructed profiles, but the system is not permitted to make decisions independently. Ultimately, the decisions must always be made by a human. The person making the decision must also substantiate the decision. This substantiation can be based on the recommendations made by the learning analytics tool. For example, a learning analytics tool is permitted to assign a failing grade to a student based on the number of mistakes made. However, the tool is not permitted to make decisions based on (particular aspects of) the student's personality. It is therefore not permitted to automatically declare a student to have committed fraud in the event that he or she suddenly achieves a high grade after years of consistently obtaining failing grades. However, a learning analytics system is permitted to indicate conspicuous improvements such as these, based on which a lecturer may wish to conduct further investigation. The lecturer must subsequently substantiate any decision to exclude the student.

Right to object

Students are always entitled to object in the event that they are affected by a decision or measure taken based on their personality profiles. The right to object must be explicitly stated upon the issuing of the decision/measure. You can offer the student this option after the measure has been implemented if there is time to correct the negative consequences of the measure. The person who receives the objection must subsequently be able to reverse the decision or measure. If assistance from a software provider is required in order to cancel this kind of action made within a tool, then you must make agreements with the supplier in relation to this matter.

7. HOW DO YOU DEAL WITH THIRD-PARTY SERVICES?

For the purposes of learning analytics, education institutions often make use of third-party services, for example by purchasing software, although institutions are increasingly outsourcing services to third parties. Examples of this include cloud-based services for students or external tools that measure performance during tests and then generate reports.

Points for attention

If you make use of third-party software or services, then you must pay attention to two aspects:

1. The institution itself is always responsible for the quality of and problems with the services. This therefore also applies in the event that the software provider does not wish to bear any responsibility. The institution is not permitted to avoid this responsibility by, for example, including a limit of liability in the statement of approval for the learning analytics tool or a disclaimer on the software's opening screen.
2. If the external provider also receives personal data, such as with cloud-based services, the institution must make separate agreements regarding what the provider is permitted to do with this data. This will be recorded in a processor's agreement. This is because the service provider qualifies as a 'processor' of the data under the Wbp. You can find more information on this matter in the section entitled 'Processor's agreement'.

Cloud-based services

For SaaS and cloud-like environments, the provider of the service makes an application available within which the institution or the student can upload data and click on the right buttons. The provider does not actively participate in these data-processing activities. Despite this, the provider of the application is still defined by the Wbp to be the processor, as the processing is done under the provider's management. Does your institution use cloud services? If so, then you are legally obliged to conclude a processor's agreement with the provider.

Processor's agreement

A processor's agreement is an agreement in which one party (the processor) processes personal data upon instruction from the other party (the party responsible). The agreement is mandatory. European providers often have their own model for this agreement. American providers do not have this kind of agreement and may refuse the request to conclude it. They often view the collected data as their property, but this is contrary to the Wbp. Processors are only permitted to process personal data for which they have been commissioned by the party responsible.

Processor's agreements must contain the following elements:

- purposes of processing
- duty of disclosure regarding data leaks
- processor's obligations
- requests by parties concerned
- transfer of personal data
- exemptions
- guarantees
- confidentiality
- security
- duration, extension and cancellation

SURF worked with educational institutions to prepare a Processors Model Agreement as part of the SURF Legal Framework for (Cloud) services. This document sets standards of confidentiality, privacy, ownership and availability for (cloud) providers. The Processors Model Agreement has developed the personal data protection standards further.

8. WHERE ARE YOU PERMITTED TO STORE DATA?

The Wbp is based on European regulations. These European regulations state that you are only permitted to store or process personal data in countries that have an 'adequate' level of data protection. This means that it is only permitted in countries that have regulations that are as strict as those applicable in Europe. These regulations force other countries to adopt regulations relating to personal data. More detailed information can be found in the 'Framework of Legal Standards for Cloud Services in Higher Education'. This document specifies standards for Dutch higher education in the areas of confidentiality, privacy, ownership and availability with respect to cloud providers.

Outside Europe

You are not obliged to store personal data in the Netherlands; storage in any other European country is permitted. Separate rules apply to transfers to so-called third countries outside Europe. Third countries are all non-EU countries plus Norway, Liechtenstein and Iceland.

The main rule for third countries is that an organisation can transfer personal data only if the level of protection is appropriate. The EC has drawn up a List of Third Countries that are considered to provide an appropriate level of protection.

In addition to the abovementioned cases, international transfers are permitted only on the basis of legal exceptions. The Personal Data Authority offers more information on international transfers and FAQ.

Enforcement of the law

As of 1 January 2016, violation of the Wbp is punishable by a fine which can total anything up to €920,000. The supervisory authority is yet to indicate what fines will be allocated to specific violations.

The supervisory authority is only permitted to impose fines once it has issued a binding instruction to the institution that the institution has then failed to comply with. However, if the violation was committed intentionally or arose as a result of serious culpable negligence, the supervisory authority is permitted to impose a fine immediately. The exact definition of serious culpable negligence is not yet clear. If an organisation has no policy regarding data leaks, then this probably constitutes serious culpable negligence. We therefore advise you to carefully establish and enforce a data policy in order to avoid risking a fine.

9. STEP-BY-STEP PLAN

Do you wish to make use of learning analytics? If so, we recommend that you follow these steps:

1.	Determine the purpose for which you wish to use learning analytics and what is required to realise these purposes.
2.	In a separate privacy statement, record the purposes of the learning analytics, what data you will be collecting and what will be done with this data.
3.	Whenever possible, aggregate the data, into combined information no longer showing any specific details of individuals. The aggregation must be irreversible. You should therefore destroy or protect the source data following aggregation.
4	Substantiate which principles the institution wishes to use and why the use of learning analytics must reasonably be deemed essential. If you wish to work with permissions, ensure that: a. the students have access to clear explanations before granting permission; b. the students can refuse permission at that moment without any consequences to them; c. the students can determine from the request for permission exactly what it is they are consenting to; d. the students are able to respond to the request for permission by explicitly granting or declining permission (yes or no).
5	Agree with the provider that the provider will give detailed explanations for you to include in the privacy statement. This is also required for updates to the tool.
6.	Monitor the use of learning analytics data, in any event if it is being used for purposes other than the original purpose. If the data is accessible, then you run the risk of it being used for new purposes.
7.	Ensure that students can easily download and correct learning analytics data.
8.	Investigate which learning analytics tools make automatic decisions that can affect students to a significant degree, and always offer clear opportunities to object to these decisions.
9.	Conclude processor's agreements with the providers of online learning analytics tools.
10.	Establish a policy to prevent data leaks and security breaches.
11.	React positively to students' privacy concerns and objections and ensure that you offer alternatives that can resolve these concerns.

PUBLICATION DETAILS

Authors
Arnoud Engelfriet, ICTRecht
Jocelyn Manderveld, SURFnet
Evelijn Jeunink, SURFnet

Project manager
Jocelyn Manderveld, SURFnet

Final editors
Erik van der Spek, Hendrikx van der Spek

Ontwerp
Vrije Stijl, Utrecht

Photography cover
Flickr

Datum
June 2017

SURFnet

Moreelsepark 48
3511 EP Utrecht

Postbus 19035
3501 DA Utrecht

088 – 787 30 00
www.surf.nl/surfnet