**University Personal Data Protection Policy**

**Status of the Policy**

The policy has been approved by the University xxxx2017 and any breach will be taken seriously and may result in action being taken under the appropriate disciplinary code.

## The General Data Protection Regulation

It is the policy of the University to ensure that University faculty, staff and students are aware of and comply with the requirements of the [General Data Protection Regulation (GDPR)](http://eur-lex.europa.eu/legal-content/EN/TXT/?uri=uriserv:OJ.L_.2016.119.01.0001.01.ENG&toc=OJ:L:2016:119:TOC), national data protection legislation and other relevant legislation in relation to their individual responsibilities. It University’s policy to ensure that compliance with legislation is clear and demonstrable at all times. This policy uses terms defined in the GDPR.

Processing personal data in an ethical manner is part of [research ethics](https://into.aalto.fi/display/endoctoraltaik/Research+Ethics) and [research integrity](http://www.allea.org/wp-content/uploads/2017/03/ALLEA-European-Code-of-Conduct-for-Research-Integrity-2017-1.pdf) (add also Aalto Code of Conduct )

**The University Commitment to Protection of Personal Data**

The University, as the [**controller**](file://C:\Users\rehbinm1\AppData\Local\Microsoft\Windows\Temporary%20Internet%20Files\Content.Outlook\4RRAUFH2\the%20natural%20or%20legal%20person,%20public%20authority,%20agency%20or%20other%20body%20which,%20alone%20or%20jointly%20with%20others,%20determines%20the%20purposes%20and%20means%20of%20the%20processing%20of%20personal%20data;%20where%20the%20purposes%20and%20means%20of%20such%20processing%20are%20determined%20by%20Union%20or%20Member%20State%20law,%20the%20controller%20or%20the%20specific%20criteria%20for%20its%20nomination%20may%20be%20provided%20for%20by%20Union%20or%20Member%20State%20law) is committed to a policy of protecting the rights and freedoms of individuals with respect to the [**processing**](file://C:\Users\rehbinm1\AppData\Local\Microsoft\Windows\Temporary%20Internet%20Files\Content.Outlook\4RRAUFH2\any%20operation%20or%20set%20of%20operations%20which%20is%20performed%20on%20personal%20data%20or%20on%20sets%20of%20personal%20data,%20whether%20or%20not%20by%20automated%20means,%20such%20as%20collection,%20recording,%20organisation,%20structuring,%20storage,%20adaptation%20or%20alteration,%20retrieval,%20consultation,%20use,%20disclosure%20by%20transmission,%20dissemination%20or%20otherwise%20making%20available,%20alignment%20or%20combination,%20restriction,%20erasure%20or%20destruction;) of their [**personal data**.](file://C:\Users\rehbinm1\AppData\Local\Microsoft\Windows\Temporary%20Internet%20Files\Content.Outlook\4RRAUFH2\any%20information%20relating%20to%20an%20identified%20or%20identifiable%20natural%20person%20(‘data%20subject’);%20an%20identifiable%20natural%20person%20is%20one%20who%20can%20be%20identified,%20directly%20or%20indirectly,%20in%20particular%20by%20reference%20to%20an%20identifier%20such%20as%20a%20name,%20an%20identification%20number,%20location%20data,%20an%20online%20identifier%20or%20to%20one%20or%20more%20factors%20specific%20to%20the%20physical,%20physiological,%20genetic,%20mental,%20economic,%20cultural%20or%20social%20identity%20of%20that%20natural%20person;)

As a centre for knowledge, research and education, much of the University’s work involves information and its use. For educational, research and administrative purposes, much of this information will relate to living persons – it is their personal data. The University needs to collect and keep personal data about individuals studying, working or co-operating with university such as employees, students, research participants and alumni.

Personal datamust be processed accordance with this policy and following approved research plans, which set out the purposes and grounds for which the University holds and processes personal data. Any breach of the policy may result in the University, as the controller, being liable in law for the consequences of the breach. This liability may extend to the individual processing the data and his/her Head of Department or Head of Unit under certain circumstances.

This policy applies regardless of where the data is held and, in respect of automatically processed data, the ownership of the equipment used, if the processing is for University purposes.

Any member of staff or student who considers that the Policy has not been followed in respect of personal data about him or herself should raise the matter initially with the University’s Data Protection Officer (who can be contacted ). If the member of staff or student is unhappy with the steps taken by the University to resolve their issue, that individual retains the right to make a complaint to the Tietosuojavaltuutettu.

## Principles Relating to Processing of Personal Data

University faculty, staff and students have to comply with the following GDPR principles in the processing of personal data:

(a) [lawfulness, fairness and transparency](file:///C:\Users\rehbinm1\AppData\Local\Microsoft\Windows\Temporary%20Internet%20Files\Content.Outlook\4RRAUFH2\processed%20lawfully,%20fairly%20and%20in%20a%20transparent%20manner%20in%20relation%20to%20the%20data%20subject)

(b) [purpose limitation](file://C:\Users\rehbinm1\AppData\Local\Microsoft\Windows\Temporary%20Internet%20Files\Content.Outlook\4RRAUFH2\collected%20for%20specified,%20explicit%20and%20legitimate%20purposes%20and%20not%20further%20processed%20in%20a%20manner%20that%20is%20incompatible%20with%20those%20purposes;%20further%20processing%20for%20archiving%20purposes%20in%20the%20public%20interest,%20scientific%20or%20historical%20research%20purposes%20or%20statistical%20purposes%20shall,%20in%20accordance%20with%20Article%2089(1),%20not%20be%20considered%20to%20be%20incompatible%20with%20the%20initial%20purposes)

(c) [data minimization](file:///C:\Users\rehbinm1\AppData\Local\Microsoft\Windows\Temporary%20Internet%20Files\Content.Outlook\4RRAUFH2\adequate,%20relevant%20and%20limited%20to%20what%20is%20necessary%20in%20relation%20to%20the%20purposes%20for%20which%20they%20are%20processed)

(d) [accuracy](file://C:\Users\rehbinm1\AppData\Local\Microsoft\Windows\Temporary%20Internet%20Files\Content.Outlook\4RRAUFH2\accurate%20and,%20where%20necessary,%20kept%20up%20to%20date;%20every%20reasonable%20step%20must%20be%20taken%20to%20ensure%20that%20personal%20data%20that%20are%20inaccurate,%20having%20regard%20to%20the%20purposes%20for%20which%20they%20are%20processed,%20are%20erased%20or%20rectified%20without%20delay)

(e) [storage limitation](file://C:\Users\rehbinm1\AppData\Local\Microsoft\Windows\Temporary%20Internet%20Files\Content.Outlook\4RRAUFH2\kept%20in%20a%20form%20which%20permits%20identification%20of%20data%20subjects%20for%20no%20longer%20than%20is%20necessary%20for%20the%20purposes%20for%20which%20the%20personal%20data%20are%20processed;%20personal%20data%20may%20be%20stored%20for%20longer%20periods%20insofar%20as%20the%20personal%20data%20will%20be%20processed%20solely%20for%20archiving%20purposes%20in%20the%20public%20interest,%20scientific%20or%20historical%20research%20purposes%20or%20statistical%20purposes%20in%20accordance%20with%20Article%2089(1)%20subject%20to%20implementation%20of%20the%20appropriate%20technical%20and%20organisational%20measures%20required%20by%20this%20Regulation%20in%20order%20to%20safeguard%20the%20rights%20and%20freedoms%20of%20the%20data%20subject%20(‘storage%20limitation’);)

(f) [integrity and confidentiality](file://C:\Users\rehbinm1\AppData\Local\Microsoft\Windows\Temporary%20Internet%20Files\Content.Outlook\4RRAUFH2\processed%20in%20a%20manner%20that%20ensures%20appropriate%20security%20of%20the%20personal%20data,%20including%20protection%20against%20unauthorised%20or%20unlawful%20processing%20and%20against%20accidental%20loss,%20destruction%20or%20damage,%20using%20appropriate%20technical%20or%20organisational%20measures)

University requires faculty, staff and students to provide documentation and processes that demonstrate the [accountability](file:///C:\Users\rehbinm1\AppData\Local\Microsoft\Windows\Temporary%20Internet%20Files\Content.Outlook\4RRAUFH2\The%20controller%20shall%20be%20responsible%20for,%20and%20be%20able%20to%20demonstrate%20compliance%20with%20%20%20GDPR%20(‘accountability’) that is, compliance with GDPR principles. As part of this commitment operation of University´s information security management system (ISMS) conforms with the ISO/IEC 27001 international standard.

Faculty, staff and students must ensure that the necessary conditions are satisfied for the processing of personal data and in addition that the extra, more stringent, conditions are satisfied for the [processing of special categories of personal data](file:///C:\Users\rehbinm1\AppData\Local\Microsoft\Windows\Temporary%20Internet%20Files\Content.Outlook\4RRAUFH2\data%20revealing%20racial%20or%20ethnic%20origin,%20political%20opinions,%20religious%20or%20philosophical%20beliefs,%20or%20trade%20union%20membership,%20and%20the%20processing%20of%20genetic%20data,%20biometric%20data%20for%20the%20purpose%20of%20uniquely%20identifying%20a%20natural%20person,%20data%20concerning%20health%20or%20data%20concerning%20a%20natural%20person's%20sex%20life%20or%20sexual%20orientation) ( also called sensitive personal data).

## Privacy by Design

University has adopted the principle of privacy by design and will ensure that the definition and planning of all new or significantly changed systems that collect or process personal data will be subject to due consideration of privacy issues, including the completion of one or more data protection impact assessments.

A research project or other project may also require a data protection impact assessment. The data protection impact assessment is concluded in the ethics self assessment and review process.

The data protection impact assessment includes:

* Consideration of how personal data will be processed and for what purposes
* Assessment of whether the proposed processing of personal data is both necessary and proportionate to the purpose(s)
* Assessment of the risks to individuals in processing the personal data
* What controls are necessary to address the identified risks and demonstrate compliance with legislation

Use of techniques such as data minimization and pseudonymisation are always considered where applicable and appropriate.

**Lawful Processing of Personal Data**

In order to comply with the first principle (lawful processing), the legal base of processing has to be at least one of the following:

|  |  |
| --- | --- |
| (a) | the data subject has given consent to the processing of his or her personal data for one or more specific purposes; |

|  |  |
| --- | --- |
| (b) | processing is necessary for the performance of a contract to which the data subject is party or in order to take steps at the request of the data subject prior to entering into a contract; |

|  |  |
| --- | --- |
| (c) | processing is necessary for compliance with a legal obligation to which the controller is subject; |

|  |  |
| --- | --- |
| (d) | processing is necessary in order to protect the vital interests of the data subject or of another natural person; |

|  |  |
| --- | --- |
| (e) | processing is necessary for the performance of a task carried out in the public interest, such as scientific research, archiving or statistics, or in the exercise of official authority vested in the controller; |

|  |  |
| --- | --- |
| (f) | processing is necessary for the purposes of the legitimate interests pursued by the controller or by a third party, except where such interests are overridden by the interests or fundamental rights and freedoms of the data subject which require protection of personal data, |

In the case of [special categories of personal data](file://C:\Users\rehbinm1\AppData\Local\Microsoft\Windows\Temporary%20Internet%20Files\Content.Outlook\4RRAUFH2\Processing%20of%20personal%20data%20revealing%20racial%20or%20ethnic%20origin,%20political%20opinions,%20religious%20or%20philosophical%20beliefs,%20or%20trade%20union%20membership,%20and%20the%20processing%20of%20genetic%20data,%20biometric%20data%20for%20the%20purpose%20of%20uniquely%20identifying%20a%20natural%20person,%20data%20concerning%20health%20or%20data%20concerning%20a%20natural%20person's%20sex%20life%20or%20sexual%20orientation), which include information about racial or ethnic origins; political beliefs; religious or other beliefs; trade union membership; health; sex life; criminal allegations, proceedings or convictions, there are additional restrictions.

**Addressing Compliance to the GDPR**

The following actions are undertaken to ensure that the University complies at all times with the accountability principle of the GDPR:

* The legal basis for processing personal data is always clear and unambiguous
* A Data Protection Officer carries specific responsibility for data protection in the university
* All faculty, staff and students involved in handling personal data understand their responsibilities for following good data protection practice
* Training in data protection has been provided to all faculty, staff and students
* Routes are available to data subjects wishing to exercise their rights regarding personal data and such enquiries are handled effectively
* Regular reviews of procedures involving personal data are carried out
* Privacy by design is adopted for all new or changed systems and processes
* Records of processing activities are maintained

**Notification of personal data processed by the university**

The University will maintain and use records of personal and sensitive personal data relating to staff and students such as is necessary for its effective operation as an educational organisation and employer. Those who are offered study places or posts of employment at the University will be notified of the standard data kept about them, and the uses to which it may be put, as declared in the University’s notification. All members of staff processing personal data as part of their work for the University are covered by this notification.

Acceptance of a place or post will be understood to signify receiving information of such standard processing of personal data. Students will be formally asked to check the accuracy of their personal data at enrolment each year and can update this data through the student portal. Staff are able to update their HR records at any time through the employee Self-Service online system but will also be formally asked to check the accuracy of the data held about them at least once every two years.

It may be necessary to process sensitive personal data to operate or monitor University policies (e.g. sick pay, equality and diversity) to ensure the University is a safe place to work or study, or to enable the institution to comply with legislation. It is recognised that in some circumstances the processing of such data may be a matter of particular concern to individuals. Accordingly, in respect of sensitive data, staff and students will be made aware of the sensitive nature of the information they are being asked for and may also be asked to give separate consent for the use of this data. The one exception to this would be if a situation occurred where there were concerns for the safety of the individual. In such a situation the Personal Data Protection Act allows sensitive personal data to be processed without referral to the individual in advance.

All staff, students and other persons about whom personal data is held, are entitled to:

* know what data the University holds and processes about them, why it is necessary to process the information and the third parties to whom that data might be given;
* know how to gain access to such data, through a Subject Access Request;
* know that it is up to date;
* know what the University is doing to comply with its obligations under data protection legislation.

The University will therefore provide its staff, students and other relevant users with a standard statement via the University web pages at the following urls:

Staff:

Students:

These statements outline the types of personal data that the University holds and processes as part of its standard procedures, and the reasons for which it is processed. Where, in addition, specific types of data are held on particular groups of students or staff for specific purposes, this will be separately notified on a group or individual basis by the department processing that data.

## Right to access data

Staff, students and other users of the University have the right under the Data Proto access any personal data that is being kept about them either in electronic or manual files. Any person who wishes to exercise this right should complete the University ‘Subject Access Request’ form available from the University’s Data Protection Officer, or from the University webpages at x.

The University will comply with requests for access to personal data as quickly as possible, but will ensure that it is provided within the statutory 40 days time limit.

**Records of University Processing Activities (Tietosuojaselosteet)**

University shall maintain records of processing activities under its responsibility. The records shall contain all of the following information:

|  |  |
| --- | --- |
| (a) | the name and contact details of the controller and, where applicable, the joint controller, the controller's representative and the data protection officer; |

|  |  |
| --- | --- |
| (b) | the purposes of the processing; |

|  |  |
| --- | --- |
| (c) | a description of the categories of data subjects and of the categories of personal data; |

|  |  |
| --- | --- |
| (d) | the categories of recipients to whom the personal data have been or will be disclosed including recipients in third countries or international organisations; |

|  |  |
| --- | --- |
| (e) | where applicable, transfers of personal data to a third country or an international organisation, including the identification of that third country or international organisation and, if applicable, the documentation of suitable safeguards; |

|  |  |
| --- | --- |
| (f) | where applicable, the envisaged time limits for erasure of the different categories of data; |

|  |  |
| --- | --- |
| ( | general description of the technical and organisational security measures  **Responsibilities of Heads of Departments, Heads of Service Units and Principal Investigators**  Heads of Departments and Heads of Service Units have the responsibility to ensure compliance with personal data legislation and this policy within their department or service unit, and to develop and encourage good personal data handling practices, within their areas of responsibility. The University has issued detailed guidance to assist Heads of Departments Service Units to fulfil these obligations.  Principal Investigators have the responsibility to ensure compliance with personal data legislation and this policy within their research projects.  Heads of Department may choose to delegate the management of, but not the responsibility for, Personal Data Protection matters to a departmental Data Protection adviser.  The University will perform periodic audits to ensure compliance with this policy and the legislation and to ensure that the notification is kept up-to-date.  Responsibility for ensuring the University's compliance with this policy and legislation with respect to alumni has been delegated to the Head of Alumni Services. All users holding and using information on alumni must keep Head of Alumni Services informed about all activities involving former students.  **Publication of information about the University**  The julkisuuslaki requires some types of information about the University and the way it is run to be publicly available. This the University does through its publication scheme at url x and by answering tietopyyntö requests made under the julkisuuslaki. Staff who receive a tietopyyntö request should ensure they know how to handle it by reading the guidance for dealing with individual tietopyyntö requests, available at url x  Personal data will not normally be included in a response to an individual request, unless names are given to identify a member of staff as a contact for any particular part of the University’s business, or where the personal data is part of a webpage established by a Department/School or service.  The document x gives an indication, however, of the types of information about staff that might be disclosed if it is warranted as part of a request.  **Responsibilities of Students**  Students must assist the University in ensuring that all their own personal data as provided to the University at registration is accurate and up to date. Students who need to notify the University of any subsequent changes of address etc. can do so via the x address.  **Handling of Personal Data by Students**  The members of the academic faculty are responsible for the conduct in these matters of the students whom they supervise. The use of personal data by students is governed by the following:   * A student should only use personal data for a University-related purpose with the knowledge and express consent of an appropriate member of faculty (normally, for a postgraduate, this would be the supervisor, and for an undergraduate the person responsible for teaching the relevant class/course or the member of faculty responsible for supervising the thesis). * The use of University-notified personal data by students should be limited to the minimum consistent with the achievement of academic objectives. Wherever possible data should be processed after pseudonymisation or anonymized so that students are not able to identify the subjects.   Use of personal data by students is subject to the regulations set out below. The University's policy stated above and the regulations are based on the principle that students must only use personal data under the guidance of a member of faculty. A breach of these regulations is an offence against University discipline.   1. Students must not construct or maintain files of personal data for use in connection with their academic studies/research without the express authority of the appropriate member of faculty. 2. When giving such authority, the member of faculty shall make the student aware of the requirements of this policy, guidelines, codes of conduct and of the appropriate level of security arrangements which attach to the particular set of personal data. 3. Any reporting/publication of thesis based on personal data must be done anonymously unless the subject has agreed in writing to their personal data being used in such a way as to identify them. 4. Students must abide by this policy and personal data legislation and follow the instructions of the University in relation to any uses of personal data notified by the University.  Processing personal data for scientific research purposes It is the goal of University [data policy](http://www.aalto.fi/en/midcom-serveattachmentguid-1e6906dc3789f48906d11e6b03bcddd29b79c379c37/2016_02_10_Aalto_University_datapolicy.pdf) that research data should be FAIR: findable, accessible, interoperable, and reusable. When processing personal data for scientific research purposes, these goals have a specific meaning.  Findable means that research data files have metadata describing the data and the metadata in found in a metadata catalogue. The metadata should be catalogued in a metadata catalogue, the [Aalto University Research](https://research.aalto.fi/en/) portal (ACRIS) is obligatory. For other metadata catalogues, see [the Research Data Management](http://www.aalto.fi/en/research/research_data_management/) pages. Metadata should mention that files do contain personal data and also metadata should document if files contain sensitive data.  Accessible means that it is clearly stated who to contact to get access to data. In case of personal data, it must be clear who are the persons allowed to access the data.  Interoperable means that the datafile formats and metadata are compatible with relevant standards.  Reusable means that there is an appropriate license to reuse the data. In the case of personal data, University goal is to allow for follow-up research while protecting personal privacy. When planning the use of personal data, it is important to consider if the data is required only for a limited use and time.  If optimal reuse of research data requires allowing long-term and follow-up research and if processing of personal data is necessary for the performance of a scientific research carried out in the public interest, then the grounds for processing is [scientific research](file://\\home.org.aalto.fi\rehbinm1\data\Documents\For%20the%20purposes%20of%20this%20Regulation,%20the%20processing%20of%20personal%20data%20for%20scientific%20research%20purposes%20should%20be%20interpreted%20in%20a%20broad%20manner%20including%20for%20example%20technological%20development%20and%20demonstration,%20fundamental%20research,%20applied%20research%20and%20privately%20funded%20research.%20In%20addition,%20it%20should%20take%20into%20account%20the%20Union's%20objective%20under%20Article%20179(1)%20TFEU%20of%20achieving%20a%20European%20Research%20Area.%20Scientific%20research%20purposes%20should%20also%20include%20studies%20conducted%20in%20the%20public%20interest%20in%20the%20area%20of%20public%20health.%20To%20meet%20the%20specificities%20of%20processing%20personal%20data%20for%20scientific%20research%20purposes,%20specific%20conditions%20should%20apply%20in%20particular%20as%20regards%20the%20publication%20or%20otherwise%20disclosure%20of%20personal%20data%20in%20the%20context%20of%20scientific%20research%20purposes.), carried out in the public interest as defined in the GDPR and national legislation, and not consent. Scientific research includes human sciences.  Personal data can be processed for research purposes, even if that was not the original purpose for which the data was collected and for scientific research purposes personal data can be kept indefinitely (contrary to usual practice) so long as the relevant conditions and safeguards are met. The relevant conditions are that the data will not be used to make or support decisions relating to particular individuals nor will it be processed in such a way as to cause damage or distress to the data subject. More about relevan conditions and safeguards : <https://into.aalto.fi/display/enregulations/The+processing+of+personal+data+in+scientific+research>  Here national code of conduct when ready  In most cases Article 6.1 e) scientific research carried out in the public interest, as defined in the GDPR and national legislation, would be the legal ground for processing personal data. University should inform of the possibility of follow-up and long-term research. If data can be made permanently non-identifiable while maintaining its value for research, this should always be done (“data minimization”).  Safeguards such as pseudonymisation are needed for processing of personal data, consent is needed for participation in research projects and data subjects have to be informed. It is important when recruiting participants for research projects, to reassure them that their personal data will be processed in accordance with the General Data Protection Act and that they have a right to see the data that is held about them, unless it has been anonymised so that they can no longer be identified by the data. This information should be given to participants in a durable format so they may refer to it after their participation in the research activity is complete.    Research data containing identifiable personal data can not be released as open data, but anonymized data can be published as open data. Due to the risks of data being re-identified, anonymisation must be done very carefully. Explicitly describe the way any data will be released in your research plan and ethical evaluation. See guidelines on data anonymization : <https://cnpd.public.lu/fr/publications/groupe-art29/wp216_en.pdf>  The service address [researchdata@aalto.fi](mailto:researchdata@aalto.fi) can provide initial advice.  **Ethical evaluation of personal data processing**  Aalto University has established the [Aalto University Research Ethics Committee](https://inside.aalto.fi/display/AboutAalto/Research+Ethics+Committee)  to be responsible for the ex-ante ethical evaluation of  the university´s **non-medical** research projects in human sciences. An ethical evaluation can be implemented if the study’s publication forum, financier or an international cooperation partner requests it. The ethical evaluation must be completed before collecting personal data can start.  Processing of sensitive personal data requires advance scrutiny and evaluation of a research plan in the light of the ethical practices generally followed in that particular discipline of science, with special emphasis on preventing any harm that the research or its results might cause to the research subject. A review applies only to precisely defined research configurations. |
|  |  |

## Rights of Participants in Research Projects

The rights of participants in research projects are related to the purpose and the lawful ground of the processing. The GDPR allows national legislation to include exceptions for the rights of individuals if processing is necessary for the performance of a scientific research.

Information on the rights of participants for those participating in research projects run by University researchers and setting out how the project uses their personal information is included within the relevant participant information sheets, consent forms, web pages or other project-specific documentation that are created and supplied by those running each individual study.

## Rights of Students

Personal data of students is always handled according to

# [Korkeakoulujen opintotietojen tietosuojan kaytannesaannot](https://wiki.eduuni.fi/display/CSCKOOTUKI/Korkeakoulujen+opintotietojen+tietosuojan+kaytannesaannot)

Ohje ammattikorkeakoulujen ja yliopistojen opintohallinnon työn tueksi.

Tietosuojavaltuutetun 2.5.2017 tarkastamat käytännesäännöt (here should be stated the legal grounds for processing of the personal data, as was done for scientific research )

**Automatic Processing of Assessments**

The University has adopted a policy that the outcome of assessments or examinations or should not be determined solely by automatic processing without any human intervention. This condition can be met, for example, by a member of faculty reviewing the outcome of automatic processing, or by an Examination Board reaching the final decision on the result. See more on Guidelines on Automatic individual decision-making and Profiling under the Regulation 2016/679 adopted on 3 October 2017, WP 251

(Explanatory Note: 'Reviewing' the outcome of automatic processing does not mean checking it in detail, but rather implies inspecting the results in order to so as to identify possible errors or anomalies so that these may be investigated further, and as such is consistent with good academic practice.)

## Rights defined in the GDPR

The GDPR defined rights in connection with personal data held about data subjects:

1. The right to be informed
2. The right of access
3. The right to rectification
4. The right to erasure
5. The right to restrict processing
6. The right to data portability
7. The right to object
8. Rights in relation to automated decision making and profiling.

In cases where the legal grounds for processing is necessary for the performance of scientific research or tasks carried out in the public interest, there is national legislation providing exceptions to these rights.

Each of these rights are supported by procedures within University that allow the required action to be taken within the timescales stated in the GDPR.

These timescales are shown in table below.

|  |  |
| --- | --- |
| **Data Subject Request** | **Timescale** |
| The right to be informed | When data is collected (if supplied by data subject) or within one month (if not supplied by data subject) |
| The right of access | One month |
| The right to rectification | One month |
| The right to erasure | Without undue delay |
| The right to restrict processing | Without undue delay |
| The right to data portability | One month |
| The right to object | On receipt of objection |
| Rights in relation to automated decision making and profiling. | Not specified |

*Table 1 - Timescales for data subject requests*

**Transfer of Personal Data**

Special precautions need to be taken when personal data is transferred to countries outside the European Economic Area, that do not provide EU-standard data protection. European Economic Area (EEA), includes all EU countries and in addition, non-EU countries Iceland, Liechtenstein and Norway.

Transfers of personal data outside the European Economic Area must be carefully reviewed prior to the transfer taking place to ensure that they fall within the limits imposed by the GDPR. This depends partly on the European Commission’s judgement as to the adequacy of the safeguards for personal data applicable in the receiving country and this may change over time. Transfer of material outside the European Economic Area includes personal data about an individual placed on the world wide web. It is important that all those preparing web pages are aware of these provisions, and seek advice if in doubt. More information see Data Transfers Outside the EU: <http://ec.europa.eu/justice/data-protection/international-transfers/index_en.htm>

Information on transferring personal data to United States and the measures required:

<https://inside.aalto.fi/pages/viewpage.action?pageId=50234487>

**Data Security**

All University users of personal data must ensure that all personal data they hold is kept securely. They must ensure that it is not disclosed to any unauthorised third party in any form either accidentally or otherwise. More information: <https://inside.aalto.fi/display/ITServices/Information+Security>

## Personal Data Breach Notification

It is University´s policy to be fair and proportionate when considering the actions to be taken to inform affected parties regarding breaches of personal data. In line with the GDPR, where a breach is known to have occurred which is likely to result in a risk to the rights and freedoms of individuals, the relevant Data Protection Authority (DPA) will be informed within 72 hours. This will be managed in accordance with our Information Security Incident Response Procedure <http://www.aalto.fi/fi/about/contact/services/it/ilmoita_tietoturvapoikkeamasta/>

which sets out the overall process of handling information security incidents.

### More information see Guidelines on personal data breach notification under Regulation 2016/679 , Adopted on 3 October 2017 wp 250 <https://ec.europa.eu/newsroom/document.cfm?doc_id=47741>

## Training

It is the responsibility of the University to ensure that staff are aware of the obligations of personal data protection and the university is providing an elearning training module accessible via the University's elearning site (Moodle). This training package also covers topics relating to the freedom of information legislation, records management and information security. The training module is core training and therefore should be taken by all members of staff. The training is accessible via x. The members of staff in the GDPR Task Force are also happy to provide bespoke training sessions for groups / departments - should you wish to

discuss further training requirements please send an email to x and you will be contacted as soon as possible. More information about data protection can be found on the data protection

webpages at x

## Retention of Data

The University is committed to the keeping and disclosing of all personal data in a responsible and secure manner and will therefore keep data for the minimum time necessary to fulfil its purpose.

The University will keep enough data about a student to be able to confirm the qualifications achieved whilst at the University for 80 years from the date that a student graduates or withdraws from the University. Any other data will be removed from student files six

years after the student graduates or otherwise leaves the University. For further details of the retention of student data see sectionStudent and Course Records of the University Retention Schedule.

The University will keep employment history data about former employees for 100 years from the staff member's date of birth in order to verify employment details of former staff. Most other data will be removed a minimum of six years after their employment with the

University has finished, in order to meet data needs for pensions, taxation, potential or current disputes or job references. For further details on the retention of staff details please see section Human Resource Records of the University's Retention Schedule

The University will also keep the health and safety records of accidents that happen to visitors to the University for three years

after the date of the accident.

Personal data that is no longer required will be destroyed in as secure a manner as possible. Paper based records will be put in a confidential waste bin for collection as soon as possible by the secure waste collection. Electronic records will be deleted if hardware such as hard drives, laptops, smart phones etc. are decommissioned. The IS department of the University has a contract with a third party organisation to dispose of

redundant electronic equipment.

**Data Protection Officer**

The University has appointed a data protection officer and communicated this information to the supervisory authority, [The Office of the Data Protection Ombudsman](http://www.tietosuoja.fi/en/). Questions related to this policy and the university´s compliance with the GDPR and other relevant legislation can be dealt with the Data Protection Officer for the University. The Data Protection Officer can be contacted using the email address below.

**Contact details of Data Protection Officer** Email: