Information about data management and privacy policy

Dear Visitor

The University of Sopron is committed to protect your personal data. In accordance with this, we have created our processes in a way that the personal data you have made available for us are properly protected. Based on the General Data Protection Regulation that entered into force on 25 May 2018 the University of Sopron has reconsidered its processes and has integrated the requirements of GDPR into its data management and privacy policies.

You can read about this in more detail in the Privacy Policy Regulation. You can read about your rights in Chapter 8.

Which principles do we follow during data management?

Our university follows the following principles during data management:

- we manage personal data lawfully and respectfully in a way that is transparent for you.
- we collect personal data only for specified, clear and lawful reasons and we do not manage them in ways not compatible with those reasons.
- personal data we collect and manage are appropriate and relevant from the aspect of the data management purpose and are limited to the necessary.
- our university takes every reasonable measure in order to ensure that the data we manage are accurate and up-to-date, when necessary, inaccurate personal data are deleted or corrected immediately.
- we store data in a form that you can only be identified for the duration during which data management purposes are reached.
- we provide the appropriate protection of personal data against unauthorized or illegal managing, accidental loss, destruction or damage by using the proper technical and organizational measures.

Our university manages your personal data

- meaning that we collect, record, classify, store and use your data based on you being preliminarily informed and your voluntary agreement, and only to a necessary extent and in every case purpose-bound.
- in certain cases the management of your data is based on legal regulations and it is compulsory, in such cases we draw your attention to this.
- in certain cases our university or a third party has a legitimate interest in managing your data, for example the operation, improvement and safety of our website.

You have the right to:

- be informed before data management is started,
- get feedback from the data manager whether your personal data are being processed, and if they are, you are entitled to access personal data and further information,
- ask for the correction or deletion of your data and to get notification about the completion of these processes,
- ask for the limitation of data managing and to get notification about the completion of this process,
- have data portability,
- protest if your personal data are used for public interest purposes or for the legitimate interest of the data manager.
- be exempted from automatic decision making including profile creation,
- to make a complaint at the supervisory authority. You may exercise your right at the following contact details: Hungarian National Authority for Data Protection and Freedom of Information, address: 1125 Budapest, Szilágyi Erzsébet fasor 22/c., Telephone: +36 (1) 391-1400; Fax:+36(1)391-1410.,www:http://www.naih.hu e-mail: ugyfelszolgalat@naih.hu
- effective judicial remedy against the supervisory authority,
- effective judicial remedy against the data manager or data processor
- be informed about a personal data breach.

Institution (data manager) data:

Name: University of Sopron

Seat: 9400, Sopron, Bajcsy-Zs. u. 4.

Tax number: 15760346-2-08

Privacy policy officer: Szakály Tamás

Privacy policy officer's contacts: szakaly.tamas@uni-sopron.hu, +3699518731

Data Protection Regulations

- Regulation (EU) 2016/679 (in the following: the Regulation) of the European Parliament and Council, entering into force on 27 April 2016, about privacy policy, free flow of personal data and about repealing Regulation 95/46/EK.
- Statute CXII of 2011 about the right of self-determination of information and information freedom.

Information about the data of the visitors on the University's homepage

When you visit the homepage of the university, one or more cookies – tiny information packages, sent by the server to the browser and then sent back by the browser to the server every time the server receives a request – will be sent to the visitor's computer and thus his/her browser will be identifiable if the visitor of the homepage has agreed to this actively - after receiving clear and unequivocal information – by continuing his/her browsing behaviour.

Cookies operate merely to improve user experiences and to automate the entering process. The cookies used on this homepage do not store information suitable for identifying a person, the university does not do personal data managing in this area.

Registration, newsletter subscription

The legal basis of data managing is registration, in case of a newsletter, it is the agreement of the affected person given by ticking the square next to the words "registration" and "newsletter subscription" after he or she was given information about managing personal data.

Affected people in case of registration, newsletter subscription: every natural person wishing to subscribe to the newsletter of the university or wishing to register on the homepage and agreeing to the managing of his/her personal data.

Data used in case of newsletter subscription: name, e-mail address.

Data used in case of registration: event specific data.

The aim of data managing in case of newsletter subscription: informing affected people about the services, products – and their changes - of the university, about news and events.

The aim of data managing in case of registration: contacting people because of contract preparation, providing free services for the affected on the homepage, access to the non-public content of the webpage, informing people about events needing registration.

Recipients of data (those who can know these data) in case of newsletter subscription, registration: university management, colleagues dealing with customer relationships, colleagues carrying out marketing tasks, data processing colleagues operating the webpage of the university.

The duration of data managing in case of newsletter subscription, registration: in case of newsletter subscription until the person unsubscribes, in case of registration until the affected ask for deletion.

Affected people can unsubscribe a newsletter whenever they want or can ask for the deletion of their registration (personal data). A newsletter can be unsubscribed by clicking on the unsubscribe link in the footer of the emails sent to the affected or by sending a letter to the institution's seat.

Using Google Analytics

This homepage uses Google Analytics application which is the web analysing service of Google Inc. ("Google"). Google Analytics uses so-called "cookies", text files, which are saved on your computer and thus help the analysis of the use of webpages visited by the user.

The information created by cookies in connection with the webpages used by the user usually land on one Google's servers in the USA and are stored there. By activating the IP anonymisation of the webpage, Google shortens the IP address of the user inside EU countries or in other countries included in the agreement about the European Economic Area.

Only in exceptional cases is the complete IP address shortened after being stored on Google's US server. On behalf of the operator of this webpage Google will use this information to evaluate how the user used this homepage and to prepare reports in connection with the activity of the homepage for the webpage's operator, moreover, to provide further services in connection with webpage and internet use.

The IP address forwarded by the browser of the user is not compared with other data of Google in the framework of Google Analytics. The user may prevent the storing of cookies by setting its browser but we warn users that in this case it may happen that not all functions of this homepage will be complete. It may also prevent Google from collecting and processing data created by cookies in connection with the user's webpage use (including the IP address) if the user downloads and installs the browser plugin via the following link. https://tools.google.com/dlpage/gaoptout?hl=hu

The process to be used in case requested by the affected

The university helps the affected to exercise their rights, it cannot deny their request to exercise their rights stated in the present data management and privacy policy, except if it can prove that the affected cannot be identified.

The university informs the affected about the measures that have been taken following their request without unjustified delay but definitely within a month after receiving the request. If necessary – considering the complexity and the number of requests – this deadline can be extended by two months. The data manager informs the affected about the extension of the deadline – with the reasons of this delay enclosed – within a month after receiving the request.
.

If the affected have submitted their request electronically, they should get the information also electronically, except if the affected ask otherwise.

If the university does not take any measures following the request of the affected, it informs the affected about the reasons of the lack of taking measures without unjustified delay but within one months after receiving the request. It also informs the affected that they have the right to make a complaint at the supervisory authority and can exercise their right for legal remedy.

The university provides the following information and measures for the affected, free of charge: feedback about personal data management, access to the data managed, correction, complementation, deletion of data, limitation of data management, data portability, protest against data management and information about data breach.

If the request of the affected is definitely unfounded or – especially if it is repeated – exaggerated, the data manager may charge a fee of 5000 HUF, considering the administrative costs of the requested information or the measure, or may deny taking the measures asked for.

The data manager must prove if a request is definitely unfounded or exaggerated.

If the data manager has grounded doubts about the identity of the natural person submitting a request according to Articles 15-21 of the Regulation, he may ask for more information to confirm the identity of the affected person without breaching Article 11 of the Regulation.

Proceedings in case of personal data breach

A personal data breach – according to the Regulation – is the damage of safety resulting in the accidental or illegal deletion, loss, change, unauthorized publication or unauthorized access to forwarded, stored or otherwise managed personal data.

In case of a personal data breach the privacy policy officer of the university carries out an investigation immediately in order to identify the personal data breach and its possible consequences. The necessary measures must be taken in order to prevent damages.

The privacy policy officer must report a personal data breach to the supervisory authority without unjustified delay, if possible, within 72 hours after learning about the breach except if the breach does not risk the rights and freedom of natural persons. If the breach is not reported within 72 hours, the reason for the delay must be enclosed.

The data processing colleague reports the personal data breach to the data manager without unjustified delay after learning about it.

If all the information cannot be reported at the same time, they may be reported later gradually without unjustified delay.

The data manager keeps records of personal data breaches with the facts - like their effects and measures to solve them - indicated. This register makes it possible for the supervisory authority to check if the requirements of Regulation 33 are met.

Regulations about data safety

The university is only allowed to manage data in accordance with activities recorded in this policy and the Data Protection Regulation and according to the purpose of data managing.

The university looks after the safety of data, commits itself to take all technical and organizational measures that are essential to enforce laws, data- and confidentiality laws, moreover, it creates the proceeding regulations necessary to enforce the above-mentioned laws.

The university protects data against unauthorized access, change, forwarding, publication, deletion or destruction, accidental annihilation and damage and inaccessibility due to technological changes by using proper measures.

The technical and organizational measures to be taken in order to provide data safety by the university are recorded in the privacy policy regulation of the institutions and related IT regulations.

While determining and applying the measures to ensure data safety, the university takes into account prevailing technological developments. If there are several data managing solutions, the institution chooses the solution providing higher level of protection except if it means disproportionate difficulties.