

Data Protection Guide

Valid from 8 June 2023 until withdrawn

The aim of this Guide is to outline that the data processing completed by the Data Controller respects the natural person's privacy and provides the enforcement of constitutional principles and data protection requirements. Furthermore, it provides details concerning the prior Guide for data subjects about the processing of their personal data by the Data Controller and determines the availability of the guidelines regarding data protection.

Name	University of Sopron
Location	4 Bajcsy-Zsilinszky Street 9400 Sopron
Tax number	19253086-2-08
Website	http://uni-sopron.hu/
E-mail	rh@uni-sopron.hu
Telephone number	+36 99 518 142
Legal representative	Prof. Dr. Attila Gábor Fábíán, rector

Location
1-4 Templom Street 9400 Sopron
9 Erzsébet Street 9400 Sopron
4-6 Baross Street 9400 Sopron
5 Ferenczy János Street 9400 Sopron
4 Bajcsy-Zsilinszky Street 9400 Sopron
30/A Várkerület 9600 Sárvár

Aim of Data Protection: Processing of Personal Data for Events	
Process	Registration and identification at an event
Data Subject	Participant at the event
Type of data	Personal data
Personal data	Position, e-mail address, workplace, name, telephone number (landline or mobile), academic degree
Claim	Necessary to the individual's contract
Law	Undefined in law
Storage time	Until the end of the event
Process	Information about the event, maintaining contact, communication

Data subject	Participant at the event
Type of data	Personal data
Personal data	E-mail address, name, telephone number (landline or mobile)
Claim	Necessary to the individual's contract
Law	Undefined in law
Storage time	Until the end of the event
Process	Taking photographs, recording video and audio; the broadcast and future use of these
Data subject	Participant at the event
Type of data	Personal data
Personal data	Portrait
Claim	Data subject consents
Law	Undefined in law
Storage time:	Objection and withdrawal of the consent
Process	Processing of data related to eating habits, allergies, illnesses, drug sensitivity
Data subject	Participant at the event
Type of data	Specific
Personal data	Data on personal health and nutrition
Claim	Specific: the data subject has given explicit consent to the processing of those mentioned personal data for one or more specified purposes, except where Union or Member State law provides that the prohibition referred to in paragraph 1 Chapter 2. Art 9 GDPR may not be lifted by the data subject
Law	Undefined in law
Storage time	Until the end of the event
Process	Sending newsletter for marketing purposes
Data subject	Participant at the event
Type of data	Personal data
Personal data	E-mail address, name
Claim	Data subject consents
Law	Undefined in law
Storage time	Objection and withdrawal of the consent (for a maximum of a year)
Aim of Data Protection: Keeping Accounting Records	

Process	Ensuring compliance with the content requirements of partner and supplier accounting documents
Data subject	Participant at the event
Type of data	Personal data
Personal data	Tax number, address, name
Claim	Legal obligation of the data controller
Law	Section 169 (2) of Act C of 2000 on Accounting (henceforward r: "Accounting Act")
Storage time	for 8 years

The photos taken during the event will be displayed by the University of Sopron as part of the official post-event report on its official website and also on its Facebook page.

Freely Given Consent

The Data Controller also processes the personal data of Data Subjects based on freely given consent. This consent may be withdrawn at any time.

The Opportunity to Alter the Data Processing Guide

The General Guide to Data Processing is available at <http://uni-sopron.hu/> and in 4 Bajcsy-Zsilinszky Street 9400 Sopron. The data controller maintains the unilateral right to alter the present data protection guide in the future.

Definitions

Data Subject is an identifiable natural person; one who can be identified, directly or indirectly by reference to any given personal data.

Consent of the data subject means any freely given, specific, informed indication of the data subject's wishes by which he or she, by a statement or by a clear affirmative action, signifies agreement to the processing of personal data relating to him or her.

Personal data means any information relating to data subjects; such as a name, an identification number, or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural, or social identity of that natural person;

Data Controller means the natural or legal person, public authority, agency, or other body which, alone or jointly with others, determines the purposes and means of the processing of personal data; makes decisions regarding data processing and implements these or has these implemented by the data processor.

Data processing means any operation or set of operations that is performed on personal data or on sets of personal data, whether or not by automated means, such as collection, recording, organisation, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or

combination, restriction, erasure or destruction, recording pictures, sound or photos or any other physical features (fingerprint, palm print, DNS, iris photo) that can identify a person.

Data transmission means making the data accessible for a determined third party

Data processor means a natural or legal person, public authority, agency or other body that processes personal data on behalf of the Data Controller

Data processing means any operation or set of operations that are performed on personal data or on sets of personal data, the completion of technical tasks irrespective of the methods, means and the place of completion.

Disclosure means making the data accessible for anybody.

Data erasure means making the data unrecognisable in a way that makes its restoration impossible.

Computerized Processing means the following operations or set of operations that are performed completely or partly by automated means, such as storage, alteration, logical or arithmetic operations, retrieval, dissemination, erasure, or transmission of data.

System means the set of technical solutions that operate the Data Controller's computerized processing and their partners' online available websites and services. (Henceforward: "System")

Data Processing Principles

Personal data must be obtained and processed fairly and lawfully.

Personal data should only be stored for a specified and legitimate purpose and should not be used in any other way.

The scope of the personal data processed must be proportionate to and compatible with the purpose for which it is stored and must not extend beyond that purpose.

Appropriate security measures should be taken to protect personal data stored in automated data files against accidental or unlawful destruction or accidental loss, and against unlawful access, alteration, or dissemination.

Data transmission

In accordance with the law, the Data Controller is entitled to and obliged to transmit to competent authorities any stored personal data at its disposal. According to law or the final decision of a public authority, the Data Controller is obliged to transmit data in any case where a suspected crime or offence has been committed. The Data Controller shall not be held liable for such transfers or the consequences thereof.

In addition, the Data Controller shall only transfer data to its contractually related co-controllers and/or processors, including only to those who are contractually bound to the Data Subject. Accordingly, the Data Controller shall only transfer data to third parties for the purposes and to

the extent necessary to fulfil the purposes set out in this Guide. Such transfers shall not put the Data Subject at a disadvantage in relation to the data processing and data security rules set out in the text of this Guide in force at the time.

Security of data processing

In accordance with its obligation under Article 32 of the GDPR, the Data Controller shall make every effort to ensure the security of the Data Subject's data, and shall take the necessary technical and organisational measures as well as establish the procedural rules necessary to enforce the GDPR and other data protection and confidentiality rules, taking into account the reasonable expectations of the Data Subject in his/her relationship with the Data Controller, as well as the state of science and technology and the costs associated with the implementation risks and the nature of the personal data to be protected.

The Data Controller processes data via paper and automated means. Where processing is completed by automated means, the processing of any data by human intervention shall be conducted only as an exception and only to the extent necessary and justified.

In particular, the Data Controller shall protect the data against unauthorised access, alteration, disclosure, erasure, destruction, accidental destruction, or accidental damage. Data that are recorded automatically and technically during the operation of the System(s) of the Data Controller shall be stored for a period from the moment they are generated, which is reasonable for the purposes of ensuring the functioning of the System. The Data Controller shall ensure that these automatically recorded data cannot be linked to other personal data, except in cases required by law.

If such a link is established, the employees of the Data Controller's departments responsible for data processing shall handle the personal data they have obtained as business secrets. To this end, the employees of the Data Controller shall also be under a specific obligation and, in the course of their work, shall ensure that unauthorised persons cannot access personal data. Personal data are stored in such a way that they cannot be accessed, retrieved, altered, or destroyed by unauthorised persons.

The Data Controller's Executive Officer, who has decision-making powers at any given time, shall determine the organisation of data protection as well as the tasks and powers relating to data protection and related activities. The Executive Officer shall designate the person responsible for supervising data processing, taking into account the specific characteristics of the Data Controller.

How the data is collected

The Data Controller receives and obtains the Data Subject's data via this Guide through a legal representative, an authorised representative, or from a public source. In all other cases, directly from the Data Subject himself or herself based on voluntary consent and the obligation to perform a contract.

In all cases, the Data Subject is responsible for the accuracy of the personal data provided. The Data Controller does not verify the personal data provided to it.

In compliance with his obligation under Article 14(3) of Chapter III of the GDPR, the Data Controller shall inform the Data Subject of any data that has not been obtained through the Data Subject, using the contact details known, preferably by e-mail, if known, without undue delay, and at the latest within one month, of the following:

- the identity and contact details of the Data Controller and the Data Controller's representative, if any;
- contact details of the Data Protection Officer, if any;
- the purposes for which the personal data are intended to be processed and the legal basis for the processing;
- the categories of personal data;
- the recipients or categories of recipients of the personal data, if any;
- where applicable, the fact that the Data Controller intends to transfer the personal data to a recipient in a third country or to an international organisation and the existence or absence of an adequacy decision by the Commission or, in the case of a transfer referred to in Article 46 of the GDPR, Article 47 of the GDPR or the second subparagraph of Article 49(1) of the GDPR, an indication of the appropriate and suitable safeguards and a reference to the means of obtaining a copy of the personal data or their availability;
- the storage duration of personal data or, where this is not possible, the criteria for determining that duration;
- where the processing is based on Article 6(1)(f) of the GDPR, the legitimate interests of the Data Controller or third party;
- the right of the Data Subject to request the Data Controller access, rectify, erase, or restrict the processing of personal data relating to him or her and to object to the processing of personal data and the Data Subject's right to data portability;
- in the case of processing based on Article 6(1)(a) or Article 9(2)(a) of the GDPR, the right to withdraw consent at any time, without prejudice to the lawfulness of the processing completed on the basis of consent prior to its withdrawal;
- the right to lodge a complaint with a supervisory authority;
- the source of the personal data and, where applicable, whether the data originate from publicly accessible sources;
- the fact of automated decision-making, including profiling, as referred to in Article 22(1) and (4) of the GDPR and, at least in these cases, the logic used and clear information on the significance of such processing and its likely consequences for the Data Subject.

Data processors

The Data Controller does not use a data processor to process data covered in this Guide.

Records of processing activities

The Data Controller maintains records of the processing activities completed under his authority and responsibility. These records shall contain the following information:

- the name and contact details of the Data Controller as well as the name and contact details of the Data Protection Officer;
- the data processing aim;

- a description of the categories of Data Subjects and the categories of personal data;
- the categories of recipients to whom the personal data are or will be disclosed, including recipients in third countries or international organisations;
- where applicable, information concerning the transmission of personal data to a third country or international organisation, including the identification of the third country or international organisation and, in the case of a transmission pursuant to the second subparagraph of Article 49(1) of the GDPR Regulation, a description of the appropriate safeguards;
- where possible, the time limits envisaged for the erasure of the different categories of data;
- where possible, a general description of the technical and organisational measures referred to in Article 32(1).
- The Data Controller shall make the register available to the supervisory authority upon request.

Data Protection Officer

A Data Protection Officer was appointed on 02/02/2021 to address the mandatory case provided for in Article 37 of the GDPR Regulation – regular and systematic large-scale monitoring of data subjects, performance of a public task, processing of sensitive data.

The Data Controller hereby informs the Data Subjects that if the Data Controller notices a procedure, incident, or other circumstance that raises data protection concerns, or that otherwise may be objectionable from a legal and/or technical or organisational perspective, or at least justifies investigation, the Data Protection Officer may be contacted, with the information of the competent employee or manager, but independently of this, at the following contact details:

Name and contact details of the Data Protection Officer: iColl Mérnöki, Tanácsadó és Szolgáltató Kft., 2089 Telki, Ózike street 14. adatvedelem@uni-sopron.hu.

Rights of the Data Subject

Right to notification

The Data Subject must be informed clearly and in detail of all the facts relating to the processing of his or her data before the processing starts.

The Data Subject

- may request information about the processing of his or her personal data;
- request the rectification of his or her personal data;
- request the erasure or restriction of his or her personal data;
- exercise his or her right to data portability;
- object to the processing of their personal data;
- withdraw consent to the processing;
- in the event of a breach of his/her rights, have recourse to the Data Controller, the Data Protection Authority, and the courts.

Right of access

In cases in which data cannot be refused by law, the Data Controller shall, at the Data Subject's request, provide data concerning the following:

- the purposes of the data processing;
- the legal basis for the processing;
- the categories of personal data concerned;
- the names and addresses of any data processors and their activities in relation to the processing;
- the categories of recipients to whom the personal data have been or will be disclosed;
- the duration of the processing;
- the circumstances and effects of a possible data protection incident and the measures taken to deal with it;
- the right to request that the Data Controller rectify, erase, or restrict the processing of personal data as well as the right to object to the processing of such personal data;
- the right to lodge a complaint with a supervisory authority;
- where the personal data have not been collected from the data subject, any available information about their source;
- where applicable, the fact of automated decision-making, including profiling, and, at least in these cases, the logic used and clear information on the significance of such processing and its consequences for the Data Subject;
- where applicable, the transfer of the Data Subject's personal data to a third country.
- The controller shall provide the information in writing in an intelligible form within the shortest possible time from the date of the request, but no later than thirty (30) days.

Right to rectification

At the Data Subject's request, the Data Controller shall adjust incorrect or inaccurate personal data relating to the Data Subject. Taking into account the purposes of the processing, the Data Subject may request the completion of incomplete personal data, including by means of a supplementary declaration. As long as the data cannot be corrected or completed, the Data Controller shall restrict the processing of personal data and temporarily suspend the processing operations, except for storage.

Right to erasure

Upon request, the Data Subject shall have the right to obtain from the Data Controller, without undue delay, the erasure of personal data in cases in which:

- the personal data are no longer necessary for the purposes for which they were collected or otherwise processed;
- the data subject has withdrawn his or her consent and there is no other legal basis for the processing;
- the Data Subject objects to the processing of his or her personal data and the Data Controller has no overriding legitimate grounds for the data processing, or the Data Subject objects to processing for direct marketing purposes;
- the personal data have been unlawfully processed;

- the personal data must be erased in order to comply with a legal obligation under Union or Member State law to which the Data Controller is subject;
- the personal data have been collected directly in connection with the provision of information society services to children, without the consent of the person having parental responsibility.

Where the Data Controller determines that there is an obligation to erase personal data that he has processed, he shall cease processing and destroy the personal data previously processed.

In cases in which the Data Controller has disclosed personal data and is under obligation to erase disclosed data, he shall take reasonable steps and technical measures, taking into account the available technology and the cost of implementation, to inform the controllers of the deletion of links to or copies or duplicates of the personal data in question.

The Data Controller may not erase personal data in cases where processing is deemed necessary

- for the exercise of the right to freedom of expression and information;
- to comply with an obligation under Union or Member State law or to exercise official authority;
- in the interest of public health;
- necessary for archiving purposes in the public interest, scientific, or historical research purposes or statistical purposes, and deletion would make the processing impossible or seriously impair it;
- for the establishment, exercise, or defence of legal claims.

Right to restriction

The Data Controller shall, at the request of the Data Subject, restrict the processing of personal data if

- the Data Subject contests the accuracy of the personal data;
- the processing is unlawful and the Data Subject opposes the erasure of the data and requests the restriction of their use;
- the Data Controller no longer needs the personal data, but the Data Subject requires the data for the establishment, exercise, or defence of legal claims;
- the Data Subject has objected to the processing and the Data Controller is still investigating.

Personal data that are subject to the restriction may be processed, except for storage, only in the following cases:

- with the Data Subject's consent;
- to assert, exercise, or defend legal claims or defend the rights of another natural or legal person,
- important to the public interest of the European Union or of a Member State.

The Data Controller shall inform the Data Subject requesting the restriction prior to lifting the restriction.

Right to data portability

The Data Subject has the right, in the case of voluntary consent, performance of a contract, or automated decision-making, to have the data that he or she has provided to the Data Controller

- provided in a structured, commonly used, machine-readable format;
- transmitted to another Data Controller;
- transmitted it directly to another Data Controller, where technically feasible.

The data subject may not exercise the right of portability where the processing is in the public interest or in the exercise of official authority.

Right to object

Data Subjects have the right to object at any time to the processing of their personal data by the Data Controller based on legitimate interest and profiling, in particular if the personal data is used for direct marketing, public interest, or scientific research purposes.

The Data Controller shall examine the objection within a maximum of thirty (30) days from the date of the request and inform the Data Subject in writing of the decision. The Data Controller shall suspend processing for the duration of the investigation, but for a maximum of five (5) days.

If the Data Subject's objection is deemed justified, the Data Controller shall terminate the processing, including any further collection and transmission of data, block the data, and provide notification of all persons to whom the data have been disclosed and who are obliged to take action to enforce the right to object.

If the Data Subject disagrees with the decision of the Data Controller, he or she has the right to take legal action within thirty (30) days of the notification of the decision or the last day of the time limit.

General notification obligation

The Data Controller shall inform each recipient of any rectification, erasure, objection, or restriction of processing to whom or with which the personal data have been disclosed, unless this proves impossible or involves a disproportionate effort. Upon request, the Data Controller shall inform the Data Subject of such recipients.

Enforcement options

In the event of questions, comments, requests and complaints, the Data Subject may contact the Data Controller in order to assert their rights, in particular at the following contact details:

Sopron University
9400 Sopron, Bajcsy-Zsilinszky Street 4.
+36 99 518 142
rh@uni-sopron.hu

Legal Remedies:

National Authority for Data Protection and Freedom of Information
Headquarters: 1055 Budapest, Falk Miksa utca 9-11.
Address for correspondence: 1363 Budapest, PO Box 9.
Phone: +36 1 391 1400
Fax number: +36 1 391 1410
E-mail: ugyfelszolgalat@naih.hu
Website: <https://www.naih.hu>
Online case start: <https://www.naih.hu/online-uegyinditas.html>

Judicial enforcement

In addition to administrative remedies, you also have the right to take legal action against the Data Controller's activities. The GDPR, the Information law, and the rules of the Civil Code shall apply to the lawsuit. The court of law has jurisdiction to decide on the lawsuit. The lawsuit may also be brought, at the discretion of the Data Subject, before the court of the place of residence of the Data Subject (for a list of courts and their contact details, please consult the following link: <http://birosag.hu/torvenyszekkek>).

This Guide is hereby accepted and entered into force.

Signed, Sopron, 8 June 2023

The University of Sopron

.....
Prof. Dr. Attila Gábor Fábán, Rector
Data Controller



