CHRIS System

User Policy and Data Protection Rules

For Front Office and Back Office Users

v2.0.0

Version history

Date	Version	Description
2023.03.31.	1.0.0	First version of User Policy and Data Protection Rules
2024.01.02.	2.0.0	Second version of User Policy and Data Protection Rules

Table of contents

User Policy

I. Definitions

a) **CHRIS IT System** (hereinafter referred to as 'CHRIS'): the information system for collecting and organizing data for the Second Swiss-Hungarian Cooperation Programme, ie the Cooperation Programme;

b) **National Coordination Unit** (hereinafter referred to as 'NCU'): as defined in the Government Decree 507/2022 (XII. 13.) on the announcement of the framework agreement between the Swiss Federal Council and the Government of Hungary on the implementation of the Second Swiss Contribution to selected member states of the European Union to reduce economic and social disparities within the European Union (hereinafter referred to as 'Gov. Decree 507/2022') the national public entity of Hungary, the Prime Minister's Office of Hungary is designated to act on its behalf for the implementation of the Swiss-Hungarian Cooperation Programme as NCU;

c) **Intermediate Body** (hereinafter referred to as 'IB'): as defined in the Gov. Decree 507/2022 the Intermediate Body of the Swiss-Hungarian Cooperation Programme is Széchenyi Programme Office Consulting and Service Nonprofit Limited Liability Company (hereinafter referred to as 'SZPO'), acting under the responsibility of the NCU. SZPO is designated – among other tasks – to coordinate the development, continuous operation and user right management of the CHRIS system as IB;

d) **Programme Operator**: the organizations specified in the Gov. Decree 507/2022;

e) **Project Operator**: the organizations specified in the Gov. Decree 507/2022;

f) **Executing Agency** (hereinafter referred to as 'EA'): umbrella term for Project Operators and Programme Operators;

g) **CHRIS Office**: SZPO IT System Coordination Unit;

h) **Front Office** (hereinafter referred to as 'FO'): a CHRIS surface for the task of providing a one-channel communication interface between Front Office Users and process-relevant responsible bodies;

i) **Front Office User** (hereinafter referred to as 'FO User'): the user who acts on Support Measure management and financial issues on behalf of the Beneficiary in the CHRIS FO surface;

j) **Back Office** (hereinafter referred to as 'BO'): a CHRIS surface for the tasks carried out by the management and control bodies of the Cooperation Programme;

k) **Back Office User** (hereinafter referred to as 'BO User'): the person in employment or in other employment relationship of the management and control bodies of the Cooperation Programme;

l) **User**: FO User and BO User collectively;

m) **Act**: Act CXII of 2011 on the Right of Informational Self-Determination and on Freedom of Information;

n) **GDPR**: Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation);

o) **Data Protection Rules**: Data protection and data processing regulation, data protection policy and cookie policy;

p) **CHRIS User Manuals**: describing the technical features and steps to follow by the Users related to specific functions, and modules of CHRIS;

q) **User Manual for User Management Tool for CHRIS**: describing the technical features and steps to follow by the User registration.

II. General provisions

1. Purpose of the Policy

The User Policy describes and records the rules, regulations, responsibilities, rights and obligations of natural persons using CHRIS.

2. Scope of the Policy

The scope of the User Policy applies to users with access to the FO or BO, regardless of whether they have been granted access as a natural person or as an agent for an organization.

3. Access to the Policy

The valid copy of the User Policy is available on the login surface of the CHRIS.

4. Reviewing the Policy

The User Policy and the Data Protection Rules shall be reviewed annually by the SZPO, if necessary amended and published.

5. Introducing and accepting the Policy

The CHRIS system cannot be used without the acceptance of the User Policy.
During login, the system requires the user to accept the current version of the User Policy. The acceptance of this fact is clearly stated by the user during the login process by the first time.

III. User access

1. User – user account creation, authorization and user roles

User may be either a private person or as a representative of an organization.

In the CHRIS system, user account creation is governed by a closed one-step workflow. The system validates the uniqueness of username and e-mail address provided, and creates the user account based on the provided data.

By providing the personal data asked, the user accepts the conditions of processing of their personal data in the CHRIS system only in order to gain access (for details see Data Protection Rules).

The FO User acting on behalf of an organization may only register on behalf of the organization holding an official mandate. The SZPO reserves the right to request for the document, in case of its absence the access to CHRIS system may be limited or withheld.

In case of change in the user's personal data, the users themselves can modify their personal data, as described in the User Manual for User Management Tool for CHRIS.

Users can requests user role through a closed workflow in the system, during this process the system does not require additional personal data input, the user is identified by the e-mail address.

There are three (3) different type of user role requests in terms of approval authorization:

- new FO user registrations are automatically granted with applicant role in the CHRIS providing access to the system; there is no need to submit a role request for applicant role;
- the FO user reporting role requests are attended by NCU/IB of the Cooperation Programme;
- the BO user role requests are attended by the CHRIS Office.

The responsibility of granting access to any user (i.e approving a user role request), falls on the user who attends to the request. Therefore, it is utterly important to handle the user approval with the utmost caution and prudenceness. The responsibility of granting application role – as it is automatically granted by the system – falls on the SZPO.

For further technical information, the User is referred to the User Manual for User Management Tool for CHRIS.

2. Password and user authentication management

During the user account creation, the user is asked to provide and confirm a **permanent** password. This password is not visible to the CHRIS system Administrator, it cannot be extracted from the system.

Validity of the user password is 90 days, after password expiry the next login an automatic password change would be requested by the system.

In case of forgotten password request a system generated e-mail would be sent to the provided e-mail address, containing a link to the user account where a new password can be set. *Note that the link is valid for only 10 minutes!*

The User can log in to the CHRIS system by a one-step authentication (i.e. using the matching username and password combination); no other authentication tool (i.e. certificate, QR scanning, etc.) is required.

The User acknowledges and accepts personal responsibility for all activities under the user ID in the system, even if they allowed access to their credentials to a third party and did not perform the specific activity themselves.

The User's attention is drawn to the fact that neither SZPO, the organizations responsible for implementing the Cooperation Programme nor the CHRIS system administrators in any case can ask for the user's password by any sort of communication channel. User's password can only be changed by the User, neither SZPO, the organizations responsible for implementing the Cooperation Programme nor the CHRIS system administrators can be requested to do so.

For further technical information, the user is referred to the User Manual for User Management Tool for CHRIS.

3. Conditions of CHRIS system access and usage

Using the CHRIS system the user is obligated:

a) to respect the secrets of other users, thus searching, alteration or copying of other users' passwords, files, and confidential data is strictly forbidden;
b) to use the CHRIS system only and exclusively for the electronic submission of Support Measure Proposals, Progress Reports, Reimbursement requests;
c) the user is allowed to operate only with their own right; they shall not engage the system on behalf of any other user.

The CHRIS system can be accessed by using any web browser, for best performance refer to the recommended browsers' list in the relevant CHRIS User Manual.

To use the CHRIS system, you must enable javascript running. This feature is available in all supported browsers, however, it can be disabled. Before attempting logging in, make sure that javascript is enabled in your browser.

By using the *https protocol*, it is to ensure that the data transfer is secure between the user's device and the CHRIS system, and the user's data may not be disclosed by a third party. For maximum security, the user should pay attention to the following:

a) always enter the *https://* prefix when entering the path; save the FO/BO in your browser bookmark with this prefix;
b) when the website is opened, the browser cannot display a warning window, if yes, its presumed cause:
    I. using a non-supported browser;
    II. using a web content filter in the network used by the user;
    III. attack attempt.

    If you have a warning window, do not log in. Have your machine checked with your system administrator or IT specialist.

Open the FO/BO search path with caution because you may be misled by a malicious third party. To avoid misuse, check in the top line of the browser before logging in to verify that the link starts with *https://*.

After first sign-up, the acceptance of this User Policy is a condition must be fulfilled for using the system. Upon acceptance, the user can enter to the FO/BO site. It is recommended to read all the documentation, review relevant training materials and CHRIS User Manuals, if necessary, in order to use the application effectively and with due diligence.

The user must use the CHRIS system as intended, as listed in the previous section.

For IT security and data protection reasons, the CHRIS system automatically breaks the connection to the server after 30 minutes of inactivity, resulting in loss of unsaved data.

When using "printscreens" of data, files or downloaded documents from the system, please abide to the following restrictions:

a) the content of the files may be managed by the user, or organization commissioning the user as a business secret; therefore, the user shall act with due diligence when handling their copy;
b) the user may only disclose their personal data or organization data that is entitled to the user's authorization;
c) any copies are considered as information, and the use of legal rights is limited.

Use the logout button to securely leave the CHRIS system, quitting insecurely may lead to misuse user's data.

4. Suspension/deactivation of user account

The user provided data cannot be deleted from the CHRIS system in line with the Data Protection Rules, however user accounts may be blocked, deactivated or suspended in a justified case.

IV. Stored data and method of treatment

1. User-provided data

The user, without limitation, authorizes SZPO and Bodies responsible for the implementation of the Cooperation Programme to use the data and information provided during the implementation of the support measure.

The data provided cannot be used by SZPO and Bodies responsible for implementation of the Cooperation Programme for any business purpose, the data may only be transmitted through a statutory authorization, to a third party authorized by law.

The FO/BO allows the user to upload files of different content and format to the servers during administration. Deleting submitted documents is not possible afterwards to maintain the integrity of the system.

At a specific point in the administrative process, the user may upload files in a specified format but of arbitrary content, however, the user must consider the following:

a) where possible, the uploaded documents should contain only the content and information required for the administrative process;
b) SZPO does not allow the subsequent deletion of submitted files, the uploaded file cannot be undone, cannot be modified or replaced;
c) if the file falls under the copyright or patent right (data, document, music, etc.) then proceed with due diligence when uploading it, the copy and/or transfer right of the author or the copyright holder must be obtained by the user;
d) uploading content that is not organically linked to the application for support is prohibited;
e) each file falls under a virus scan, FO/BO will refuse uploading infected or suspected files.

The user acknowledges that any activity performed by their username will be logged and can be retrieved logically. The collected event logs are retained by SZPO in compliance with the requirements of domestic and international legislation, until the official closing of the relevant Programme.

2. Technical data collected by the CHRIS

The user acknowledges that the computer, browser, Internet address in use are considered to be technical data, and are automatically transmitted to FO/BO in the course of use, due to the technology's operation.

Using the CHRIS system, the user acknowledges that the application places the so-called cookies suitable for tracking in the browser for efficient and user-friendly operation. Cookies are used by the system for technical and non-data collection purposes, the primary purpose of it is to record session status after logging in to make navigation on the surface easier and safer.

Given that these data are typically transmitted together with the data provided by the user, they cannot be separated from them, therefore, the user acknowledges that the retention time of these data is the same as the retention time of the data provided by the user.

V. Prohibited activities

The user is expressly prohibited to look for mistakes in the operation or security of the CHRIS system, to circumvent the operational logic of the CHRIS system, or to attempt to do so.

It is forbidden to log in to the system in any automated manner, or effectuate any action using a bot or any other automated ways.

The IT device used to access the CHRIS system is also the user's responsibility. SZPO takes legal action against the user even if a malicious code or attack is caused by a third party against the CHRIS system through the user's device. It is the user's responsibility to handle the device used to access CHRIS system with the utmost care that can be expected, while respecting the general IT security rules, which includes, but not limited to:

a) installing updates timely and regularly on your device, especially for the browser;
b) the use of an up-to-date antivirus system;
c) use of a local firewall.

VI. SZPO contacts

For technical questions, contact CHRIS Office on the chrissupport@szpi.hu e-mail address. In professional matters, the NCU, EA or IB should be addressed directly. In data protection related issues, contact on the adatvedelmitisztviselo@szechenyiprogramiroda.hu.

VII. User responsibilities

The User is obliged to notify SZPO if experiencing any sort of malfunction of the CHRIS system.
The User must *immediately* notify SZPO (at chrissupport@szpi.hu) in the following cases:

a) receiving any suspicious correspondence requesting on behalf of SZPO, requesting User's access credentials or any information about their user account;
b) if any personal data breach is detected in according to the Data protection and data processing regulation Article (XV);
c) any module or the entire system is inaccessible;
d) the user has access to information that they are not authorized to access during normal use (i.e. information on other than the support measures managed by the user).

The User must not share the information of erroneous functioning with other users or third parties.
Following the notification and investigation of the case, the user will be informed by the SZPO.
A deliberate violation of the User Policy shall result in suspension of the user.
While the case of suspension is being investigated, the user account is blocked, so the user will not be able to access the CHRIS system.
Following the collection and evaluation of evidence, SZPO shall examine whether the act committed is a criminal offense. In case of suspicion of a criminal offense, the necessary measures would be taken governed by law.

Data protection and data processing Regulation

I. Purpose of the regulation

With regard to CHRIS IT system the secure processing of personal data, the application of principles of data processing and the rights of data subjects shall be ensured for which purpose the controller shall implement appropriate technical and organizational measures.
The purpose of the regulation is the controller to comply with the Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation) and the Act CXII of 2011 on information self-determination and freedom of information (hereinafter referred to as 'Info Act').

II. Scope of the regulation

Personal scope: the personal scope of the regulation extends to the controller, the processor on behalf of the controller and all users processing data with regard to the system.

Material scope: the material scope of the regulation extends to the processing on behalf of the controller, the processor and all users processing data – of personal data recorded in the system – wholly or partly by automated means and to the processing other than by automated means of personal data which form part of a filing system or are recorded in the system.

III. Definitions

a) processor: a natural or legal person, public authority, agency or other body which processes personal data on behalf of the controller;

b) processing: any operation or set of operations which 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;

c) controller: a 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; where the purposes and means of such processing are determined by Union or Member State law, the controller or the specific criteria for its nomination may be provided for by Union or Member State law;

d) personal data breach: a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data transmitted, stored or otherwise processed;

e) data subject: identified or identifiable natural person on the basis of any information;

f) recipient: a natural or legal person, public authority, agency or another body, to which the personal data are disclosed, whether a third party or not. However, public authorities which may receive personal data in the framework of a particular inquiry in accordance with Union or Member State law shall not be regarded as recipients; the processing of those data by those public authorities shall be in compliance with the applicable data protection rules according to the purposes of the processing;

g) third party: a natural or legal person, public authority, agency or body other than the data subject, controller, processor and persons who, under the direct authority of the controller or processor, are authorised to process personal data;

h) Authority: National Authority for Data Protection and Freedom of Information;

i) personal data: any information relating to an identified or identifiable natural person ('data subject'); an identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person.

IV. Data protection principles

1. Principle on the protection of fundamental rights

   The protection of natural persons in relation to the processing of personal data is a fundamental right. Article 8 (1) of the Charter of Fundamental Rights of the European Union and Article 16 (1) of the Treaty on the Functioning of the European Union (TFEU) provide that everyone has the right to the protection of personal data concerning him or her.

2. Lawful and fair processing of data and principle of transparency

   Any processing of personal data should be lawful and fair and it should be transparent to natural persons that personal data concerning them are collected. Any processing of personal data is only considered lawful if at least one of the following conditions are met:
   a) the natural person concerned has given consent to the processing of his or her personal data for one or more specific purposes;
   b) the processing of data 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) the processing of data is necessary for compliance with the legal obligation to which the controller is subject;
   d) the processing of personal data should also be regarded to be lawful where it is necessary to protect an interest which is essential for the life of the data subject or that of another natural person;
   e) the processing of personal data for the performance of a task carried out in the public interest 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 particular where the data subject is a child.

3. Principle of purpose limitation

   Personal data is collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes. Further processing for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes shall not be considered to be incompatible with the initial purposes.

4. Principle of data minimization

   Personal data for processing shall be adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed.

5. Principle of accuracy

   Personal data shall be accurate and, where necessary, kept up to date. The controller must take every reasonable step to ensure that personal data are inaccurate, having regard to the purposes for which they are processed, are erased or rectified without delay.

6. Principle of storage limitation

   Personal data shall be kept in a form which permits identification of data subjects for no longer than is necessary for the purposes for which the personal data are processed. Personal data may be stored for longer periods insofar as the personal data will be processed solely for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes subject to implementation of the appropriate technical and organisational measures required by data protection regulations in order to safeguard the rights and freedoms of the data subject.

7. Principle of integrity and confidentiality

   Personal data shall be processed in a manner that ensures appropriate security of the personal data, including protection against unauthorised or unlawful processing and against accidental loss, destruction or damage, using appropriate technical or organisational measures.

8. Principle of data protection by design

   Taking into account the state of the art, the cost of implementation and the nature, scope, context and purposes of processing as well as the risks of varying likelihood and severity for rights and freedoms of natural persons posed by the processing, the controller shall, both at the time of the determination of the means for processing and at the time of the processing itself, implement appropriate technical and organisational measures. These measures are designed to implement data-protection principles, such as data minimisation, in an effective manner and to integrate the necessary safeguards into the processing in order to meet the requirements of this Regulation and protect the rights of data subjects.

9. Principle of liability

   In case of the infringement of data protection regulations – in accordance with the provisions of the relevant regulations – those concerned shall render themselves liable to disciplinary action depending on their administrative, civil and criminal law and user relationship.

10. Principle of monitoring

    The data protection officer on behalf of the controller shall ensure the compliance with the provisions of the relevant regulation and rules and regularly check the application of regulation initiating the amendment of regulation if necessary.

11. Accountability

    The controller shall be responsible for, and be able to demonstrate compliance with the abovementioned principles.

V. Rights of data subjects

1. Principle on rights of information

   The controller shall take appropriate measures to provide any information and any communication relating to processing to the data subject in a concise, transparent, intelligible and easily accessible form, using clear and plain language. The information shall be provided in writing, or by other means, including, where appropriate, by electronic means. When requested by the data subject, the information may be provided orally, provided that the identity of the data subject is proven by other means.

   The controller should communicate to the data subject a personal data breach, without undue delay, where that personal data breach is likely to result in a high risk to the rights and freedoms of the natural person.

2. Right of access by the data subject

   The data subject shall have the right to obtain from the controller confirmation as to whether or not personal data concerning him or her are being processed, and, where that is the case, access to the personal data and the information.

   The data subject shall have the right to access information about the categories of personal data concerned, the purposes and period of processing, the recipients to whom the personal data will be disclosed, and where the personal data are not collected from the data subject, any available information as to their source.

   The controller shall provide a copy of the personal data undergoing processing. For any further copies requested by the data subject, the controller may charge a reasonable fee based on administrative costs. Where the data subject makes the request by electronic means, and unless otherwise requested by the data subject, the information shall be provided in a commonly used electronic form.

3. Right to certification

   The data subject shall have the right to obtain from the controller without undue delay the rectification of inaccurate personal data concerning him or her. Taking into account the purposes of the processing, the data subject shall have the right to have incomplete personal data completed, including by means of providing a supplementary statement.

   The controller shall communicate any rectification of personal data carried out to each recipient to whom the personal data have been disclosed, unless this proves impossible or involves disproportionate effort. The controller shall inform the data subject about those recipients at request.

4. Right to erasure and right to be forgotten

   The data subject shall have the right to obtain from the controller the erasure of personal data concerning him or her without undue delay where one of the following grounds applies:
   a) the personal data are no longer necessary in relation to the purposes for which they were collected or otherwise processed;
   b) the data subject withdraws consent on which the processing is based and where there is no other legal ground for the processing;
   c) the data subject objects to the processing;
   d) the personal data have been unlawfully processed;
   e) the personal data have to be erased for compliance with a legal obligation in Union or Member State law to which the controller is subject;
   f) the personal data have been collected in relation to the offer of information society services.

   The controller shall communicate any erasure of personal data carried out to each recipient to whom the personal data have been disclosed, unless this proves impossible or involves disproportionate effort. The controller shall inform the data subject about those recipients if the data subject requests it.
   Where the controller has made the personal data public and is obliged to erase the personal data, the controller, taking account of available technology and the cost of implementation, shall take reasonable steps, including technical measures, to inform controllers which are processing the personal data that the data subject has requested the erasure by such controllers of any links to, or copy or replication of, those personal data.

5. Right to restriction of processing

   The data subject shall have the right to obtain from the controller restriction of processing where one of the following applies:
   a) the accuracy of the personal data is contested by the data subject, for a period enabling the controller to verify the accuracy of the personal data;
   b) the processing is unlawful and the data subject opposes the erasure of the personal data and requests the restriction of their use instead;

c) the controller no longer needs the personal data for the purposes of the processing, but they are required by the data subject for the establishment, exercise or defence of legal claims;
d) the data subject has objected to processing pending the verification whether the legitimate grounds of the controller override those of the data subject.

Where processing has been restricted, such personal data shall, with the exception of storage, only be processed with the data subject's consent or for the establishment, exercise or defence of legal claims or for the protection of the rights of another natural or legal person or for reasons of important public interest of the Union or of a Member State.

The controller shall communicate any restriction of processing carried out to each recipient to whom the personal data have been disclosed, unless this proves impossible or involves disproportionate effort. The controller shall inform the data subject about those recipients. The controller shall inform the data subject at whose request the restriction was performed about the lifting of restriction beforehand.

6. Right to data portability

The data subject shall have the right to receive the personal data concerning him or her, which he or she has provided to a controller, in a structured, commonly used and machine-readable format and have the right to transmit those data to another controller or – where technically feasible – enquire transmitted directly from one controller to another. The conditions of the above are that the processing is based on consent or on a contract or the processing is carried out by automated means.

The right to data portability shall not apply to processing necessary for the performance of a task carried out in the public interest.

7. Right to object

The data subject shall have the right to object, on grounds relating to his or her particular situation, at any time to processing of personal data concerning him or her, if:
a) processing is necessary for the performance of a task carried out in the public interest or in the exercise of official authority vested in the controller;
b) 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 particular where the data subject is a child.

The controller shall no longer process the personal data unless the controller demonstrates compelling legitimate grounds for the processing which override the interests, rights and freedoms of the data subject or for the establishment, exercise or defence of legal claims.

VI. Submission of data subject request

The data subject shall have the right to submit a request to the data protection officer on behalf of the controller in relation to access, rectification, restriction, erasure, object or data portability.

The data subject submitting a request shall ensure that his or her identity is clearly identifiable and provide the following data in the request:
- surname and first name,
- user name,
- e-mail address.

The controller shall provide information on action taken on a request to the data subject without undue delay and in any event within 30 days of receipt of the request. That period may be extended once by 60 days where necessary, taking into account the complexity and number of the requests. The controller shall inform the data subject of any such extension within 30 days of receipt of the request.

VII. Institutional system of the controller

The Managing Director of the Company assigns the data protection organization, task and responsibilities related to data protection and appoints the person for data protection supervision.

On behalf of the controller the data protection officer shall have the following tasks related to data processing:

a) to inform and advise the controller or the processor and the employees who carry out processing of their obligations pursuant to this Regulation and to other Union or Member State data protection provisions;
b) to monitor compliance with this Regulation, with other Union or Member State data protection provisions and with the policies of the controller or processor in relation to the protection of personal data, including the assignment of responsibilities, awareness-raising and training of staff involved in processing operations, and the related audits;
c) to provide advice where requested as regards the data protection impact assessment and monitor its performance;
d) to cooperate with the Authority;
e) to act as the contact point for the Authority on issues relating to processing, including the prior consultation and to consult, where appropriate, with regard to any other matter;
f) to investigate notifications, in case of unauthorized data processing detected, to call the head of controller to terminate the unauthorized processing and to propose to hold liable the person who breaches lawful data processing
g) to initiate the amendment, modification of the present Regulation if necessary;
h) to keep a data protection record on behalf of the controller;
i) to keep the incident management report (in accordance with the template in Annex 1 of the present Regulation);
j) to cooperate in the organization and management of the data processing and data protection organization system and to take necessary measures to ensure the necessary personal, material and technical conditions for the operation thereof;
k) to introduce the data protection and data security system of the controller.

The controller and processor shall support the data protection officer in performing the tasks related to data protection issues. Any data subject may contact the data protection officer.
The processors of the systems in performing their tasks may appoint a data protection officer.

VIII. Requirements for engaging data processor

1. The processor shall take the proper measures to ensure the compliance with the requirement of data protection law. Taking into account the state of the art, the costs of implementation and the nature, scope, context and purposes of processing as well as the risk of varying likelihood and severity for the rights and freedoms of natural persons, the processor shall implement appropriate technical and organisational measures to ensure a level of security appropriate to the risk, including inter alia as appropriate.

2. The processor shall not engage another processor without prior specific or general written authorisation of the controller. In the case of general written authorisation, the processor shall inform the controller of any intended changes concerning the addition or replacement of other processors, thereby giving the controller the opportunity to object to such changes.

3. Processing by a processor shall be governed by a contract or other legal act under Union or Member State law, that is binding on the processor with regard to the controller and that sets out the subject-matter and duration of the processing, the nature and purpose of the processing, the type of personal data and categories of data subjects and the obligations and rights of the controller.

4. The processor processes the personal data only on documented instructions from the controller, including with regard to transfers of personal data to a third country, unless required to do so by Union or Member State law to which the processor is subject; in such a case, the processor shall inform the controller of that legal requirement before processing, unless that law prohibits such information on important grounds of public interest.

5. The processor ensures that persons authorised to process the personal data have committed themselves to confidentiality or are under an appropriate statutory obligation of confidentiality.

6. The processor taking into account the nature of the processing, assists the controller by appropriate technical and organisational measures, insofar as this is possible, for the fulfilment of the controller's obligation to respond to requests for exercising the data subject's rights.

7. The processor assists the controller in security of data processing, management of incidents and in performing tasks related to data protection impact assessment and prior consultation taking into account the nature of processing and the information available for the processor.

8. The processor at the choice of the controller, deletes or returns all the personal data to the controller after the end of the provision of services relating to processing, and deletes existing copies unless Union or Member State law requires storage of the personal data.

9. The processor shall immediately inform the controller if, in its opinion, an instruction infringes Union or Member State data protection provisions.

10. The processor makes available to the controller all information necessary to demonstrate compliance with the obligations and allow for and contribute to audits, including inspections, conducted by the controller or another auditor mandated by the controller.

IX. Processing of user's personal data

The controller shall process the user's personal data in system access, establishment and termination of rights to use and the use of system (working and data recording in the systems) in accordance with data protection principles. The controller is obliged to inform the user about the above and further data management purposes.

In order to establish his / her rights, the user may only be required to make a statement or provide information that does not infringe his / her rights and is relevant to the establishment, termination or proper use of the user rights. In order to set the rights required to use the systems and to operate the user register, the user concerned shall provide data directly or, where appropriate, with the assistance of user support colleagues. The data subject is obliged to report the change in the data scope of the user register immediately in writing.

The user's access rights must be established to the extent necessary to perform their legal relationship, their responsibilities and the data processing activities they may perform in the systems.

The beneficiary submitting payment application guarantees that the personal data of additional partners (other persons acting on behalf and for the benefit of the Beneficiary and any consortium partners, suppliers, owners and final beneficiaries of the support measures) listed in the data sheets submitted in the payment application and support measure implementation documents and their annexes is processed by the beneficiary and transferred to the supporting institutional system on an appropriate legal basis and after appropriate information has been provided to the data subjects.

The user must be informed in a documented manner of the following before obtaining his or her consent to data processing:

a) the name and contact details of the controller and, where applicable, the name and contact details of the controller's representative;
b) the name and contact details of the data protection officer;
c) the purpose, legal basis and envisaged duration of personal data processing;
d) the recipients to whom the personal data have been or will be disclosed;
e) the enforcement possibilities related to data processing;
f) the available legal remedies;
g) the legitimate interests of the controller and the third party, provided that they are the legal basis of the data processing;
h) the right to consent in the case of consent-based data processing;

i) whether the provision of personal data is a statutory or contractual requirement, or a requirement necessary to enter into a contract, as well as whether the data subject is obliged to provide the personal data and of the possible consequences of failure to provide such data.

The controller ensures the users to access the personal data processed about him or her electronically.

X. Security of processing

The controller ensures the security of data related to the records in the system. The controller takes the technical and organizational measures and develops rules of procedures that are necessary to comply with the relevant data security, data and confidentiality rules.

The controller takes measures to ensure the appropriate level of security in particular of the risks that are presented by processing, in particular from accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to personal data transmitted, stored or inaccessibility due to alteration in the technique used.

The controller provides the relevant documents to ensure the application of data and information security rules.

The controller shall, both at the time of the determination of the means for processing and at the time of the processing itself, implement appropriate technical and organisational measures taking into account the state of art. The controller shall ensure several possible data protection and data security solutions that provide a higher level of protection unless this involves disproportionate effort.

The tasks of the controller related to IT protection involves in particular:

a) measures taken to protect against unauthorized access, involving the protection of software and hardware instruments and physical protection;
b) revision of the access rights of users;
c) possible measures taken to default set of data files, involving the regular backup and the separate, secure handling of copies;
d) protection of data files against viruses;
e) physical protection of data files and data carriers, involving protection against fire, water damage, lightning or other elemental damage, and the recovery of damage resulting from such events.

Those persons covered by the current Regulation shall ensure the safe storage of the data carriers and external records used by or held by them containing personal data from the system – regardless the method of recording – against unauthorized access to, transmission, disclosure of, alteration, deletion, accidental or unlawful destruction and damage.

XI. Transfers of personal data

When transferring personal data, the legal basis for data processing must be ascertained in all cases, in case of doubt, the assistance of a legal expert should be sought. Personal data may be transferred only if the legal basis is clear and the purpose and recipient is clearly defined. The transfer shall be recorded in such way that the process and legality thereof is evident.

A transfer of personal data required by law and based on a contractual obligation shall be performed by the controller. Personal data may be transferred by the legitimate interest based on a substantiated balance of interests of the controller or if the data subject unambiguously consents thereto. The consent can be demonstrated only if documented. In the case of the personal data transfer related to consent the statement of data subject is provided with the acknowledgement of the recipient and purpose thereof.

The systems record transfers and the controller records transfers from the system in order to determine to whom on what legal basis and purpose the personal data are transferred to.

The personal data transfer to a third country based on GDPR Article 45 Section (3)[1].

XII. Verification

The compliance with legal provisions and internal regulatory documents must be continuously verified by the data controller. The data protection officer performs general and target verification.

The verification shall assess in particular:

a) the up-to-datedness of users' access and access rights;
b) from time to time change of passwords;
c) compliance with the present Regulation and the provisions of IT security regulations.

In case an official authority conducted a verification mission in the period of which the above were subject, the verification obligation for the given item shall be considered fulfilled in the given period.

The authorized regarding the purpose of verification may request information from data controllers and may have an insight in data processing which is related to the verified data processing activity.

The Authority is entitled to check compliance with data protection rules at the data controller and to investigate the content in the notification received.

Without prejudice to any other administrative or judicial remedy, every data subject shall have the right to lodge a complaint with a supervisory authority, if the data subject considers that the processing of personal data relating to him or her infringes the provisions of data protection regulations.

Without prejudice to any other administrative or non-judicial remedy, each data subject shall have the right to an effective judicial remedy against a legally binding decision of the Authority concerning them.

Without prejudice to any available administrative or non-judicial remedy, - including the right to lodge a complaint with the Authority – the data subject shall have the right to an effective judicial remedy where he or she considers that his or her rights laid down in provisions adopted have been infringed as a result of the processing of his or her personal data in non-compliance with the provisions of data protection regulations.

The controller shall cooperate with the Authority and comply with the Authority's request within a time limit set by the Authority and in case of disagreement with the findings shall take the appropriate steps set out in data protection legislation.

Contact details of the Authority:

Postal address: 1363 Budapest, Pf. 9.
Address: 1055 Budapest, Falk Miksa utca 9-11.
Telephone: +36-1-391-1400
Fax: +36-1-391-1410
Website: www.naih.hu
E-mail: ugyfelszolgalat@naih.hu

XIII. Data processing register

Each controller shall maintain a record of processing activities under its responsibility. Each processor shall maintain a record of all categories of processing activities carried out on behalf of a controller. The records shall be in writing, including in electronic form.

[1] 2000/518/EC: Commission Decision of 26 July 2000 pursuant to Directive 95/46/EC of the European Parliament and of the Council on the adequate protection of personal data provided in Switzerland (notified under document number C(2000) 2304) (Text with EEA relevance.)

The purpose of the internal data processing register is to demonstrate which data processing the data subject may be affected by and what the elements of these processing are. The data processing register identifies data processing however, it does not replace the detailed information of the data subject. The data processing register shall be kept by the data protection officer.

In order to keep the data processing register up to date, the data controller shall review its content at least annually.

XIV. Data protection impact assessment, prior consultation

Where a type of processing in particular using new technologies, and taking into account the nature, scope, context and purposes of the processing, is likely to result in a high risk to the rights and freedoms of natural persons, the controller shall, prior to the processing, carry out an assessment of the impact of the envisaged processing operations on the protection of personal data.

A data protection impact assessment shall in particular be required in the case of:

a) a systematic and extensive evaluation of personal aspects relating to natural persons which is based on automated processing, including profiling, and on which decisions are based that produce legal effects concerning the natural person or similarly significantly affect the natural person;
b) data processing for special categories of personal data;
c) a systematic monitoring of a publicly accessible area on a large scale
d) processing large amounts of data;
e) matching or merging data sets;
f) data processing of vulnerable data subjects;
g) innovative use and application of new technological or organizational solutions;
h) the processing may prevent the data subjects from exercising their rights, using services or enforcing a contract.

The guidance available on the Authority website shall be taken into account in the process of impact assessment.

The controller shall consult the Authority prior to processing where a data protection impact assessment indicates that the processing would result in a high risk in the absence of measures taken by the controller to mitigate the risk.

XV. Incident management procedure

Personal data breach means a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data transmitted, stored or otherwise processed. The controller shall implement appropriate technical and organizational measures to prevent and effectively manage data protection incidents including incident detection, detection and resolution, documentation and relevant notifications.

In the case of a personal data breach, the controller shall without undue delay and, where feasible, not later than 72 hours after having become aware of it, notify the personal data breach to the Authority, unless the personal data breach is unlikely to result in a risk to the rights and freedoms of natural persons. Where the notification to the supervisory Authority is not made within 72 hours, it shall be accompanied by reasons for the delay.
Where the personal data breach is likely to result in a risk to the rights and freedoms of natural persons, the controller shall communicate the personal data breach to the data subject without undue delay.

In case a user becomes aware of
a) the occurrence of data protection incident;
b) an event or security incident occurred that raises the possibility of a data protection incident

the controller shall be informed without delay via the e-mail address adatvedelmitisztviselo@szechenyiprogramiroda.hu. Any notification sent to other e-mail addresses of the Company shall not be considered as notification on data protection incident.

The data protection incident may be reported in English or Hungarian.

The notification is examined by the controller according to the following criteria:

a) the existence of information security incident,
b) personal data concerned.

The data protection officer of the controller shall inform the controller and the members of the data protection incident management committee of his/her position on the notification.

The members of the data protection incident management committee are:

a) data protection officer,
b) the heads of the professional and methodological departments concerned by the notification.

Replacement is possible in the absence or impediment of a member of the data protection incident management committee.

The data protection officer may request measures and information relating to the detection of an incident from the members of the data protection incident management committee and, where appropriate, from the data processors employed by the controller.

The members of the data protection incident management committee shall assess the details of the notification on the basis of the information available and taking into account the methodological recommendations published on the Authority's website and:

a) establish, where possible, the actual occurrence of the incident;
b) assess the personal rights risks of the incident, if possible;
c) formulate the organizational and technical measures necessary to deal with the incident;
d) take measures to detect the occurrence of the incident if the existence of the incident is not clear.

The members of the data protection incident management committee shall prepare a summary report on the notification, including a proposal for a decision. The data protection incident management committee's decision proposals include informing the Authority and data subjects.

The proposed decision to notify the Authority may be:

a) full notification provided to the Authority;
b) notification to the Authority is not required;
c) partial notification to the Authority if an incident has occurred but all information necessary to inform the Authority is not available within 72 hours;
d) full notification to the Authority of the delay and the reason for the delay if an incident has occurred but all the information necessary to inform the Authority is not available within 72 hours.

The proposed decision to notify the data subjects may be:

a) notification to data subjects is required;
b) notification to data subjects is not required.

Proposals for decisions must be made within 48 hours of notification. If, on the basis of the report, the occurrence of the data protection incident cannot be clarified, an investigation must be carried out immediately to identify it, and a proposal can be made within 48 hours after the identification of the incident.
On the basis of the proposals of the data protection incident management committee, the data protection officer shall prepare a summary report containing the proposals of each committee member as well as the position of the committee.

Based on the summary report, the representative of the data controller shall, within 60 hours of the notification or identification of the incident:

a) approve the overall proposal of the data protection incident management committee;
b) take a different decision with regard to the notification and the information of the data subjects concerned, giving reasons.

At the discretion of the controller’s representative, the data protection officer shall take the necessary measures with regard to the information.

If an investigation has led to an actual incident, the data protection officer shall record its details as set out in Annex 1.

XVI. Right to compensation and damages

Any person who has suffered material or non-material damage as a result of an infringement of data protection regulations shall have the right to receive compensation from the controller or processor for the damage suffered in accordance with relevant legislation.

If the controller violates the data subject's right to privacy by unlawfully processing the data subject's data or by violating data security requirements, the data subject may claim damages from the controller.

Against the data subject, the controller is liable for the damage caused by the processor and the controller is also obliged to pay the data subject damages in the event of a personal data breach caused by the processor. The processor shall only be liable for damages caused by the data processing if he or she has not complied with the obligations specified in the data protection legislation, which are specifically imposed on the processors, or if he or she has disregarded or acted contrary to the controller's lawful instructions.

The controller or processor shall be released from liability if he or she proves that he or she is not liable in any way for the event giving rise to the damage.

No damages shall be payable and no damages shall be claimed if the damage was caused by the intentional or grossly negligent conduct of the injured party or the breach of the right to privacy.

Annex 1

INCIDENT MANAGEMENT RECORDS

serial number of incident	date and circumstances of incident	subject of the incident	the range and number of 'data subject'	the potential consequences of the incident	measures taken to deal with the incident	classification of risk	date of notification to the Authority	date of notification to the 'data subject'	other relevant information

Data protection and data processing policy

The purpose of the present data protection and data processing policy (hereinafter referred to as 'Policy') is to define data protection and data processing principles related to the data recorded in the CHRIS IT System (hereinafter referred to as 'CHRIS') operated by the Széchenyi Program Office Consulting and Service Non-Profit Limited Liability Company (hereinafter referred to as 'Data Controller' or 'Company') and therefore, the data subject will be provided with adequate information of data processed by the Company based on the General Data Protection Regulation.

Acts and their abbreviations used and considered in relation to the Policy

Act	Act CXII of 2011 on the Right of Informational Self-Determination and on Freedom of Information
GDPR	Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation)
197/2018 Gov. Decree	Government Decree 197/2018 (X. 24.) on Széchenyi Program Office Consulting and Service Nonprofit Limited Liability Company
507/2022 Gov. Decree	Government Decree 507/2022 (XII. 13.) on the announcement of the framework agreement between the Swiss Federal Council and the Government of Hungary on the implementation of the Second Swiss Contribution to selected member states of the European Union to reduce economic and social disparities within the European Union
563/2022 Gov. Decree	Government Decree 563/2022 (XII. 23.) on implementation of the Second Swiss-Hungarian Cooperation Programme

I. Definitions

Definitions in the present Policy meet definitions of Article 4 of GDPR:

personal data	any information relating to an identified or identifiable natural person ('data subject'); an identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person
processing	any operation or set of operations which 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
controller	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; where the purposes and means of such processing are determined by Union or Member State law, the controller or the specific criteria for its nomination may be provided for by Union or Member State law
processor	a natural or legal person, public authority, agency or other body which processes personal data on behalf of the controller

third party	a natural or legal person, public authority, agency or body other than the data subject, controller, processor and persons who, under the direct authority of the controller or processor, are authorised to process personal data
recipient	a natural or legal person, public authority, agency or another body, to which the personal data are disclosed, whether a third party or not. However, public authorities which may receive personal data in the framework of a particular inquiry in accordance with Union or Member State law shall not be regarded as recipients; the processing of those data by those public authorities shall be in compliance with the applicable data protection rules according to the purposes of the processing
personal data breach	a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data transmitted, stored or otherwise processed
supervisory authority	means an independent public authority which is established by a Member State pursuant to Article 51

Where definitions of GDPR in force are different from the definitions of the present Policy, definitions of GDPR in force shall prevail.

II. Data controller and contact details

name:	**Széchenyi Programme Office Consulting and Service Nonprofit Limited Liability Company**
registered office:	1053 Budapest, Szép utca 2. 4. em.
company reg. no:	01 09 916308
represented by:	Mr. Áron Szakács (managing director)
e-mail:	info@szechenyiprogramiroda.hu

III. Data processor

The developer of CHRIS can only process personal data in extraordinary cases, in case of a special authorization procedure.

name:	**R&R Software Zrt.**
registered office:	1038 Budapest, Ráby M. u. 8.
represented by:	Mr. Csaba Rozenberszki
e-mail:	info@rrsoftware.hu

IV. Data protection officer and contact details

Data protection officer designated by the Company:

name:	Ms. Réka Selmeczi dr.
postal address:	1053 Budapest, Szép utca 2. 4. em.
e-mail:	adatvédelmitisztviselő@szpi.hu

V. Personal data, purpose of processing, legal basis for processing, period of processing

Back office users (employees of the Company) related:

personal data	purpose of processing	legal basis for processing	means of processing	period of processing
surname and first name of the user	user identification	GDPR Article 6 (1) (b)	electronic	duration specified by the European Union / time to maintain the system
user name	user identification	GDPR Article 6 (1) (b)	electronic	duration specified by the European Union / time to maintain the system
e-mail address of the user	contact with the user	GDPR Article 6 (1) (b)	electronic	duration specified by the European Union / time to maintain the system
phone number of the user	contact with the user	GDPR Article 6 (1) (b)	electronic	duration specified by the European Union / time to maintain the system
postal address of the user	contact with the user	GDPR Article 6 (1) (b)	electronic	Duration specified by the European Union / time to maintain the system

Back office users (employees of the other institutions of the Cooperation Programme) related:

personal data	purpose of processing	legal basis for processing	means of processing	period of processing
surname and first name of the user	user identification	GDPR Article 6 (1) (e)	electronic	duration specified by the European Union / time to maintain the system
user name	user identification	GDPR Article 6 (1) (e)	electronic	duration specified by the European Union / time to maintain the system
e-mail address of the user	contact with the user	GDPR Article 6 (1) (e)	electronic	specified by the European Union / time to maintain the system
phone number of the user	contact with the user	GDPR Article 6 (1) (e)	electronic	duration specified by the European Union / time to maintain the system
postal address of the user	contact with the user	GDPR Article 6 (1) (e)	electronic	duration specified by the European Union / time to maintain the system

Front office users related:

personal data	purpose of processing	legal basis for processing	means of processing	period of processing
surname and first name of the user	user identification	GDPR Article 6 (1) (e)	electronic	duration specified by the European Union /

				time to maintain the system
user name	user identification	GDPR Article 6 (1) (e)	electronic	duration specified by the European Union / time to maintain the system
e-mail address of the user	contact with the user	GDPR Article 6 (1) (e)	electronic	specified by the European Union / time to maintain the system
phone number of the user	contact with the user	GDPR Article 6 (1) (e)	electronic	duration specified by the European Union / time to maintain the system
postal address of the user	contact with the user	GDPR Article 6 (1) (e)	electronic	duration specified by the European Union / time to maintain the system
during the applications, implementation of support measures, personal data required for the identification of the beneficiaries and verification of expenditures	identification of beneficiaries, control of eligibility of costs	GDPR Article 6 (1) (e)	electronic	duration specified by the European Union / time to maintain the system

The personal data transfer to a third country based on GDPR Article 45 Section (3)[2].

VI. Principles

The Company processes personal data in accordance with principles of good faith and fair dealing and transparency and subject to law in force and provisions of the present Policy.

The Company processes personal data only on the basis of the present Policy and for a specific purpose(s) and does not go beyond them.

If the Company intends to use personal data for purpose(s) other than the original purpose(s), the Company informs the data subject of such a purpose and use and obtain the previous and express consent of the data subject (where there is no other legal basis determined by GDPR) and the Company allows the opportunity to defy the use of personal data.

The Company does not control personal data provided, person who provided the personal data, shall be liable for adequacy.

The Company does not transfer personal data, except that the Company is entitled and obliged to transfer or forward personal data available to and properly stored by the Company to competent authority where transfer and forward of personal data is determined by law or legally binding order of authority. Company shall not be liable for such a transfer or its consequences.

The Company ensures the security of personal data, takes all technical and organizational measures and establishes rules of procedure that guarantee protection of recorded, stored and

[2] 2000/518/EC: Commission Decision of 26 July 2000 pursuant to Directive 95/46/EC of the European Parliament and of the Council on the adequate protection of personal data provided in Switzerland (notified under document number C(2000) 2304) (Text with EEA relevance.)

processed personal data, and prevent accidental losses, destruction, unauthorised access, unauthorised use, unauthorised alteration and unauthorised dissemination.

VII. Rights of the data subject

The data subject may exercise right in the following ways:

- e-mail
- by post
- in person

➢ *Right of information and access personal data*

The data subject may at any time request the Company to provide information on data processed by the Company or the data processor involved by or according to the order of the Company, purpose of the processing, legal basis for the processing, period of processing, name and address of data processor, activity of data processor related to data processing, the circumstances, effect of a personal data breach, measures taken for averting personal data breach, furthermore, where personal data is transferred the legal basis for and recipient of transfer of personal data.

In relation to the above, the data subject may request a copy of his/her processed data. In case of an electronic request the Company executes the request first electronically (PDF format), except where the data subject requests expressly otherwise.
The Company already draws attention to the fact that if the above right of access affects adversely the rights or freedoms of others, including in particular trade secrets or intellectual properly, the Company may refuse the execution of the request, to the extent it is necessary and proportionate.

➢ *Right to rectification and modification*

The data subject may request the rectification, modification and completion of personal data processed by the Company.

➢ *Right to data portability*

The data subject has the right to receive the personal data concerning him or her, which he or she has provided to the Company, in a structured, commonly used and machine-readable format and has the right to transmit those data to another controller without hindrance from the Company.
Furthermore, the data subject has the right to have the personal data transmitted directly from one controller to another, where technically feasible.

➢ *Right to erasure ('right to be forgotten')*

The data subject may request the erasure of one or all personal data concerning him or her.

In this case, the Company erasures the personal data without undue delay and the controller shall have the obligation to erase personal data without undue delay where one of the following grounds applies:

- the personal data are no longer necessary in relation to the purposes for which they were collected or otherwise processed;
- the data subject withdraws consent on which the processing is based and where there is no other legal ground for the processing;
- data processing is based on legitimate interest of the Company or third person but the data subject objects to the processing and (except objection to processing related to direct marketing) there are no overriding legitimate grounds for the processing;
- the personal data have been unlawfully processed;
- the personal data have to be erased for compliance with a legal obligation.

The Company informs the data subject of the refusal to the request of erasure in any event (e.g. data processing is required for the establishment, exercise or defence of legal claims), indicating the

reason of the refusal. Erasure of personal data is executed that after fulfilment of request of erasure personal data (erasured) cannot be restored.

In addition to the exercise of right to erasure, the Company erases personal data if the data processing is unlawfully, the purpose of data processing is no longer exists, data storage period determined by law is already expired, it is ordered by court or authority.

➢ *Right to restriction of processing*

The data subject shall have the right to obtain from the controller restriction of processing where one of the following applies:

- the accuracy of the personal data is contested by the data subject, for a period enabling the Company to verify the accuracy of the personal data;
- the processing is unlawful and the data subject opposes the erasure of the personal data and requests the restriction of their use instead;
- the Company no longer needs the personal data for the purposes of the processing, but they are required by the data subject for the establishment, exercise or defence of legal claims;
- the data subject has objected to processing pending the verification whether the legitimate grounds of the Company override those of the data subject.

Where processing has been restricted, such personal data will not be processed or will, with the exception of storage, only be processed with the data subject's consent or for the establishment, exercise or defence of legal claims or for the protection of the rights of another natural or legal person or for reasons of important public interest of the Union or of a Member State.
A data subject will be informed by the Company before the restriction of processing is lifted.

➢ *Right to object*

Where the legal basis for processing is legitimate interest of the Company or third person (except compulsory data processing) or data is processed for direct marketing, scientific or historical research purposes or statistical purposes, the data subject has the right to object to processing of personal data concerning him or her. Objection may be rejected if the Company demonstrates

- compelling legitimate grounds for the processing which override the interests, rights and freedoms of the data subject; or
- that data processing is related to the establishment, exercise or defence of legal claims of the Company.

The Company examines the lawfulness of the objection of the data subject and where the objection is grounded, the Company stops data processing.

➢ *Right to legal remedy*

See section VIII.

VIII. Modification of the Policy

The Company reserves the right to modify the present Policy through an unilateral decision at any time.

If the data subject does not agree with the modification, he or she may request the erasure of his or her personal data as determined above.

IX. Legal remedies and enforcement

The Company as data controller may be contacted for the purpose of any question or comments related to data processing using contact details above.

In case of any violation related to data processing, the data subject may make a complaint to the competent data protection supervisory authority of the Member State of residence, workplace or the place of the alleged violation.

In Hungary, complaint shall be made to Hungarian National Authority for Data Protection and Freedom of Information ('NAIH', address: 1055 Budapest, Falk Miksa utca 9-11.; 1363 Budapest, Pf. 9.; phone: +36-1-391-1400; e-mail: ugyfelszolgalat@naih.hu; website: www.naih.hu).
The data subject may bring the following cases before court:

- violation of rights,
- against the legally binding decision of the supervisory authority,
- if the supervisory authority does not deal with the filed complaint or does not inform the data subject of aspects or result of the procedure related to the filed complaint within 3 months.

Cookie policy

I. What are cookies?

A cookie is a small text file that a website stores on your computer device when you visit the site.

First party cookies are cookies set by the website you are visiting. Only that website can read them. In addition, a website might potentially use external services, which also set their own cookies, known as **third-party cookies**.

Persistent cookies are cookies saved on your computer and that are not deleted automatically when you quit your browser, unlike **a session cookie**, which is deleted when you quit your browser.

The purpose is to enable the site to remember your preferences (such as user name, language, etc.) for a certain period of time.
That way, you do not have to re-enter them when browsing around the site during the same visit.

Cookies can also be used to establish anonymised statistics about the browsing experience on our sites.

It is important that the data is transferred only in relation to the relevant website / domain, it does not make the visitor's other browsing habits and history known.

With your first visit this website, it is obligatory to accept the cookies we used.

II. How do we use cookies

This website only use session cookies.

Session cookies are temporary cookies that are only stored on a user's device for the duration of their stay on a given website, their session. The minute they click away, these cookies expire. These are typically used for functions like keeping the items in your shopping cart, while you click around on a website's subpages.

III. How can you manage cookies

Removing cookies from your device

You can delete all cookies that are already on your device by clearing the history of your browser. This will remove all cookies from all websites you have visited.
Be aware though that you may also lose some saved information (e.g. saved login details, site preferences).

Managing site-specific cookies

For more detailed control over site-specific cookies, check the privacy and cookie settings in your preferred browser.

Blocking cookies

You can set most modern browsers to prevent any cookies being placed on your device, but you may then have to manually adjust some preferences every time you visit a site/page. And some services and functionalities may not work properly at all (e.g. profile logging-in).

It is important to emphasize that the protection of personal data can be increased by restricting or deleting cookies, however, these operations significantly affect the usability of the website and the operation of certain functions.

Third party web analytics services

We may use third party web analytics services on our websites, such as Google Analytics. The service providers that administer these services use technologies such as cookies, web server logs and web beacons to help us analyse how visitors use the site. The information collected through these means (including IP address) is disclosed to these service providers, who use the information to evaluate use of the website. To disable the Google Analytics cookie and any other third party web analytics service provider cookies, some browsers indicate when a cookie is being sent and allow you to decline cookies on a case-by-case basis.

IV. Privacy information

The privacy information about the cookies used is summarized in the following table:

name of the cookie	purpose	type	data consent	duration
KC_RESTART Oauth_token_request_state	keycloak login with continuous support	first party session cookie	technical identifiers for the login process	time of the login
AUTH_SESSION_ID KEYCLOAK_IDENTITY KEYCLOAK_IDENTITY_LEGACY KEYCLOAK_SESSION KEYCLOAK_SESSION_LEGACY AUTH_SESSION_ID_LEGACY	keycloak user authentication and session maintenance	first party session cookie	user identity and session technical ID	validity period set in keycloak when using session time or "remember me" (currently 30 days)
KEYCLOAK_REMEMBER_ME	support for "Remember-me" function	first party session cookie	user ID	1 year when using the "remember me" function, otherwise not used
JSESSIONID SRV	maintain an in-app user session	first party session cookie	session technical IDs	time of the session