Privacy Policy
Status: May 2018

1. Name and contact details of Data Controller and Data Processor

INTERNATIONAL KODÁLY SOCIETY
1149, Budapest, Róna utca 120-122
Registered at Fővárosi Törvényszék (Court of the Capital) under No. 01-02-0007044
Email: office@iks.hu
Website: http://iks.hu/
Tax No. 30001664-1-42
(hereinafter Controller)

Web hosting for the Controller is provided by:
CRISCOMP INFORMATIKA KFT
4030, Debrecen, Gyoma u. 17
Email: titkarsag@criscomp.hu
Website: http://criscomp.hu/

2. Contents and aim of this Policy

The present Privacy Policy describes how and why the Controller collects the personal data of the users (hereinafter User or You) of the webpages operated by them (hereinafter Website), and how they protect them. This Privacy Policy only refers to processing personal data of natural persons.
Website: http://iks.hu

Scope of the Privacy Policy:
- the person of the Controller
- the scope your personal data collected by the Controller
- the legal basis of data collection
- the way of data processing (including access by the Controller or giving access to third parties)
- the aim of data processing
- the time of data processing
- the requirements of data protection and safety
- the legal rights of Users

The original language of the present Privacy Policy is Hungarian.

3. Primary legal basis for processing personal data

- The legal basis for processing personal data is Article 13 of the Order 2016/679 (April 27, 2016) of the European Parliament and Council (EU) about the protection and free flow of personal data of individuals, and revoking the order 95/46/EK (General Data Protection Regulation or GDPR).
• Act CXII of 2011 about the right to informational self-determination and freedom of information ("Info Law")
• Act CVIII of 2001 about certain topics of electronical commercial services and informational services ("Eker Act")

4. Modification

The Controller reserves the right to unilaterally modify this Privacy Policy. However, they will post an announcement on the Website about the modification at least five (5) days before entry into force, and email it to registered users. To be able to review the modifications you must have internet access and regularly check the Website and your email inbox.

5. Scope of users, underage users

Registered User: Users can register on the Website on one occasion, in one way (hereinafter Registration). You can order products or services on the Website from the Controller (hereinafter Order). Based on the personal data given during Registration or Order you can avail yourself of the services (hereinafter Services) provided by the Controller on its Website, regulated by the Terms and Conditions ("T&C").

Unregistered User: If you are browsing the Website without Registration or Order, the regulations of the present Privacy Policy do not apply to the handling of your personal data. This Privacy Policy also applies to orders sent in hard copy or otherwise.

Special regulations for Registration or Order:
• You should provide the necessary data during Registration or Order
• You should declare that you have read and understood this Data Protection Regulation
• You should accept the T&C of the Website
• You should be over 18 years of age to be able to place and Order.

Special regulations for underage Users:

Children, underage Users: You cannot place an Order on the Website. If you would like to order something, ask your parents to help you. If you are under 16, always ask permission from your parents when you share your name, phone number or other personal data on a website. If you are a child under 14, never give any data (like your name, email address, phone number) without your parents’ knowledge, but ask them to help you. Moreover, ask them to read the below lines, meant for parents.

For parents:

Accepting this Privacy Policy, Registration: If your child is under 16 years of age (or under guardianship owing to full or partial incapacitation) but is over 14, they cannot register on the Website on their own, and cannot accept this Policy on their own. The approval of a parent or legal guardian is needed for registration or acceptance.
This article also refers to those who are under guardianship in relation to handling personal data.

**Orders:** If your child is under 18 years of age (or is underage and incapacitated) they cannot place an order. Their legal representative (usually parent) can place the order for them. This article also refers to those who are under guardianship in relation to handling personal data.

Due to the above, if a child is under 18 years of age or is incapacitated for some other reason, but is over 14 years of age, the prior approval of their parent or legal representative is needed for the use of the Website. The approval covers full responsibility for the child’s user activity as well. The approval should be sent to the contact details of the Controller mentioned in point 1 of this Policy.

In case the child is under 14 years of age or is under guardianship for full incapacitation, they cannot use the Website on their own. Their legal representative (usually parent) can register or place an order for them, can use the Website, and should be responsible for their user activity.

### 6. What does it mean if you accept the Privacy Policy

By using the Website you confirm that you have fully read and understood the whole present Policy.

By ticking the relevant box at Registration or Order on the Website about reading the Privacy Policy you are accepting that the Controller processes your data according to this Policy. Accepting the Privacy Policy is a prerequisite of an Order or Registration, otherwise you will not be able to order the required service.

In case you do not agree with the above, do not tick the relevant box and do not use the Website.

If you place an Order in hard copy or by other means, we are going to process your date in accordance with this Policy.

### 7. Data Processing

In the following passages it is detailed in which cases we ask for or collect personal data from you and how we process them.

The regulations pertaining to the protection of the personal data of Users solely refer to natural persons (individuals), hence the present Privacy Policy only discusses the processing of the personal data of natural persons.

**Collecting and processing of data for online registration**

**Whose data are processed:** All registered Users of the Website.

**Why are these data processed (purpose of data procession):**
- to be able to identify our Users
- to be able to contact you

(The provided data are used for confirming the Registration, for sending information connected to the Services, for updating data, or sending system messages and reminders about Services, or for answering your queries.)
What happens if you do not provide the data:
Providing these data is a minimal prerequisite of Registration, so providing them is obligatory to complete the Registration. If you do not provide the data, you cannot register on the Website.

Cancellation of Registration:
You can freely cancel your Registration at any time by contacting the Controller at the contact details mentioned in point 1 of this Policy.

What data are processed at Registration:
- Name
- Username
- Email address
- Password

What is the legal basis for data processing:
Data processing is required by the Standard Contractual Clauses or the fulfilment of a contract, or for the processing procedures for pre-contractual measures (Article 6 (1) b) of GDPR).

How long are these data stored:
The storage period is five (5) years after the cancellation of Registration, since this is the period in which the Controller or a third party might launch a civil law claim against the User or against the Controller because of the User’s activity.

To whom are these data passed on:
They are not passed on.

Collecting and processing of data connected to invoicing

Whose data are processed: Users who placed an Order which involves payment.

Why are these data processed (purpose of data procession):
To keep records which directly and indirectly support accounting.

What happens if you do not provide the data:
Providing these data is a legal obligation. If you do not provide the data, your Order cannot be fulfilled.

Data erasure:
These data are automatically erased when the legal deadline expires, before that deadline it is not possible.

What data are processed:
Obligatory data on records which directly and indirectly support accounting: name, address.

What is the legal basis for data processing:
Data processing is legally required by the Act C of 2000 on Accounting §169 Article (1)-(2) (Article 6 (1) c) of GDPR).

How long are these data stored:
The storage period is eight (8) years after the date of the record.

To whom are these data passed on:
Anna Mária Hernádi, certified accountant. Address: 1133 Budapest, Pannónia St 89. V/19.
Collecting and processing of data connected to complaints and customer service

**Whose data are processed:** Users who submit a complaint or contact customer service (ex. enquire about a service), report an incident, apply for an alternative reconciliation forum.

**Why are these data processed (purpose of data procession):**
To identify you and your Order or case, to investigate and resolve complaints and connected procedures.

**What happens if you do not provide the data:**
Providing these data is a legal obligation, you must provide them in order for the complaint to be recorded. If you do not provide the data, your complaint or issue cannot be handled.

**Data erasure:**
These data are automatically erased when the legal deadline expires, before that deadline it is not possible.

**What data are processed:**
Data for complaint minutes: number, description of complaint.
Further data for customer service: name, email address.
Data for those reporting an incident: name, email address, phone number.
Data for those using an alternative reconciliation forum: name, email address, phone number.

**What is the legal basis for data processing:**
Data processing is legally required by the Act CLV of 1997 on Consumer Protection §17/A Article (7) (Article 6 (1) c) of GDPR.

**How long are these data stored:**
For complaints: five (5) years (legal deadline) after the date of the minutes (start of handling the complaint).
For incidents: the closure of the incident.
For alternative reconciliation forum: closure of the reconciliation.

**To whom are these data passed on:**
They are not passed on. In case of official subpoena: to the authority legally entitled to get them.

**Other activity on the Website:** For certain activities the Controller may ask for other personal data of the Users as well (ex. raffles, promos), however, their provision is voluntary. In such cases the Controller informs the Users in special announcements about data processing, and the provided personal data are only used for the given purpose, connected to the particular activity and within the stipulated time period. Those data processing cases are also governed by the present Policy.

**8. Data access, data security**

Conform to Article 32 of GDPR the Controller takes all the necessary measures to ensure the safety of the data, takes the necessary technical and organizational measures and works out procedures which are needed to comply with the GDPR and other regulations concerning data and secret protection.
The required level of data security is guaranteed in the following way:

Among others, but not exclusively

(i) User data are stored in secure technical surroundings, they are not made accessible to the public.
(ii) User data can only be accessed by the colleagues named below, after appropriate identification, and only them.
(iii) Whenever possible, TLS encryption is used.
(iv) The Controller uses https protocol when processing data, so the User and the server communicate through a secure connection.
(v) Individuals having access to personal data may only process personal data adhering to the instructions of the Controller.
(vi) Pseudonymisation.
(vii) Security measures are regularly, monthly tested and evaluated, corrected if needed.
(viii) Before exercising User rights we check the User’s identity, protecting the security of personal data so that they cannot be accessed by unauthorized persons.

Your personal data processed by the Controller can be accessed by the following persons: Ágnes Sztana Patakiné, Executive Secretary.

Incident connected to data: In case an incident happens connected to your data, after the Controller becomes aware of it they will do everything they can to reduce risks. If an incident happens connected to your data which, in spite of the security measures taken by the Controller (or their data Processor), is likely to result in a probable high risk for the rights and freedoms of individuals, you and the authorities will be immediately notified free of charge.

Links: There are links on the Controller’s Website to sites maintained by other service providers (including the login, share buttons, logos) where the Controller has no influence on the data processing practices. Users must be aware that if they click on such links they may land on other servers’ sites. In such cases it is advisable to read the privacy policy of those sites. The present Privacy Policy is only relevant to the Website maintained by the Controller. If a User changes, deletes any of their data on an outside website, it will not affect data processing by the Controller. Such changes must be done on the Website as well.

9. Data transfer

Data Processors: Data controlled by the Controller are handed over to the data processors. Contact details of the current data processors:
Anna Mária Hernádi, certified accountant. Address: 1133 Budapest, Pannónia St 89. V/19.

Transfer: Cross-border data transfers to a recipient in a third country may take place if the third country ensures the appropriate level of security. In such a case no special permission is needed.
Recipients of such a transfer are bound by secrecy and data protection obligation.
10. Anonymous identifiers (cookies)

**Anonymous identifiers (cookies)** are unique series of characters – suitable for identification or storing profile information – that are automatically dropped on your computer as you browse the web. In and of themselves they are not able to identify a User, it can only recognize the User’s computer. On the internet network it is only possible to provide customized service, personalized information if providers are able to uniquely identify the habits and requirements of their customers. Providers use anonymous identifiers to get to know more about the profiles of their customers in order that they can further improve the level of their service and offer more opportunity of customization to them.

**Blocking of cookies:** Users may, at any time, prevent the placing of cookies by means of a corresponding setting of the Internet browser used, and may thus permanently deny the setting of cookies or only allow placing only certain cookies. In such a case, however, not all functions of the Website may be entirely usable. Blocking cookies may be done in the “Privacy and Security” options of the browser’s settings.

**Cookies used on the Website:** identifiers generated from random alphanumerical characters.

11. Profiling

**Google Analytics:** The Controller measures the visits to the Website by Google Analytics, provided by Google, Inc. (“Google”). Google Analytics compile their reports using tracking cookies about the user interactions detected on the websites of their clients. The advertising functions of Google Analytics may be activated by Google-ad cookies – like remarketing – in connection with Google Display Network products, like AdWords. Each computer and device connected to the internet gets a unique number, it is called IP address (internet protocol address). These numbers are assigned in blocks of countries, so an IP address may identify a country, state, county and city where the computer is connected to the internet. Since the operating system of the internet uses website IP addresses, the owners of websites may get to know the IP address of their users even if they do not use the services of Google Analytics. But Google Analytics collects the IP addresses of the website’s users to safeguard the service, and to make it possible for website owners to see where their users come from (this is called IP address geolocation). Instead of traditional file systems or databases Google stores data in efficiency optimized, coded form. Data are distributed into several physical and logical volumes because of redundancy and to make access more difficult, preventing data abuse. Google applications are running at multiple locations. Data of certain clients are not stored on one single computer or computer group but the data of all Google’s clients (clients, enterprises, moreover, Google’s own data) are stored mixed, on a divided infrastructure of many homogenous computers in Google’s datacenters. You can read more about Google’s data protection principles here: [https://policies.google.com/privacy](https://policies.google.com/privacy). You can also choose to opt-out of Google Analytics if you download the Google Analytics Opt-out Browser Add-on and install it to your browser: [https://tools.google.com/dlpage/gaoptout](https://tools.google.com/dlpage/gaoptout). You can read more about this here: [https://support.google.com/analytics/?hl=en#topic=3544906](https://support.google.com/analytics/?hl=en#topic=3544906)
12. User rights and right enforcement possibilities

In connection with their personal data Users may request the Controller to obtain the following:

- access to their data processed by us
- correction
- erasure of data
- restriction of data processing
- data transfer
- objection against the processing of data.

The Controller notifies you without delay, but within one month the latest after the receipt of your request about the measures taken in connection with your request or the reason why measures were not taken. If the request is complex or there are multiple requests, the deadline can be extended by two months. Notification is sent electronically, if possible. Notification and measures are free of charge, except for spurious or excessive – mostly repetitive – requests. In such cases a reasonable fee is charged or the request is denied. You may be asked to provide further information needed to confirm your identity. A copy of your personal data processed by us is also free of charge on the first occasion, further copies incur a fee equal to administration expenses.

In connection with our measures Users may submit a complaint to the supervising authority or turn to a court.

Users can have access to the following information:

- What data are we processing about you.
- Why are we processing your data.
- How long are we processing your data.
- Who have received or will receive your personal data.
- Data protection guarantees outside the EU or in international transfers.
- Where we got your data from if you did not give them to us.
- Automated decision making, including profiling, information about applied logic, importance of - data protection and its consequences for you.
- Your rights and right enforcement possibilities in connection with data processing.

Correction: Users have the right to require immediate correction of their incorrect personal data or completion of incomplete personal data.

Erasure: Users have the right to request erasure of their personal data if:

- the User’s personal data are not needed for the purpose they were collected
- the User cancels their consent that data collection was based on and there is no other legal reason for data collection
- the User protests against data collection and there is no primary legal right for data collection
- the personal data were processed illegally
- the legal obligation requires erasure of data
- services are offered directly to children.
Right to be forgotten: If one of the aforementioned reasons applies, you can ask erasure of your data, and if we have made your personal data public we shall take the necessary steps to inform other data controllers that you have asked to erase the links pointing to these personal data and erase the copies thereof.

We are not able to fulfill your request of erasure if your data are still required by the Controller to establish, exercise or defend legal rights or if by doing so the right to free speech and information would be limited, or if we have a legal obligation (public interest, scientific, research or statistical purpose) opposing erasure.

Restriction: It means that such personal data can only be stored or processed with your permission (except for legal procedures, the defense of other people’s rights, or important public interest). You have the right to ask for restriction of your data processing if
- the accuracy of the data is contested (and only for as long as it takes to verify that accuracy)
- the processing is unlawful and you request restriction (as opposed to exercising the right to erasure)
- the Controller no longer needs the data for their original purpose, but the data are still required by the Controller to establish, exercise or defend legal rights
- you protest against data processing, in this case the restriction refers to the time period while it is clarified whether our justified reasons take precedence over your justified reasons.

We are going to notify all third parties of the rectification, erasure or restriction of data processing to whom we have disclosed personal data, except when it is impossible or would require disproportionate effort. You may ask to receive a list of these addressees.

Data portability: Users have a right to receive a copy of their personal data and to transfer their personal data to another controller, if data processing is based on their permission or on a contract and is done in an automated way. Portability cannot offend the rights and freedom of others or their right to be forgotten.

You may also ask the Controller to directly transfer your personal data to the new service provider if this is technically possible.

Objection: Users have the right to object, on any compelling legitimate grounds, to the processing of personal data, where the basis for that processing is either public interest, or legitimate interests of the Controller. Users have the right to object to the processing of personal data for the purpose of direct marketing, including profiling. Where the User’s objection is justified, we cease the relevant processing activity in relation to those data.

Profiling: Users have the right not to be subject to a decision based solely on automated processing which significantly affect them (including profiling). Such processing is permitted where it is necessary for entering into or performing a contract with the User provided that appropriate safeguards are in place, or it is authorized by law, or the User has explicitly consented and appropriate safeguards are in place. In this case Users have the right to ask for human intervention, express their opinion, and submit objection against the decision.

Judicial remedy: Users have the right to a judicial remedy for any breach of their data protection rights. They can turn to a court of law or submit a complaint to the supervising authority, based on the GDPR and the Civil Code of Hungary.
Users can submit a complaint to the supervising authority of their location, workplace or the member state where the alleged breach of law took place if they think an infringement of the applicable data protection laws happened. In Hungary the supervising authority is the National Data Protection and Information Freedom Authority, headquarters: 1024 Budapest, Szilágyi Erzsébet fasor 22/C, website: [www.naih.hu](http://www.naih.hu), phone: +36 (1) 391-1400. Decisions taken by the supervising authority that are legally binding for you, or if the authority fails to respond within three month about the procedure and its result, may be appealed through the courts. A suit can be initiated against the supervising authority before the national court of the member state.

If a User has **suffered harm** as a result of the unlawful processing of their personal data they have the right to receive compensation from the Controller (or Processor) for the harm suffered. The suit should be launched before the court of the member state where the Controller (or Processor) is located. Such a lawsuit may also be launched before the court of the User’s location.

If a User considers that we have not processed their personal data according to the GDPR and so harmed their rights, they can turn to a court for remedy. The suit should be launched before the court of the member state where the Controller (or Processor) is located. Such a lawsuit may also be launched before the court of the User’s location.

Launching a suit does not exclude the possibility of resorting to other administrative or non-judicial remedies.

Suits demanding administrative fines or claims for property (i.e. damages) not exceeding 30 million forints belong to the jurisdiction of the municipal courts, and property lawsuits exceeding HUF 30 million to the jurisdiction of the court of justice. A suit may be launched before the court at the Controller’s location according to the general rules, however, if you are a customer, you may also choose to launch the suit at your domestic residence, lacking this, at your domestic dwelling place. You may also launch a suit against the supervising authority at your domestic residence, lacking this, at your domestic dwelling place, as you choose.

### 13. Person responsible for data protection, appointed by the Controller

Since the Controller does not abide by the obligatory appointment of a data protection officer owing to the below reasons, they did not appoint a data protection officer:

- a) if data processing is done by public authorities or other bodies with public-service mission (except for courts acting in their judicial function);
- b) if the main activities of the Controller or Processor include data processing operations which necessitate regular and systematic, large-scale observation of the subjects;
- c) if the main activities of the Controller of Processor include handling special categories of personal data, or numerous data relating to decisions on the determination of criminal liability or on criminal offenses.
14. Existing law, other provisions

The present Privacy Policy is governed by Hungarian law.

If existing law in your country prescribe more severe rules than the ones stipulated here, you must abide by them. You acknowledge, however, that this Privacy Policy was made under the jurisdiction of its relevant legislation which determines the responsibility of the Controller who, in accord with the relevant statute and case law, therefore rejects any responsibility for any potential breaches of privacy laws of the country of the User.

The chapter titles of this Privacy Policy are informative only and do not suffice by themselves to understand data processing procedures.

If you have a question that is not properly detailed in this Privacy Policy, please write to office@iks.hu.

© INTERNATIONAL KODÁLY SOCIETY (2018)