ISKO Privacy Policy
https//www.isko.org

Who are we?

ISKO, the International Society for Knowledge Organization, is a Canada not-for-profit (NFP) corporation no. 1163010-5, which is dedicated to promoting the theory and practice of Knowledge Organization. ISKO is registered at the following address:

ISKO
140 Saint George Street
Toronto ON
M5S 3G6
Canada

Email: secr@isko.org

The Secretary to the ISKO Board of Directors is the Privacy Officer for ISKO.

What type of information do we collect?

We currently collect and process the following information:

- your name
- email address(es)
- name of the organisation you belong to (when appropriate)
- telephone number
- postal address (only if you request the printed copies of the *Knowledge Organization* journal)
- bank account details to enable transfer of expenses claims and payment of research grants and travel grants to awardees

Most of the personal information we process is provided to us by your national/regional chapter when:

- you apply for or renew your membership of ISKO
- you register for meetings and events
- you respond to a poll sent out by ISKO

The bases we rely on for processing this information are (from the EU GDPR):

(a) Your consent. Where other legal bases do not apply we will ask for your explicit consent to process your personal data. You are able to withdraw your consent at any time. You can do this by contacting secr@isko.org

(b) Contract fulfilment. When we need to fulfil contracted services such as membership benefits, events, publications and information services, we will process your personal data to enable us to provide the services in question

(c) Legitimate interest. Where it is in ISKO's legitimate interests to inform you of services and events that may be of interest following attendance at an ISKO event or purchase of a publication, we will use contact details gathered in order to provide the original service.

What do we do with your personal data?

We use the information that you have given us in order to:

- send you email announcements for forthcoming events and meetings
- process membership applications and renewals
- process registration to ISKO events and meetings
- administer payments of expenses, grants and awards
- circulate voting polls

We share this information with:

Ergon Verlag, who publish ISKO's peer-reviewed journal, Knowledge Organization, conference proceedings and other ISKO publications. They use the personal data to process members' access to online resources and member discounts for relevant publications:

Nomos Verlagsgesellschaft mbH & Co. KG
Waldseestraße 3-5,
76530 Baden-Baden
Germany
E-Mail: nomos@nomos.de

How do we store your information?

Your information is securely stored in the membership database held in the Membership Management System (MMS), which gathers personal data of members of all chapters of ISKO.

We keep your personal information and contact details for the duration of your membership to ISKO and for a two-year period of lapsed membership. We will then delete your data from the Membership Management System.

What are your data protection rights?

As a Canadian not-for profit organization ISKO is exempt from the Personal Information Protection and Electronic Documents Act (PIPEDA). However, as far as possible it adheres to its 10 principles. It does this in order to be compatible with legislation in other jurisdictions that might affect ISKO's members, such as the EU General Data Protection Regulation (GDPR). The 10 PIPEDA principles are:

1. Accountability: An organization is responsible for personal information under its control. It must appoint a Privacy Officer whose purpose is to ensure compliance with Canada's data protection law.
2. Identifying Purposes: Organizations must identify the purposes for which personal data is being collected before or at the time of collection.
3. Consent: Individuals' consent is needed for the collection, use or disclosure of personal information. Some exemptions apply to this principle such as, for example, in cases where legal, medical or security reasons make seeking consent impossible or impractical.
4. Limiting Collection: Information must be collected by fair and lawful means and must be limited to the data needed for the purpose identified by the organization.
5. Limiting Use, Disclosure, and Retention: Personal information can only be used or disclosed for the purposes for which it was collected and must be kept solely for the duration required to serve those purposes unless the individual consents otherwise or it is required by law.
6. Accuracy: Personal information must be as accurate, complete, and as up-to-date as possible in order to properly satisfy the purposes for which it is to be used.
7. Safeguards: Personal information must be protected through appropriate security safeguards against loss or theft, as well as unauthorized access, disclosure, copying, use, or modification.

8. Openness: Organizations must be open about their policies and practices relating to the management of personal data and ensure that such information is easily available to individuals in a generally understandable format.
9. Individual Access: Upon request, an individual must be informed of the existence, use, and disclosure of their personal information and be given access to it. Individuals have the right to challenge the accuracy and completeness of that information and have it amended as appropriate. Organizations may deny access to personal data if the information cannot be disclosed for legal, security, or commercial proprietary reasons or is subject to solicitor-client or litigation privilege.
10. Challenging Compliance: An individual can challenge an organization's compliance with PIPEDA's principles and address their challenge to the company's Privacy Officer in charge of PIPEDA compliance.

Responsibilities

Overall and final responsibility for data protection lies with the office bearers of the ISKO Board of Directors, who are responsible for overseeing activities and ensuring this policy is upheld.

All volunteers are responsible for observing this policy, and related procedures, in all areas of their work for ISKO.

We will endeavour to keep personal data secure. In the event of a data breach, we will endeavour to rectify the breach by getting any lost or shared data back. We will evaluate our processes and understand how to avoid it happening again. Serious data breaches which may risk someone's personal rights or freedoms will be reported to the appropriate national data protection authority within 72 hours of our becoming aware of the breach. If the breach is likely to have a negative impact on individuals whose data has been breached, they will be informed in a timely manner.

To uphold this policy, we will maintain a set of data protection procedures for our committee and volunteers to follow.

Complaints and data access requests

If you wish to complain about the way in which your data is kept or processed or wish to make a subject access request, please contact the Secretary of ISKO: secr@isko.org

Updated 21st October 2020

Approved by the ISKO Board of Directors 2020-11-18