



Data Protection Policy

Last Updated: 31 January 2024 by Emilia Carson

The purpose of this document is to convey the Organization of International Social Scientists' data protection principles to those persons in the organization who maintain or process personal data files in the organization's possession.

The organization currently has the following filing systems in its possession: list of members, and event sign-up registers. CISSI may also file data from survey results as and when appropriate and necessary.

This document and the privacy statements of the filing systems mentioned above must be updated annually when the Board and officials have changed.

Access to data and filing systems

Access to data and the filing systems should be given only to the core board of the organization: Chair, Treasurer, Secretary, Events, and Communication (Rosaliina Frantti, Andrew Armstrong, Emilia Carson, Caro Carter, Mia Pickering and Rin Ito respectively). The Secretary has overall responsibility for data and the management of filing systems of CISSI in 2024.

The 2023 board will lose access to the filing systems on March 31 2024. From March 31st 2024, the 2024 core board of CISSI will be the only ones with access to the aforementioned data. It is the role of the outgoing and incoming secretaries to coordinate this switch.

Data life cycle

Data in the filing systems should be stored for as long as necessary.

Upon the collection of data for one-time events, dates for deletion will be explicitly stated. This date will be no more than one month after the date of the event.

Specifically on membership data collection, new members will be asked to state in which year they want their data to be erased.

Technical securing of data

Collected data will be stored in internet servers: E-Iomake from University of Helsinki and Google Drive. Access to the data is restricted with a password and is encrypted.

A person's right of inspection and right to request rectification

Anyone has a right to inspect and rectify their personal data collected and stored by the organization, and only if necessary will identification of the individual be requested. All requests should be processed within a month of receiving the initial request.