

**PRIVACY STATEMENT - DUTIES AND OBLIGATIONS OF**

**THE ISA DATA BASE SYSTEM USER**

**ROLES AND OBLIGATIONS OF THE ISA DATA BASE USER**

**PRIVACY STATEMENT**

You hereby declare that, in order to carry out your duties within the INTERNATIONAL SOCIOLOGICAL ASSOCIATION, you may process personal data for which the ASSOCIATION is responsible, and you therefore declare that you are aware of and accept the DUTIES AND OBLIGATIONS OF THE STAFF specified in this document,

AND ACKNOWLEDGE

that in your duties as a user of the system of the INTERNATIONAL SOCIOLOGICAL ASSOCIATION and in accordance with the provisions of the General Data Protection Regulation (EU) 2016/679, in the event that you may have access to personal data, or that in the performance of your duties you have to receive, process or transport such information, you must do so by adopting all necessary measures to ensure the security and integrity of the data to prevent its alteration, loss, processing or unauthorised access.

You will only process the data for the purposes specified by the organisation and will not apply or use them for any other purpose, nor will you communicate them, not even for their conservation to other persons.

And you undertake to maintain professional secrecy regarding the data of which you have knowledge, maintaining their confidentiality.

If for the exercise of your functions, you are given a corporate e-mail account, you undertake to make a strictly professional use of it, and the ASSOCIATION may audit its use and content.

AND ACCEPT THE FOLLOWING FUNCTIONS AND DUTIES

***File user***

Data protection regulations must be complied with by all users with access to automated personal data and information systems.

File users will process the data using the management tools provided, following the instructions of the data controller.

***Workstations***

Each user shall be responsible for his workstation and shall make every effort to ensure that the information on their equipment is not visible to unauthorised persons. If you are temporarily absent from your workstation, you must use a screen saver that does not allow data to be viewed, using a password for reactivation.

With regard to printers, you must remove documents as they come out, making sure that no documents containing personal data are left in the tray, especially if the printers are used by several users.

It is strictly forbidden to make external connections to the Internet, other networks or computer systems from workstations containing files with personal data that are not related to your work functions, unless authorised by the person responsible for the files.

It is forbidden to use the resources of the workstation or computer systems to which you have access for private use or for any purpose other than strictly work-related ones.

The creation of new files or databases involving the processing of personal data without the prior authorisation of the data controller is prohibited.

All temporary files that may be generated in the course of your work must be deleted once the purpose for which they were created has been fulfilled.

The configuration of the applications that process personal data may not be changed under any circumstances, not even in their attributes or indicators, access records, etc. Both the configuration of the applications and the operating systems may only be changed with the authorisation of the person responsible for security or by the systems administrator in charge of these functions.

No computer products may be installed on workstation equipment. Software or applications to carry out your work shall be installed by the system administrator or by the organisation providing computer maintenance and support services.

***Personal passwords***

The user is responsible for the safeguarding and confidentiality of their password. Should it become known to other people, they must immediately change it and inform the security manager so that it can be recorded in the incident log.

Easily deducible passwords such as: names, telephone numbers, date of birth, vehicle registration numbers, etc., shall be avoided.

The computer system shall not be accessed using common passwords or the password of another user. Responsibility for any access using a particular password rests with the user to whom that password has been assigned.

***Media management***

Computer media containing personal data, information transfers, temporary data, backup copies, etc., must allow the type of information they contain to be identified with a label: what file it is, what data it contains, the process that gave rise to it and the date of its creation. They must be recorded and stored by authorised personnel on restricted access devices.

Discarded copies must be physically destroyed, making subsequent access to the information contained therein impossible.

Reusable media, if they contain personal data, must be physically erased before reuse, so that the data they contain cannot be recovered.

Media containing personal data shall be stored in restricted-access storage locations or devices to which unauthorised persons have no access.

The sending of personal data by e-mail must be authorised and must comply with the instructions of the INTERNATIONAL SOCIOLOGICAL ASSOCIATION.

***Security Breach Management***

Any user who becomes aware of any incident must notify the security officer or, where appropriate, the administrator of the computer system for it to be rectified and, in any case, for it to be recorded in the incident log.

Failure to report the incident shall be considered a breach of file security.

***Manual files (hard files). Access to documentation***

Access to documentation is limited to authorised personnel only.

If there are documents that can be used by multiple users and it is mandatory for the required level of security, this shall be recorded in the access log.

***Archiving of documents***

The documents must be filed in the storage devices intended for each file with total diligence to guarantee the correct conservation of the documents, the location and consultation of the information.

***Safekeeping of documents***

As long as documents containing personal data are not stored in the storage devices because they are being processed, the persons in charge of the documents must safeguard them and prevent unauthorised persons from accessing them at all times.

***Transfer of documentation and work outside the premises***

Whenever documents containing personal data are physically transferred, they must be protected to prevent loss or theft with the folders or cases provided for this purpose, in order to prevent access to or manipulation of the information being transferred and to act with the greatest possible diligence and caution to protect the documentation.

Any work carried out outside the premises of the location of the file must have the authorisation of the INTERNATIONAL SOCIOLOGICAL ASSOCIATION and must be carried out with the corresponding guarantees in order to maintain a level of security appropriate to the risk.

***Duty of confidentiality***

It is strictly forbidden to communicate to any person outside the organisation any information to which you have had access in the performance of your duties. All the above obligations and commitments must be maintained, even after the termination of the contract with the INTERNATIONAL SOCIOLOGICAL ASSOCIATION. It is also recalled that the user of the system shall be liable to the INTERNATIONAL SOCIOLOGICAL ASSOCIATION and to third parties for any damage that may arise for one or the other as a result of the breach of the above commitments.

**RC/WG/TG President**

Name:

Date and signature:

**RC/WG/TG Secretary**

Name:

Date and signature:

**Please sign and return to ISA Secretariat <isa-secretariat@isa-sociology.org>**