CIO-101: Personal Information Protection – 2 February 2021

Purpose

This policy defines the requirements for collection, retention and disposal of INCOSE membership records and all personal data.

Applicability

This policy applies to all of INCOSE, including chapters and collaborating organizations operating under a Memorandum of Understanding (MOU) or Memorandum of Agreement (MOA). Specific actions apply to the INCOSE central administrative office and all handling of personal information under INCOSE jurisdiction. Local administrative offices outside the United States of America that manage membership and retain membership records and personal information as required by local rules and regulations must also comply with this policy at a minimum.

Definitions

GDPR: European General Data Protection Regulation is a regulation that was implemented in May 2018 that forms a key part of the background for this INCOSE policy.

Personal Data or Information: information by which you may be personally identified, such as name, postal address, E-mail address, telephone number, and any other identifier by which you may be contacted online or offline.

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, organization, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction

Consent: any freely given, specific, informed and unambiguous indication of the data subject's wishes by which he or she, by a statement or by a clear affirmative action, signifies agreement to the processing of personal data relating to him or her.

Policy Content

INCOSE collects personal information when members or visitors register with INCOSE, INCOSE Chapters or INCOSE Events or place an order for INCOSE products. INCOSE will use this information to provide the services requested, maintain membership records, and, with explicit consent, to send additional information about INCOSE and related services and products. Under data protection laws, INCOSE is only permitted to process personal data where there is a legal basis for doing so, and with the provided permission of the person. INCOSE will only hold or process personal data in compliance with applicable law.

This includes individual membership files, records, and database entries, event meeting registrations (including any invoices), applications for certification and disposition, orders of products or services, and any other collected personal information held by INCOSE.
This policy also applies to membership or personal data collected or handled by groups, chapters and teams throughout INCOSE.

Access to personal information and correction

INCOSE must make sure that members and non-members are able to ensure personal data held is accurate and up to date.

Members and non-members shall be able to access and modify their personal data. A member can:

- View the data that INCOSE holds on them by logging in to their account
- Modify data, as necessary
- Select or remove explicit consent to any sharing of personal information
- Request INCOSE to correct or remove information they think is inaccurate or otherwise inappropriate to be retained
- Request a copy of the information that INCOSE holds about them; this applies to non-members as well as members.

INCOSE will process, transfer or disclose personal data when we have a legitimate interest in doing so, as is necessary to:

- Carry out core services such as managing membership and related data
- Comply with applicable law or respond to valid legal process, including from law enforcement or other government agencies;
- Maintain membership information between INCOSE central and an MOU chapter that maintains membership records.

If we do transfer information, we will ensure that the transfer mechanism provides an adequate level of protection, which has been recognized by the applicable laws.

Assessment of Legitimate Interest or Purpose

INCOSE must satisfy all three of the following tests to establish a legitimate interest in processing data:

The “Purpose” test, ensures that INCOSE’s use of the information is in-line with the data processing principles of the applicable laws and what users would reasonably expect. The key issue with the Purpose test is fairness – whether it is fair to use someone’s information.

The “Necessity” test, requires that the processing of the personal information be necessary for INCOSE’s purpose, is proportionate to achieving the organization’s goals and whether there are less intrusive alternatives.

The “Balancing” test, requires INCOSE to balance its legitimate interest in processing the information with the individual’s interests and privacy rights, and consider the likely impact of the processing of the data on its members and/or users.

Length of Time that Personal Data Can Be Retained

INCOSE will keep personal data for as long as needed to fulfill a legitimate purpose. The retention period depends on the purpose of the data, whether to support providing services to the person, to manage membership and related information, or to comply with the law.
Personal data will periodically be reviewed and when there is no longer a legitimate purpose (e.g., membership, legal or business need), it will either be securely deleted or, in some cases, anonymized.

If anyone whose data INCOSE holds has consented to receive marketing and related communication, they may opt out at a later date. They have a right at any time to stop INCOSE from contacting them for marketing purposes.

Consequences of Non-Compliance

Under the terms of the GDPR and other applicable national and international laws, major fines can be demanded for non-compliance. Such fines could have a major negative impact on viable operations of INCOSE.

Responsible Position

Under the authority of the Board of Directors of INCOSE, the CIO shall take the necessary action to comply with the requirements defined in this policy. The CIO shall also ensure that the INCOSE central administrative office complies with this policy.

Related Policies

ADM-102 governs the handling of Confidential Information

ADM-104 sets out Minimum Requirements for Document Retention.

Related Procedures

Procedures for the INCOSE central office, groups, chapters and members are being developed.

A public statement of the “INCOSE Privacy Policy” is available on the incose.org website and is applicable to all INCOSE online resources and services under the INCOSE name.

SUPERSEDES: CIO-101 dated 21 July 2019

APPROVED BY: INCOSE Board of Directors, Virtual, 2 February 2021

POLICY OWNER (RACI Responsible R): CIO

MAINTAINED BY (RACI Accountable A): President-Elect