System Dynamics Society

Data Protection Policy

- Policy prepared by: System Dynamics Society
- Approved by board / management on: July 21, 2019
- Policy became operational on: July 21, 2019
- Next review date: TBD

Introduction

The System Dynamics Society needs to gather and use certain information about individuals. These can include members, customers, suppliers, business contacts, employees, donors, journal subscribers and contributors, and other people the organization has a relationship with or may need to contact. This policy describes how this personal data must be collected, handled and stored to meet the Society's data protection standards — and to comply with the law.

Definitions

Society	means the System Dynamics Society, Inc., a registered 501(c)(3) non-profit organization, incorporated in Massachusetts and with primary offices located in Albany, New York, USA
GDPR	means the General Data Protection Regulation.
Register of Systems	means a register of all systems or contexts in which personal data is processed by the Society.

Why this policy exists

This data protection policy ensures the System Dynamics Society:

- Complies with data protection law and follow good practice
- Protects the rights of members, partners, employees, volunteers, and other related parties
- Is open about how it stores and processes individuals' data
- Protects itself from the risks of a data breach

Policy scope

This policy applies to:

- The head office of the Society
- All branches, including Chapters, Special Interest Groups (SIGs), and Affiliate organizations
- All editors, contributors, reviewers, and subscribers to the *System Dynamics Review*
- All staff and volunteers of the Society
- All contractors, suppliers and other people working on behalf of the Society

It applies to all data that the Society holds relating to identifiable individuals, even if that information technically falls outside of the GDPR. This can include: Names of individuals; Postal addresses; Email addresses; Telephone numbers; plus any other information relating to individuals.

This policy helps to protect the Society from some very real data security risks, including:

- Breaches of confidentiality. For instance, information being given out inappropriately.
- Failing to offer choice. For instance, all individuals should be free to choose how the Society uses data relating to them.
- Reputational damage. For instance, the Society could suffer if hackers successfully gained access to sensitive data.

1. Data protection principles

The GDPR describes how organizations — including the System Dynamics Society, Inc.— must collect, handle and store personal information. These rules apply regardless of whether data is stored electronically, on paper or on other materials. To comply with the law, personal information must be collected and used fairly, stored safely and not disclosed unlawfully. The Society is committed to processing data in accordance with its responsibilities under the GDPR.

Article 5 of the GDPR requires that personal data shall be:

a. processed lawfully, fairly and in a transparent manner in relation to individuals;
b. collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes; further processing for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes shall not be considered to be incompatible with the initial purposes;
c. adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed;
d. accurate and, where necessary, kept up to date; every reasonable step must be taken to ensure that personal data that are inaccurate, having regard to the purposes for which they are processed, are erased or rectified without delay;
e. kept in a form which permits identification of data subjects for no longer than is necessary for the purposes for which the personal data are processed; personal data may be stored for longer periods insofar as the personal data will be processed solely for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes subject to implementation of the appropriate technical and organisational measures required by the GDPR in order to safeguard the rights and freedoms of individuals; and
f. processed in a manner that ensures appropriate security of the personal data, including protection against unauthorised or unlawful processing and against accidental loss, destruction or damage, using appropriate technical or organisational measures."

2. General provisions

Everyone who works for or with the Society has some responsibility for ensuring data is collected, stored and handled appropriately. Each team that handles personal data must ensure that it is handled and processed in line with this policy and data protection principles.

a. This policy applies to all personal data processed by the Society.
b. The Policy Council shall take responsibility for the Society's ongoing compliance with this policy and is ultimately responsible for ensuring that the Society meets its legal obligations. This includes:
    i. Checking and approving any contracts or agreements with third parties that may handle the Society's sensitive data.
    ii. Where necessary, working with other staff or volunteers to ensure activities abide by data protection principles.
    iii. Reviewing this policy annually.
c. The Executive Director is responsible for:
    i. Keeping the Policy Council updated about data protection responsibilities, risks and issues.
    ii. Reviewing all data protection procedures and related policies, in line with an agreed schedule.
    iii. Handling data protection questions from staff and anyone else covered by this policy.
    iv. Dealing with requests from individuals to see the data the Society holds about them.
    v. Evaluating any third-party services the Society is considering using to store or process data.
    vi. Approving any data protection statements attached to communications such as emails and letters.
    vii. Where necessary, working with other staff or volunteers to ensure activities abide by data protection principles.
d. General staff and volunteers responsibility guidelines:
    i. The only people able to access data covered by this policy should be those who need it for their work.

ii. Data should not be shared informally. When access to confidential information is required, staff or volunteers may request it from the Executive Director or Policy Council.
iii. Staff and volunteers should keep all data secure, by taking sensible precautions and following the guidelines in Section 7 (Security) below.
iv. Staff or volunteers should ask the Executive Director or Policy Council if they are unsure about any aspect of data protection.

3. Lawful, fair and transparent processing

a. To ensure its processing of data is lawful, fair and transparent, the Society shall maintain a Register of Systems.
b. The Register of Systems shall be reviewed at least annually.
c. Individuals have the right to access their personal data and any such requests made to the Society shall be dealt with in a timely manner.

4. Lawful purposes

a. All data processed by the Society must be done on one of the following lawful bases:
   i. Consent: the individual has given clear consent for the Society to process their personal data for a specific purpose.
   ii. Contract: the processing is necessary for a contract the Society has with the individual, or because they have asked the Society to take specific steps before entering into a contract.
   iii. Legal obligation: the processing is necessary for the Society to comply with the law (not including contractual obligations).
   iv. Vital interests: the processing is necessary to protect someone's life.
   v. Public task: the processing is necessary for the Society to perform a task in the public interest or for the Society's official functions, and the task or function has a clear basis in law.
   vi. Legitimate interests: the processing is necessary for the Society's legitimate interests or the legitimate interests of a third party, unless there is a good reason to protect the individual's personal data which overrides those legitimate interests.
a. The Society shall note the appropriate lawful basis in the Register of Systems.
b. Where consent is relied upon as a lawful basis for processing data, evidence of opt-in consent shall be kept with the personal data.
c. Where communications are sent to individuals based on their consent, the option for the individual to revoke their consent should be clearly available and systems should be in place to ensure such revocation is reflected accurately in the Society's systems.
d. In certain circumstances, personal data may be disclosed to law enforcement agencies without the consent of the data subject. However, the Society will ensure the request is legitimate, seeking assistance from the Society's legal advisers where necessary.

5. Data minimisation

a. The Society shall ensure that personal data are adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed.
b. To ensure that personal data is kept for no longer than necessary, the Society shall put in place an archiving policy for each area in which personal data is processed and review this process annually.
c. The archiving policy shall consider what data should/must be retained, for how long, and why.

6. Accuracy

a. The Society shall take reasonable steps to ensure personal data is accurate. The more important it is that the personal data is accurate, the greater the effort the Society should put into ensuring its accuracy.
b. Where necessary for the lawful basis on which data is processed, steps shall be put in place to ensure that personal data is kept up to date.
c. Data should be regularly reviewed and updated if it is found to be out of date. If no longer required, it should be deleted and disposed of.
d. It is the responsibility of all staff and volunteers who work with data to take reasonable steps to ensure it is kept as accurate and up to date as possible.
e. Data will be held in as few places as necessary. Staff and volunteers should not create any unnecessary

additional data sets.

f. The Society will make it easy for data subjects to update the information the Society holds about them. For instance, via the Society website.
g. Data should be updated as inaccuracies are discovered.

7. Security

These rules describe how and where data should be safely stored.

a. The Society shall ensure that personal data is stored securely using modern software that is kept-up-to-date.
b. When data is stored on paper, it should be kept in a secure place where unauthorized people cannot see it. These guidelines also apply to data that is usually stored electronically but has been printed out for some reason:
    i. When not required, the paper or files should be kept in a locked drawer or filing cabinet.
    ii. Staff and volunteers should make sure paper and printouts are not left where unauthorized people could see them, like on a printer.
    iii. Data printouts should be shredded and disposed of securely when no longer required.
c. When data is stored electronically, it must be protected from unauthorized access, accidental deletion and malicious hacking attempts:
    i. Data should be protected by strong passwords that are changed regularly and never shared between employees.
    ii. If data is stored on removable media (like a CD or DVD), these should be kept locked away securely when not being used.
    iii. Data should only be stored on designated drives and servers, and should only be uploaded to an approved cloud computing services.
    iv. Servers containing personal data should be sited in a secure location, away from general office space.
    v. Data should be backed up frequently. Those backups should be tested regularly, in line with the Society's standard backup procedures.
    vi. Data should never be saved directly to laptops or other mobile devices like tablets or smart phones.
    vii. All servers and computers containing data should be protected by approved security software and a firewall.
    viii. When personal data is deleted this should be done safely such that the data is irrecoverable.
    ix. Appropriate back-up and disaster recovery solutions shall be in place.

8. Breach

In the event of a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data, the Society shall promptly assess the risk to people's rights and freedoms and if appropriate report this breach in accordance with appropriate state, federal, and international regulations.

9. Individual Access Requests

All individuals who are the subject of personal data held by the Society are entitled to:

a. Ask what information the Society holds about them and why.
b. Ask how to gain access to it.
c. Be informed how to keep it up to date.
d. Be informed how the Society is meeting its data protection obligations.

Personal data access requests from individuals should be made by email, addressed to the Society at: office@systemdynamics.org. The Society can supply a standard request form, although individuals do not have to use this. The Society will aim to provide the relevant data within 14 days. The Society will always verify the identity of anyone making a subject access request before handing over any information.

END OF POLICY