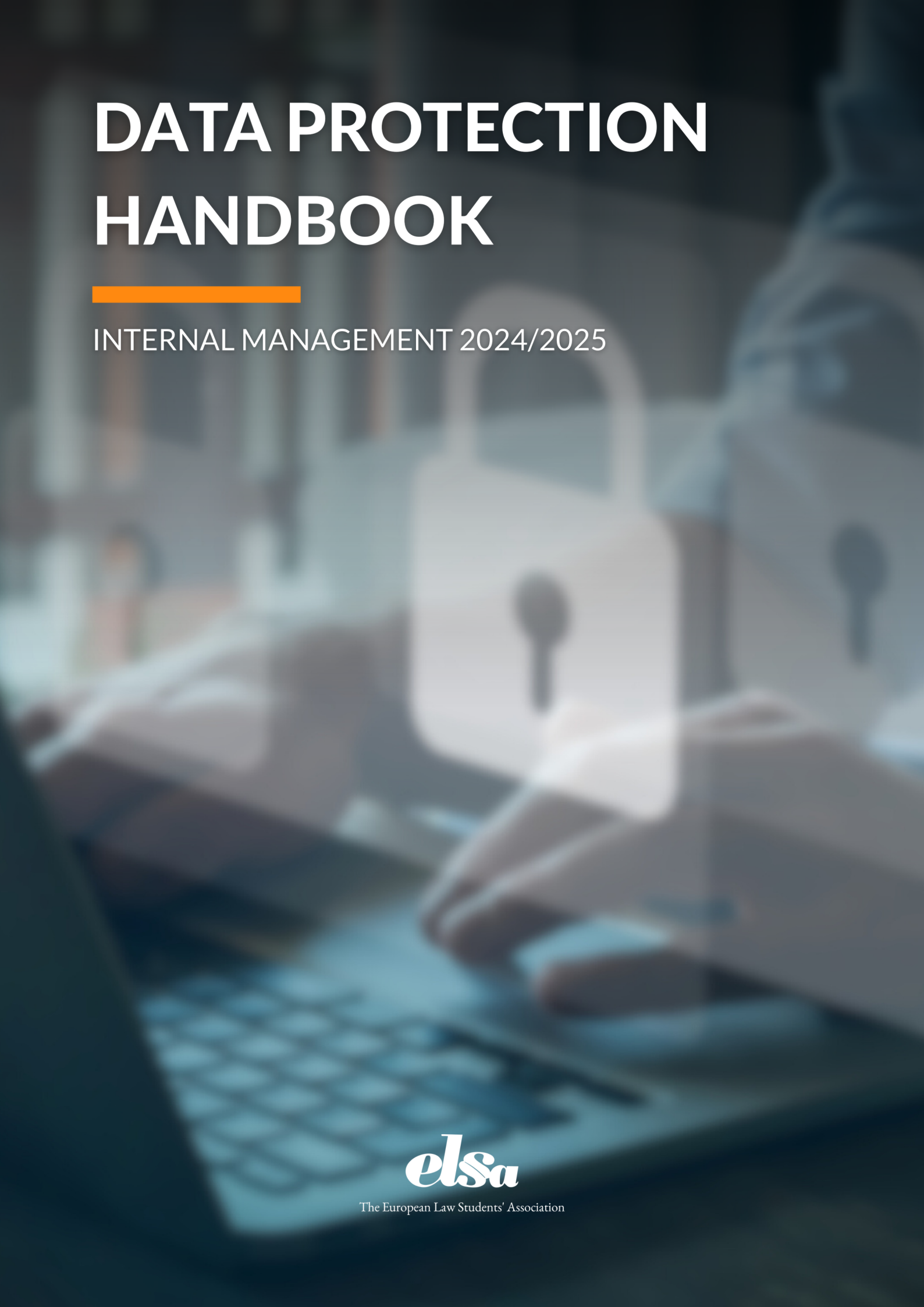


DATA PROTECTION HANDBOOK

INTERNAL MANAGEMENT 2024/2025

elsa

The European Law Students' Association

Foreword

Dear Network,

In an increasingly interconnected world, data is the core of our operations, fueling our initiatives, connecting our members, and driving our collective success. Embracing data protection is not just a legal obligation; it is an ethical imperative and a strategic advantage. For ELSA, the trust placed in us by our members, partners, and stakeholders is paramount. This trust reinforces the confidence our members have in us, strengthens our relationship with partners, and allows us to focus on our core mission: A just world in which there is respect for human dignity and cultural diversity.

This Data Protection Handbook is more than just a collection of documents and knowledge; it reflects our commitment to data privacy and security, as well as cultivates responsibility and vigilance throughout our association. Within these pages, you will find guidance on how to handle personal data responsibly, from its collection and storage to its use and eventual disposal. It covers essential topics such as data protection principles, record of processing activities, privacy policies, data subjects rights, data breaches and archiving.

This handbook is designed to be used in your daily activities in ELSA. It has been developed primarily as an internal guide to foster best practices in data protection, provide practical advice and raise awareness regarding the responsible handling of personal data within our association.

ELSAfully Yours,

Mie Tveit
Secretary General | International Board of ELSA 2024/2025

Assisted in the drafting of the Handbook by:

Eila Karlsson
Director for Administration | ELSA International Team 2024/2025

Nives Deborah Edler
Assistant for Data Protection | ELSA International Team 2024/2025

Based on the ground work of:

Yordan Kyurkchiyski
Secretary General | International Board of ELSA 2023/2024

Nives Deborah Edler
Assistant for Data Protection | ELSA International Team 2023/2024

Table of Contents

General Disclaimer for the ELSA Data Protection Handbook

This Data Protection Handbook has been developed by ELSA International as an internal educational and guidance resource. Its primary purpose is to raise awareness, foster a culture of data protection, and provide practical best practices for the responsible handling of personal data within the day-to-day operations of our student organisation.

Important Limitations and Scope
Please read this disclaimer carefully, as it defines the scope and limitations of the information provided within this handbook:

1. **Not Legal Advice**: The content of this handbook is for internal and educational purposes only. It does not constitute legal advice, nor should it be relied upon as such. Data protection laws are complex, constantly evolving, and highly specific to individual circumstances and jurisdictions. For any specific legal questions, interpretations, or compliance requirements, particularly concerning your local laws or cross-border transfers, you must consult with qualified legal professionals.

2. **Non-Exhaustive Nature**: While this handbook aims to cover the key aspects of data protection relevant to ELSA's activities, it is not exhaustive. It cannot anticipate every possible scenario, data processing activity, or legal nuance that ELSA or its members might encounter. It focuses on general principles and common practices.

3. **ELSA's Characteristics as a Student Organisation**:
    - **Volunteer-Driven**: ELSA is run by dedicated student volunteers who contribute their time and effort alongside their academic commitments. This volunteer-based structure means that resources, including specialised legal expertise, and dedicated personnel for compliance management, are inherently limited compared to professional organisations.
    - **Educational Focus**: Our primary mission is to provide educational opportunities and foster legal professional development for students. This handbook aligns with that mission by educating our members on data protection fundamentals, rather than serving as a comprehensive legal compliance manual for all potential legal obligations.
    - **Dynamic Membership & Activities**: As a student organisation, ELSA experiences regular turnover in leadership and membership. Our activities, projects, and data processing needs can also evolve rapidly. This handbook provides a stable foundation, but specific situations may require fresh legal review.
    - **Resource Constraints**: Developing and maintaining detailed, öegally binding procedures for every aspect of data protection compliance requires significant time, financial investment, and specialised legal knowledge that may exceed the typical resources of a student association.

4. **Focus on Internal Practices**: This handbook is primarily designed to guide internal conduct and promote good habits among ELSA members. While it touches upon external interactions, its core emphasis is on how ELSA members should handle data internally to minimise risks.

5. **No Guarantee of Compliance:** Adhering to the guidelines in this handbook is a significant step towards responsible data handling, but it does not guarantee full compliance in all situations. Legal compliance is an ongoing responsibility that requires continuous assessment, adaptation, and, where necessary, external legal consultation.

Recommendations

ELSA strongly recommends that for any specific or complex data protection matters, particularly those with legal implications (such as data breaches requiring external notification, international data transfers, or new data processing activities), you seek independent legal advice from professionals qualified in data protection law.

By using this handbook, you acknowledge and agree to these limitations. This document serves as a valuable internal tool to promote data protection awareness and best practices within ELSA, contributing to our overall commitment to ethical and responsible conduct.

1. Core Considerations for Data Protection and GDPR

1.1. Purpose of Data Protection

The purpose of data protection is to ensure that individuals' personal information is handled responsibly, transparently, and securely. The collection, storage, and processing of personal data have become integral to both public and private sector operations. Data protection laws exist to safeguard individuals from misuse, unauthorised access, or exploitation of their personal information and to preserve their fundamental rights to privacy.

Personal data is any information relating to an identified or identifiable natural person. This can include but is not limited to:

- Names, addresses, ID numbers;
- Email addresses or phone numbers;
- IP addresses;
- Photos or video recordings;
- Information about physical, physiological, genetic, mental, economic, cultural, or social identity.

An **identifiable person** is someone who can be directly or indirectly identified through this data.

Processing refers to any operation performed on personal data, whether automated or not. This includes but is not limited to:

- Collecting;
- Recording;
- Organising;
- Storing;
- Altering;
- Retrieving;
- Deletion or destruction.

Even viewing or sorting personal data is considered processing under the GDPR.

1.2. The Regulation

The **General Data Protection Regulation (GDPR)** is a binding EU regulation (Regulation (EU) 2016/679) that entered into force on May 25, 2018. It replaced the 1995 Data Protection Directive and is directly applicable in all EU member states without the need for national implementation, as well as in EEA countries.

The GDPR contains 99 articles, organised into 11 chapters. These articles define the rights of individuals and the obligations of those handling personal data, such as data controllers, processors, and data protection officers. They also outline mechanisms for compliance, enforcement, and penalties.

Each chapter targets specific aspects of data protection and different roles within an organisation. The structure of the regulation reads as following;

- **Chapter I: General Provisions (Articles 1–4)**
  Defines the scope, objectives, and key terms used in the Regulation.

- **Chapter II: Principles (Articles 5–11)**
  Outlines the fundamental principles of personal data processing such as lawfulness, purpose limitation, and data minimization.

- **Chapter III: Rights of the Data Subject (Articles 12–23)**
  Details individual rights including access, rectification, erasure, restriction, data portability, and the right to object.

- **Chapter IV: Controller and Processor (Articles 24–43)**
  Sets out the responsibilities and obligations of data controllers and processors, including security measures, documentation (e.g., ROPA), and appointment of Data Protection Officers (DPOs).

- **Chapter V: Transfers of Personal Data to Third Countries or International Organisations (Articles 44–50)**
  Regulates how personal data may be transferred outside the EU/EEA to ensure protection is maintained.

- **Chapter VI: Independent Supervisory Authorities (Articles 51–59)**
  Establishes national data protection authorities and defines their tasks, powers, and independence.

- **Chapter VII: Cooperation and Consistency (Articles 60–76)**
  Outlines how supervisory authorities should cooperate and coordinate to ensure consistent GDPR application across the EU.

- **Chapter VIII: Remedies, Liability and Penalties (Articles 77–84)**
  Covers individuals' rights to lodge complaints, liability of controllers and processors, and conditions for administrative fines.

- **Chapter IX: Provisions Relating to Specific Processing Situations (Articles 85–91)**
  Addresses special cases such as processing for journalistic, research, or public interest purposes.

- **Chapter X: Delegated Acts and Implementing Acts (Articles 92–93)**
  Grants the European Commission powers to make supplementary rules and adaptations to the GDPR.

- **Chapter XI: Final Provisions (Articles 94–99)**
  Contains legal finalities including repeal of prior directives and entry into force of the Regulation.

1.3. Scope of GDPR

The GDPR **applies to any organisation that processes personal data of individuals in the EU or EEA,** including associations like ELSA. Since ELSA operates across Europe and engages with students, members, speakers and partners, GDPR applies to all levels of the organisation, from the International Board of ELSA to the national and local groups.

This means ELSA must handle personal data such as names, email addresses, applications and event registrations lawfully, fairly and securely. Every part of the association needs to document how personal data is collected, stored, used and shared. Consent, transparency and accountability are essential. Data protection measures must be in place to prevent misuse or loss of data and any data breaches must be reported when required. ELSA must also respect the rights of individuals under GDPR including the right to access their data and the right to have it erased.

By complying with GDPR, ELSA protects the privacy of its members and partners and strengthens trust in its role as a responsible and professional European network.

1.4. The Parties of GDPR

1.4.1. Data Subject

As already said, personal data means any information relating to an identified or identifiable natural person - the **data subject**. An identifiable person is one who can be identified, directly or indirectly, in particular by reference to an identifier (e.g. name, identification number, location data etc.). Data subjects are natural persons that are the only beneficiaries of data protection rules.

In practice our data subjects within ELSA are most likely to be board or team members of ELSA Groups, all members of ELSA Groups or participants to events and projects of ELSA.

1.4.2. Recipient

Any person to whom personal data is disclosed is a **recipient**. This can be a natural or legal person, public authority, agency, or another body, whether a third party or not.

In practice a recipient could be an OC, a hotel, restaurant or partner, IT or other service providers. Technically, also a ELSA Group can be a recipient, e.g. if you are organising a Study Visit to another City and the ELSA Group there is organising a brunch, then the ELSA Group of the City you are visiting is a recipient of the data of your participants.

1.4.3. Controller and Joint Controller

The Controller is the party responsible for ensuring that personal data is processed in accordance with the Regulation. According to Article 4 GDPR an ELSA Group acts as **Controller** if it determines the purposes and means of the processing of personal data. This also includes the determination which data will be collected, who to collect data from, how long to retain the data etc.

In practice the controllers within ELSA are most likely to be an ELSA Group.

If more than one ELSA Group is jointly defining the purposes and means, the Groups act as joint-controllers. They decide together to process personal data for a joint purpose. **Joint**

Controllership can take many different forms and participation which can lead into unequal positions. Joint Controllers must therefore determine their respective responsibilities for compliance with GDPR. This is usually done through the formulation of a Joint Controllership Agreement. This agreement aims to specify the responsibilities and common grounds of data protection and the controlling and processing of data. Further information can be found in the chapter "Data Protection Agreements".

In practice our joint-controllers are most likely to be an ELSA Group together with an Organising Committee of a project, event or NCM.

When deciding the purposes and means of the processing, the controller (or joint-controllers) must ensure that the individuals' personal data is protected. To achieve this, the controller (or joint controllers) has to put measures in place.

As a controller or joint-controller you have responsibilities in regards to GDPR. Further details can be found in the chapter on Data Processor Agreements.

1.4.4. Processor

A **Processor** acts under the instructions of the Controller only, by processing personal data on behalf of the Controller. The processing must fall within the parameters provided by the Controller in accordance with GDPR. In every Controller-Processor relationship there is the need of having a Processing Agreement in place. Contracts between Controllers and Processors have specific requirements which are listed in Article 28 GDPR. . This agreement aims to specify the common grounds of data protection and the processing of data. Further information can be found in the chapter "Data Protection Agreements".

A Processor may engage another Processor to help with the processing of the personal data, called Sub-processor.

sA **Sub-processor** acts under the instructions of the Processor, meaning that they may process individuals' personal data on behalf of the Processor. To note, a Sub-processor can only be appointed if the controller, or joint controller, authorises it in a written form. If this is the case, the Processor must draw up a binding contract with the sub-processor detailing the responsibilities of the Sub-processor. This processor-sub-processor contract must provide for the same protection of individuals' personal data as the initial controller-processor contract.

In practice an example of processor and subprocessor would be the following: Your ELSA Group is organising a conference. Therefore you are sending the names of the participants to the hotel to complete the booking of the rooms. The hotel is your processor. If the hotel is using any cloud service provider (e.g. Google Ireland Limited) or other IT and software providers, these software providers are sub-processors of your processor.

As a processor you have responsibilities in regards to GDPR. Further details can be found in the chapter on Data Processor Agreements.

1.4.5. Third Party

A **third party** is a natural or legal person other than the data subject, the Controller, the Processor and persons who are authorised to process personal data under the direct authority of the Controller or Processor.

In practice: a third party can be anyone who is involved in the processing of data.

1.4.6. Supervisory Authority

In all European countries there is an independent public authority with the responsibility to monitor the application of the EU GDPR, in order to protect the fundamental rights and freedoms of natural persons in relation to processing of data.

The national supervisory authorities are required to co-operate with each other and with the European Data Protection Board (EDPB) to ensure the consistent enforcement of GDPR. The European Data Protection Board (EDPB) is composed of representatives of the EU national data protection authorities, and the European Data Protection Supervisor (EDPS). The supervisory authorities of the EFTA EEA states (IS, LI, NO) are also members with regard to the GDPR related matters and without the right to vote and being elected as chair or deputy chairs.

1.5. Six Data Processing Principles

The six data protection principles serve as the foundation for the regulation's approach to data protection. They are designed to ensure that personal data is processed in a responsible and ethical manner, safeguarding individual privacy while allowing organisations to use data effectively. These principles not only guide organisations on how to handle data but also provide individuals with clear rights and protections regarding their personal information. By adhering to these principles, ELSA can foster trust, maintain compliance with the law, and mitigate the risk of misuse or breaches of personal data.

Principle 1: Lawfulness, Fairness and Transparency
Data must be processed in a lawful, fair and transparent manner. This ensures that individuals are informed about how their data is being used, and their consent is obtained when necessary.

Principle 2: Purpose Limitation
Personal data should only be collected for specified, legitimate purposes and not used in ways that are incompatible with those purposes. This principle ensures that data isn't used for unexpected or unauthorised activities.

Principle 3: Data Minimisation
Only the minimum amount of personal data necessary to achieve the intended purpose should be collected and processed. This helps limit the exposure of unnecessary data.

Principle 4: Accuracy
Personal data must be accurate and kept up to date. Any inaccuracies should be corrected as soon as possible to prevent incorrect information from being used.

Principle 5: Storage Limitation
Personal data should not be kept longer than necessary for the purposes for which it was collected. Once data is no longer needed, it must be securely deleted or anonymised.

Principle 6: Integrity and Confidentiality

Data must be processed securely, ensuring protection against unauthorised access, loss, or destruction. This is achieved through appropriate technical and organisational measures to maintain confidentiality and integrity.

1.6. Legal Bases as the key to process personal data lawfully

Data controllers need to rely on a "legal basis" in order to process personal data lawfully. It is essential to identify the appropriate legal basis as it may come with specific requirements (e.g. consent must be free, specific, informed and unambiguous) and have consequences on individuals' rights (e.g. the right to portability only applies when the legal basis is consent or a contract).

1.6.1. What are the possible legal bases under the GDPR?

Data controllers can only process personal data in one of the following circumstances (legal bases):

- with the **consent** of the individuals concerned;
- where there is a **contractual obligation** (a contract between your organisation and an individual);
- to meet a **legal obligation** under EU or national legislation;
- where processing is necessary for the performance of a task carried out in the **public interest** under EU or national legislation;
- to protect the **vital interests** of an individual;
- for your organisation's **legitimate interests** (except if these are overridden by the interests or fundamental rights of individuals) .

1.6.2. Processing of sensitive personal data

Additional requirements apply if you intend to process data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade union membership, and the processing of genetic data, biometric data for the purpose of uniquely identifying a natural person, data concerning health. These special categories of data are commonly referred to as "sensitive data".

The processing of sensitive data is generally prohibited, except in the following specific cases:

- The individual has given their **explicit consent** for their sensitive data to be processed.
- The processing of sensitive data is **necessary for the data controller to fulfil their obligations**, specifically in the context of employment, social security and social protection. For example, the data controller may need to process a person's sensitive data to be able to determine if they are entitled to certain social security benefits or employment stipends.
- The processing of sensitive data is **necessary to protect the vital interests** of a person where the individual is physically or legally incapable of giving consent. For example, if an individual is left unconscious as a result of an accident and requires immediate medical care, their special categories of personal data may need to be processed for the appropriate medical care to be delivered.
- The sensitive data was manifestly made public by individuals.
- The processing of sensitive data is **necessary in the context of legal proceedings**.

- The processing of sensitive data is **necessary for matters of substantial public interest**.
- The processing of sensitive data is **necessary in the context of preventive or occupational medicine.** For example, assessing an individual's sensitive data, such as their medical data, may be necessary to determine their working capacity as an employee.
- The processing of sensitive data is **necessary for matters of public health on the basis of EU or national law.** For example, processing individuals' sensitive data may be necessary to ensure a high quality of health care and a high quality of medical products, or to combat serious health threats, such as viruses.

Checklist for processing sensitive personal data

- ☐ Ask yourself whether you need to process an individual's special categories of personal data for the processing envisaged.
- ☐ Identify the legal basis (= legal justification) for processing an individual's personal data. You should refer to Art.6 GDPR.
- ☐ Identify if the additional conditions for the processing of sensitive data are respected. You should refer to Art. 9 GDPR.
- ☐ Identify the risks and data protection safeguards, such as the technical and organisational measures, that your organisation may need to put in place when processing individuals' special categories of personal data.
- ☐ Do not forget to keep a record of your reasons for processing an individual's special categories of personal data, of the risks that this may entail, and of the measures you have put in place to mitigate those risks.

2. Data Protection Strategy

2.1. Strategy as Guide towards being compliant

Having a clear strategy within an association is crucial for providing direction, ensuring efficient use of resources, and helping the association to achieve its goals effectively. A data protection strategy is essential for any organisation because it ensures compliance, safeguards sensitive information, and builds trust with stakeholders (especially our dear members).

The key reasons why a data protection strategy is important are:

1. **Compliance with Regulations**:
   Laws like GDPR and other data protection regulations require organisations to handle personal data responsibly. A strategy helps ensure compliance, reducing the risk of fines and legal action.
2. **Protection Against Data Breaches:**
   Cyber threats, hacking, and accidental data leaks can cause severe damage. A strong data protection strategy minimises vulnerabilities and ensures security measures are in place.
3. **Trust and Reputation Management:**
   Members, participants, officers, and partners expect their data to be handled securely. A well-defined strategy helps maintain trust and credibility, which is crucial for success.
4. **Continuity & Risk Management:**
   Data loss due to cyberattacks, system failures, or human error can disrupt operations. A strategy includes backup plans and disaster recovery measures to ensure continuity in our projects.
5. **Efficient Data Management & Governance:**
   A clear strategy defines who can access data, how it is stored, and when it should be deleted, preventing unnecessary data hoarding and ensuring proper governance.
6. **Adapting to Evolving Threats**
   Cyber threats are constantly evolving. A data protection strategy ensures that security policies are regularly updated to address new risks.
7. **Empowering Officers & Reducing Human Error**
   Many data breaches result from human mistakes. A strategy includes training and clear guidelines, ensuring officers understand their role in data protection.
8. **Legal and Contractual Obligations**
   Our association works with third parties and needs to prove they handle data securely. A data protection strategy ensures compliance with contractual agreements and standards.

2.2. Best-Practise Example: ELSA International's Strategy

The following table is the step-by-step data protection strategy tailored to ELSA and to start working on GDPR compliance and data protection.

Step 1: Define Responsibilities & Awareness

- ☐ Appoint a Data Protection Lead – A responsible person or team to oversee data handling (Director or Assistant for Data Protection)
- ☐ Train Board Members and Team Members – Brief them on GDPR basics, handling personal data, and cybersecurity

Step 2: Groundwork to Identify & Categorise Data

- ☐ Implement a Record of Processing Activities (ROPA) to see the initial data flow
- ☐ Audit your Record of Processing Activities (GAP Analysis)

Step 3: Secure Data Handling & Access Control

- ☐ Limit Access – Only essential members should access personal data
- ☐ Use Secure Platforms – Store data in password-protected, encrypted locations (e.g. Google Drive with restricted sharing)
- ☐ Regularly Review & Delete Unnecessary Data – Don't keep attendee lists forever!
- ☐ Implement an IT & Cybersecurity Policy

Step 4: Obtain Consent & Communicate Clearly

- ☐ Use Consent Forms – When collecting personal data (e.g., event registration, mailing lists, photography…)
- ☐ Be Transparent – Clearly inform members why you are collecting data and how it is used through Privacy Policies

Step 5: Third-Party Tools & Service Compliance

- ☐ Check Privacy Policies – Ensure platforms like Google Forms, Mailchimp or any other service providers comply with GDPR
- ☐ Use GDPR-compliant event registration tools - avoid storing personal data in insecure spreadsheets
- ☐ Have Data Protection Agreements with third parties in place

Step 6: Manage Photography & Social Media Privacy

- ☐ Ask Before Posting Photos – Use a photo consent form or inform attendees that photos will be taken
- ☐ Be careful with tagging – avoid tagging individuals on social media without consent

Step 7: Data Breach Prevention and Response Plan

- ☐ Prevent Data Breaches - set appropriate technical and organisational measures in place (e.g., strong passwords, enable 2FA (Two Factor Authentication), avoid sharing login details…)
- ☐ Have a Breach Response Plan – If data is lost or exposed, notify affected individuals and take corrective action

Step 8: Regular Reviews & Updates

- ☐ Annual Data Review – Delete old data and update policies every year (work with archiving guidelines to have continuity)
- ☐ Feedback & Improvement – Gather feedback on data handling to improve practices from network, board and team members

2.3. Onboarding to the World of Data Protection

Everyone handling personal data has to understand their responsibilities and the importance of data protection. For a student association organizing events and projects, **GDPR training should be simple, engaging, and practical**.

One of the most important parts of onboarding is **continuous learning and support**. Therefore:

- Send regular reminders & updates (share GDPR reminder in meetings, post updates in your Group Chat)
- Do training sessions during NCMs or Training Meetings of your ELSA Group
- Include a Training Session for GDPR within the transition phase of the new board
- Access to GDPR resources (store GDPR policies, consent form templates, guidelines, checklists or this handbook in a shared drive)
- Appoint a Data Protection Contact Person (this is the go-to person for GDPR questions and concerns within your ELSA Group or refer to the Assistant for Data Protection of ELSA International)

Engaging ways to train board members, team members, officers and organising committees can be:

- Short interactive workshops (in-person or online)
    - Use real life scenarios (e.g. "What if an attendee asks you to delete their data after a SELS?")
    - Quick quizzes or Kahoot-style games to make learning fun
- Provide a GDPR Cheat Sheet
    - A simple and short guide with key rules and best practices for their daily business
- Q&A sessions & case studies
    - Let officers ask questions about GDPR in their role
    - Discuss past mistakes & how to avoid them

As it can be quite tricky to find the key topics to cover in a GDPR Training, the following table shall show you potential ideas on what can be covered in such a training session.

- What is GDPR & why does it matter?
- What is personal data and what are the categories of personal data
- How to collect & use data correctly (Data Protection Principles)
- Data Security & Storage (best practise)
- GDPR & Events (where do we collect, use or process data when organising event/project)
- GDPR & Photography/Social Media (informing attendees, get consent)
- What to do in case of a data breach

3. Record of Processing Activities

3.1. General Information about ROPA

3.1.1. What is a Record of Processing Activities?

A ROPA, or Record of Processing Activities, is a formal document required under Article 30 of the GDPR. It provides a **comprehensive overview** of how, why, and what types of personal data are processed within an organisation.

Maintaining a ROPA is **mandatory for organisations** that process personal data on a regular basis, especially if the processing is not occasional, involves sensitive data, or poses a risk to individuals' rights and freedoms.

The primary **purpose** of a ROPA is to:

- Create a clear overview of all personal data processing activities within the organization.
- Ensure GDPR compliance by making processing activities transparent and traceable;
- Support communication with supervisory authorities, such as providing detailed documentation;
  in the event of an audit or investigation.

A well-maintained ROPA also:

- Helps identify and reduce unnecessary data collection or retention;
- Supports the structuring of data archiving and retention practices;
- Serves as a foundation for privacy policies and internal data protection guidelines;
- Enhances awareness within the organisation regarding data responsibilities and processing flows.

3.1.2. Structure of a ROPA

A well-structured ROPA should include the following sections:

1. **Organisation Details**
   Name and contact details of the data controller and/or processor, including any joint controllers, representatives in the EU (if applicable), and the Data Protection Officer (DPO).
2. **Purpose of Processing**
   A clear explanation of why personal data is being processed, linked to a lawful basis under the GDPR (e.g. consent, contract, legal obligation).
3. **Description of Data Subjects and Data Categories**
   The types of individuals whose data is processed (e.g. members, event participants) and the categories of personal data (e.g. names, contact details, ID numbers).
4. **Categories of Data Recipients**
   A list of internal and external parties with whom personal data is shared, such as service providers or public authorities.
5. **International Data Transfers**
   Details of any transfers of personal data outside the EU/EEA, including the third countries involved and safeguards in place (e.g. Standard Contractual Clauses).

6. **Retention Periods**
   How long each category of personal data will be stored and the criteria used to determine this.
7. **Security Measures**
   A general description of the technical and organisational measures used to protect personal data, such as encryption, access controls, and training.

In particular the **Record of Processing Activities of Controllers** (and Joint-Controllers) include the following information:

1. Name and Contact Details of the Controller and any Joint-Controllers
2. The purpose of processing
3. Description of the categories of Data Subjects and data collected
4. The categories of recipients
5. Transfers to third countries or international organisations with identification
6. Retention Periods
7. A general description of technical and organisational measures to protect data

In particular the **Record of Processing Activities of Processors** include the following information:

1. Name and Contact Details of the Processors, any additional Sub-processors, each Controller under which they act
2. The categories of processing carried out on behalf of the Controller (or Processor)
3. Transfers to third countries or international organisations with identification
4. Retention Periods
5. A general description of technical and organisational measures to protect data

The ROPA should be **regularly updated** to reflect changes in processing activities. It is not only a compliance tool but also a **valuable resource for improving transparency,** minimising risk, and responding to data protection authorities if required.

3.2. Checklist of Creating and Reviewing a Processing Activity

Step 1: Generalities ☐ What is the title of the processing activity? ☐ What is the purpose/are the purposes of the collection? ☐ Who is responsible? ☐ Data of Last Review of Processing ☐ Who is the Controller? Is there a Joint Controller? ☐ Active or Passive Processing?
Step 2: Description of the Processing Activity? ☐ What are the categories of data subjects? ☐ What are the categories of data collected? ☐ What is the data source?
Step 3: Lawfulness ☐ What is the legal basis of the purpose? ☐ What is the way of Collection? (direct vs. indirect collection)

☐ What is the place of storage? (drive, email, paper?) ☐ What is the time of collection? (throughout the year, a specific period/time) ☐ Privacy Policy Link
Step 4: Data Transfers and Sharing ☐ Is data shared within ELSA? ☐ Is data shared to any third party outside of ELSA?
Step 5: TOMs and DPIAs ☐ Are there any special Technical and Organisational Measures (TOMs)? ☐ Data Protection Impact Assessments

3.3. How to get the process started

Creating a ROPA for your ELSA group first and foremost takes time and a little patience. Your ROPA does not have to be perfect, but it is worth investing some time.

First hint: Think in areas.
ELSA is already a structured organisation. Divide your activities in areas (BEE, IM, FM, MKT, AA, C, PD, S&C). This division gives you a good overview of your individual activities in each area and you have a competent contact person for each area who knows about the individual events and procedures in the area.

Second hint: Divide the work into smaller sections.
It is a lot easier if you go through area by area, project by project, activity by activity.

Third hint: Start by brainstorming and rough mapping.
Firstly, think about what activities you already know. Firstly, think about which activities you already know. Where do you get your data from? What do you do with it? Where does it flow to? Does it leave your ELSA group again? Record your initial thoughts in writing. This can be in the form of a flow chart, in words or as a mind/concept map.

Fourth hint: Discussions.
Plan an appointment for each individual area to go through all the activities in the area together with the person(s) responsible. What do people do in their day-to-day work? Many processing activities are not immediately visible at first glance. Go through the process of creating a privacy policy as stated below. At this point do not worry about having it in a perfect manner. Your focus is to write everything down and to know what you actually do.

Fifth hint: Tidying up.
After having the discussions with the board and team member(s), it is the time to clean up the notes you have taken. Collect all missing responses and finalise your first ROPA.

Sixth hint: Get help.
At any point in the process of creating a ROPA you can always reach out to ELSA International (dataprotection@elsa.org) or other competent persons, to help you with any questions you may have.

3.4. How to create your ROPA

As all beginnings are difficult, we have a template for your ROPA ready. It is an excel file with a sheet for every area and is designed to help you be organised, structured and a helpful instrument. The following steps are guiding you through the process of identifying the processing activity entierly.

3.4.1. Step 1 - Generalities

What is the title of the processing activity?
First of you need to identify the processing activity. Therefore ask yourself which specific project or general activity is taken into consideration.
In practice and for our example this could be "organisation of an NCM".

What is the purpose / are the purposes of the Collection?
The next step is to define the different purposes of the collection and the processing. This shall be a brief description of why the data is collected and processed. In practice you will find quite a lot of different purposes for one processing activity.
In practice and for our example the different purposes for the processing activity "organisation of an NCM" are registering of participants, organising academic programme (workshops, plenaries), appoint NCM officer, manage application for NB, to give access to the voting platform, to provide meals, accommodation, additional services, to process health data in order to provide proper meals adapted to food restrictions, answer inquiries and provide support, to contact participants, to keep minutes available internally to the ELSA network, to maintain and improve NCM, to draft minutes of the NCM, to notify about changes made to the privacy policy, to comply with applicable legislation, for the legal enforcement of claims and rights, etc.

Date of last review of Processing
Indicate the date when you last reviewed the processing activity - be explicit and transparent!

Who is the Controller? Is there a Joint-Controller?
The second consideration is the identification of the controller or if applicable the joint-controller. For this you can consult once again the explanations done in this handbook in the chapter "Controller" on page 5.
In practice and for our example this is going to be a joint-controllership of the ELSA Group hosting the NCM and the ELSA National Group having the NCM.

Active or Passive Processing
The next step you are required to indicate is, if the data is processed actively or passively.
Active processing involves actively engaging with information, such as making connections, asking questions, taking notes, summarising information, structuring data, teaching others, and actively participating in discussions.
Passive processing, on the other hand, involves simply receiving and perceiving information without intentional effort to retain or engage with it.

3.4.2. Step 2 - Description of Processing Activity

Who is the category of Data Subjects?
In this section you are defining who the data subjects of your processing activities are. Here you can find a list of categories of data subjects:

- National/Local Group Representatives
- National Group Team Officers

- International Guest
- Chairs
- Auditors
- Representatives of the Board
- Representatives of former Boards for Relief of Responsibility
- Alumni
- Partners
- Speakers
- Emergency Contacts of Participant
- Participants of the project (and coaches of teams)
- Panelists
- …

Note that for one processing activity there may be several data subject categories applicable.

What are the Types of Personal Data Collected & Processed?

The following shall give you an overview of how data is typically defined in different categories within ELSA:

- Personal identification (name, surname)
- Contact information (e-mail address)
- Financial information (IBAN, amounts)
- ELSA Activity (ELSA Position, National Group of origin, Alumni Status)
- Emergency contact (name, surname, phone number)
- Professional and Educational Details (e.g. CV, level of studies completed, studies currently pursued; current and past occupation; education and knowledge background)
- Application process (e.g. motivation letter);
- Meal details (e.g. selection of meals)
- Health data (dietary restrictions, allergies and other special requirements)
- Transfer details, if applicable (e.g. time of pick-up, place of pick-up, flight number, departure and arrival)
- Accommodation details (period of stay, room, room preferences)
- Choice of additional services (Services and products purchased, prices)
- Event Activity; e.g.
    - ICM Activity (Workshops to attend, participation in the event, statements said during the sessions, presences, special role taken during the event (e.g. nominations committee, workshop chair)
    - Participation in the Competition (e.g. team number, clarification questions, written pleadings, assigned Regional Round, participation in the Final Oral Round);
    - Performance in the Competition (e.g. scores, evaluation by the panellists, prizes won, content of the team appearance sheets and team evaluation sheets);
    - Participation in the Law School (e.g. application to which SELS, attendance of academic and social programme, merch)

What is the data source?

In this section you will provide specific information about the way of collection and the data source from where you collected the data.

- Data can be collected **directly** (=the data subject provides you the data directly by themselves) and **indirectly** (=You receive the data indirectly without the involvement of the data subject).

- Further you need to provide the specific data source e.g. Website Form, JotForm, GoogleForm, Email, Word/Excel/pdf Document that is filled out and sent (through?), social media, etc.).

3.4.3. Step 3 - Lawfulness of Processing

What is the Legal Basis of the Collection?
This is the essential step of identifying the appropriate legal basis.
Data controllers can only process personal data in one of the following circumstances (legal bases):

- with the **consent** of the individuals concerned;
- where there is a **contractual obligation** (a contract between your organisation and an individual);
- to meet a **legal obligation** under EU or national legislation;
- where processing is necessary for the performance of a task carried out in the **public interest** under EU or national legislation;
- to protect the **vital interests** of an individual;
- for your organisation's **legitimate interests** (except if these are overridden by the interests or fundamental rights of individuals)

In order to find the correct legal basis you can consult the legal basis pathway. Please keep in mind that there is the possibility that more than one legal basis is applicable.

Consent
Your ELSA Group may decide to rely on **consent** for the processing of personal data.

If a data controller uses consent as a legal basis for the processing of personal data, they must **ensure that this consent is freely given, informed, specific and unambiguous.** This means that individuals must have a genuinely free choice regarding whether or not they agree with the processing of their personal data; they need sufficient information so that they can understand which data is processed, for what purpose, and how this is done; and they need to be able to freely withdraw their consent (without any negative consequences) if they change their mind later on.

If the organisation has to process the data and cannot truly enable individuals to withdraw their consent, this is an indication that consent is not the appropriate legal basis of the processing, and there is a need to assess if another legal basis could be applicable.

Checklist Consent

- ☐ give individuals the ongoing power to decide whether or not you process their data (genuine choice)
- ☐ no position of power over the individual (Individuals do not feel like they need to say yes)
- ☐ consent to processing is not a precondition of your service

Performance of a Contract
Processing the personal data of an individual for the performance of a contract is a valid legal basis, for example, in the following cases:

- Your ELSA Group needs to process an individual's personal data to provide a service.

- A potential member, participant or customer has asked you to do something before entering into a contract with your organisation, for example they may wish to receive a quote for the services that you provide, for which you may need to process some of their personal data.

The **processing must be necessary for the performance of a contract**. In practice, this means that your organisation cannot proceed with the execution of the contract or service without the personal data in question. It is recommended that your organisation documents the reasons explaining why the processing of an individual's data is necessary for the performance of a contract.

In addition, you should **try to collect the least amount of personal data necessary to perform the contractual service or for taking relevant pre-contractual steps**. In particular, you cannot use the contract to artificially expand the categories of personal data or types of processing operations. Rather, you should ensure that there is a genuine mutual understanding of the contractual purpose, based on the expectations of an average individual when entering into the contract.

This legal basis may also apply to certain actions related to contractual warranty, and to certain actions that can be reasonably foreseen and necessary within a normal contractual relationship, such as sending formal reminders about outstanding payments or correcting errors or delays in the performance of the contract.

This **legal basis does not apply, however, if you wish to process an individual's personal data for marketing purposes, fraud prevention, targeted advertising or any other purposes related to your organisation's business model.** In such cases, other legal bases may be available, such as consent or legitimate interest, provided that the relevant criteria are met. Legislations may also impose the processing of personal data, even after the termination of the contract (for instance, to keep records for accounting purposes). Naturally, the contract must also be valid under the applicable law.

Checklist Contract

- ☐ contract or intent to have a contract
- ☐ processing to perform the contract or carry out a pre-contractual request

Legal Obligation

The GDPR provides for another legal basis, namely: it is necessary for compliance with a legal obligation to which the data controller is subject.

This legal basis can be relied on where a processing operation is imposed on an organisation by EU or national legislation. More specifically, four conditions must be met:

- the legal obligation must be defined by EU or national law to which the controller is subject;
- these legal provisions must establish a clear and specific obligation to process that personal data;
- these provisions must at least define the purposes of the processing;
- this obligation should be imposed on the controller and not on the data subjects.

If these conditions are not met, the processing operation cannot be based on the legal obligation and another legal basis must be sought.

The GDPR provides for many different circumstances in which data controllers are legally obliged to process their customers' or clients' personal data. For example, employers usually need to process their employees' personal data for social security purposes, or a business often needs to process their clients' or customers' personal data for tax purposes.

Checklist Legal Obligation

- ☐ processing the personal data to comply with the law
- ☐ point the obligation set out in statute, common law or appropriate source of guidance

Vital Interests

Processing data to protect the vital interests of an individual can be relied on only in rare and specific cases. This may be the case, for instance, if you need to process personal data to protect someone's life. However, based on the GDPR, this legal basis is very limited in scope and can only be relied on in the case of emergencies.

Checklist Vital Interests

- ☐ processing the personal data to save or protect someone's life
- ☐ cannot reasonably protect their life without processing the data
- ☐ Is any other lawful basis obviously available? (In particular give consent for any health data?)

Public Interests

In some specific cases, your organisation may be able to process individuals' personal data for a task carried out in the public interest. In this case, the processing must have a basis in EU or national law. Its purpose must be determined in that legal basis or be necessary for the performance of a task carried out in the public interest or in the exercise of official authority vested in the data controller. Therefore, this legal basis may be relevant, in particular, for processing operations by public authorities for the purpose of carrying out their tasks.

Checklist Public Interest

- ☐ processing the data to carry out your official tasks, functions or specific tasks in the public sector
- ☐ point to a clear basis in law for your task or function

Legitimate Interests

Your organisation may be able to process individuals' data for matters of legitimate interests, provided that these interests (commercial, protecting your property, etc.) do not create an imbalance to the detriment of the rights and interests of individuals.

While the GDPR and relevant case law of the Court of Justice of the European Union (CJEU) provide for examples of legitimate interests, there is no exhaustive list.

However, you must ensure that this interest respects a certain number of requirements:

- it must be lawful, clear, real and present;
- the processing must be a necessary for pursuing this interest;
- the legitimate interest must take into account the individual's rights to data protection, which cannot be overridden. In the context of this requirement, the controller must

weigh its legitimate interest and the interests or fundamental rights and freedoms of individuals and must also consider what they may reasonably expect. This balancing exercise must be made in light of the concrete conditions under which these operations are carried out.

Checklist Legitimate Interest

- ☐ identify a legitimate interest
- ☐ legitimate interest compelling enough to justify the potential impact on individuals (inability of exercise rights, loss of control over the use of data or any other disadvantage)
- ☐ no other reasonable way to achieve your purpose without processing the data

Time of Collection

Indicate when this set of data is collected exactly (e.g. date, month(s), period of application, throughout the year, etc.). The time of collection may help you further for the determination of the retention period.

Place of Storage

Indicate here where you store your collected data. This could be your google drive, paper archive, gmail or any other kind of storage. This shall simplify the case of individuals exercising their rights in relation to GDPR and also helps as guidance for any archiving activities.

Retention Questions

Within the subject of retention you first need to set the retention period. This is the period of time for how long you store and retain the data as it is in your storage. Common retention periods are until the termination of an event, end of the term (31st of July), 2 years or even 5 years. Depending on the data this period can vary. It is advisable to set the date to the 31st of July as the end of the term to simplify your archiving process. In this case most probably there is data that needs to be stored longer (financial data, board information) to meet legal requirements.

As soon as the retention period terminates you are obliged to delete or in some cases at least irreversibly anonymise the data. In the ROPA you will therefore indicate if you have deleted the data from previous terms in order to fulfill your obligations of archiving and deletion of data.

Privacy Policy Link

For your own help and overview indicate if there is a privacy policy in place and when it is last updated.

3.4.4. Step 4 - Data Transfers and Sharing

Transfers within ELSA

For your own overview and the transparency of your processes, you need to clarify if and to whom you are sharing the data within ELSA. This can be:

- Your own National/Local Board
- Your own National/Local Team
- Your own National/Local Council
- Your Local Groups
- ELSA International

- Other National/Local Groups
- Organising Committees

Transfers to other third parties (outside of ELSA)
The next question you need to answer is if the collected data is being transferred to anyone outside of your ELSA Group? This can be:

- Cloud Software Providers (Google, Microsoft, cloud service providers, Mailing Providers, etc.)
- Online Meeting Platforms (Google Meet, ClickMeeting, Zoom…)
- IT Software Providers
- Public agencies and institutions (e.g. tax authorities)
- Partner organisations who we engage with in the course of the performance of your tasks
- Auditors and payroll tax auditors
- Accommodations
- Restaurants, Bars, Clubs,...
- International Organisations (UN, Council of Europe, etc.)
- Partners
- Speakers
- Event Organiser (Museum, Institutions, etc.)
- Etc.

If you are transferring data to a third party, indicate the contractual basis for this data transfer.

Further you are obliged to indicate if data is transferred outside of the EEA with the specific countries involved. This is not only important when individuals are exercising their Data Protection Rights but moreover shall help you when drafting any privacy policies or data protection agreements.
Especially when transferring data to third parties you need to indicate if you have taken any additional measures to protect the data. This includes but is not limited to annexes to the data protection agreement made, any other clauses in any agreement made with them, sharing specifications (platform used, password protection, etc.).

3.4.5. Step 5 - TOMs and DPIAs

The last step when filling in the ROPA are as previously mentioned any special measures taken throughout the collection and processing of data in this specific processing activity. These measures need to be set out in your own Technical and Organisational Measures (TOMs). A document containing all these measures, template TOMs as minimal standards within ELSA can be found here.

The very last part is the indication of Data Protection Impact Assessment (DPIAs). Data Protection Impact Assessments are required by law under certain conditions according to article 25 of the GDPR. These situations are some examples of such:

- If you are using new technologies
- If you are tracking people's location or behavior
- If you are systematically monitoring a publicly accessible place on a large scale
- If you are processing personal data related to racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade union membership, and the processing of genetic data, biometric data for the purpose of uniquely identifying a natural person, data concerning health or data concerning a natural person's sex life or sexual orientation.

- If your data processing is used to make automated decisions about people that could have legal (or similarly significant) effects.
- If you are processing children's data.
- If the data you are processing could result in physical harm to the data subjects if it is leaked.

None of the above mentioned situations applies in the general day to day work of ELSA. Therefore, you are not required to have Data Protection Impact Assessments. However, it may still be prudent to conduct a DPIA to minimise your liability and ensure best practices for data security and privacy are being followed in your ELSA Group.

3.5. How to review your ROPA

You should review your ROPA on a regular basis. The easiest way to keep a clean and neat ROPA is to update it as soon as you are identifying any changes or as soon as you implement a change in your process. However, it is advised to do a review at least once every term.

When approaching the review, make sure you have the people involved with the processing activities nearby. It is important to reflect the reality of processing activities, not a dream perspective of it. You will go through every processing activity and always ask yourself if this is the reality in your ELSA Group and take the checklist mentioned above as a guide through the processing activities.

4. Privacy Policies

4.1. Basics about Privacy Policies

What is a Privacy Policy?
A privacy policy is a formal **document that explains** how an organisation collects, uses, stores and protects personal data. It **informs individuals** about what data is processed, why it is processed and their rights regarding that data. A privacy policy **ensures transparency** and helps us build trust between ELSA and our members. .

Obligations covered
Under GDPR, organisations are required to **provide clear and accessible information about their data processing activities**. This includes specifying the purposes of processing, the legal basis for processing, data recipients, data retention periods and how individuals can exercise their rights. The privacy policy must also explain how personal data is safeguarded and include contact details for questions or complaints.

Structure of a Privacy Policy
A Privacy Policy is made of two sections: a Summary Section for overview and a Detailed Section to explain all your processing activities. The following table is showing you how such a Privacy Policy may be structured as we have it structured in the template.

Summary Section	Detailed Section
• Who we are • Personal Data we process • Purposes of the Processing • Your Rights	1. About us 2. Personal Data Collection a. Categories of Personal Data Collected b. How we collect personal data 3. Legal Basis and Purposes 4. Data Retention 5. Data Transfers & Sharing a. Data Recipients b. Third-Country and International Organisations Transfers c. Data Disclosure 6. Data Security 7. Your Rights 8. Changes to the Privacy Policy 9. Contact us

Where to get needed information
To create an accurate and comprehensive privacy policy, it is important to gather information about how personal data is handled within the organisation. This includes identifying what types of data are collected, how and why they are collected, where the data is stored and with whom it is shared. The easiest way is if you have a Record of Processing Activities (ROPA). The ROPA summarises all information you will need in order to write your Privacy Policy.

4.2. How to create your Privacy Policy

Preparations

Before you start writing your Privacy Policy you need to make sure that you have all materials needed in place:

1. If you have a **ROPA**, the creation of a privacy policy is going to be quite simple, as it is like assembling a puzzle. If you do not have a ROPA, you are advised to get all the information needed for a privacy policy by following the questions stated in the chapter about ROPA of this handbook.

2. Check the ROPA, if the processing in question is already covered by your ROPA, and if so if there is anything missing. If there are any questions left unanswered in the ROPA, please make sure to talk to the responsible person (Person indicated in column D of the ROPA Template) of the processing and get all the information you need.

3. Prepare your Privacy Policy Template to get your privacy policy. As all beginnings are hard, you can access our Privacy Policy Template here - please be aware, that the template by no means claims to be complete or legally valid- it serves as an aid and is intended to provide guidance. In particular, national laws must be observed when applying it.

The Policy Itself

After having all preparations in place the writing of the policy takes its turn. On the basis of the information of the ROPA you are able to fill in all parts of the template and build your custom privacy policy. The following table aims to give guidance on what is needed to be implemented and where to find the information on the ROPA. Please be aware to cover all purposes under the processing activity!

The Summary

Section	What to do	Where to find it in ROPA Template
Who we are	Implement the Contact Details of the Controller or where applicable Joint-Controllers. Contact Details needed are Name/Organisation, Address, E-Mail and Phone Number	Column F "ELSA's Role in the Data Processing"
Personal data we process	Add all categories of Personal Data Collected & Processed including the exact data set in bullet points	Column I "Type of Personal data Collected & Processed"
Purposes of the Processing	Add all purposes listed under the processing activity in bullet points	Column C "Purpose of Collection and Processing"
Your Rights	Nothing. Leave section as it is in the template.	–

The Detailed Section

Section	What to do	Where to find it in ROPA Template
About us	Implement the Contact Details of the Controller or where applicable Joint-Controllers. Contact Details needed are Name/Organisation, Address, E-Mail and Phone Number	Column F "ELSA's Role in the Data Processing"
About us	(if applicable) For Joint Controllers: Add purposes for which you act as sole controller	Column C "Purpose of Collection" is added if Column F "ELSA's Role in the Data Processing" states "Controller" (not "Joint-Controller" nor "Processor")
Personal data we process	Categories of Personal Data Collected Add all categories of Personal Data Collected & Processed including the exact data set in bullet points	Column I "Type of Personal Data Collected & Processed"
Personal data we process	How we collect personal data Indicate from where you acquire the data (specific data source) and separate in direct and indirect collection	Column K "Specific Data Source" with the help of Column J "Way of Collection"
Legal Basis and Purposes	Add all purposes listed under the processing activity in bullet points according to the legal basis	Column C "Purpose of Collection and Processing" according to section L-R "Legal Basis of Processing, Secondary Legal Basis of Processing, Additional Legal Basis…"
Data Retention	Nothing. Leave section as it is in the template.	–
Data Transfers & Sharing	Data Recipients Add all recipients of this processing activity	Column Z-AC "Is Personal Data Transferred inside ELSA, To Whom, Third Parties, To Whom" (be aware that you do not need to list the Controller & Joint-Controllers, this includes the respective Board and Team or OC.
Data Transfers	Third-Country and International Organisation Transfer	

& Sharing	• If you are sharing the data to any International Organisations indicate here. • List all countries	Column AC "Third Parties - to whom?" Column AF "To which countries"
Data Security	Nothing. Leave section as it is in the template.	–
Your Rights	Nothing. Leave section as it is in the template.	–
Changes to this Privacy Policy	Check the days for notification of changes are applicable and reasonable for you	–
Contact us	Indicate the Contact Details of you as Controller	Column F "ELSA's Role in the Data Processing"

4.3. How to implement Privacy Policies

4.3.2. Consent Banner

After having written the privacy policy, you need to **publish it where the individual is providing you with their information**. Most probably this will be application forms or your website.

Make sure that you include **any consent banner** where they are needed. If you have to insert such a consent banner, keep in mind the following points:

Checklist Consent Banner

- ☐ Freely given: Consent must be given voluntarily, without coercion or pressure
- ☐ Specific: Consent should be obtained for specific purposes, not blank agreement; specify the purpose for which the legal basis is consent
- ☐ Informed: Users need clear information about what they are consenting to (make sure to include all types of data collected, how it will be used, and who it will be shared to).
- ☐ Unambiguous: Consent must be indicated by a clear, affirmative action, such as clicking an "accept" button.
- ☐ Equal Prominence: "accept" and "reject" buttons should be displayed with equal prominence and accessibility.
- ☐ No Pre-ticked boxes
- ☐ Easily withdrawn: It should be as easy to withdraw consent as it is to give it. Inform users how to withdraw consent.
- ☐ Use clear and simple language.

The following box would be a good example for the implementation and creation of a consent banner:

What we need your consent for:
Below you will find specific data processing activities for which we ask for your prior consent in order for them to take place. This means that before doing so, we will not process your personal data for these specific purposes.

To share your personal data with the Council of Europe. They are granted access to your personal data solely to the extent required to:

- Contact you regarding visibility materials;
- Send and deliver visibility materials to you;
- Contact you regarding the Study Visit in the case you are selected as the winner of the Annual Human Rights Campaign Competition.

The data we collect: Name, surname, ELSA e-mail address, phone number and ELSA position.

What This Means: By saying "yes", you are allowing us to gather the above mentioned personal data in order to contact you as a prospective Trainer or member of the Organising Committee of future editions of the Train the Facilitators' Conference of the Rule of Law Education Programme. By saying "no", we will not collect, store or share the above mentioned personal data. Bear in mind that we will also be unable to contact you in the future in order to become a Trainer or member of the Organising Committee of a future edition of the TtF
Your consent: By selecting "I hereby consent to the processing of my data" you explicitly authorise us to start processing the personal data mentioned above for the purpose you consent to. Additionally, you can reject this processing through the "I do not consent to the processing of my data" button. If you choose this latter, we shall not process your personal data for those purposes.
Your rights: You retain the right to revoke this consent at any time, affecting future processing, but not the lawfulness of the processing done before the withdrawal. Additional details are available in our Privacy Policy for the Annual Human Rights Campaign. You may reach out to us with any privacy-related inquiry at: secgen@elsa.org.

☐ Yes, I hereby consent to the processing of my data.
☐ No, I do not consent to the processing of my data.

4.3.1 Changes to a Privacy Policy

Privacy Policies have to be up-to-date. If you are changing any of your activities, please make sure to adapt your privacy policy accordingly. Keep in mind that you need to inform about the changes made.

In practice this means the following: You are organising a webinar and therefore the participants were able to sign up through an online form. After the termination of the application period you decide to send the participants an evaluation form after the webinar. Unfortunately you did not include anything about evaluation in your privacy policy. Therefore, you are adding a new purpose which says "To evaluate and improve webinars" and further add in the section on direct collection the evaluation form. After this amendment of the privacy policy you are sharing the new privacy policy with all participants. The new privacy policy comes into force after 7 days of the publication to the participants (according to your privacy policy in section "8 - Changes to this Privacy Policy".

5. Data Subjects Rights

One of the aims of the GDPR is to empower individuals and give them control over their personal data. The GDPR has a chapter on the rights of data subjects (individuals) which includes the right to be informed, the right of access, the right to rectification, the right to erasure, the right to restrict processing, the right to data portability, the right to object and the right not to be subject to a decision based solely on automated processing. **Please note that some of those rights do not apply in all situations!**

5.1. The Rights

Under the GDPR, data subjects have rights that need to be complied with by data controllers, under the conditions set out therein. These rights are:

- Right to be informed
- Right of access
- Right of rectification;
- Right of erasure;
- Right of restriction
- Right to data portability;
- Right to object;
- Right to withdraw consent;
- Right not to be subject to a decision based solely on automated processing.

It is important to bear in mind that these rights are directed towards controllers. In cases where ELSA operates as a processor, its role is limited to assisting the controller comply with its obligations under the GDPR. Furthermore, in situations of joint-controllership, the agreement between the parties establishes who is responsible for fulfilling data subjects' rights.

5.1.1. Right to be informed

Right to be informed	right to obtain confirmation as to whether their personal data is being processed and, if so, access to that data along with information about the processing activities.
Requirements to accept the request	Exceptions
All data subjects have the right to receive information when you process their data.	The data subject already has the information. However, where the information is incomplete, the controller must supplement it accordingly (this applies to personal data both collected directly and obtained indirectly).

In practice: The following table shall explain which information you need to provide depending on whether you have collected the personal data directly from the data subject (direct collection in accordance with Art. 13 GDPR) or whether you have obtained it from another source (indirect collection in accordance with Art. 14 GDPR).

Information	Direct	Indirect
The purpose of the processing	✔	✔
The legal basis of the processing	✔	✔
The identity of the controller	✔	✔
Contact details of the controller	✔	✔
The recipients or categories of recipients of the data	✔	✔
Information if the data will be transferred outside the EEA	✔	✔
If legal basis is legitimate interest: specific information about the legitimate interest relate to the specific processing	✔	✔
The categories of personal data processed		✔
The source of personal data		✔
Retention period	✔	✔
If the data subject is required to provide the personal data (by law or by contract or to enter into a contract) and what the consequences of refusing to provide the data are	✔	

A good way of providing information is to work with different layers of information. This avoids that an excessive amount of information is provided at one time, which may be detrimental to transparency and drown the data subject with information. This not only simplifies the task of the controller but also allows the data subject to grasp the essential information quickly and efficiently. The presentation of information could be as follows:

A first layer of basic information	
WHAT? Provide a summary of the basic information that the data subject needs to assess the impact and scope of the processing	HOW? For instance in a table format, clearly visible
A second layer of additional information and more detailed information	
WHAT? Part presents in an understandable and comprehensive way the remaining information that the organisation is required to provide under Art. 13 & 14 GDPR	HOW? By means of hyperlinks included in the basic information, drop down format…

5.1.2. Right of Access

Right of access	right to request and receive a copy of their personal data, along with details on how and why it is being processed.
Requirements to accept the request	Exceptions
All data subjects have the right to access when you process their data.	Where the controller holds a large quantity of data relating to the data subject, they may ask the data subject to specify the information or processing activities to which their request relates. Where granting access to the data would affect other rights (e.g., trade secrets, intellectual property rights), the controller may restrict or refuse to provide the data requested (following assessment).

In practice: When individuals are exercising their right of access, data subjects should get a confirmation from the controller as to whether or not their personal data is being processed. If this is the case, data subjects have access to their personal data and the following information:

- the purposes of the processing;
- the categories of personal data concerned;
- the recipients (or categories of recipients) of the personal data;
- the retention period for the personal data, or the criteria used to determine that period;
- the existence of the right to request from the data controller rectification or erasure of personal data or restriction of processing of personal data concerning the data subject or to object to such processing;
- the existence of the right to lodge a complaint with a data protection authority;
- the source of the data (when the personal data is not directly collected from the data subject);
- the existence of automated decision-making, including profiling, meaningful information about the logic involved, as well as the significance and the envisaged consequences of such processing for the data subject;
- when personal data is transferred out of the European Union, all the appropriate safeguards put into place (pursuant Art. 46 GDPR relating to data transfers).

Before you provide a copy of the personal data, you must check that doing so will not affect the rights and freedoms of others (e.g. if information relating to more than one person is processed in the same file, or information relating to trade secrets and intellectual property).

5.1.3. Right of Rectification

Right of rectification	personal data is inaccurate or incomplete, data subjects can request that it be corrected or updated.
Requirements to accept the request	Exceptions
The request is to be accepted if the data subject provides reasonable evidence that the personal data is incorrect.	None.

In practice a participant informs you that they have moved to another city. You are required to change their address in your member database.

5.1.4. Right of Erasure (Right to be forgotten)

Right of Erasure	Individuals can request the deletion of their data when it is no longer needed, consent is withdrawn, or processing is unlawful.
Requirements to accept the request	Exceptions
• the personal data is no longer necessary for the purpose for which they were collected • the organisation processes the personal data unlawfully • the organisation has to erase the personal data due to a legal obligation • the data subject withdraws consent and the processing has no other legal basis • the data subject has successfully exercised the right to object • minors who have given their consent to use an online service can always request the erasure of such personal data (regardless of their current age)The personal data is no longer necessary for the purposes it was collected for	• the exercise of the right to freedom of expression and information; • the establishment, exercise or defence of a legal claims; • compliance with a legal obligation to which the organisation is subject or the performance of a task in the public interest or in the exercise of official authority entrusted to the organisation; • reasons of public interest in the area of public health; • archiving purposes in the public interest, scientific or historical research purposes or statistical purposes (under specific conditions).

In practice a former ELSA member no longer wishes to receive marketing emails from your ELSA Group and requests that you erase their contact details. As there are no compelling reasons for you to continue processing the contact details, you must erase them.

5.1.5. Right of Restriction

Right of Restriction	Data subjects can ask to limit the processing of their data, for example, while its accuracy is being checked.
Requirements to accept the request	Exceptions
• The accuracy of the personal data is contested, for the period enabling ELSA to verify its accuracy; • The data subject has objected to the processing, pending the verification of whether ELSA's legitimate grounds override those of the data subject; • The processing is unlawful and the data subject only requests the restriction (and not e.g. erasure); • ELSA does not need the personal data anymore for the purposes it was originally collected for, but they are required by the data subject for the establishment, exercise or defence of legal claims.	If the restriction is lifted, the data subject must be informed before this takes place. If the data subject successfully exercises their right to restriction of the processing, your ELSA Group can only use the data in certain specific circumstances, for example with the consent of the data subject or for the defence of legal claims

In practice: Have you previously passed on the 'restricted' data to other recipients? You must then inform these recipients of the restriction of processing, unless this proves impossible or requires disproportionate efforts.

5.1.6. Right to Data Portability

Right to Data Portability	Individuals can request their data in a structured, machine-readable format (e.g. XML, JSON, CSV; pdf format is not sufficient) and have it transferred to another controller.
Requirements to accept the request	Exceptions
The request is to be accepted if, cumulatively: ● the data processing is based on consent or a contract; ● the data processing is carried out by automated means; and ● the data subjects have provided the data themselves. This includes also any data that your organisation has observed based on the data subject's behaviour (e.g. with connected accessories).	If any of the three mentioned requirements is not applying, the request can be denied.

In practice: Make sure that your data storing is in a clean manner, that the exercise of the right to data portability is not causing too much effort on your part.

5.1.7. Right to Object

Right to Object	Data subjects can object to processing based on legitimate interests of the controller or of a third party; or for direct marketing, requiring the controller to stop unless compelling reasons exist.
Requirements to accept the request	Exceptions
● The data processing is based on the legitimate interests of ELSA and the data subject objects on grounds related to his/her particular situation; ● The objection relates to a decision based on solely automated processing which produces legal or similarly significant results on the data subject); or ● The objection relates to the processing for direct marketing purposes.	The objection to data processing based on the legitimate interests of ELSA (first condition) shall only be accepted if ELSA does not have compelling legitimate grounds that override the interests and the particular situation of the data subject (e.g. for the establishment, exercise or defence of legal claims).

In practice: In other situations, the data subject cannot use the right to object because, for the other legal bases, there are alternatives to achieve the same purpose: in case of consent, the data subject can simply withdraw consent. The data subject cannot object to a processing imposed by law.

When data subjects exercise their right to object, your organisation needs to balance the interests of both parties. It shall cease all processing of this personal data unless it can show compelling legitimate reasons that override the rights and freedoms of the data subject (e.g. it is pursuing a legal action). Your organisation must document and communicate these reasons to the data subject.

When the data is processed for marketing purposes, the data subject has a right to object to this processing without providing any reasons. In this case, the reasons why your organisation is processing this data are not of relevance, instead the objection must lead to the immediate end of the processing for this purpose.

5.1.8. Right to Withdraw Consent

Right to withdraw consent	Individuals can revoke their permission for the processing of their personal data at any time, after having initially given it.
Requirements to accept the request	Exceptions
The data subject informs of what processing activities he/she is withdrawing consent from.	The processing only needs to be stopped if there is no additional legal basis for the processing.

In practice It should be as easy to withdraw as to give consent. If consent is withdrawn your ELSA Group can no longer process the data. Once consent has been withdrawn, your ELSA Group needs to ensure that the data is deleted unless it can be processed on another legal ground (for example storage requirements or as far as it is a necessity to fulfil the contract).

If the data was being processed for several purposes your ELSA Group can't use the personal data for the part of the processing for which consent has been withdrawn or for any of the purposes, depending on the nature of the withdrawal of consent.

5.1.9. Right not to be subject to a decision based solely on automated processing

Right not to be subject to an automated decision process.	Individuals have the right not to be subject to decisions made solely by automated means that significantly affect them, unless certain safeguards apply.
Requirements to accept the request	Exceptions
For this right to apply, the automated processing must entail: ● a decision that is based exclusively on automated processing, without human intervention. This means that no natural person has any significant control over the decision and cannot, for example, change or reverse the decision; and ● a decision which has legal effects for the data subjects or which significantly affects them.	Exceptions are made when the decision is based on one of the following: ● Contractual necessity; ● Union law; ● The data subject's consent (!be aware of the right to withdraw consent).

In practice a decision that significantly affects the person could be found in the following examples (though of course context must always be taken into account when evaluating if the impact on the data subject is significant) :

- decisions that affect people's financial circumstances, such as their eligibility to withdraw credit;
- automatic refusal of applicants who apply via an online platform;
- price differentiation based on a consumer's browsing history and purchasing habits;
- decisions that affect someone's access to education, for example university admissions.

If **sensitive data is involved**, the automated decision making is only possible on the basis of explicit consent or a substantial public interest under Union or national law and you need to take suitable measures to safeguard the data subject's rights, freedoms and legitimate interests.

5.2. Which rights come in place with which legal basis?

	Consent	Contract	Legal Obligation	Vital Interests	Public Interest**	Legitimate Interest
Information	✔	✔	✔	✔	✔	✔
Access	✔	✔	✔	✔	✔	✔
Rectification	✔	✔	✔	✔	✔	✔
Erasure	✔	✔	✘ Not applicable*	✔	✘ Not applicable	✔
Restriction of processing	✔	✔	✔	✔	✔	✔
Portability	✔	✔	✘ Not applicable	✘ Not applicable	✘ Not applicable	✘ Not applicable
Object	✘ Not applicable: Withdraw consent instead	✘ Not applicable	✘ Not applicable	✘ Not applicable	✔	✔ At all times for Direct Marketing
Not fully automated decision incl. profiling	Right to a human intervention	Right to a human intervention	Right to a human intervention	✔	✔	✔

*Erasure can be requested if the personal data has to be erased for compliance with a legal obligation.
** The basis for processing must be laid down by Union or Member State law.

5.3. How to handle data subject rights request - The process of a Request

Best Practice how the process of request is structured within ELSA International
To comply with GDPR, we must respond to data subject rights requests in a timely, fair, and secure manner. When a request is received, it should be acknowledged promptly. If necessary, steps should be taken to verify the identity of the individual before proceeding.

Once verified, we must assess the nature of the request, determine whether it is valid under the law, and gather the relevant data. A full response must be provided within one month of receiving the request. This deadline may be extended by up to two additional months for

complex or multiple requests, but the data subject must be informed of the extension and the reasons for it.

All requests and responses should be documented for accountability. If data is to be shared, it must be transmitted securely to protect confidentiality. Anyone whose data is processed can submit a request. There is no need to explain the reason for the request. A request may also be made on someone else's behalf with proper authorisation, such as from a parent, legal representative or guardian

It is good practice to appoint someone responsible for overseeing the request process. While this is often the Data Protection Officer, they do not need to respond to every request themselves. Automation and clear procedures can help ensure all requests are tracked and answered on time.

5.4. How to implement Data Subject Rights Process

Implementing a process for handling data subjects' rights under the GDPR requires a clear and coordinated approach across the organisation.

Checklist of what do do concerning data subject rights:

- ☐ **Be prepared**: Develop systems and procedures to respond to data subject rights requests and train your officers to integrate data subject rights requests into your internal workflows
- ☐ **Know your data flows**: Keep your register up to date to rapidly identify the data you process and to locate and retrieve information efficiently.
- ☐ **Facilitate the exercise of rights**: Make it easy for data subjects to know what their rights are and how to contact you to exercise them
- ☐ **Be transparent**: Always inform data subjects in a clear and understandable way about the personal data you process, prior to the processing (for instance in your privacy policy) and during the processing (for instance when complying with a data subject access request).
- ☐ **Answer within 1 month**: Always answer a data subject request within one month. If you need additional time to answer or if you cannot comply with the request: inform the data subject of this within the one month period.
- ☐ **Pass it on**: When you receive a request concerning personal data you have transferred to other recipients, do not forget, if need be, to inform the recipients of the result of the request.
- ☐ **Document**: Keep track of requests from data subjects, and record your answers, also keep track of your reasoning when you do not reply to a request.

Create your own Data Subject Rights Policy to ensure all steps are taken when a request is submitted. You can find a template here.

6. Data Breaches

6.1. What is a personal data breach?

A personal data breach can be broadly defined as a **security incident that has affected the confidentiality, integrity or availability of personal data**. In short, there will be a personal data breach whenever any personal data is accidentally lost, destroyed, corrupted or disclosed; if someone accesses the data or passes it on without proper authorisation; or if the data is made unavailable and this unavailability has a significant negative effect on individuals.

In practice personal data breaches can include:

- access by an unauthorised third party;
- deliberate or accidental action (or inaction) by a controller or processor;
- sending personal data to an incorrect recipient;
- computing devices containing personal data being lost or stolen;
- alteration of personal data without permission; and
- loss of availability of personal data.

Such typical examples of data breaches are sending emails to an open mailing list using CC instead of BCC, loss of a data carrier (e.g. a pen drive, hard drive, laptops); hacking from third parties or system malfunctions that lead to the disclosure of customer data.

Organisations are expected to implement appropriate technical and organizational measures (TOMs) to prevent data breaches from occurring in the first place. However, data breaches may at all times occur. In the following parts you can find our suggestion to you how to handle a data breach as an ELSA Group.

6.2. Checklist Preparing for an incident of personal data breach

Before you can handle a Data Breach in a professional and secure way, we recommend that you do some preliminary preparations, which includes the following:

- ☐ You know how to recognise a personal data breach.
- ☐ You understand that a personal data breach isn't only about loss or theft of personal data.
- ☐ You have prepared a response plan for addressing any personal data breaches that occur (see next part "Response Plan for addressing a personal data breach")
- ☐ Controllers: You have allocated responsibility for managing breaches to a dedicated person or team. (e.g. Secretary General, Director for Data Protection)
- ☐ Processors: You know the responsible person or team of the controller for managing breaches and how to inform them.
- ☐ Your officers know how to escalate a security incident to the appropriate person or team in our organisation to determine whether a breach has occurred.
- ☐ Have a data breach response policy (containing its purpose & your procedure).

6.3. Checklist Response Plan in case of a data breach

- ☐ We have in place a process to assess the likely risk to individuals as a result of a breach.
- ☐ We have a process to inform affected individuals about a breach when their rights and freedoms are at high risk.
- ☐ We know we must inform affected individuals without undue delay.
- ☐ We know what information about a breach we must provide to individuals, and that we should provide advice to help them protect themselves from its effects.
- ☐ We document all breaches, even if they don't all need to be reported.

6.4. Response Plan for addressing a personal data breach

This suggested response plan for addressing a personal data breach contains two parts. First of all you need to assess the risk to the individual. If the risk is high, you need to inform the individual about the data breach - therefore there is a second part about the process for informing the affected individual.
These processes are summarised and set in a so-called Data Breach Response Policy.

6.4.1. Response Plan for assessing the risk

1 Emergency mitigation measures and assessment of the breach	Once you become aware or suspect the occurrence of a data breach, whether terminated or ongoing, you are to: ● Assess whether any immediate mitigation measures are required; ● Determine whether personal data is affected. You are only to communicate with parties outside ELSA if and to the extent required to mitigate any immediate risks. Before doing so, you will obtain approval from the National/Local Board. Furthermore, depending on whether personal data is affected or not, you will have the following possibilities: ● If personal data is involved, advance to the next step; ● If personal data is not involved, report the security incident to your IT team.
2 Internal Escalation	You have to report the data breach immediately and at the latest **within an hour** to the **person responsible for data breach management** (e.g. Secretary General or Director for Data Protection). The following information needs to be provided with the report: ● Type and description of the data protection violation that occurred; ● Date, time and duration of the data breach; ● The affected (categories) of data subjects and, to the extent possible, the number of affected data subjects; ● The affected (categories) of personal data and, to the extent possible, the number of affected personal data records; ● What are the risks identified for data subjects; ● What are the further mitigation actions that are suggested to be taken;

	• What further information is required to mitigate the mentioned risks.
3 Initial assessment of the data breach	The person responsible for data breach management makes an initial assessment of the data breach in cooperation with the relevant departments. This assessment needs to be made **within 24 hours** of the initial awareness of the data breach (in Step 1). The assessment focuses on: • The risk for data subjects derived from the data breach; • What further immediate mitigation actions are to be taken; • Whether any reporting obligation applies to you, relating to the data controller and the data subjects.
3.1. Definition of the risk	When analysing the risk posed by the data breach, the person responsible for data breach management shall take the following elements into consideration: • The possible damage (e.g. discrimination, identity theft, fraud, financial loss or damage to the reputation of the data subjects); • Estimation of the probability of occurrence and severity of the identified damages, considering, namely: ○ The category(ies) of data subjects affected (e.g. children, health patients require additional protection); ○ The number of data subjects affected; ○ The number of people who were/are able to access or in general had/have access to personal data as a consequence of the data breach; ○ The category(ies) of personal data affected (e.g. special categories of data and other particularly sensitive information such as banking details require additional protection); ○ The duration of the data breach (the longer it lasts, the more damaging it may be); ○ The possibility to revert or mitigate the risks caused by the data breach; ○ Other relevant details of the data breach and the affected datasets that show particular importance.
3.2. Notification requirements	Report to data subjects • If there is a high risk to the rights and freedoms of natural persons, or under the instruction of the supervisory authority **and** • ELSA acts as Controller or joint-controller, and acts according to the distribution of responsibilities between the joint-controllers. Report to the controller • If ELSA acts as a processor **or** • ELSA acts as joint-controller and acts according to the distribution of responsibilities between the joint-controller.

6.4.2. Response Plan for Notification to Data Subjects

4 Notification of Individuals	When a decision to report to data subjects has been taken, this must be done **without undue delay**. This notification shall, in clear and plain language, include: • A description of the nature of the data breach; • The name and contact details of the DPO (if applicable) and the person responsible for data breach management; • The likely consequences of the data breach; • The measures taken or proposed to address the data breach.

We recommend, that the communication to the data subject shall not be required if:

- ELSA has implemented appropriate technical and organisational protection measures, and those measures were applied to the personal data affected by the data breach, in particular those that render the personal data unintelligible to any person who is not authorised to access it, such as encryption;
- ELSA has taken subsequent measures which ensure that the high risk to the rights and freedoms of data subjects that were identified are no longer likely to materialise;
- It would involve a disproportionate effort. In this case, ELSA shall make a public communication or similar measure whereby the data subjects are informed in an equally effective manner.

6.4.3. Response Plan for Notification to the Controller

5 Notification to the Controller	When a decision to report to the controller has been taken, this must be done in accordance with the respective data processing agreements, **typically within 24 hours** of becoming aware of the data breach. Any communication to the controller shall: • Only contain facts relating to the breach. This includes the timeline, description of the data breach, personal data and data subjects affected, measures taken and proposed; • Avoid legal assessments, as it is up to the controller to decide on any legal assessment (e.g. avoid stating whether a notification to the regular or data subjects is required); • Avoid statements regarding who is at fault and premature conclusions. At such an early stage, it is often too soon to identify who was at fault for the data breach. Focus on reporting the facts.

6.5. Record Keeping of Data Breaches

Organisations as ELSA must maintain records of all data breaches, regardless of whether notification is required. Following the closure of the data breach the person responsible for data breach management must update ELSA's incident register.

To that end, the person responsible for data breach management must conduct a review of the response procedure followed during the data breach to determine and appropriately register:

- Adequacy of the response given to the breach;

- Impact on ELSA before and after the corrective actions that were taken;
- Risks identified that were not closed as part of the management of the breach;
- Review of similar breaches over time to consider whether additional controls/measures are required.

DISCLAIMER on the important limitation regarding supervisory authorities

Please be advised that the approach and content of this handbook do not include detailed procedures or guidance for reporting data breaches or other data protection incidents to relevant supervisory authorities, even where such reporting might be legally prescribed under applicable data protection laws (e.g. GDPR, national data protection acts).

Why this aspect is not included: As a student-run organisation, ELSA operates with specific characteristics that influence the scope and focus of this internal handbook:

1. Resource Constraints: ELSA, like many student associations, relies on the dedication of student volunteers. Our resources, including time, specialized legal expertise, and financial capacity, are inherently limited. Developing and maintaining comprehensive, legally compliant procedures for external reporting to supervisory authorities is a complex task that typically requires dedicated legal counsel and significant organisational resources.
2. Focus on Internal Best Practices: This handbook prioritises empowering our members and officers with the knowledge and tools to implement fundamental data protection principles internally. Our primary aim is to prevent incidents through awareness and good practice, and to provide a framework for internal response should an incident occur.
3. Complexity of Legal Obligations: The precise legal requirements for reporting to supervisory authorities can vary significantly depending on the nature of the data breach, the type of data involved, the jurisdiction, and the specific legal framework applicable. Interpreting these nuanced legal obligations and ensuring timely, accurate reporting is a highly specialized area.

Recommendation:
Therefore, this handbook should not be considered a substitute for professional legal advice. For any specific legal obligations concerning data protection, particularly those involving external reporting to supervisory authorities, we strongly advise consulting with qualified legal professionals who can provide tailored guidance based on the specific circumstances and applicable laws.

This handbook serves as a foundational internal document to promote a strong data protection culture within ELSA, but it is incumbent upon the relevant ELSA entities or individuals to ensure compliance with all external legal requirements, including those pertaining to report obligations.

7. Data Protection Agreements

A Data Processing Agreement (DPA) is a legal contract required under the GDPR when personal data is processed on behalf of a data controller by a third party. Its purpose is to ensure that personal data is handled in a secure, transparent, and compliant manner. The DPA sets out how data should be processed, which security measures must be in place, and what responsibilities each party has. It helps to reduce risk, clarify accountability, and demonstrate compliance with data protection regulations.

7.1. The Agreements

There are several types of data processing agreements, depending on the nature of the relationship between parties and how personal data is handled. These agreements ensure that data is processed in compliance with GDPR and that responsibilities are clearly defined.

Controller-to-Processor Agreement
This is used when a data controller (the party that decides why and how personal data is processed) engages a data processor (a third party that processes data on the controller's behalf). The agreement outlines what data is processed, for what purpose, and what security and compliance obligations the processor must follow.

Joint Controller Agreement
A joint controller agreement is required when two or more parties jointly determine the purposes and means of processing personal data. Instead of one party instructing the other, both share responsibility for data decisions. The agreement must clarify each party's role, responsibilities, and how data subjects can exercise their rights.

Processor-to-Sub-Processor Agreement
When a processor outsources part of its data processing to another external party, a separate agreement is needed between them. This ensures that the sub-processor complies with the same data protection obligations the main processor has toward the controller.

International Data Transfer Agreements
If personal data is transferred outside the EU/EEA to a country that does not have an EU adequacy decision, additional safeguards must be in place. Typically, this is done through Standard Contractual Clauses (SCCs) or other legally recognised mechanisms. These clauses ensure that the personal data remains protected according to EU standards.

7.2. How to decide which agreement is relevant?

1. Determine the Role of Each Party
    - If your ELSA group decides why and how personal data is processed, you are a controller.
    - If your organisation processes personal data on behalf of another party, you are a processor.

2. Define the Relationship
    - If your ELSA group is using a third-party service provider to process data: a Controller-to-Processor Agreement is required.
    - If you and another organisation are making joint decisions about personal data: a Joint Controller Agreement is appropriate.
    - If you, as a processor, are engaging another party to help you process data: a Processor-to-Sub-Processor Agreement is necessary.

3. Assess International Transfers
    - If any personal data is being transferred to a country outside the EU/EEA that is not covered by an adequacy decision, you will need to implement Standard Contractual Clauses or an equivalent transfer mechanism in addition to the DPA.

4. Legal Review and Documentation
    - Keep the agreement under regular review, especially when processing activities or service providers change.

To put a data processing agreement in place with another party, you start by confirming whether it is needed, based on how personal data is being handled. This means working out whether ELSA is the controller, the processor or sharing responsibility as a joint controller. Once that is clear, you gather the key details, including what kind of personal data is involved, why it is being processed, how long it will be kept and whether it is shared with any third parties or transferred outside the EU.

To simplify your implementation of data protection agreements you can use the following template agreements as a basis for your own agreements:
- Controller Processor Agreement (Intra EU);
- Controller Processor Agreement (Outside EU);
- Joint Controllership Agreement (Intra EU);
- Joint Controllership Agreement (Outside EU).

7.3. The Responsibilities

Checklist of Responsibilities of Controller or Joint Controllers

- ☐ Complying with data protection principles under Article 5 GDPR
- ☐ Upholding individual's data protection rights
- ☐ Keeping records of processing activities (ROPA)
- ☐ Ensuring the security of processing
- ☐ Choosing an appropriate data processor
- ☐ Detailing in a binding contract the controller-processor relationship (and if applicable between the Joint Controllers)
- ☐ Notifying personal data breaches
- ☐ Being accountable for the processing operations (practicing data protection by design and by default, carrying out data protection impact assessments when necessary)
- ☐ Complying with the data protection obligations on international transfers of personal data
- ☐ Cooperating with data protection authorities

Checklist of the Responsibilities of a Processor

- ☐ Following the Controller's instructions
- ☐ Keeping records of processing activities (ROPA)
- ☐ Ensuring the security of processing
- ☐ Respecting and upholding the binding controller-processor contract
- ☐ Obtain the authorisation of the Controller before engaging a new Sub-processor (and give the Controller a possibility to object). If applicable, a Processor - Sub-processor contract must be put in place and equate to the initial controller- processor contract
- ☐ Notifying personal data breaches to the Controller
- ☐ Notifying GDPR breaches to the Controller
- ☐ Being accountable for the processing operations (e.g. practising data protection by design & default)
- ☐ Ensuring that international transfers are authorised by the Controller and comply with the GDPR
- ☐ Cooperating with data protection authorities

8. Archiving

Effective archiving and data retention is important for safeguarding data protection principles, supporting operational efficiency and meeting legal and regulatory responsibilities. This section outlines why archiving matters, how to manage data responsibly and what practical steps to take to ensure a consistent and secure approach throughout the year.

By archiving data that is no longer actively needed, the organisation can reduce the volume of information vulnerable to breach and improve system performance. Moreover, keeping a clear and traceable record of how data is stored or removed demonstrates accountability.

8.1. What to Keep, Delete or Anonymise

Archived information typically includes data that is no longer in active use but is still needed for legal, historical or research reasons. This may include documents from completed projects, records tied to past transactions or information required to meet regulatory deadlines.

Data that can be deleted includes duplicates, old drafts and files with no ongoing purpose. Temporary working documents should also be removed once the final versions are stored properly. Any data that has passed its legal retention period without a continuing justification should be securely deleted.

In cases where data is used for research or reporting, it should be anonymised. This means removing or masking identifiable details so that individuals can no longer be recognised. Anonymised data can be retained for broader use without compromising privacy. Data shared externally without consent must be anonymised unless there is a clear, documented reason not to.

8.2. How to Anonymise Personal Data

Anonymisation is the process of stripping data of any identifiable elements. It starts with removing direct identifiers such as names, addresses and phone numbers. Indirect identifiers like date of birth should be generalised, for example, by converting it to an age range. Where individual details are not needed, information should be aggregated. Anonymised data must not be reversible. If individuals can reasonably be re-identified, the data is not truly anonymised and must be handled accordingly.

In some cases, pseudonymisation may be used, which replaces identifiers with coded references while keeping the decoding key stored separately and securely.

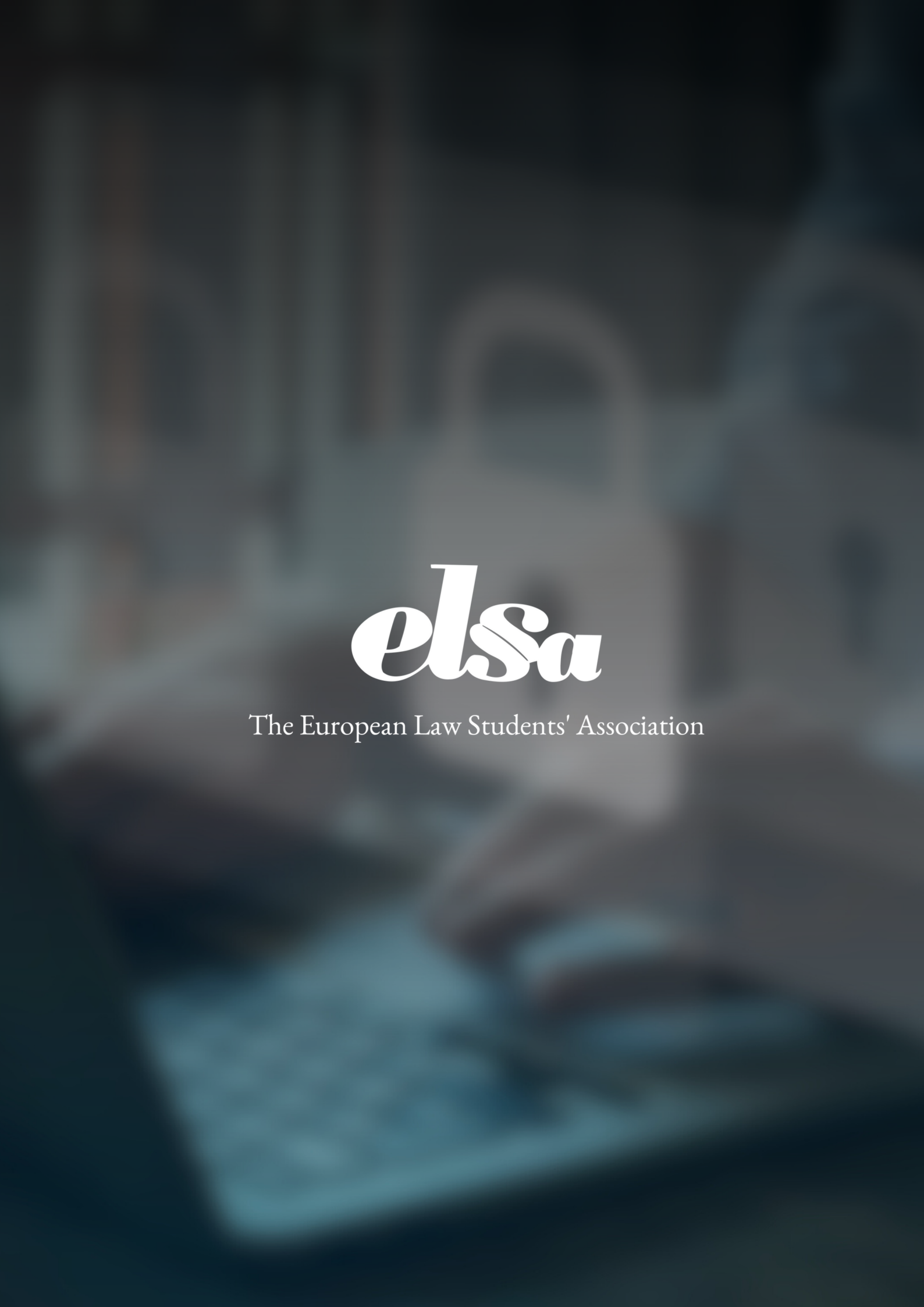
8.3. Implementing a Sustainable Archiving System

To manage data consistently over time, ELSA groups should maintain a clear data retention schedule that outlines how long different types of data are to be kept. Responsibility for data oversight should be assigned to specific individuals or teams. Information should be provided to ensure all officers understand the data lifecycle, including how and when to archive or delete information. Regular reviews and audits help confirm that retention policies are being followed and that archived data remains secure and relevant.

For this purpose it is advisable to have Archiving Guidelines in place. An example on how these could look like and what is included in them, can be found here. Please be aware that these are compatible with Belgian Law in regards to the documentation and timeline of how long it has to be stored - however, they serve as a good basis for you to build upon your own Archiving Guidelines.

8.4. Best Practice Checklist – Archiving and Data Retention

- ☐ **Follow the Data Retention Schedule**: Keep data only for as long as needed. Review regularly to stay compliant.
- ☐ **Archive Inactive but Relevant Data:** Store data no longer in use but still required for legal, historical or research purposes.
- ☐ **Delete Unnecessary Files Promptly:** Remove duplicates, outdated drafts and temporary files once final versions are saved.
- ☐ **Anonymise Where Appropriate:** Strip identifiable information from data used for analysis or shared externally.
- ☐ **Document All Archiving Actions:** Keep clear records of what was archived, when and why.
- ☐ **Restrict Access to Archived Data:** Limit access to authorised members and use secure systems with logging.
- ☐ **Train All Officers Regularly:** Ensure everyone understands the importance of responsible data handling.
- ☐ **Review and Audit Periodically:** Check that data retention and deletion processes are being followed correctly.Complying with data protection principles under Article 5 GDPR.


elsa
The European Law Students' Association