Document Title	Privacy Policy
Organisation	ESOT (European Society for Organ Transplantation)
Document Version	Version 1.0
Effective Date	November 13, 2024
Prepared by	Devi MEY, ESOT CEO Mateus Mateus Welnowski, ESOT DPO (Privacy Company)
Reviewed by	Frank Dor, ESOT Treasurer and GDPR Compliance Offier
Approval Date	November 13, 2024
Next Review Date	November 2025
Purpose	To outline ESOT's commitment to data privacy and explain how we collect, use, and protect personal information.
Contact Information	dpo@esot.org

Contents

Introduction

ESOT is increasingly working with very sensitive personal data of patients, through its scientific research projects or through the creation and maintenance of the Registries. On top of that, ESOT is processing the personal data of its members, employees, visitors of its events, external partners, and other groups. ESOT is determined to use these personal data only in a way that is safe for and respectful of the people they concern. This privacy policy outlines how ESOT aims to protect the personal data under its care.

ESOT's mission

ESOT is dedicated to the pursuit of excellence in the field of organ transplantation. This means that ESOT wants to extend its knowledge about organ donation and transplantation and disseminate state-of-the-art understanding to the professionals working in the field. ESOT's ultimate goal is to improve outcomes in patients that underwent organ transplantation. . ESOT uses personal data to achieve these overarching purposes, which it considers to be "designed to serve mankind", to quote the GDPR[1]. This includes the processing of personal data of ESOT members, staff, external contacts, and, where appropriate, of donors and recipients of organs.

ESOT is primarily active within the territory of the Council of Europe and, most of the time, within the European Union. This means that ESOT aims to comply with the GDPR requirements in all its data-processing activities. ESOT adheres to a strict interpretation of how it should protect the personal data it works with.

Scope of this privacy policy

This privacy policy governs all processing of personal data by ESOT or on behalf of ESOT, including when collaborating with external parties. This privacy policy applies both to the activities of ESOT Society itself and to the activities of foundation Steunstichting ESOT. All data processing within either organisation is required

[1] Recital 4, GDPR: "The processing of personal data should be designed to serve mankind".

to follow the rules laid out in this document. Any deviation will be subject to approval by the Board after consultation with the DPO[2]

About this privacy policy

This policy represents the strategic choices ESOT has made for the way it handles personal data and serves as an internal basis for designing the way ESOT works with personal data. Where necessary, it outlines clear choices, whenever necessary to create a firm basis for ESOT's data protection landscape. This document aims to keep it brief and delegates creating detailed work instructions to several procedures/SOPs and work instructions where possible.

[2] The internal roles will be defined in paragraph 1.2.

1. Principles of data protection

1.1. Definitions

Tabel 1 - Definitions of terms used in this policy

Term	Definition
Personal data	All information relating to a data subject.
Special categories of personal data	Sensitive categories of personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, trade union membership, genetic data, biometric data for the purpose of uniquely identifying a natural person, data concerning health, sex life or sexual orientation.
Processing and processing activities	Any operation or set of operations which is performed on personal data or on sets of personal data, whether or not by automated means, such as collection, recording, organisation, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction.
RoPA	Record of Processing Activities, the mandatory overview of all processing activities undertaken by ESOT either as a controller or as a processor.
Controller	The party (organisation or natural person) that determines the purpose and the means for a processing activity.
Joint controllers	The parties (organisation and/or natural persons) that collectively determine the purpose and the means for a processing activity – including when the control is unevenly distributed.
Processor	The party (organisation or natural person) who processes personal data on behalf of another party and who does not determine the purpose or the means of the processing activity.
Receiver	An external party (organisation or natural person) to whom personal data are transferred.

Term	Definition
Data subject	An identified or identifiable natural person whose personal data are being processed by or on behalf of ESOT. This includes natural persons whose identity can only be found with the help of external sources.
Retention period	The legal or self-determined period for which ESOT can retain a record of each category of personal data.
Privacy risk	A risk to the rights and freedoms of data subjects.
DPIA	Data protection impact assessment – a formalised assessment of the way a processing activity could impact the rights and freedoms of natural persons.
Pseudonymisation	Personal data that cannot be directly related to a natural person but that could be indirectly related to a data subject, for instance, by using external data from partner organisations through the use of a pseudonymous identifier.
Anonymisation	Data that cannot be directly or indirectly related to a natural person and therefore will no longer be considered personal data.
Sponsor	Pharmaceutical company funding scientific research.
Aggregation	The combination of personal data about multiple data subjects into a single overview through statistical means, creating non-personal data where the individual data subject can no longer be distinguished.
Data breach	A breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data transmitted, stored or otherwise processed.

1.2. Roles and responsibilities

Working in a way that is compliant with privacy regulations is a team effort. All members of ESOT's staff share in the responsibilities of ESOT towards the data subjects. Everyone is responsible for processing personal data in a lawful, fair, and transparent way, in accordance with the directions provided in this privacy policy. Every staff member shall diligently follow the procedures associated with this privacy policy and carefully record the processings they perform in the registry of processing. They shall be alert to the possibility of data

breaches and requests made by any data subject. Below, specific roles have been defined. A full RASCI-table of roles and responsibilities can be found in Appendix 1.

1.2.1. Executive Committee

The decision-making body of the Society consists of the President, Secretary, Treasurer, Past President, President-elect and Chief Executive Officer. This body ensures the daily management and strategic direction of the Society and is ultimately responsible for all data processing activities by or on behalf of ESOT.

1.2.2. Chief Executive Officer (CEO)

The CEO is directly accountable for all data processing activities by or on behalf of ESOT and is a member of the Executive Committee.

1.2.3. ESOT Council

The corporate body is made up of representatives (afgevaardigden) (indirectly) appointed by and from the European Members of the Society in accordance with Article 9 of the ESOT Bylaws, which has the function of general meeting as meant in Article 2:39 and further of the Dutch Civil Code, by the Society also referred to as the ESOT Council; Europe is defined as all countries that are members of the Council of Europe (Raad van EuRoPA). The Council consists of:

a. such number of at least two (2) Councillors appointed by the General Assembly from the European Members, the number to be determined by the Council; and
b. each chair of the Sections/Committees from time to time established.

2. A Councillor appointed by the General Assembly is appointed for a period of four (4) years, unless the appointment is the result of an intermediate-election, in which case the appointment is valid until the next four-yearly election. Such Councillor may be re-appointed immediately after his/her first term once.

1.2.4. Department and programme leads

The Department leads are accountable for the protection of personal data that ESOT processes within their department or programme.

1.2.5. Compliance Officer

The compliance officer will be responsible for the day-to-day execution of this privacy policy, especially where it concerns data breaches and data subject requests.

1.2.6. Data Protection Officer (DPO)

The DPO oversees the application of this privacy policy as well as applicable privacy legislation and advises the Executive Committee as well as the staff about the application of privacy law and regulations. The DPO is independent from ESOT and is not accountable for compliance by ESOT but will provide guidance to the organisation to facilitate improved compliance.

1.2.7. ESOT staff members

Everyone who works for ESOT, including employees and contract staff, interns and volunteers, will be required to work according to this Privacy Policy. They will receive training to be able to understand and apply data protection in their daily work. In particular, they are expected to be mindful of the risks the processing of personal data implies for the data subjects, and to be diligent and attentive to situations that may require special care, including breaches of security, data breaches, requests by data subjects and sharing data with external parties.

1.3. Relevant laws and regulations

This privacy policy is based on the laws that govern the operation of ESOT. ESOT is based in the Netherlands. Therefore, the laws of the Netherlands and the EU primarily apply to the processing of personal data by or on behalf of ESOT. In the list below, the most important laws and regulations concerning data protection are listed.

Tabel 2 - Relevant laws and regulations concerning data protection

Name	Abbr.	Jurisdiction	Comments
General Data Protection Regulation	GDPR	EU	Determines how personal data must be handled in the EU.
Dutch General Data Protection Regulation Implementation Act	uAVG	NL	Determines how the GDPR is implemented in the Netherlands.
ePrivacy Directive 2002/58/EC	ePD	EU	Determines how to handle privacy in an online environment – contains the cookie law and specific requirements for unsolicited email. Implemented in TW.
Dutch Civil Code	BW	NL	Describes how civil society is organised in the Netherlands, including how Societies and Foundations can operate and how contracts and employment are organised.

Name	Abbr.	Jurisdiction	Comments
Dutch Telecommunication Act	TW	NL	Contains implementation of the ePD, with the Cookie law and unsolicited email regulation.
Dutch Organ Donation Act	-	NL	Describes how organ donations are organised and registered.
Dutch Security and Quality of Bodily Materials	-	NL	Describes how bodily materials, including donated organs, are registered, kept and transported safely.
Dutch Demand Decision Bodily Materials 2006	-	NL	Implementing decision specifying requirements around handling donated organs.
Medical Treatment Contract Act	Wgbo	NL	Describes the obligations and expectations around medical treatments.
European Health Data Space	EHDS	EU	European regulation creates rules for primary and secondary use of health data throughout the EU. (to be adopted by the EU as of May 2024)

Tabel 3 - Related internal policies and procedures

Name	Purpose	Responsible	Comments
Information Security Policy	Define the way ESOT protects all internally available information, including personal data.	CEO	To be created
Scientific research guidelines	Defines the ways in which ESOT handles scientific research and ethical and scientific requirements and best practices.	CEO	To be created
Data Subject Requests SOP	Details the way in which ESOT responds to data subject requests (GDPR)	CEO	To be created
Data Breach SOP	Details the way in which ESOT responds whenever a possible data breach is detected.	CEO	To be created
Data Retention Policy	Details how long ESOT will or must retain personal data of each category.	CEO	To be created

Name	Purpose	Responsible	Comments
Privacy risk assessment form	To assess whether any processing of personal data creates high privacy risks.	CEO	To be created

2. Using personal data

Three main principles are the basis for data protection: lawfulness, fairness, and transparency. The ways in which these principles influence the choices ESOT makes when dealing with personal data will be outlined in this chapter.

2.1. The purposes for which ESOT processes personal data

Each lawful processing of personal data requires a specific and clear purpose. ESOT generally uses personal data for one of several possible overarching purposes, which are defined in the by-laws of the Society:

a. to promote sustainable scientific advancement through multidisciplinary communities of healthcare professionals;
b. to deliver first-class education, training and career advancement opportunities to all healthcare professionals, with specific training programs for low-income countries;
c. to work with partner organisations, professional bodies, and competent authorities to improve public and institutional awareness of organ donation and the latest research in the field; and
d. to develop and promote policies for equitable access to transplantation and related therapeutic strategies.

And one additional purpose that is served primarily by the Steunstichting ESOT:

e. funding the activities of the Society.

These overarching purposes give meaning and direction to each specific processing activity and the purpose for which ESOT processes personal data. Whenever ESOT processes personal data for a purpose that does not follow from one or several of these overarching purposes, the CEO will make a decision about the processing activity before it takes place, in consultation with the DPO. Within these overarching purposes, several groups of processing activities can be identified:

a. To promote sustainable scientific advancement through multidisciplinary communities of healthcare professionals:
    a. Scientific Registries
    b. Scientific research projects
    c. Transplant International

   d. Organising scientific conferences and other events
b. To deliver first-class education, training and career advancement opportunities to all healthcare professionals, with specific training programs for low-income countries:
   a. Education
   b. Transplant Live
   c. ESOT Courses
   d. Scholarships, fellowships, and grants programmes
   e. Online fora
c. To work with partner organisations, professional bodies, and competent authorities to improve public and institutional awareness of organ donation and the latest research in the field:
   a. EU Funded Projects
d. To develop and promote policies for equitable access to transplantation and related therapeutic strategies.
   a. Clinical Practice Guidelines, Consensus Guidelines and Recommendations
e. Providing quality services to ESOT members
   a. Membership registration and service
   b. Organisation of the ESOT members congress and other member events
   c. Board and other internal elections
   d. Running a professional organisation:
      i. Facilitating a professional and efficient staff
      ii. Providing financial stability and accountability
   e. Other necessary internal purposes
f. Funding ESOT's activities:
   a. Raising funds for the activities of ESOT
   b. Organise fundraisers
   c. Offering services to Sponsors
   d. Maintain a network of potential donors
   e. Other fundraising not-for-profit activities.

The fulfilment of these purposes requires that ESOT processes personal data of the following groups of data subjects (some may overlap):

a. Pseudonymous patients, who are donors or receivers of organs
   This group can include people who are younger than 16, and people who may in other ways be considered vulnerable.

b. Members and past members of ESOT
c. Visitors, including delegates and attendees, of ESOT events
d. Participants in ESOT education programmes
e. People publishing articles in or getting mentioned in Transplant International
f. People who supported ESOT financially
g. Visitors of ESOT's websites
h. Staff members of ESOT, including former staff and applicants, and including (former) contract workers and (former) board members
i. Employees of business relations of ESOT, including Sponsors, suppliers, and trainers.

2.2. What makes ESOT's processing activities lawful

Every processing activity undertaken by ESOT requires a valid legal ground under GDPR. For each group of data subjects, ESOT can claim a valid legal ground, as described in the table below:

Tabel 4 - Valid legal grounds for processing

Data subject group	Legal grounds	Applicability
Pseudonymous patients	ESOT's legitimate interest to improve patient outcomes and to raise professional standards through scientific research. Under specific circumstances, ESOT may also be assigned a task in the public interest to process data for these purposes.	For all scientific Registries and in modified form for each research project.
Members and past members	Contract: the membership agreement and the membership terms and conditions	For all processing activities that are necessary for the administration and purposes of the membership
	Consent: consent given for specific processings	
	ESOT's legitimate interest to provide important services to the members and to administer the functioning of the Society and the Foundation	When the interests of ESOT are not overridden by the interests, fundamental rights and freedoms of the data subjects
Visitors of events	Contract: the registration to the event and the event terms and conditions that apply	

Data subject group	Legal grounds	Applicability
	Consent: consent given for specific processings	
Participants in education programmes	Contract: the registration to the programme and the programme terms and conditions that apply	
Authors of articles	Contract: the submission of an article for publication constitutes a contract between the author and ESOT that requires the data processings	
Financial supporters	ESOT's legitimate interest to process information about financial contributions	When the interests of ESOT are not overridden by the interests, fundamental rights and freedoms of the data subjects
Website visitors	ESOT's legitimate interest to provide the general public with detailed information about its activities and its goals, as well as other information it deems valuable	When the interests of ESOT are not overridden by the interests, fundamental rights and freedoms of the data subjects
	ESOT's legitimate interest to improve its website and the way it was designed and functions	When the interests of ESOT are not overridden by the interests, fundamental rights and freedoms of the data subjects
Staff members	Contract: the employment agreement, or any other contract underlying the relationship	For all processing activities that are necessary for the fulfilling of the terms of the agreement
	ESOT's legitimate interest to process personal data of employees to perform the necessary tasks of the organisation	When the interests of ESOT are not overridden by the interests, fundamental rights and freedoms of the data subjects
	Consent: consent given for specific processings	Only when staff members are free to give or withhold consent for a specific processing activity
Volunteers (including TI authors, editors, fellows, etc.)	Consent: consent given for specific processings	Only when staff members are free to give or withhold consent for a specific processing activity

Data subject group	Legal grounds	Applicability
	ESOT's legitimate interest to process personal data of volunteers to perform the necessary tasks of the organisation	When the interests of ESOT are not overridden by the interests, fundamental rights and freedoms of the data subjects
Employees of business relations	ESOT's legitimate interest to communicate with its external partners and to run its business in an efficient and orderly fashion	When the interests of ESOT are not overridden by the interests, fundamental rights and freedoms of the data subjects
All groups	To comply with legal obligations	When a specific legal obligation exists

The legal grounds listed in the table above should provide for most lawful processing activities of personal data by ESOT. Whenever ESOT finds it necessary to use a different legal ground, the CEO will decide before the processing activity takes place, after consultation with the DPO.

Whenever ESOT processes personal data based on its legitimate interests, the staff member responsible for the processing activity will demonstrate through a Legitimate Interest Assessment that the interests of ESOT are not overridden by the interests, fundamental rights and freedoms of the data subjects. This is especially important in those cases where ESOT processes information about patients, even if the identities of the data subjects are unknown. ESOT obtains such pseudonymous personal data for its Registries and scientific research projects from data providers only after they have obtained the informed consent from the patients or their representatives, whenever this is required.

When ESOT processes personal data on the basis of consent, the staff member responsible for the processing activity will ensure that a clear record of the consent given by the data subject is kept and that the location of the consent is clearly documented.

2.3. How ESOT protects sensitive personal data

Medical research requires the use of health information and other sensitive types of personal data. The processing of so-called special categories of personal data, which includes health data and genetic information, ethnicity and sexual behaviour, is prohibited under the GDPR, unless an exception applies. ESOT only processes these types of personal data (in particular health data and genetic data) for the purpose of

scientific research. That means that as long as ESOT makes sure the processing of these types of data is protected by appropriate safeguards, the processing is allowed. In the context of the Registries and any scientific research that ESOT or its partners undertake using these types of sensitive information, ESOT will ensure the necessary safeguards are in place, including specifically the pseudonymisation of the data. This means that ESOT will only include personal data in its Registries and scientific research projects that were fully pseudonymised by the data provider and that ESOT and its research partners will not engage in the re-identification of any of the patients in its records.

ESOT will process some sensitive data, including health data and national identification numbers, about its staff members, in the course of the normal employer processing activities. Here, the exception applies that an employer can, under specific conditions, process employee health data and is required under Dutch law to obtain the national registration number of its employees and to provide it to the Tax Authority and other official organisations.

Any other use of these sensitive types of personal data than described above must be approved in advance by the DPO.

2.4. Data minimisation: How ESOT limits what is collect and kept

2.4.1. Registries and scientific research

In its scientific undertakings, ESOT needs a lot of information for as large a group of patients as possible. The more patients are available for analyses, the more statistical power can be generated to prove or disprove the hypotheses ESOT is working on. This is also true for the number of variables available for research purposes. Sometimes, unexpected correlations can lead to new discoveries that can help patients and improve the outcome of transplantation. At the same time, including more variables in the Registries inevitably leads to a higher privacy risk (see chapter 4). ESOT aims to resolve this by including those variables that are likely to be related to the transplantation outcome and tries to reduce the number of variables in the Registries that have not been shown to have any relationship with transplantation outcome, based on the weighing of privacy risks and scientific principles. In scientific studies, more detailed information about the patient may be obtained through the data providers for a limited number of patients, so that scientists can test whether new and sometimes unexpected variables may lead to new innovations around transplantations.

ESOT will draft a Data Protection Impact Assessment for each Registry (Registry DPIA). Every scientific research project will be required to submit an assessment of additional privacy risk, that will demonstrate that the study will not present additional privacy risks above what was foreseen in the relevant Registry DPIA.

When this cannot be demonstrated, the DPO will require the study leader to submit a full Study DPIA based on the relevant Registry DPIA to demonstrate that the study does not lead to high risks for the data subjects that cannot be mitigated. The study cannot begin before ESOT's DPO has accepted the Study DPIA.

The revolution in artificial intelligence (AI) may have specific implications for the way ESOT organises scientific research. The potential of AI to discover improvements in patient outcomes is offset by potential new risks and challenges in protecting adverse effects on the rights and freedoms of the people whose personal data is being analysed. Therefore, ESOT believes that any research project that involves some form of AI must be judged against a higher standard and must be presumed to imply additional privacy risks. Any such project will therefore be required to submit a Study DPIA, addressing the potential issues with the use of AI, including additional legal burdens created by the EU's new AI Act.

2.4.2. Other processing activities

In other processing activities, the relationship between what ESOT needs and what it uses is more direct. ESOT knows what is necessary for each processing activity and will make sure that personal data that is no longer necessary for those processing activities will be deleted from its systems or otherwise destroyed. ESOT will design (or redesign) its systems to only collect the information that are needed to achieve its purposes.

2.5. Retention: How long to keep information

The Registries depend on having a life-long overview of patient outcomes. Once enrolled, and unless the informed consent gets revoked, a patient's pseudonymised personal data will remain in the registry and will be augmented by any new information that the data provider adds. This provides a clear long-term overview of the effects of receiving a transplantation and is the source of scientific progress. After the death of a receiver of a transplantation, the pseudonymised data is no longer considered personal data. ESOT will however keep protecting the information in the same way as it would for a living recipient.

The personal data in the Registries about (living) donors will also be kept indefinitely, as the information is directly necessary to ESOT's scientific research.

For other types of data, lawful minimum or maximum retention periods may apply. If not, ESOT will determine a reasonable retention period. ESOT's CEO will be responsible for setting up a retention policy that will describe how long each type of personal data will be retained by ESOT and how it will be deleted or destroyed after the retention period expires.

2.6. The Foundation and the Society

ESOT consists of both a Foundation and a Society. These two legal entities are separate, helping ESOT to fund its activities. This privacy policy applies to both entities. The Foundation is primarily active in seeking funding for the activities of the Society. Personal data about Sponsors and Members, as well as members of the staff, may be shared between the two entities, when necessary for the purposes. The Society is the only party that has access to personal data of pseudonymised patients that ESOT processes in the Registries or in scientific research projects. The raw data, including in aggregated or reworked format, can never be used for the commercial activities of the Foundation or for any other commercial purpose, except where ESOT makes its routine periodic statistical reports or publications based on scientific research that do not contain any observations that can be related to any identified or identifiable natural person.

2.7. How ESOT demonstrates compliance

ESOT will maintain a register of processing activities (ROPA), that will include all categories of processing activities that ESOT undertakes as a controller, as joint controller, or as a processor on behalf of another party. The ROPA will be built under the direct responsibility of the CEO, based on advice from the DPO. The department and programme leads will be responsible for the maintenance of the ROPA, with each lead responsible for recording and maintaining the processing activities they are responsible for, including:

- The role of ESOT in the processing as (joint) controller or processor
- The specific purpose of the processing activity
- The categories of data subjects involved
- Information about vulnerabilities for the data subjects included, such as the presence of children or mentally disabled, etc.
- The categories of personal data included
- Whether the personal data are pseudonymised and by whom
- The presence of special categories of personal data
- The legal ground for the processing, including the necessary reference to the source of the legal ground
- If applicable, the legal exemptions for the processing of special categories of personal data
- The systems used for the processing activity
- List of technical and organisational measures that are applied to the processing activity
- The risk assessment (pre-DPIA)
- For high-risk processing activities: a reference to the relevant DPIA (see paragraph 2.2).

- List of technical and organisational measures required by the DPIA
- The external parties involved in the processing activity, their roles, their location when outside of the EU, and any agreements made about data protection
- The country or countries where the processing takes place.

Every lead will be responsible for the accuracy and completeness of the information in the ROPA. The DPO will oversee the accuracy and completeness of the information in the ROPA, as well as the lawfulness of the processing activities described. The CEO, after consultation with the DPO, will determine how the ROPA will be organised and maintained.

3. Working with external parties

Whenever ESOT shares personal data with external parties, additional safeguards are required to make sure the data does not lose protection because of the external party's access. This chapter aims to clarify how ESOT shares information.

3.1. Outsourcing to processors

ESOT will use external parties to facilitate the processing of personal data. In these cases, the external party will be considered to be a processor when ESOT determines the purpose of the processing activity AND influences the means used for the processing activity AND the proposed data processing is inherently tied to the core of the job the external party was hired to do for ESOT (see example). Processors that work on behalf of ESOT will sign a data processing agreement. ESOT will develop a default processing agreement based on the Standard Contractual Clauses (controller to processor) as developed by the European Commission. Whenever a processor prefers to have its processing agreement used instead, the DPO will review the proposed agreement and advise the CEO about the validity of the agreement and suggest improvements. The CEO will decide whether to adopt the proposed data processing agreement rather than the default ESOT processing agreement.

3.2. Sharing personal data with joint controllers

ESOT also engages in collaborations where personal data gets shared with one or more parties in the pursuit of joint objectives. The department and programme leads are responsible for the documentation and for the lawfulness of such collaborations and the CEO will sign a data sharing agreement for each collaborative project, whenever ESOT acts as a joint controller for any processing activity. Such joint control agreements can be custom made or can be based on existing standards. Wherever possible, ESOT will standardise the application of data sharing agreements, such as when dealing with requests for access to the Registries for scientific research purposes. All scientific research done with personal data collected in the Registries will be done under joint controllership with ESOT and every scientific partner will be required to sign a standardised joint control agreement. The CEO, after consultation with the DPO, will determine under what general conditions such access for scientific purposes will be allowed, in line with the agreements made with data providers. Specific exceptions may be allowed for specific research purposes, but these will be subject to approval by the CEO and the DPO.

3.3. Sending personal data to an independent external controller

Whenever ESOT sends personal data to an external party that is not a processor, but that independently determines the purpose and means of the processing activity, this party will be seen as an independent receiver of personal data, such as an accountant, lawyer, pension fund, tax authority, etc. ESOT does not control the personal data after sending it to such a party but does need to comply with all requirements from Chapter 2 for the processing activity where the data gets shared with the external party. Depending on the circumstances, ESOT may require the external party to sign a confidentiality agreement, or other agreements about technical and organisational safeguards, including limits to the extent the external party can re-use the personal data obtained from ESOT for its own purposes. The CEO will be responsible for the agreements made in compliance with this policy and can request the opinion of the DPO. The agreement will be made available to the DPO for review.

3.4. International transfers of personal data

As an international society, that is based in the EU, but active in the whole world, it is inevitable that some personal data may be transferred by ESOT to parties outside of the EU. As a rule, ESOT will not collaborate with any parties outside of the European Economic Area (EEA) for the Registries or scientific research projects. Exceptions to this rule will be allowed for parties in countries that have been determined by the European Commission to have a level of data protection that is adequate and in essence equivalent to that offered in the EU. ESOT will confirm this commitment to keeping the personal data in the registries within the EEA in the agreements it makes with the data providers.

For other processing activities, such as ESOT events, education programmes, and Transplant International, ESOT will work with international parties when necessary to further its interests, provided the international transfer of personal data does not lead to high risks to the rights and freedoms of the data subjects. This means that ESOT will make contractual agreements with the importing party about the protection of the personal data after the transfer. ESOT will use the EU's official Standard Contractual Clauses and will perform a Data Transfer Impact Assessment to establish that the transfer of the data will not severely impact the rights and freedoms of the data subjects. The department or programme lead responsible for the transfer will create the DTIA on the basis of established templates, and in collaboration with the DPO. The DPO will determine whether the DTIA shows that the transfer can take place without impacting the rights and freedoms of the data subjects.

4. Managing privacy risks

Whenever ESOT processes personal data, this implies a risk to the rights and freedoms of the data subjects. ESOT refers to these types of risks as privacy risks. It is ESOT's responsibility to ensure that the risk is well-managed and mitigated whenever necessary. This chapter aims to guide ESOT in managing privacy risks.

4.1. Preliminary assessment of privacy risks

Every processing of personal data creates at least a minor risk to the rights and freedoms of the data subjects. ESOT handles the privacy risks its processing activities create by applying a two-step process. For every processing activity, the department or programme lead will perform a preliminary assessment of privacy risk. The CEO will be responsible for creating an assessment form, after consultation with the DPO about the requirements. When the preliminary assessment shows that the processing activity may lead to high risks to the rights and freedoms of natural persons, the DPO will determine whether a Data Protection Impact Assessment (DPIA) is required.

4.2. DPIAs

When a DPIA is required, the department or programme lead will be responsible for its creation, in close collaboration with the DPO. The DPIA may be done internally or by an external consultant. The processing activity will not start before the DPIA has been approved by the DPO. The DPIA will investigate the potential impact of the processing activity on the rights and freedoms of natural persons. This will involve an investigation of:

- The nature of the processing activity, including:
- The purpose of the processing
- The actors involved in the processing
- The systems used for the processing
- The data subjects and types of personal data involved
- The architecture of the processing activity
- The legal and regulatory framework that applies to the processing activity
- The applicable retention periods

- The lawfulness of the processing activity
- The validity of the legal ground
- The validity of the exception for processing of special categories of personal data
- The validity of any further processing
- The necessity, including the proportionality and subsidiarity of the processing activity
- The application of the rights of data subjects
- The privacy risks created by the processing activity
- The technical and organisational measures that can mitigate the high privacy risks identified.

When the DPIA is finalised, the DPO will advise on its validity and will determine whether prior consultation with the Data Protection Authority is required before the processing activity can commence. The opinion of the DPO here is final, unless new mitigating measures can be implemented, after which the DPO will review the earlier decision. The DPO will also regularly assess whether all technical and organisational measures that were implemented to mitigate risks identified in a DPIA are still effective in sufficiently reducing privacy risks and will report the findings of the assessment to the CEO.

4.3. Information security

The protection of personal data requires a professional information security policy. Where this privacy policy determines the rules for the lawful processing of personal data, the information security policy is needed to protect the confidentiality, integrity and availability of all of ESOT's information. The CEO will be responsible for maintaining an integral information security policy.

5. Handling data subject rights

Data subjects have rights. ESOT aims to honour those rights in a way that is transparent and efficient.

5.1. The Right to information

ESOT must be upfront about all data processings, so that data subjects can understand how their data is being processed. For this purpose, ESOT uses the channels that are most appropriate. This way, ESOT fulfils its obligations under the right to information. The table below lists the ways in which ESOT communicates about the processing activities it uses for each group of data subjects:

Tabel 5 - Overview of privacy statements and the right to information

Data subject group	Privacy Statement	Location
Pseudonymous patients	Statement on paper provided to the Data Provider	t.b.d.
	Online Statement on the Registry website	t.b.d.
Members and past members	Privacy statement on the ESOT website	https://www.esot.org/privacy-policy/
Visitors of events	Privacy statement on event website	Event registration page and events tab on ESOT website
Participants in education programmes	Privacy statement provided on the participation enrollment page of the website	t.b.d.
Financial supporters	Privacy statement on ESOT Foundation website	ESOT Foundation website
Website visitors	Privacy statement on each website	https://www.esot.org/privacy-policy/
Staff members	Privacy statement for staff members on central employee platform (e.g. Google Drive)	t.b.d.
Prospective staff members	Privacy statement on ESOT website	https://www.esot.org/privacy-policy/

Data subject group	Privacy Statement	Location
Volunteers	Privacy statement on ESOT website	
Employees of business relations	Privacy statement on ESOT website	https://www.esot.org/privacy-policy/

5.2. The other rights

Data subjects have a right to see the personal data ESOT has about them and to have that information corrected or deleted. They also have the right to object to certain processing activities and a right to data portability. To handle these data subject rights, the CEO, in collaboration with the DPO, will be responsible for creating a procedure for handling Data Subject Rights that outlines how ESOT handles these types of requests in a timely and efficient manner. This procedure will ensure that every request is dealt with without delay and at most within 30 days. The CEO can extend the reaction period for ESOT only if it is not possible to respond fully and will inform the data subject about the delay within the first 30 days of receiving the request.

6. Dealing with data breaches

Whenever a data breach occurs, either directly at ESOT's hands, or at one of its processor's or co-controller's hands, ESOT must act swiftly, both to prevent further damage and to limit the effects of the data breach as well as to comply with the requirement to report data breaches to the data protection authorities and to inform the data subjects affected by the breach.

Data breaches occur whenever a breach of security leads "to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data transmitted, stored or otherwise processed", as the GDPR defines it. A data breach requires the breach of the security measures of ESOT or of its partners and it must affect the personal data that is being processed under the responsibility of ESOT. Every data breach, even minor ones, must be recorded internally. This chapter explains what ESOT expects its staff to do when confronted with a data breach.

The CEO will implement a procedure for the handling of data breaches, which will clarify in more detail how ESOT handles data breaches.

6.1. Recognising data breaches

Every staff member needs to be aware of the risk of data breaches and will be expected to notify the CEO and the DPO of any data breaches immediately, including outside of office hours. The CEO will be responsible for ensuring that the staff is trained and capable of recognising and handling data breaches. After a data breach is reported to the CEO and the DPO, the CEO will activate the data breach procedure. All necessary staff will support the CEO in minimising the effects of the data breach when called upon. The first priority will be to end the breach and to limit the extent of the damage, as well as inform any secondary parties that may be affected by the data breach, in particular joint controllers.

Possible data breaches that must be reported internally include:

- Loss of a laptop or other electronic device
- Virus or malware infections
- Emails or letters sent to a wrong address

- Leaving ESOT documents behind in a bar
- Sending the wrong document to a contact person

6.2. Solving the problem

The CEO, with the collaboration of all necessary staff, will take measures to limit the possible damage caused by the data breach and will make efforts to prevent the breach from occurring. This may include requesting information about the nature of the data breach, taking technical or organisational measures to repair the cause of the breach, or reaching out to erroneous recipients to request the deletion of any personal data obtained unlawfully, whether by accident or not. The CEO will document the steps taken to solve the issue and prevent the damage from compounding and provide all documentation to the DPO for review without delay. The CEO will maintain a record of all data breaches that were handled, including minor data breaches that did not lead to a risk to the rights and freedoms of the data subjects. The CEO will take particular care to note all available information about the data subjects involved in the data breach, as well as the categories of personal data, and the presence of special categories of personal data or otherwise particularly sensitive data. If a data breach involves (partly) pseudonymous data subjects, the CEO will report this as well.

The primary task of the DPO will be to monitor the actions of ESOT in minimising the damage and to advise on the best ways to do so and on the requirements of data protection law that ESOT has to satisfy.

If the CEO or the DPO is not available at the time of the incident, the Executive Committee will act provisionally in their place.

6.3. Reporting the authorities and informing the data subjects

Based on the information available, the DPO will make a recommendation to the CEO about the need to report the data breach to the data protection authorities. This must be done within 72 hours of ESOT becoming aware of the breach. If the information about the data breach is not sufficiently in time to decide about reporting the data breach to the data protection authority, the DPO will recommend filing a preliminary report that can later be supplemented or withdrawn. The CEO will keep a copy of the report number, and the information shared with the data protection authority.

The DPO will also make a recommendation about the need to inform the affected data subjects about the breach. When the DPO recommends that informing the data subjects is required, the CEO will decide on the most appropriate way to do so. This may include:

- Calling or emailing the data subjects directly.
- Informing a party that acts as a go-between and requesting that they communicate with the data subjects.
- When ESOT does not have a feasible way to directly or indirectly communicate with the data subjects, the CEO may decide to make public information about the data breach.
- Evaluating and taking preventative measures.

Once a reported data breach has been resolved, the DPO will organise a meeting with the principal actors within ESOT and where necessary its partners to discuss the data breach. The causes of the data breach and the way it was resolved will be discussed and technical and organisational measures will be proposed to prevent a reoccurrence of the breach. The DPO will recommend reasonable measures to the CEO, who will decide on the implementation of the measures.

7. Ensuring compliance

This privacy policy will only be effective if all staff members understand what ESOT expects of them, and if they are trained in the way ESOT aims to protect the personal data under its care.

7.1. Training ESOT staff to comply

ESOT will annually train all staff members about its values regarding data protection as well as about the practicalities of data protection to the extent they need to know this. Staff in key positions will be additionally trained to make sure they understand their specific roles. The Compliance Officer will suggest a training schedule and a focus for the training for the next year. The CEO will ultimately determine the scope and schedule for the training.

7.2. Keeping records

ESOT is required to demonstrate that it complies with GDPR and other data protection regulations. This means that ESOT will keep records of the way it processes personal data, and other information that is necessary to demonstrate compliance. These records will be maintained under the ultimate supervision of the CEO. The table below provides an overview of the necessary records ESOT keeps, their locations and the person responsible for their maintenance. Based on what is written in this privacy policy, or the procedures associated with it, other staff members may also be expected to help keep these records correct and up to date.

Tabel 6 - Overview of data protection registries

Name	Purpose	Location	Maintenance
Record of Processing Activities (RoPA)	To document the details of each processing activity on a meta level.	t.b.d.	CEO
Registry of data breaches	To document each data breach and demonstrate that decisions about reporting and informing were validly taken.	t.b.d.	CEO
Registry of requests of data subjects	To document each request made by a data subject and the way it was handled.	t.b.d.	CEO

Name	Purpose	Location	Maintenance
Registry of external parties	To document each external party that processes personal data on ESOT's behalf, that receives personal data from ESOT for its own purposes, or with which ESOT collaborates in processing activities.	t.b.d.	CEO
Registries of consent	For each processing activity based on consent, a separate registry of consent will be used, demonstrating who has given consent for the processing in what way and on what date.	t.b.d.	CEO

The CEO can appoint staff members to maintain any registry on their behalf and may determine where and how each data protection registry is organised.

7.3. Making sure to get it right

After the closing of each book year, the DPO will present an overview of the state of data protection within ESOT to the Executive Committee. The DPO will include a recommendation of necessary and desirable changes in the way ESOT organises the protection of personal data, either by minimising data, or by improving other technical and organisational measures used in the processing activities.

Annex I. RASCI-matrix

The table below shows the roles within the ESOT organisation with regard to data protection and the responsibilities each role has.

Activity	Staff	Leads	EC	CEO	IT	Compliance Officer	DPO
Privacy policy		C	A	R			C
Information security		C	A	R	C		I
Processing personal data:							
- Privacy by design	R	A		I	C		I
- Registration	R	A					I
- Execution of processing activities	R	A					I
- Create privacy statement (staff)	S		A	R			I
- Create privacy statement (other)	S	R	A				I
Privacy risk management:							
- Pre-DPIA risk analysis	R	A			S		I
- Draft DPIA	R				C		C
- Implement DPIA measures	S	R		A	S		I
- Monitor DPIA measures	S	C		A	S		R
External parties:							
- Draft data-processing agreements	S	R	C	A		C	C
- Draft data sharing agreements	S	R	C	A		C	C
- International data transfers	S	R	C	A		C	C
Rights of data subjects:							
- Deal with data subject requests	S	C		A	S	R	C
- Register data subject requests				A		R	C
Retention periods:							
- Determine retention periods	S	R	A		C	C	C
- Implement retention periods	S	R		A	S		I

Activity	Staff	Leads	EC	CEO	IT	Compliance Officer	DPO
- Monitor application of retention periods			C	A			R
Data breaches:							
- Recognise and report	R	A			S	C	I
- Notify data protection authority				A	S	R	C
- Inform data subjects				A	S	R	C
- Prevent repetition	S	C		A	R	C	C

Legend: R - Responsible; A - Accountable; S - Support; C - Consulted; I - Informed