

# INFORMATION SECURITY & PRIVACY POLICY

EUROPEAN SOCIETY OF REGIONAL ANAESTHESIA  
& PAIN THERAPY

RUE DE CHANTEPOULET 10, 1201 GENÈVE  
<https://esraeurope.org/>

Version: 1

Date: 05.08.2024

VERSION HISTORY				
VERSION	DATE	AUTHOR	APPROVED BY	REFERENCE PAGES
1	05.08.2024	Quality Officer	ESRA President	

**TABLE OF CONTENTS**

1	POLICY STATEMENT.....	3
2	SCOPE.....	3
3	DEFINITIONS .....	3
4	INFORMATION SECURITY POLICY .....	3
5	PRIVACY POLICY.....	4
6	ROLES AND RESPONSIBILITIES .....	10
7	DISTRIBUTION LIST.....	11
8	FILE KEEPING.....	11

## 1 POLICY STATEMENT

The European Society of Regional Anaesthesia and Pain Therapy (ESRA) is committed to protecting the confidentiality, integrity, and availability of all physical and electronic information assets of the organization.

ESRA is dedicated to safeguarding the privacy of personal data in compliance with applicable data protection laws and regulations.

This policy establishes a framework to safeguard information and personal data from threats, whether internal or external, deliberate or accidental, to ensure the continuation of ESRA's operations, minimize risks, and comply with legal and regulatory requirements.

## 2 SCOPE

This policy applies to all employees, contractors, consultants, temporary staff, and other workers at ESRA, including all personnel affiliated with third parties. It covers all information assets owned, leased, or managed by ESRA, and extends to all locations where ESRA conducts its operations.

## 3 DEFINITIONS

**Confidentiality:** Ensuring that information is accessible only to those authorized to have access.

**Integrity:** Safeguarding the accuracy and completeness of information and processing methods.

**Availability:** Ensuring that authorized users have access to information and associated assets when required.

**Threat:** Any circumstance or event with the potential to cause harm to an information asset.

**Risk:** The potential that a given threat will exploit vulnerabilities of an asset or group of assets and thereby cause harm to the organization.

## 4 INFORMATION SECURITY POLICY

ESRA shall establish, implement, maintain, and continually improve an Information Security, privacy and data confidentiality procedures in accordance with international standards and the General Data Protection Regulation provisions.

ESRA will comply with all relevant legal, regulatory, and contractual requirements related to information security.

This policy will be implemented, and all aspects will be managed holistically to achieve the information security objectives.

Risks will be evaluated and treated based on their potential impact on the organization.

Risk treatment plans will be developed and implemented to mitigate identified risks.

Access to information and information systems will be controlled based on business and security requirements.

Users will be granted access based on the principle of least privilege, ensuring they only have access to information necessary for their role.

Regular reviews of access rights will be conducted to ensure appropriate access levels.

A procedure for incident management will be established and maintained to ensure a quick, effective, and orderly response to information security incidents. All employees must report any observed or suspected information security incidents immediately.

Environmental controls will be in place to safeguard information assets from environmental threats.

Procedures for the secure management of information processing facilities and operations will be established and maintained.

Controls will be implemented to protect against malware, data loss, and unauthorized software.

Regular compliance checks and audits will be conducted to ensure adherence to these requirements.

Information security training and awareness programs will be provided to all employees and relevant third parties.

Training will be conducted regularly to ensure all personnel are aware of their information security responsibilities.

## 5 PRIVACY POLICY

### What Information is Collected

ESRA will collect, process and store personal data only if it is directly provided by the users (as the user of ESRA's Website, by enquiring in relation to ESRA's goods or services, becoming a member, customer or supplier, or potential supplier).

Personal information covers any information which is related to the user as an identifiable person. Below are examples of the type of data that this may include:

- **Identity Data** including forenames, last name, maiden name, date of birth, gender, marital status, and username or similar identifier.
- **Contact Data** may include invoicing; purchase order; home or work address, email address and telephone numbers, personal or job title and position.
- **Financial Data** may include bank account and payment card details.
- **Transaction Data** may include payments made for products and services you have purchased from us, or in relation to payments that we have made to you.
- **Technical Data** may include internet protocol (IP) address, browser type and version, time zone setting and location, browser plug-in types and versions, operating system and platform and other technology on the devices used to access this Website.
- **Profile and Usage Data** may include enquiries submitted by you, purchases information, feedback and survey responses, and how you use our website, products and services.
- **Marketing Data** may include details of any preference that you have advised us of in relation to marketing communications from us.

ESRA may also collect non-personal data such as Aggregated Data which is data that may be obtained from personal data, but which does not directly or indirectly identify. This may include Usage Data detailing how the user uses ESRA's Website and the features and areas that the user have interacted with.

#### How Information is collected

A range of different methods may be used to collect data which may include the following methods:

- **Direct interactions** with us in person, by post, phone, email or otherwise. You may give us your Identity, Contact and Financial Information.
- **Automated technologies or interactions** with our website, by using the web enquiry form, or by purchasing ESRA products through our website (Membership, workshops, examinations). You may give us Identity, Contact and Financial Information.
- **Third parties or publicly available sources** (third parties may be used in processing Identity, Contact and Financial categories of personal data).

#### Data accuracy

It is important that the data that ESRA holds about the user is accurate and up to date. If the data changes please notify ESRA so that the records are updated.

#### How information is used

Approved by: ESRA President  
Code- Version: ESRA\_SOP01P2\_vs01  
Date: 05.08.2024

ESRA may hold and process personal data that the user provides in accordance with the GDPR.

The information that ESRA collects and store relating to the user is primarily used:

- To enable ESRA to provide our services to the user, to communicate with the user and to meet ESRA's contractual commitments to the user. This may include Identity, Contact, Financial and Transactional data.
- To notify the user about any changes to our business, such as improvements to ESRA's Website or service/product changes, that may affect ESRA's service or relationship with the user. This may include Identity and Contact data.
- If the user is an existing customer/member, ESRA may contact them with information about goods and services similar to those that were the subject of a previous sale to them. This may include Identity and Contact data.
- Where the user has consented to receive such information, to provide information on other parties' products or services that ESRA feel may be of interest to them. This may include Identity, Contact and Marketing data.
- Where the user has consented to receive ESRA's e-newsletters to provide that to them. This may include Identity and Contact data.
- Where ESRA needs to comply with a legal obligation. This may include Identity, Contact and Transactional data.
- Where it is necessary for ESRA's legitimate interests (or those of a third party) and the user's interests and fundamental rights do not override those interests. This may include all types of data.

Where ESRA collects the user's data for marketing purposes ESRA will always request their consent, at the point the data is collected, to use their data for that purpose.

ESRA will always obtain their prior consent to share their personal data with any third party for their marketing purposes. This may be to enable relevant third parties to advise the user of products or services that may be of interest to you.

ESRA will only use their personal data for a reason other than the purpose for which it was originally obtained if ESRA considers that ESRA needs to use it for that other purpose and has a legitimate interest in doing so.

#### How Information is disclosed

There are a range of circumstances where ESRA may disclose your data to third parties. These include:

Regulatory bodies. ESRA may disclose the user's data to regulatory bodies to enable ESRA to comply with the law and to assist fraud protection and minimize credit risk. This may include Identity, Contact and Transactional data.

ESRA's Suppliers. ESRA may disclose the user's data to third parties that are involved in the fulfilment of ESRA's services to them. This may include Identity, Contact and Transactional data.

Please be advised that we do not reveal information about identifiable individuals to ESRA's advertisers/sponsors, but ESRA may, on occasion, provide them with Aggregated Data about our Website visitors and customers.

If the user does not want ESRA to share their data with third parties they will have the opportunity to withhold their consent to this when they provide their details to ESRA on the form on which ESRA collects your data, or they can send an email to office@esraeurope.org at any time.

#### How information is Controlled

Where ESRA relies on consent as the lawful basis for processing the user's data they can revoke or vary that consent at any time.

If the user does not want ESRA to use their data or want to vary the consent that they have provided they can send an email to office@esraeurope.org at any time.

#### How Information is stored and transferred

As part of the services offered to the users, for example through ESRA's Website, the information they provide to ESRA may be transferred to and stored in countries outside of the European Economic Area (EEA) as ESRA use remote website server hosts to provide the website and some aspects of ESRA's service, which may be based outside of the EEA, or use servers based outside of the EEA – this is generally the nature of data stored in "the Cloud". It may also be processed by staff operating outside the EEA who work for one of ESRA's suppliers, e.g. ESRA's website server host, payment processing provider, membership management system provider or work for ESRA when temporarily outside of the EEA.

A transfer of the user's personal data may happen if any of ESRA's servers are located in a country outside of the EEA or one of ESRA's service providers is located in a country outside of the EEA.

If the user uses ESRA service while they are outside the EEA, their personal data may be transferred outside the EEA in order to provide them with these services.

If ESRA transfers or stores their personal data outside the EEA in this way, ESRA will take steps with the aim of ensuring that their privacy rights continue to be protected, as outlined in this privacy policy.

Where ESRA uses suppliers based in the US, ESRA may transfer data to them if they are part of the Privacy Shield which requires them to provide similar protection to personal data shared between the Europe and the US.

#### Security

The transmission of information via the Internet or email is not completely secure. Although ESRA will do its best to protect the user's personal data, ESRA cannot guarantee the security of data while they are transmitting it to ESRA's site or email address; any such transmission is at their own risk.

ESRA has put in place security measures to prevent their data from accidental, loss or disclosure. Once ESRA has received their personal data, ESRA will use strict procedures and security features to try to prevent unauthorized access.

Where the user has chosen a password so that they can access certain parts of ESRA's site such as the members zone, they are responsible for keeping this password confidential. The user should choose a password that is difficult for someone to guess. ESRA does not have access to their personal password and cannot retrieve it for them. Should they need a new password, they can contact ESRA by email and ESRA will send them a link to update their password.

In the event of a data breach ESRA will notify the users if the breach results in any likelihood of loss or damage to them.

#### Data retention

The length of time that ESRA retains, and stores data depends on the purpose for which it was collected. ESRA will only store data for as long as is required to fulfil that purpose, or for the purpose of satisfying legal requirements.

It is a legal requirement that ESRA keeps certain data about its customers and suppliers for at least six years. The type of data includes Contact, Identity, Financial and Transaction Data.

Where the user has requested that ESRA provides them with marketing materials ESRA will retain their data until such time as consent is withdrawn by them.

#### Use of cookies

ESRA's Website uses cookies. ESRA uses cookies to gather information about the user's computer for ESRA's services and to provide statistical information regarding the use of ESRA's Website. Such information will not identify the user personally – it is statistical data about ESRA's visitors and their use of ESRA's Website. This statistical data does not identify any personal details whatsoever.

ESRA may also gather information about the user's general Internet use by using a cookie file. Where used, these cookies are downloaded to their computer automatically. This cookie file is stored on the hard drive of their computer, as cookies contain information that is transferred to their computer's hard drive. They help ESRA to improve our Website and the service that ESRA provides to them.

All computers have the ability to decline cookies. This can be done by activating the setting on the user's browser which enables them to decline the cookies. Please note that should the user choose to decline cookies; they may



be unable to access particular parts of our Website. In the unlikely case where ESRA works with advertisers on its Website, ESRA's advertisers may also use cookies, over which they have no control. Such cookies (if used) would be downloaded once the user clicks on advertisements on ESRA's Website.

### User's rights

The GDPR gives the user a range of rights in relation to the personal data that ESRA collects from. They have the right to:

Access to its personal data. This right is commonly known as the 'data subject access request' and enables the user to receive a copy of the personal data we hold about them. The user will not need to pay a fee to access their personal data unless ESRA can justifiably demonstrate that the request is repetitive or excessive. ESRA will respond to all legitimate data access requests within one month, but ESRA may need to obtain further information from the user to confirm their identity and the legitimacy of the request.

Request update of the personal data. This enables the user to have any incomplete or inaccurate data corrected.

Erasure of your personal data. This enables the user to ask ESRA to delete personal data where there is no justifiable reason for ESRA continuing to retain and process it. ESRA may not always be able to delete the data such as if there is an ongoing contractual relationship between them or if ESRA is legally required to retain the data.

Object to processing of the user's personal data where ESRA is relying on consent or its legitimate interests (or those of a third party) as the justification for processing the data.

Restrict the processing of the user's personal data. This enables the user to ask ESRA to change the processing of their personal data. For example, the user may wish to vary the basis on which ESRA contact them.

Request the transfer of their personal data to them or to a third party. ESRA will provide the user, or a third party chosen, their personal data in a structured, machine-readable format.

Withdraw consent. Where ESRA is relying on consent to process their personal data the user may withdraw that consent. If the user withdraws their consent, ESRA may not be able to provide certain products or services to the user. ESRA will advise the user if this is the case at the time you withdraw their consent.

The user can exercise these rights at any time by sending an email to [office@esraeurope.org](mailto:office@esraeurope.org)

### Third party links

The user might find links to third party websites on ESRA's website. If the user clicks a link to a third-party website and visit that site, the user may be allowing that site to collect and share certain data about them. These websites should

Approved by: ESRA President

Code- Version: ESRA\_SOP01P2\_vs01

Date: 05.08.2024

have their own privacy policies, which the user should check. ESRA does not accept any responsibility or liability for their policies whatsoever as ESRA has no control over them.

### Complaints

If the user wishes to raise a complaint regarding ESRA's use of their personal data, then the user can contact their national data protection authority.

If the user does wish to raise a complain then ESRA would welcome the opportunity to discuss their concerns before the user contacts their national data protection authority to see if ESRA can resolve the issue for them.

## **6 ROLES AND RESPONSIBILITIES**

### President

- Ensures that quality standards are integrated into ESRA's strategic vision and operations.
- Approves major quality improvement projects and policies.
- Leads efforts to promote a culture of excellence within ESRA.

### Quality Officer

- Monitor compliance with quality standards across all processes.
- Conduct regular quality audits and report findings.
- Identify areas for improvement and recommend corrective actions.
- Train employees on quality standards and procedures.
- Ensure all deliverables meet organizational and stakeholder expectations.

### Board Members

- Provide strategic oversight and ensure information security aligns with ESRA's strategic objectives.
- Approve the information security policy and allocate resources for its implementation.
- Adhere to the information security policy and procedures.
- Report any observed or suspected information security incidents immediately.

### Data Protection Officer

- Develop, implement, and maintain the applied procedures
- Supervise and support implementation of the policy.
- Ensure compliance with relevant legal, regulatory, and contractual requirements.
- Report on the performance of the applied procedures to the Executive Board members.

### All Employees

Approved by: ESRA President

Code- Version: ESRA\_SOP01P2\_vs01

Date: 05.08.2024

- Adhere to the information security policy and procedures.
- Participate in information security training and awareness programs.
- Report any observed or suspected information security incidents immediately

## 7 DISTRIBUTION LIST

All personnel.

## 8 FILE KEEPING

The QMS shall keep the records for at least 5 years.

This document shall enter into force, be revised and distributed in accordance with the applicable procedures for controlled documents of ESRA.

This document:

- ✓ It is the property of the ESRA and its unauthorized disclosure, reproduction and use in whole or in part, nor its use for work not related to the activities of ESRA is not permitted.
- ✓ It is an internal controlled document, distributed according to the distribution list and acknowledged under the responsibility of the recipient.
- ✓ It shall be subject to a review procedure at least once every three years since the last adoption or amendment.

		<b>SIGNATURE</b>	<b>DATE</b>
<b>AUTHOR</b>	<b>Quality Officer</b>	Aline Christen	10.07.2024
<b>APPROVAL</b>	<b>ESRA President</b>	Eleni Moka	05.08.2024

