



Privacy notice for self-employed Board members

What we do with your data

Last update: September 2018

Applicable to all self-employed board members of Euroclear Sweden

Table of contents

1	About this Privacy Notice	3
1.1	Who and what is this notice for?	3
1.2	Who controls your personal data?	3
2	Personal data	3
2.1	What personal data do we collect from you and why?	3
2.2	How long is personal data kept?	4
2.3	Where does your personal data come from?	5
2.4	Who do we share your personal data with?.....	5
2.5	What are your rights regarding personal data?	6
2.6	What about data security and quality?	7
3	Updates to this notice	8
4	Questions or concerns?	8

1 About this Privacy Notice

1.1 Who and what is this notice for?

This notice applies to the personal data of individuals who are self-employed board members (“board members”) of Euroclear Sweden (“you”, “your”):

The purpose of this notice is to inform you on:

- what personal data we collect;
- why we collect that personal data;
- how we use it;
- who we share it with and why; and
- your rights in relation to that personal data.

This notice also includes the information that we are required by the General Data Protection Regulation (“GDPR”) to provide to you.

1.2 Who controls your personal data?

Euroclear Sweden takes its data protection obligations seriously. We, Euroclear Sweden AB, with registered office at Klarabergsviadukten 63, Po Box 191, SE - 101 23 Stockholm (Sweden) and registered under organisation number 556112-8074 (“Euroclear”, “we”, “us” or “our”), are the controller of the personal data that is processed about you in the context of this notice and are therefore responsible for processing it in accordance with the law.

It is important that the personal data we hold about you is accurate and current. Please keep us informed if your personal data changes during your working relationship with us.

2 Personal data

2.1 What personal data do we collect from you and why?

We will only collect and use your personal data for a specific purpose and when we have legal grounds to do so under the GDPR. Therefore, our main purposes for collecting and processing your personal data are:

- When we have a legal obligation to process your personal data (such as the legal and compliance checks before appointing you as a board member, the legal obligation to issue communications, disclosures and publications pertaining to your appointment as a board member etc.);
- When it is necessary to perform the contract we have with you (when your appointment as a board member becomes effective). In this respect, we use your personal data in order to approve, manage, administer or execute your appointment as a board member, to process invoices and payments of expenses, to organise board meetings etc.;
- When it is in our legitimate business interests (e.g. prevent and detect security threats to our IT infrastructure or buildings);
- When it is necessary to protect our legal position (in the event of legal proceedings etc.); or

- When you have, in strictly defined circumstances, given your consent to the processing, e.g. for the use of a picture of you taken during an event.

Details of what personal data we process and the types of processing can be found in the below table.

Purposes of the Processing	Types of Personal Data
Provide IT services for board members (provide system access, provide office tools, provide communication services, ensure system security)	<ul style="list-style-type: none"> • Business card details ¹ • Device type and model, Operating system • Log data (IP Addresses and connection data; URLs of visited websites etc.) • Details of calls (caller ID, time and date, recipient, call recording)
Organisation of board meetings and administration around board membership and decisions (drafting board minutes, organising board meetings, executing board decisions, compliance with legal requirements etc.)	<ul style="list-style-type: none"> • Business card details • Professional / Educational background • Statement of good repute • Details of other mandates/positions (conflicts of interest) • Agenda • Intervention during board meetings (reflected into board minutes) • Copy of ID card • Private address and phone number
Respond to requests of regulator and public authorities, perform legal disclosures (with regards to regulatory / legal requirements, or investigations), handle litigation, perform internal audit	<ul style="list-style-type: none"> • Business card details • Professional / Educational background • Statement of good repute • National registry
Social events (attendance, advertising events, communications on internal social platforms, media relationship)	<ul style="list-style-type: none"> • Personal details • Professional details • Recording of images (picture and videos)

2.2 What are the legal bases for processing personal data

As described above, we normally only process personal data about you where:

- We need the personal data to carry out a contract with you;
- We need the Personal Data to comply with our legal obligations; or
- The processing is in our legitimate business interests, e.g. building security within our office premises, protecting our IT infrastructure.

2.3 How long is personal data kept?

As a general rule, we keep personal data as long as we have a contractual relationship. However, we keep all or part of such data for an additional period of 7 years (to answer any

¹ Business card details include name, title, company, mailing address, and telephone numbers.

contractual liability issues following the statutory period of limitations set by the Swedish Accounting Act) or for 10 years (if required by the EU Central Securities Depository Regulation).

Images recorded by security cameras in and around our premises are kept for 30 days from the visit, except otherwise requested by the police / public prosecutor and / or legal department (this will notably be the case if the recorded images show potential criminal activity or incidents).

2.4 Where does your personal data come from?

The personal data we collect from you come from the following sources:

We may collect your personal data in a variety of ways. The personal data we process from you will be primarily provided to us directly by you in order for us to assess your application for a board position or manage our contractual relationship.

In some cases, we may collect personal data about you from other sources, such as references, recruiting agencies, public authorities, screening agencies, publicly available sources to confirm signatory powers, details on your intervention in board meetings (i.e. through board minutes), or publicly accessible information sources such as the internet, and public social media profiles, or, if required by law, extract of criminal records.

2.5 Who do we share your personal data with?

a) Transfer within the Euroclear Group or to third parties

- We may transfer personal data only to other Euroclear affiliated entities or our business partners (e.g. joint venture companies), who legitimately need the information to carry out their normal duties.
- As a board member or as a prospect to a board position, we will share your personal data with our shareholders and publish your personal data in corporate or regulatory publications, in accordance with the law (such as the shareholders' resolutions appointing you as a board member, our annual accounts and management report etc.). We may also share your personal data for marketing purposes and within the framework of our proposals for services.
- We may also provide your personal data to any competent law enforcement body, regulatory, government agency, court or other third party such as but not limited to, the police, the financial supervisory authorities, tax and social security agencies, where we believe disclosure is necessary (i) as a matter of applicable law or regulation, or (ii) to exercise, establish or defend our legal rights.
- We may also disclose your personal data to our third party vendors, service providers and partners who provide data processing services to us (e.g. IT platform management or support services, infrastructure and application services, data analytics, security agents, billing tool, etc.), or who otherwise process personal data for purposes that are described in this privacy notice or notified to you when we collect your personal data.
- We may also disclose your personal data with our auditors, advisors, legal representatives and similar agents in connection with the advisory services they provide to us for legitimate business purposes.

- Finally, we may also disclose your personal data to a potential buyer, seller or joint venture (and its agents and advisers) in connection with any proposed purchase, merger, acquisition or transaction, provided that we inform our contractual party that it must use your personal data only for the purposes disclosed in this notice.

b) International personal data transfers

It is possible that in some circumstances we may transfer some of your personal data outside the European Economic Area (EEA), but we shall only do so after having taken appropriate safeguards required by applicable data protection laws. Such measures may include (without this list being exhaustive) transferring the personal data to a recipient in a country that the European Commission has decided provides adequate protection for personal data, to a recipient that has executed standard contractual clauses adopted or approved by the European Commission or, in exceptional cases, reliance on the derogations under the applicable data protection law.

2.6 What are your rights regarding personal data?

This section summarises the rights you have as a “data subject” under the GDPR.

The exercise of these rights are subject to conditions which are set out in the GDPR and while they are wide-ranging, in limited circumstances it may not be possible to fully exercise them, e.g. if you request personal data to be deleted but the law requires that we keep it.

The right to be informed	Euroclear is publishing this privacy notice to keep you informed as to what we do with your personal data. We strive to be transparent about how we use your personal data.
The right to access	You have the right to access your personal data. Please contact Euroclear’s Data Protection Officer if you wish to access the personal data Euroclear holds about you, at the postal address mentioned in section 4 of this notice.
The right to rectification	If the personal data Euroclear holds about you is inaccurate, not complete or up to date, you have the right to ask us to rectify or update it. If such personal data has been disclosed to a third party in accordance with this privacy notice, then we shall also ask them to rectify or update your personal data. Please contact our Data Protection Officer if you need us to rectify your information at the postal address mentioned in section 4 of this notice.
The right to erasure	This is sometimes called ‘the right to be forgotten’. If you want to request Euroclear to erase your personal data and we do not have a legal reason to continue to process and hold it, please contact our Data Protection Officer at the address mentioned in section 4 of this notice.
The right to restrict processing	In some circumstances, you have the right to ask Euroclear to restrict how we process your personal data. This means we are permitted to store the data but not further process it. If you want us to restrict processing of your personal data, please contact our Data Protection Officer at the address mentioned in section 4 of this notice.

<p>The right to data portability</p>	<p>In some circumstances, Euroclear allows you to obtain the personal data we hold about you in a structured, commonly used and machine-readable format and to transmit those personal data to another controller without any hindrance. Please contact our Data Protection Officer at the address mentioned in section 4 of this notice, if you want information how to transfer your personal data elsewhere. This right only applies to personal data that you have provided to us as a data controller. The personal data must be processed on the basis of your consent or for the performance of a contract and processing of your personal data must be carried out by automated means.</p>
<p>The right to object</p>	<p>In some circumstances, you have the right to object to Euroclear processing your personal data. If you wish to object please contact our Data Protection Officer at the address mentioned in section 4 of this notice.</p>
<p>The right to withdraw consent</p>	<p>If you have given us your consent to process your data but would change your mind later, you have the right to withdraw your consent at any time, and Euroclear will then stop processing your personal data. If you want to withdraw your consent, please contact our Data Protection Officer at the address mentioned in section 4 of this notice. Withdrawing your consent will not affect the lawfulness of any processing we conducted prior to your withdrawal, nor will it affect processing of your personal data conducted in reliance on lawful processing grounds other than consent.</p>
<p>The right to complain to a Supervisory Authority</p>	<p>You have the right to complain to your local data protection authority about our collection and use of your personal data if you feel that Euroclear has not sufficiently addressed a concern or complaint. For more information, please contact your local data protection authority. You can find contact details for data protection authorities in the European Economic Area, Switzerland and certain non-European countries (including the US and Canada) here. Contact details for the Swedish Data Protection Authority can be found here: https://www.datainspektionen.se.</p>

2.7 What about data security and quality?

We implement risk-appropriate measures and processes that are designed to provide a level of security appropriate to the risk of processing your personal data to help us to keep your personal data secure and to maintain its quality.

In order to keep your personal data secure, we have implemented a number of security measures, including:

- **Secure operating environments** - We store your data in secure operating environments and only accessible to Euroclear employees, contractors and consultants on a need-to-know basis. Euroclear also follows generally accepted industry standards in this respect.
- **Encryption** - We use industry-standard encryption to provide protection for information that is transmitted to us.
- **Prior authentication for IT access and access to premises** - We require our employees to verify their identity (e.g. through login ID, password, pin codes and badges) before they can access IT bases and business premises. This is aimed to prevent unauthorized accesses.

3 Updates to this notice

We may update this notice from time to time in response to changing legal, technical or business change/developments. You can see when the notice was last updated by checking the “last updated” date displayed at the top of it. Please consider the version available online www.euroclear.com/Sweden-GDPR as the latest version.

4 Questions or concerns?

If you want to request information about this notice, you can contact our Data Protection Officer by e-mailing us at es.dpo@euroclear.eu or writing to our Data Protection Officer by writing to Euroclear Sweden AB, Data protection officer, PO Box 191, SE-101 23 Stockholm, Sweden.