

# How East Capital Financial Services Processes Your Personal Data

## 1. GENERAL INFORMATION

East Capital Financial Services AB (ECFS) places the utmost importance on protecting your personal privacy and is committed to maintaining a high standard of data protection. This document sets out how we collect and process your personal data, outlines your rights in relation to that data, and explains how you may exercise those rights. It is essential that you read and understand this information to remain fully informed and confident in how we handle your personal data. Should you have any questions, you are welcome to contact us at any time.

## 2. WHAT IS PERSONAL DATA AND HOW IS IT PROCESSED

Personal data refers to any information that directly or indirectly relates to an identified or identifiable living individual. For example, images and audio recordings processed electronically may constitute personal data even if no names are mentioned. Encrypted data and various forms of electronic identifiers (such as IP addresses) also qualify as personal data if they can be linked to an individual.

The processing of personal data encompasses any operation or set of operations performed on personal data, whether by automated means or otherwise. Typical examples include the collection, recording, organisation, structuring, storage, alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure, or destruction of such data.

## 3. WHAT PERSONAL DATA DOES EAST CAPITAL FINANCIAL SERVICES PROCESS?

East Capital Financial Services generally processes the following personal data:

- Name
- Personal identity number
- Address details
- Email
- Telephone number
- Log files
- ID card number
- Passport number
- Financial information such as bank account number, credit card number, salary information, payment details
- User data: Customer number, order history
- Photos (if they can be used to identify a person), e.g. in passport copies

#### 4. **WHAT IS OUR LEGAL BASIS FOR PROCESSING YOUR PERSONAL DATA?**

The primary legal basis for our processing of personal data is the consent you have given in accordance with Article 6.1(a) of the GDPR.<sup>1</sup> This applies particularly to processing for the following purposes:

- Sending marketing to you if you are not yet a customer
- Using certain cookies or analytical tools
- Processing special categories of data (if applicable)

You have the right to withdraw your consent at any time. However, withdrawal does not affect the legality of processing carried out before consent was withdrawn.

In some cases, we may also process your personal data based on our legitimate interest, in accordance with Article 6.1(f) of the GDPR. This applies, for example, to marketing to existing customers or certain technical analyses. In such cases, we conduct a balancing test to

---

<sup>1</sup> “GDPR” stands for the Regulation (EU) 2016/679 of the European Parliament and the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, also known as the General Data Protection Regulation.

ensure our interest outweighs your interest in not having your data processed. You always have the right to object to processing based on legitimate interest.

#### 5. **WHO IS RESPONSIBLE FOR THE PERSONAL DATA WE COLLECT?**

East Capital Financial Services AB, reg. no. 556988-2086, Box 1364, 111 93 Stockholm, is the data controller for the company's processing of personal data. ECFS also operates under the trade names Hjerta Invest, East Capital Direct, Espiria, and Adrigo.

#### 6. **FROM WHERE DO WE COLLECT YOUR PERSONAL DATA?**

In addition to the data you provide to us or that we collect based on your use of our services, contract agreements, and any purchases, we may also collect personal data from other sources (third parties). Generally, data from other sources is limited as far as possible and mainly concerns information from public registers to ensure we have correct address information and to fulfil checks required to combat money laundering.

#### 7. **WITH WHOM MAY WE SHARE YOUR PERSONAL DATA?**

*Processors.* Where necessary to provide our services, we share your personal data with companies acting as processors for us. A processor is a company that processes data on our behalf and according to our instructions. We use processors for:

- Invoice and payment solutions (mainly banks and payment service providers)
- Anti-money laundering checks (collecting customer due diligence when establishing a business relationship)
- Marketing (print and distribution, social media, media agencies, or advertising agencies)
- IT services (companies managing operations, technical support, and maintenance of our IT systems)
- SPAR and Dun & Bradstreet (business, marketing, and credit information)

When your data is shared with processors, it is only for purposes compatible with those for which we collected it (e.g. to fulfil our contractual obligations, general terms, consents, or legitimate interests). We ensure that all processors provide adequate security and confidentiality guarantees. We have written agreements with all processors requiring them to

ensure the security of the personal data they process, comply with our security requirements, and restrict international transfers.

Other companies as independent controllers. We also share data with companies acting as independent data controllers. This means we do not control how they process the data we share. These include:

- Public authorities (Police, Tax Agency, or others) if required by law or in cases of suspected crime
- Companies handling general transportation (e.g. PostNord and courier companies)
- Companies providing invoice and payment solutions (acquiring companies, banks, payment service providers)
- Companies providing identification services (e.g. BankID)

When data is shared with such companies, their privacy policies govern their processing.

## 8. **WHERE DO WE PROCESS YOUR PERSONAL DATA?**

We always strive to process your data within the EU/EEA, and all our IT systems are located within this area. However, in cases of system support and maintenance, data may be transferred to countries outside the EU/EEA. This occurs, for example, if a processor or its subcontractor is located or stores data in such a country. In these cases, only data relevant for the purpose is shared (e.g. log files).

Regardless of location, we take all reasonable legal, technical, and organisational measures to ensure the same level of protection as within the EU/EEA. When data is processed outside the EU/EEA, protection is ensured either through an EU Commission adequacy decision or through appropriate safeguards, such as approved codes of conduct, standard contractual clauses, or binding corporate rules.

ECFS is part of the East Capital Group. To provide our services efficiently, securely, and tailored to clients, we may share your data within the group. When shared for internal administrative purposes, such as IT operations or support, the receiving company acts as a processor. When shared to enable the receiving company to offer its own products or services, it acts as an independent controller.

The legal basis for such intra-group sharing is our legitimate interest in managing internal

administration and providing group services. We always conduct a balancing test to ensure your rights are not adversely affected. You may object to this processing at any time.

We never share personal data, even within the group, if it would breach our duty of confidentiality regarding your financial affairs.

## 9. **HOW LONG DO WE KEEP YOUR PERSONAL DATA?**

We keep your data as long as necessary to fulfil the purposes for which it was collected, and only to the extent required by applicable laws, industry practice, and regulatory requirements.

Examples of retention periods:

- **Investment advisory and customer relationship data:** up to 10 years after the business relationship ends, per the Securities Market Act (2007:528) and to defend legal claims.
- **Data processed under anti-money laundering laws:** minimum of 5 years and maximum of 10 years after the customer relationship ends, per the Money Laundering and Terrorist Financing Prevention Act (2017:630).
- **Data processed based on consent:** until consent is withdrawn or no longer valid.
- 

If data is needed to defend legal claims or investigate an incident, it may be retained longer but never beyond what is necessary for that specific purpose.

## 10. **WHAT RIGHTS DO YOU HAVE AS A DATA SUBJECT?**

### *Right of access*

You can request information on what data we process about you (data extract).

### *Right of rectification*

You can request correction of inaccurate data. Some data can be updated directly by logging into our website.

#### *Right to erasure*

You can request deletion under certain conditions, unless legal obligations require us to retain data.

#### *Right to restriction*

You can request limitation of processing under certain circumstances

#### *Right to object*

You can object to processing based on legitimate interest, including direct marketing.

#### *Right to data portability*

You can request to transfer your data to another controller if processing is based on consent or contract.

### **11. HOW DO WE PROCESS PERSONAL IDENTITY NUMBERS?**

We only process your personal identity number when clearly justified for the purpose, necessary for secure identification, or for other acceptable reasons, and always minimise its use.

### **12. WHAT ARE COOKIES AND HOW DO WE USE THEM?**

Cookies are small text files of letters and numbers sent from our web server and stored on your browser or device. We use:

- Session cookies (temporary, deleted when browser closes)
- Persistent cookies (remain until deleted or expired)
- First-party cookies (set by our website)
- Third-party cookies (set by other websites, e.g. for analytics like Google Analytics)
- Similar technologies storing information in browsers or devices

These help us improve services, remember setting, analyse usage, and target marketing. You can read more on our website.

13. **CAN YOU CONTROL THE USE OF COOKIES YOURSELF?**

Your browser or device allows you to adjust cookie settings, such as blocking all cookies, accepting only first-party cookies, or deleting cookies when closing the browser. Note that some services may not work if cookies are blocked or deleted. For certain cookies (e.g. analytics and marketing), we obtain your consent in advance, and you can withdraw consent at any time via our cookie manager or browser settings.

14. **HOW IS YOUR PERSONAL DATA PROTECTED?**

Our IT systems are designed to ensure high confidentiality, integrity, and availability of personal data. Special security measures protect your data against unauthorised processing, access, loss, destruction, or damage. Only those needing access for specified purposes can access your data.

15. **SUPERVISORY AUTHORITY AND THE RIGHT TO COMPLAIN**

The Swedish Authority for Privacy Protection (IMY) supervises GDPR compliance. You have the right to lodge a complaint if you believe we process your data unlawfully. For cookies and electronic communication, the Swedish Post and Telecom Authority (PTS) is the supervisory authority.

16. **HUR KONTAKTAR DU OSS LÄTTAST VID FRÅGOR OM DATASKYDD**

East Capital takes data protection seriously and have appointed dedicated staff to to handle any questions you may have. You can always contact us by emailing [data.protection@eastcapital.com](mailto:data.protection@eastcapital.com) or calling +46 8 505 885 00 and asking for our Data Protection Officer.

Please be advised that this information may be updated periodically. The most current version will always be available on our website. In the event of any material changes, we will provide prior notice on our website and, where applicable, via email, including a detailed explanation of the amendments and their potential implications for you.