HYGGEX FINANCE
PRIVACY NOTICE

HYGGEX FINANCE – PRIVACY NOTICE VER. 1.0

Approval date	Version	Description
19/01/2025	1.0	Initial Policy.

Document Information:

Document Property	Document Details
Document Title:	Privacy Notice
Document file name:	Hyggex Finance - Privacy Notice
Revision Number:	Version 1.0
Issued by:	Julija Zablocka
Issue date:	19/01/2025
Status:	Final
Board approval:	Approved

Table of Contents

1. Information about the Data Controller

The Company name is **Hyggex Finance ApS** (hereinafter also referred to as the "Company"). **Company Registration No.: 45085643**

Registered : Maglebjergvej 6, 2800 Kongens Lyngby, Denmark

Contact the Company as follows:

- **By calling:** + 45 92 450388
- **By e-mail:** info@hyggex.dk

Contact Information for Personal Data Protection Matters
Any inquiries regarding this Notice or the processing of personal data may be directed via:

- The communication channels listed above;
- By e-mailing: compliance@hyggex.dk

2. General Description of Personal Data Processing

This Notice describes how personal data is processed in relation to the Company's customers, customer representatives and contact persons, website visitors, and any other individuals whose personal data may be collected in the course of business operations. It is assumed that before engaging with the Company's website or entering into a business relationship, the data subject has read and accepted the terms of this Notice.

The purpose of this Notice is to provide a general overview of personal data processing activities and their purposes. Additional details may be found in other documents issued by the Company, such as service contracts, cooperation agreements, general terms of business, and website usage rules. The provisions herein apply exclusively to the processing of personal data of natural persons.

Additional personal data processing notices are available at:
• Website Usage Rules (available at [Insert Website URL]);
• Privacy Policy (available at [Insert Website URL]).

The Company recognises the value of personal data and commits to processing it in accordance with the highest standards of confidentiality and security as required by applicable Danish and EU legislation.

3. Purposes for Processing Personal Data and the Lawful Basis

Personal data is processed solely for the defined and legitimate purposes arising from regulatory requirements and the Company's own legitimate interests, including the provision of financial services. The lawful bases for such processing are established under the Danish Data Protection Act and the EU General Data Protection Regulation (EU GDPR).

a) Customer Accounting and Service Provision

Processing is required for the establishment, commencement, and ongoing provision of services, including:

- Identifying and verifying data subjects;
- Performing due diligence and customer risk assessments;
- Retaining copies of identification and due diligence documents;
- Facilitating transaction execution and recording; and
- Managing communications regarding service provision and contractual performance, including recovery of outstanding obligations.

For this purpose, the following types of data are processed:

- **Identification data:** first name, surname, identity number, date of birth, citizenship, nationality, identity document details (including copies), visa/residence permit details, and, where applicable, customer photographs.
- **Contact details:** address, telephone number, email address, and preferred language.
- **Professional, economic, and personal activity information:** education, occupation, work experience, transaction details, and counterparty information.
- **Tax and special status information:** country of tax residence, tax registration number, and details indicating if the data subject is a politically exposed person.
- **Family-related information:** family status and composition, along with personal data of family members.
- **Transaction data:** details of beneficial ownership, information regarding affiliated parties, business activity, and counterparty data.
- **Financial data:** information on income sources, amounts, property ownership, shareholdings, bank accounts, loan obligations, etc.
- **Usage data:** account transactions, types of services utilised (such as lending, investment, or trading), and communication records.

b) Compliance with Statutory Requirements for AML/CTF

Processing is carried out to meet the statutory requirements for anti-money laundering and counter-terrorism financing. This includes:

- Identifying customers and establishing beneficial ownership;

- Verifying the origin of funds;
- Conducting due diligence on transactions and counterparties; and
- Reporting suspicious transactions.

Data processed under this purpose encompasses identification data, professional and transaction details, and financial information, in line with Danish AML regulations and relevant EU directives.

c) Customer Risk Assessment

For risk assessment purposes, additional information may be obtained from public or statutory registers to:

- Determine the appropriate products and services to offer;
- Establish terms and conditions; and
- Comply with statutory risk assessment obligations.

This involves processing identification, professional, financial, and transaction data, as well as data specifically used for risk profiling.

d) Fulfilment of Other Statutory Requirements

Processing may also occur to comply with other legal obligations, including responding to supervisory, tax, or law enforcement requests. In such cases, personal data as described in section (a) is processed, excluding family-related data when not required.

e) Execution of Payment System Transactions

The execution of domestic and international transactions necessitates processing of personal data, including identification, transaction details, and, if needed, financial status and fund origin, to meet EU and international payment system standards and security obligations.

f) Protection of Company and Customer Interests

Processing is undertaken to protect the legitimate interests of both the Company and its customers. This includes:

- Ensuring service quality (e.g. retaining transaction records and call logs);
- Preventing and investigating unauthorized or fraudulent activity; and
- Conducting internal training and maintaining IT security measures.

g) Enforcement of Rights and Debt Recovery

The Company may process personal data to enforce contractual obligations, exercise the right of claim, and facilitate debt recovery. This includes retaining identification data, contact information, and records related to orders, contractual performance, and outstanding obligations.

h) Prevention of Threats to Security and Property

Processing for security purposes may involve video surveillance, telephone recordings, and other

measures to protect physical and digital assets, in accordance with applicable security standards and legal provisions.

i) Marketing Activities

Processing for marketing involves the use of contact data to send commercial messages, promote services, and inform about public events. This is based on either explicit consent, contractual necessity, or the Company's legitimate interests in effective communication.

j) Technical System Maintenance and Improvement

To ensure the proper functioning and continuous improvement of technical systems and IT infrastructure, personal data may be processed in relation to system usage and performance.

Main Lawful Bases

The primary legal bases for the above processing activities are:

- Consent of the data subject (where applicable);
- Necessity for the performance of a contract;
- Compliance with legal obligations; and
- Legitimate interests pursued by Hyggex Finance ApS (such as risk assessment, fraud prevention, and service quality).

4. Why Provide Personal Data?

Personal data is collected primarily to enable the provision of services, fulfil contractual obligations, comply with legal requirements (including AML/CTF obligations), and support the Company's legitimate interests. The specific information required is essential for:

- Establishing and maintaining a business relationship;
- Delivering tailored services and favourable contractual terms; and
- Ensuring the ability to meet regulatory and statutory obligations.

Where submission of certain data is not mandatory, it may be indicated as voluntary if it contributes to an improved service offering or more favourable contract terms.

Key statutory requirements include:

1. Provision of personal data (as defined in section a) is required primarily under AML/CTF regulations and associated legal obligations;
2. In business transaction documents involving natural persons, data such as first name, surname, identity number (if applicable), and the residential or declared address is essential.

5. How Is Personal Data Obtained?

Personal data may be obtained through various channels, including:

- Direct provision during the contract formation process;
- Submission of data by an authorised representative or legal/authorized contact person when entering into a contract with a third party;
- Provision of data through applications, emails, or telephone calls;
- Online application for services via the Company's website;
- Authorization through online banking or mobile applications;
- Collection via cookies during website visits; and
- In some cases, from third-party databases (e.g. for creditworthiness assessments or due diligence purposes).

5.1. Profiling and Automated Decision-Making

In some instances, personal data may be processed for profiling purposes to assess risk levels, adjust services to meet specific needs, and enhance user experience. This may include customizing service displays, preparing tailored offers, and gathering statistics on typical behaviour and lifestyle habits through both internal and external data sources. Automated decision-making is not used in isolation; where profiling informs personalised offers or marketing, it is implemented in a manner that allows for easy data subject choice and intervention via the Company's digital platforms.

6. Who Can Access Personal Data?

Access to personal data is strictly controlled and granted only to:

- Employees or directly authorised personnel who require access to perform official duties;
- Data processors providing services on behalf of the Company, restricted to the necessary scope;
- Third parties that ensure contractual obligations are met (e.g. surety providers, guarantors, or pledgors);
- Supervisory authorities and law enforcement agencies as required by law;
- Entities maintaining public registers (e.g. population or commercial registers);
- Rating agencies, credit institutions, financial institutions, insurance providers, and financial intermediaries involved in trading, payments, and reporting.

7. Selection of Data Processors and Counterparties

Personal data is transferred to data processors only after careful evaluation and under agreements that require confidentiality and secure processing. Current data processors include:

- Legal entities and structural units within the Company's group (e.g. representative offices abroad);
- Outsourced accountants, auditors, financial and legal advisers, and translators;
- Participants in European and international payment systems, including SWIFT and associated entities;
- Debt collectors engaged under assigned rights of claim;
- IT infrastructure providers and database maintainers;
- Other entities related to the provision of services (e.g. archiving, courier services, or providers involved in ancillary service delivery).

Data processor arrangements may change over time in line with operational needs.

8. International Data Transfers

Personal data processing primarily occurs within the European Union (EU) and the European Economic Area (EEA). Transfers of personal data to countries outside these regions occur only when an appropriate legal basis is established. Such transfers are permitted if based on:

- The data subject's explicit consent after being informed of potential risks;
- Compliance with a legal obligation;
- The necessity for the performance or formation of a contract;
- Adequate security measures, such as those provided by standard data protection clauses or binding corporate rules.

Adequate security measures include confirmation by the European Commission (or relevant Danish authority) that the recipient country ensures an adequate level of data protection, or the implementation of contractual safeguards.

Additional details regarding international data transfers can be provided upon request.

9. How Long Is Personal Data Stored?

Personal data is retained only as long as necessary for the purposes for which it is processed and in compliance with applicable legal and regulatory requirements. In determining retention periods, the Company considers:

- Legislative and regulatory obligations;

- Contractual requirements;
- Data subject instructions (where processing is based on consent); and
- The Company's legitimate interests.

Common retention periods include:

- Data necessary for contractual performance is retained until the contract is fully executed and any statutory retention requirements have expired;
- Data obtained through customer identification and due diligence (including copies of identification documents, transaction records, and correspondence) is stored during the business relationship and for five (5) years following its termination;
- Data required for transaction registration and accounting is retained for the periods specified by regulatory enactments;
- Information maintained to substantiate the fulfillment of legal obligations is stored in line with statutory limitation periods; and
- Personal data processed on the basis of consent is retained for the duration of consent unless another legal basis applies.

Once personal data is no longer required for the specified purposes, it will be securely erased, destroyed, or anonymised.

10. Rights of the Data Subject

The following rights are granted to data subjects under the Danish Data Protection Act and the EU GDPR:

- **Right of Access and Data Portability:**
  Entitlement to obtain an electronic copy of the personal data held, along with supplementary information regarding its processing.
- **Right to Rectification and Erasure:**
  Right to request corrections of inaccurate data or deletion of data that is no longer necessary, subject to legal obligations.
- **Right to Restrict Processing:**
  Right to limit processing under specific circumstances, such as when data accuracy is contested or processing is unlawful.
- **Right to Object:**
  Right to object to processing based on legitimate interests, including for direct marketing purposes.
- **Right to be Informed of New Processing Purposes:**
  Right to receive notification when personal data is processed for a new purpose not originally specified.

- **Rights Relating to Automated Decision-Making and Profiling:**
  Entitlement to request human intervention or opt out of decisions made solely by automated means.
- **Right to Withdraw Consent:**
  Withdrawal of consent for data processing at any time, without affecting the lawfulness of processing carried out prior to the withdrawal.

Data subjects may submit requests to exercise these rights by sending an application (with appropriate identification) to:

- **By post: Maglebjergvej 6, 2800 Kongens Lyngby, Denmark**
- **By e-mail:** info@hyggex.dk or compliance@hyggex.dk.

The Company will respond to such requests within the timeframe stipulated by law, typically within one month. If further time is needed, the Company will inform the data subject of the delay and provide a reason.

11. Filing a Complaint

If a data subject has any concerns or objections regarding the processing of personal data by Hyggex Finance ApS, initial contact should be made using the communication channels specified above. Should the issue remain unresolved, a complaint may be submitted to the supervisory authority, the **Danish Data Protection Agency (Datatilsynet)**, at:

- **Address:** Carl Jacobsens Vej 35, 2500 Valby, Denmark
- **Telephone:** +45 33 19 32 00
- **Website:** www.datatilsynet.dk