Energy Risk Management Fondsmæglerselskab A/S

Privacy Policy 2025

Table of Contents

1. Introduction

1.1 This document describes how Energy Risk Management Fondsmæglerselskab A/S ("ERM", "the Company", "we", "us" or "our") processes personal data in accordance with applicable data protection legislation.

1.2 The Board of Directors has adopted this Privacy Policy ("the Policy") to ensure that all processing of personal data within the Company is carried out in accordance with applicable data protection legislation.

1.3 Protecting the confidentiality and integrity of personal data is essential to ERM's operations and to maintaining the trust of our clients, partners and employees.

2. Purpose

2.1 The Policy provides a framework for how personal data is collected, used, stored and protected. The Policy ensures that all processing activities within the Company are carried out lawfully, fairly and transparently.

3. Legal Basis

The Company processes personal data in accordance with the General Data Protection Regulation ("GDPR"), which applies to all companies and organisations that process personal data of individuals located in the European Union ("EU") or the European Economic Area ("EEA"). The GDPR sets out the core principles, rights, and obligations relating to the processing of personal data and requires that such processing is lawful, fair, and transparent.

4. Data Controller

4.1 The Company acts as the Data Controller, processing personal data primarily for its own purposes. As the Data Controller, the Company is responsible for determining both the purposes and methods of processing personal data.

4.2 Energy Risk Management Fondsmæglerselskab A/S
Address: Petersbjerggård 4, 1. th, DK-6000 Kolding
Company registration no.: 45226077
Email: backoffice@ermh.dk
Telephone: +45 69 13 08 88

5. Data Subject

5.1 As the data subject, you have certain legal rights under applicable data protection laws, which are outlined in this section. These rights ensure that your personal data is processed fairly and give you control over how we handle your information. If you wish to exercise any of your rights or require further clarification, please contact us using the details provided in cf. Section 4.2 so that we can assist you. Please note that these rights may change, and we recommend referring to official sources for the most up-to-date information.

Right to be Informed

In accordance with Articles 12-14, you have the right to be informed about the collection and use of your personal data. The Privacy Policy provides clear and concise information about how we collect and process your data. If you require further clarification, please contact us at backoffice@ermh.dk.

Right of Access

As outlined in Article 15, you have the right to obtain confirmation from us as to whether personal data concerning you is being processed, and if so, to access the personal data and the following information.

Right of Rectification

Under Article 16, you have the right to have inaccurate or incomplete personal data rectified. To exercise this right, please submit a request in writing or verbally, and we will respond within one month. If we are unable to fulfil your request, we will provide the reasons.

Right to Erasure

Article 17 grants you the right to have your personal data erased. This right is not absolute and applies only under certain conditions. We will respond to such requests before the time of our regular general deletion.

Right to Restrict Processing

As per Article 18, you have the right to restrict the processing of your personal data under certain circumstances. If you exercise this right, we may, apart from storing the data, only process it with your consent, for the establishment, exercise or defence of legal claims, to protect another individual, or for reasons of important public interest.

Right to Data Portability

Article 20 allows you to obtain and reuse your personal data across different services. You can request your data in a structured, commonly used, and machine-readable format, and have it transmitted from one data controller to another without hindrance.

Right to Object

Under Article 21, you have the right to object to the processing of your personal data. you have the right to object, to the processing of your personal data where it is based on Article 6(1)(e) or (f), including profiling based on those provisions.

Right to Withdraw Consent

When our processing of your personal data is based on your consent, you have the right to withdraw your consent at any time.

5.2 If you believe that our processing of your personal data infringes applicable data protection law, you may lodge a complaint with the Danish Data Protection Agency (Datatilsynet). Contact details are available at www.datatilsynet.dk.

5.3 You can read more about your rights in the Danish Data Protection Agency's guide on the rights of data subjects, which can be found at www.datatilsynet.dk.

6. Lawful Basis for Processing Personal Data

6.1 The Company only processes personal data where a lawful basis exists, and ensures that the data is adequate, relevant and limited to what is necessary in relation to the purposes for which it is processed.

6.2 The Company communicates clearly and transparently with data subjects regarding the purpose and scope of processing. Personal data is processed in a manner that ensures appropriate security, including protection against unauthorised access, loss, or destruction.

6.3 The Company may process personal data based on one or more of the following legal grounds, in accordance with Article 6 of the General Data Protection Regulation (GDPR):

Consent

Where the data subject has given clear, informed, and voluntary consent to the processing.

Contractual necessity

Where processing is required to perform a contract with the data subject or to take steps at the data subject's request prior to entering a contract.

Legal obligation

Where processing is necessary for the Company to comply with a legal obligation.

Legitimate interest

Where processing is necessary for purposes that are in the Company's legitimate interest, provided such interests are not overridden by the interests or fundamental rights and freedoms of the data subject

Vital interests

In rare cases, where processing is necessary to protect the vital interests of the data subject or another person.

Public interest or official authority

Where processing is necessary for the performance of a task carried out in the public interest or in the exercise of official authority vested in the Company.

7. Datatypes

7.1 The Company may collect and process the following categories of Personal Data, depending on the nature of the relationship and interaction with the data subject:

Identification data

Includes e-mail address, telephone number and similar information.

Organisational Information

Includes company name, business address, registration number, department contacts, telephone numbers, and official email addresses, used for onboarding, correspondence, and compliance purposes.

Employment Details

Includes CV, job title, employer history, references, tax details, social security / national insurance number, and bank account information, typically collected for recruitment, employment, or onboarding of company representatives.

Identity Verification Data

Includes contact data and personal identification documents required for contractual and compliance purposes. May cover date of birth, passport number, driver's license, national ID, and verification data related to company directors or shareholders.

Financial Information

Includes account number, BACS, SWIFT, IBAN, credit/debit card data, invoicing records, purchase orders, and payment amounts, used to process financial transactions and maintain accounting records.

Transactional Details

Covers data related to specific transactions, such as timestamps, transaction references, contact and account data, payment records, consent logs, customer support actions, and related metadata.

Cookies

When you visit our website, we use cookies to ensure the website functions properly. Please see our separate *cookie policy* for detailed information about the types of cookies used, their purposes, storage periods, and your options for granting or withdrawing consent.

User Activity Data

Includes logs of user interactions such as website visits, email opens, seminar registrations, report downloads, and related behavioural metrics.

Correspondence and communication records

This includes emails, meeting notes, and other communication logs.

Preferences and interests related to risk management solutions

This includes data provided directly by you or inferred from interactions.

Digital identifiers and usage of data

This includes IP address, MAC address, browser type and version, device information, operating system, location data, time zone, and website usage behaviour.

7.2 The Company may collect and process the following categories of Sensitive Personal Data, depending on the nature of the relationship and interaction with the data subject. Processing of such data is subject to strict legal safeguards and is only carried out where necessary and legally justified:

Health Information

Includes information about physical or mental health, disabilities, or medical conditions, which may be collected in limited cases, such as to accommodate accessibility needs during events or to fulfil obligations related to employee health and safety.

Political beliefs

Includes information relating to political opinions or affiliations, only collected where explicitly provided by the data subject and relevant to specific professional or public engagements. Such data is not actively sought by the Company.

Criminal Offenses or Convictions

Includes data related to criminal records or proceedings, which may be collected where legally required or permitted, for example during due diligence processes or when fulfilling regulatory compliance obligations.

7.3 To protect both your and our interests from potential fraudulent or malicious activities, we may request additional identification methods to verify that we are dealing with the lawful data subject.

7.4 We do not knowingly engage in business interactions or store information about children.

8. Use of Personal Data

8.1 The Company uses personal data solely for specified, explicit, and legitimate purposes, based on one or more of the legal grounds outlined cf. Section 5.1. Personal data may be used for the following purposes:

Engagement of Service

Personal data is processed to provide, maintain, and improve the Company's services, including onboarding, contract administration, support, and delivery of relevant updates or communications. This involves the processing of identification data, contact details, and transactional records necessary to fulfil obligations under agreements entered with clients, partners, employees, or other stakeholders. Where applicable, data may also be shared with regulators or partners in connection with service delivery or compliance.

Security and Privacy

The Company processes personal data to ensure system integrity, prevent unauthorized access, and maintain appropriate technical and organisational security measures. This includes user authentication, device verification, access control, logging of activity, and fraud prevention. All such processing is conducted in accordance with legal requirements and internal security protocols to safeguard confidentiality and protect the interests of data subjects.

Legal Requirements

The Company processes personal data to comply with applicable laws, regulatory obligations, and judicial or administrative requests. This includes the documentation of transactions, fulfilment of anti-money laundering and financial supervision obligations, and response to data subject requests under the GDPR. The Company may also use personal data to assess and manage risks, investigate incidents, and notify authorities and data subjects in case of personal data breaches.

Transfers and Change of Control

Where necessary, personal data may be transferred to third parties, including group companies, service providers, or legal successors, in accordance with applicable legislation. This includes cross-border transfers subject to appropriate safeguards. In connection with mergers, acquisitions, restructurings, or other forms of corporate transformation, personal data may be disclosed to or acquired by the relevant parties, always ensuring that confidentiality, integrity, and lawfulness are preserved.

Direct Marketing

Personal data may be used to provide information about the Company's services, market insights, and relevant events, either on the basis of legitimate interest or explicit consent, depending on the nature of the communication. This includes sending newsletters, promotional material, or tailored content based on individual preferences or professional interests. The Company respects all opt-out requests and ensures that data subjects can withdraw consent or object to such processing at any time.

Service Improvement and Analytics

The Company may use personal data to analyse performance, identify usage patterns, and enhance the relevance and efficiency of its services. This includes evaluating website traffic, email engagement, support interactions, and feedback submissions. All such analysis is conducted in aggregated or pseudonymised form where appropriate and in accordance with applicable data protection principles.

Compliance Monitoring and Record-Keeping

The Company maintains records of processing activities, consent logs, data subject requests, and incident reports to demonstrate accountability and compliance with the GDPR. These records support internal audits, regulatory inspections, and risk assessments and are stored in accordance with statutory retention requirements.

9. Data Retention

9.1 Personal data is stored securely and only for as long as necessary to fulfil the purposes for which it was collected, or to comply with legal, regulatory, or contractual obligations. The Company applies appropriate technical and organizational measures to protect data against unauthorized access, alteration, disclosure, or destruction. When personal data is no longer required, it is securely deleted or anonymized in accordance with the Company's data retention policy. Retention periods may vary depending on the nature of the data and the applicable legal requirements.

Customer Data

Retained for up to 5 years after the end of the customer relationship for documentation and legal purposes.

Employee Data

Retained for up to 5 years after the end of employment to address potential legal claims.

General Market Information Subscriptions

Retained for up to 2 years when a data subject unsubscribes from the newsletter in accordance with the Consumer Ombudsman's spam guidelines cf. Section 11.3.

Transaction and Accounting Data

Retained for a minimum of 5 years after the end of the financial year in accordance with the Danish Bookkeeping Act.

Job Applications

If you submit an unsolicited application, we will promptly assess its relevance and delete your data if there is no match. If you apply for a specific job posting, your application will be deleted if you are not hired, and immediately after the right candidate has been selected. If you enter a recruitment process and/or are employed, you will receive separate information about how we process your personal data in that context.

10. Shared Data

10.1 The Company may share personal data with third parties where necessary to fulfil the purposes described in the Policy and where such sharing complies with applicable data protection legislation. Data is only shared with trusted entities under appropriate legal, technical, and organisational safeguards to ensure the continued protection of personal data cf. Section 11.

Service Providers

Personal data may be shared with service providers acting as data processors, who assist in the provision of IT infrastructure, cloud storage, email systems, CRM platforms, compliance tools, or other services essential to the Company's operations.

Regulatory Authorities

Where required, personal data may also be shared with regulatory authorities, courts, law enforcement agencies, or other public bodies, for purposes including compliance with legal obligations, supervision, fraud detection, dispute resolution, or the protection of the rights and safety of individuals.

Professional Advisers

The Company may further share data with professional advisers such as auditors, lawyers, or financial consultants, where such sharing is necessary to fulfil contractual or legal obligations, defend legal claims, or obtain expert advice.

Mergers, Acquisitions, Restructurings or Transfers of Business Activities

In the context of mergers, acquisitions, restructurings, or transfers of business activities, personal data may be disclosed to potential or actual acquiring entities, subject to confidentiality obligations and relevant safeguards.

Transfers to Third Countries

Our standard practice is to use data processors located within the EU/EEA or who store data within the EU/EEA. In certain cases, we may use data processors outside the EU/EEA, provided that they can offer an adequate level of protection for your personal data.

10.2 Personal data is not sold, rented, or otherwise disclosed to third parties for commercial purposes unrelated to the Company's services or legitimate interests, unless the data subject has provided explicit consent for such disclosure.

11. Data Security

11.1 At ERM, we take the protection of personal data seriously and have implemented robust technical, procedural, and organisational measures to ensure its security. Our approach is designed to protect personal information from unauthorised access, disclosure, alteration, or destruction.

Technical Measures

We utilise advanced encryption technologies to protect personal data both at rest and in transit. Additionally, all administrative accounts are secured with multi-factor authentication to ensure that only authorised personnel have access to sensitive data. Access to personal data is strictly limited using Role-Based Access Control (RBAC) and is granted on a "need-to-have" basis, ensuring that only those who require access for legitimate business purposes can obtain it.

Organisational Measures

We ensure that all employees are educated about the importance of personal data protection and are aware of their responsibilities in handling such information. Staff members are also instructed on how to respond to data protection requests and who to contact for assistance. We regularly review and update our internal training to reflect evolving data security best practices.

11.2 To ensure a high level of data protection, we conduct regular risk assessments of our personal data processing activities. Based on these assessments, we implement and adjust technical and organisational measures to maintain an appropriate level of security. One of our key organisational safeguards is employee awareness. All staff members receive continuous GDPR awareness training and participate in dedicated data protection courses. Additionally, we regularly review and discuss our internal GDPR procedures with employees to ensure they are equipped to handle personal data responsibly and in compliance with applicable regulations.

11.3 While we take every reasonable step to protect our systems and the data within them, no system is completely immune to vulnerabilities. In the event of a security breach, whether caused by malicious intent or human error, we have implemented a breach notification procedure that complies with data protection regulations. Upon discovery of a breach, we initiate a breach log and conduct a thorough investigation to assess the scope and impact of the incident. We then take immediate steps to contain and stop the breach. The potential impact on data subjects is evaluated, and where required by law, affected individuals and regulatory authorities are notified within the prescribed timeframes. If necessary, we use data forensics to trace the cause of the breach and ensure that all corrective actions are taken to mitigate further risks.