GDPR POLICY

for

AK Jensen Investment Management ("AKJIM")

AK Jensen Limited ("AKJL")

AK Jensen Norway Limited ("AKJNO")

AKU

Table of Contents

1. Introduction

The General Data Protection Regulation (GDPR) is the primary legislative framework governing data protection in the European Economic Area (EEA) and the UK. It standardizes regulations to safeguard individuals' personal data and enforce accountability on data controllers and processors. The UK GDPR, adapted post-Brexit, continues to align with EU GDPR requirements but may evolve separately in the future.

AK Jensen entities, including AK Jensen Investment Management ("AKJIM"), AK Jensen Limited ("AKJL"), AK Jensen Norway Limited ("AKJNO"), and AK Jensen Crypto Plc. ("AKJC"), are committed to full compliance with GDPR regulations to ensure transparency, security, and accountability in handling personal data.

2. Regulatory Framework

The European Union (EU) General Data Protection Regulation (GDPR) applies uniformly across all EU member states and sets stringent guidelines for data processing, security, and individual rights. It requires organizations to adopt comprehensive compliance measures, including transparency, accountability, and data subject rights enforcement. The regulation also establishes the European Data Protection Board (EDPB) to ensure consistency in application and enforcement across the EU.

In Norway, the GDPR is implemented through the Personal Data Act (Personopplysningsloven), ensuring alignment with EU regulations. The Norwegian Data Protection Authority (Datatilsynet) oversees compliance and enforcement, providing guidance and investigating breaches. Norway, as a member of the European Economic Area (EEA), follows GDPR principles while incorporating additional national provisions to address local data protection concerns and enforcement mechanisms.

The United Kingdom (UK) retained the GDPR within its domestic legislation following Brexit, now referred to as the UK GDPR, supplemented by the Data Protection Act 2018. The UK Information Commissioner's Office (ICO) enforces compliance and provides guidance on evolving data protection standards. Future UK-specific amendments may introduce divergences from the EU GDPR, particularly concerning international data transfers and regulatory enforcement mechanisms.

3. Purpose

In essence, the purpose of the GDPR is twofold: first, to safeguard the fundamental rights and freedoms of individuals, specifically their right to the protection of personal data, and second, to establish a unified data security law across the UK and all EU member states. By creating a standardized approach to data protection, GDPR eliminates the need for individual member states to develop their own data protection laws, ensuring consistency and harmonization throughout the EU and UK.

The regulation empowers European and UK privacy regulators with increased authority, enhancing their ability to enforce compliance effectively. These regulators now have the power to impose significant fines and sanctions for non-compliance, reinforcing the necessity for businesses to adopt stringent data protection practices. AKJ acknowledges these regulatory developments and remains committed to maintaining a strong data protection framework that aligns with the evolving compliance landscape.

Moreover, GDPR's stringent requirements highlight the importance of proactive data security measures. AKJ emphasizes the need for continuous employee education, robust security protocols, and clear data governance policies to mitigate risks associated with data breaches. All AKJ employees must fully understand their responsibilities in protecting personal data and ensuring compliance with GDPR principles. This commitment helps protect the privacy rights of individuals while fostering trust between AKJ and its stakeholders.

4. Scope

Within the EEA, this policy applies to all AKJ entities processing personal data in compliance with the EU GDPR. It governs data collection, storage, transfer, and processing activities concerning individuals within the EU. Any data transfers outside the EEA adhere to regulatory mechanisms such as adequacy decisions, standard contractual clauses, or binding corporate rules to maintain high data protection standards.

In the UK, this policy follows the UK GDPR framework and applies to all personal data processing activities conducted by AKJ entities. The UK Information Commissioner's Office (ICO) enforces compliance, and data protection measures align with both the UK GDPR and the Data Protection Act 2018. Future regulatory changes may impact UK-specific data protection requirements, necessitating periodic policy updates.

5. Data Protection Principles

AKJ follows the core GDPR principles: lawfulness, fairness, and transparency; purpose limitation; data minimization; accuracy; storage limitation; integrity and confidentiality; and accountability. Compliance with these principles is mandatory across all AKJ operations.

To ensure full compliance with GDPR, AKJ implements strong data protection measures. Regular training programs are provided to all employees to enhance their awareness of data protection responsibilities and best practices. This cultivates a culture of privacy and security within the organization, ensuring that personal data is handled in accordance with regulatory requirements.

Incident reporting is a critical component of AKJ's data protection framework. Any incidents involving personal data are logged and registered in the incident register. The Risk team oversees the management of incident reporting, ensuring that vulnerabilities are promptly identified, rectified, and mitigated to prevent future occurrences.

Privacy by design and default is integrated into all AKJ projects and initiatives. From IT system development to data sharing policies, privacy considerations are embedded at the core of all

operations. This proactive approach ensures that data protection is a key priority throughout the entire lifecycle of any project.

AKJ employs a structured defense mechanism, beginning with first-line monitoring. Designated Data Protection Officers (DPOs) are responsible for ensuring compliance with GDPR within key business areas, particularly HR and Fund Coordination. These roles ensure that both employee and client data are managed securely and in full compliance with regulatory obligations.

In addition to first-line monitoring, AKJ's Compliance team serves as the second line of defense. They assess the efficacy of data protection measures, review security controls, and monitor access logs to ensure ongoing compliance with GDPR requirements.

Data minimization is a fundamental principle at AKJ. Personal data is collected, processed, and retained only to the extent necessary for achieving specified purposes. Regular audits and reviews are conducted to identify and securely dispose of any redundant or obsolete data, reducing the risk of unauthorized access or breaches.

6. Legal Basis for Data Processing

Under GDPR, personal data can only be processed if a lawful basis applies. AKJ adheres to the six legal bases defined in the regulation. The first basis is obtaining explicit consent from the data subject, ensuring they have given clear permission for their data to be processed for a specific purpose. The second basis is the necessity of processing for the performance of a contract, where personal data is required to fulfil contractual obligations with a data subject.

The third legal basis is compliance with legal obligations, where processing is required to meet statutory or regulatory requirements. The fourth basis involves protecting the vital interests of a data subject or another individual, typically in life-threatening situations. The fifth basis allows processing when it is necessary for carrying out tasks in the public interest or exercising official authority granted to AKJ.

Lastly, AKJ may process personal data under the legitimate interests basis, provided such interests are not overridden by the rights and freedoms of the data subject. This is applicable where data usage is expected, necessary, and has minimal privacy impact. AKJ ensures that all personal data processing aligns with at least one of these legal bases, safeguarding compliance with GDPR and maintaining transparency in its operations.

7. Rights of Data Subjects

AKJ is committed to upholding the rights of data subjects as outlined in the General Data Protection Regulation (GDPR). Individuals are entitled to the following rights concerning their personal data:

1. **Right of Access:** Data subjects can request confirmation as to whether their personal data is being processed and, if so, access that data along with supplementary information.

2. **Right to Rectification:** Individuals have the right to request the correction of inaccurate personal data and to have incomplete data completed.
3. **Right to Erasure (Right to be Forgotten):** Under certain circumstances, data subjects can request the deletion of their personal data, particularly if the data is no longer necessary for the purposes for which it was collected or processed.
4. **Right to Restrict Processing:** Individuals can request the limitation of their personal data processing under specific conditions, such as when contesting the accuracy of the data or objecting to its processing.
5. **Right to Data Portability:** Data subjects have the right to receive their personal data in a structured, commonly used, and machine-readable format and to transmit that data to another controller without hindrance.
6. **Right to Object:** Individuals can object to the processing of their personal data based on legitimate interests or for direct marketing purposes. In accordance with Article 21 of the GDPR, AKJ will cease processing upon objection unless there are compelling legitimate grounds for the processing that override the interests, rights, and freedoms of the data subject.
7. **Rights Related to Automated Decision-Making and Profiling:** Data subjects have the right not to be subject to decisions based solely on automated processing, including profiling, which produces legal effects concerning them or similarly significantly affects them.

To facilitate the exercise of these rights, AKJ has established procedures to respond promptly to data subject requests. Requests can be submitted via email to compliance@akj.com. AKJ will address all inquiries in accordance with GDPR requirements and applicable local regulations.

Furthermore, AKJ ensures that personnel involved in the processing of personal data receive comprehensive training on GDPR requirements and the importance of maintaining confidentiality. This commitment to education underscores AKJ's dedication to safeguarding personal data and upholding the principles of data privacy.

In alignment with guidance from regulatory authorities, including the Financial Conduct Authority (FCA) and the Information Commissioner's Office (ICO), AKJ acknowledges that GDPR does not impose requirements incompatible with existing financial regulations. Compliance with GDPR complements AKJ's obligations under the FCA's Senior Management Arrangements, Systems and Controls (SYSC) framework, ensuring a holistic approach to data protection and regulatory adherence.

8. Data Protection Measures

To ensure compliance with GDPR and protect the privacy rights of individuals, AKJ has implemented comprehensive data protection measures. These measures include:

- **Employee Training and Awareness:** All personnel handling personal data receive regular training on GDPR compliance, security best practices, and data confidentiality.

- **Incident Management Procedures:** A well-defined protocol for identifying, reporting, and mitigating data security incidents is in place to minimize potential breaches.
- **Access Controls and Encryption:** Only authorized personnel can access personal data, and encryption methods are used to protect sensitive information from unauthorized access or interception.
- **Third-Party Risk Management:** Vendors and partners who process personal data on behalf of AKJ must comply with GDPR and adhere to stringent data security measures.

9. Data Retention and Deletion

AKJ retains personal data only for as long as necessary to fulfil legal, regulatory, and operational requirements. Data is categorized based on its nature and processing purpose to determine an appropriate retention period. Once data is no longer required, it is securely deleted or anonymized to prevent unauthorized access or misuse.

For the EEA, retention policies align with GDPR standards, ensuring that personal data is not kept longer than necessary unless required for legal obligations or legitimate interests. Regular audits are conducted to review data retention practices, ensuring compliance with the principle of data minimization.

In the UK, AKJ follows the UK GDPR and the Data Protection Act 2018, which provides similar requirements. Records necessary for financial transactions, compliance reporting, or regulatory oversight may be retained longer based on FCA guidelines. Any retention beyond the initial purpose must have a clearly documented legal basis.

10. Transfer of Personal Data

AKJ ensures that any transfer of personal data outside the European Economic Area (EEA) and the United Kingdom (UK) complies with the respective data protection regulations to maintain a high level of protection.

Transfers from the EEA:

Under the General Data Protection Regulation (GDPR), personal data may only be transferred to countries outside the EEA if specific conditions are met. These include:

Adequacy Decisions: Transfers can occur to countries that the European Commission has deemed to provide an adequate level of data protection.

Appropriate Safeguards: In the absence of an adequacy decision, transfers are permissible if appropriate safeguards are in place, such as Standard Contractual Clauses (SCCs) or Binding Corporate Rules (BCRs).

Transfers from the UK:

Following Brexit, the UK has established its own framework for international data transfers under the UK GDPR. The UK's Information Commissioner's Office (ICO) has introduced the International Data Transfer Agreement (IDTA) and an addendum to the new EU SCCs, which became effective on 21 March 2022. These tools facilitate lawful data transfers from the UK to countries without an adequacy decision.

AKJ's Commitment:

AKJ is committed to implementing appropriate safeguards for international data transfers, including: 1. Conducting Transfer Impact Assessments to evaluate the legal environment of the recipient country. 2. Ensuring that data subjects' rights and effective legal remedies are available in the event of a breach.

11. Breach Notification and Incident Reporting

AKJ has a structured incident response plan to detect, assess, and mitigate data breaches. Any data breach that poses a risk to individuals' rights is reported to the relevant supervisory authority within 72 hours. If the breach is likely to result in significant harm, affected individuals are informed promptly.

All incidents are documented, including details of the breach, risk assessment, and remedial actions taken. AKJ regularly reviews security protocols, conducts employee training, and enforces strict access controls to prevent breaches. These measures ensure compliance with GDPR and UK GDPR while protecting data integrity and confidentiality.

12. Data Protection by Design and Default

AKJ integrates privacy and security into all business operations from the outset, ensuring compliance with GDPR's principles of data protection by design and default. This approach mandates that data protection measures are embedded in systems and processes from their initial development stages.

Regular risk assessments and Data Protection Impact Assessments (DPIAs) are conducted to proactively identify and mitigate risks associated with personal data processing. AKJ enforces strict access controls, encryption, and pseudonymization techniques to enhance data security. Employees receive ongoing training to uphold best practices in privacy and security. By embedding these measures, AKJ ensures personal data is processed lawfully, fairly, and transparently while maintaining compliance with evolving data protection regulations.

13. Data Protection Officer

AKJ is not required to appoint a Data Protection Officer (DPO). As such, Compliance acts as the primary point of contact for data subjects and regulatory authorities, managing queries, handling data access requests, and ensuring GDPR compliance.

14. Complaints and Queries

Filing a complaint under the GDPR allows individuals to raise concerns or report violations regarding the processing of their personal data. Data subjects have the right to file a complaint with AKJ regarding the use of their Personal Data by contacting AKJ via email at compliance@akj.com.

Alternatively, they may choose to approach the relevant supervisory authority, which, in the UK, would be the Information Commissioner's Office (https://ico.org.uk) and in Norway the Norwegian Data Protection Authority (https://www.datatilsynet.no), or the equivalent national regulator in any EU country, as mandated by the GDPR.

AKJ is committed to addressing complaints promptly and transparently. All complaints will be assessed thoroughly, and where necessary, corrective actions will be implemented to ensure compliance with data protection regulations. Data subjects will be kept informed throughout the complaint resolution process.

15. Document History

Version	Changes	Date
1.0	Previous policy revision aligning with emerging data protection requirements.	December 2023
1.1	Revision incorporating GDPR updates post-2023.	January 2025
1.2	Annual Revision. Minor updates.	January 2026

Document Owner: Head of Compliance for the respective AKJ Entity.