E|C|M
fund management

September 2025

Contents

1. Policy Statement 4
2. Purpose and Scope 4
3. Objectives 4
4. Legal Framework 5
5. GDPR Principles 5
6. Governance 6
7. Privacy by Design and Default 6
8. Legal Basis for Processing 7
9. Processing Special Category Data 7
10. Records of Processing Activities (RoPA) 7
11. Third-Party Processors 8
12. Data Retention and Disposal 8
13. Information Provided to Data Subjects (Privacy Statement) 8
14. Data Subject Rights Procedures 9
14.1 Right of Access (SARs) 9
14.2 Right to Data Portability 10
14.3 Right to Erasure ("Right to be Forgotten") 10
14.4 Right to Rectification 10
14.5 Right to Restriction 10
14.6 Right to Object 10
15. Consent 10
15.1 Consent Collection 10
15.2 Withdrawal of Consent 10
15.3 Child Data 11
16. Transfers & Data Sharing 11
16.1 Data Sharing 11
16.2 Transfers Within the EEA 11
16.3 Transfers Outside the EEA 11
17. Audits & Monitoring 11
18. Training 11
19. Personal Data Breach Notification 12
19.1 Internal Reporting: 12

19.2 Breach Notification to Supervisory Authority (Article 33): 12
19.3 Breach Notification to Data Subject (Article 34): 12
20. Data Protection Impact Assessment (DPIA) Procedure 13
21. Prior Consultation (Article 36 GDPR) 13
22. Review of Policy 13

1. Policy Statement

ECM Partners Cyprus Limited. hereafter referred to as the "the Company" or "ECM", collects and processes personal data to carry out its business functions, deliver services effectively, and meet its legal and regulatory obligations. Personal data may be collected from employees, customers, suppliers, and third parties, and includes information such as identification details, contact data, financial information, and other sensitive categories of data.

The Company complies with the General Data Protection Regulation (Regulation (EU) 2016/679), Law 125(I)/2018 of the Republic of Cyprus, and any other applicable data protection laws and codes of conduct.

The Company has established policies, procedures and controls to ensure compliance, including staff training, documented procedures, internal audits, and impact assessments. Maintaining the confidentiality, integrity, and availability of personal and special category data is a top priority. The Company adopts a "Privacy by Design and by Default" approach, embedding data protection principles in systems, processes, and decision-making.

Commitment to this Policy extends to senior management and all employees and compliance is mandatory for all staff, contractors and relevant third parties.

2. Purpose and Scope

This Policy ensures the Company meets its obligations under data protection laws and upholds the rights of individuals. It promotes accountability and governance by implementing effective measures to minimize the risk of breaches and safeguard personal data.

The Policy serves as a reference for all employees and third parties on responsibilities for handling personal data and responding to data subject requests.

It applies to all personnel, including permanent, temporary, and fixed-term staff, contractors, consultants and partners. Non-compliance may result in disciplinary or contractual action.

3. Objectives

The Company ensures that:

- Individuals' rights regarding their personal data are protected.
- Data protection policies, procedures, audits and training are maintained.
- All business practices and processes comply with data protection laws.
- Personal data is processed only when lawfulness is established.
- Special category data is processed only under GDPR conditions.
- Consent is obtained, recorded and demonstrable.

- Employees receive appropriate training and understand their obligations.
- Individuals feel secure in providing personal data to the Company.
- Monitoring, reviews and improvements are ongoing to address risks and non-compliance.
- Complaints and breaches are handled through documented procedures.
- A Data Protection Officer (DPO) oversees compliance under GDPR Article 37.
- Personal data is stored and destroyed in line with legal retention schedules.
- Information provided to data subjects is concise, clear and transparent.
- Records of processing activities (Article 30), (RoPA) are maintained and yearly reviewed.
- Appropriate technical and organizational security measures are in place to safeguard private and sensitive personal data, ensure their lawful processing and retention, while effectively implementing the established data subject rights.

4. Legal Framework

This Policy is based on:

- GDPR (EU 2016/679), applicable from 25 May 2018.
- Law 125(I)/2018 of the Republic of Cyprus.
- Guidance from the European Data Protection Board and the Cyprus Commissioner of Personal Data Protection.

The Company, as a data controller, is obligated to comply fully with these laws in processing personal data.

5. GDPR Principles

The Company applies the seven GDPR principles:

1. **Lawfulness, Fairness, and Transparency:** Personal data shall be processed lawfully, fairly, and in a transparent manner in relation to the data subject. Processing is based on one of the legal bases defined in Article 6 GDPR, and the data subject is informed about how and why their data is used.

2. **Purpose Limitation:** Personal data shall be collected for specified, explicit, and legitimate purposes and not further processed in a manner incompatible with those purposes. Any new processing requires a compatible purpose or the data subject's consent.

3. **Data Minimisation:** Personal data shall be adequate, relevant, and limited to what is necessary in relation to the purposes for which it is processed. The Company ensures only the minimum required data is collected and processed.

4. **Accuracy:** Personal data shall be accurate and, where necessary, kept up to date. Every reasonable step shall be taken to rectify or erase inaccurate data without delay.

5. **Storage Limitation:** Personal data shall be kept in a form that permits identification of data subjects for no longer than necessary for the purposes for which it is processed. Retention periods are defined, monitored, and enforced according to regulatory and business requirements.

6. **Integrity and Confidentiality:** Personal data shall be processed in a manner that ensures appropriate security, including protection against unauthorized or unlawful processing, accidental loss, destruction, or damage. Appropriate technical and organizational measures are applied to maintain data integrity and confidentiality.

7. **Accountability:** The Company is responsible for demonstrating compliance with all GDPR principles. Policies, procedures, training, audits, and records of processing activities are maintained to ensure and demonstrate GDPR compliance.

6. Governance

- Board of Directors / CEO: Ensure oversight, resources and approval of policies.
- HR Department: Ensure onboarding includes privacy notices and staff awareness.
- CTO/ Designated IT Officer and Cybersecurity Committee: Provide technical input, support the DPO and secure electronic data
- Compliance Officer/ DPO: Ensure compliance, advise management, monitor processing, liaise with authorities and maintain independence.
- Employees: Follow training, protect customer data and escalate concerns.

7. Privacy by Design and Default

The Company integrates data protection into all processes, systems and activities from the outset. This includes:

- Data Minimization: Collect only data necessary for lawful purposes.
- Encryption: Apply encryption for transfers and sensitive data.
- Restriction: Apply strict access controls and limit processing to authorised purposes.

8. Legal Basis for Processing

Personal data is processed under GDPR Article 6, including consent, contractual necessity, legal obligations, vital interests, public interest, or legitimate interests.

Special category data is processed under GDPR Article 9, only under defined legal bases (e.g., consent, legal obligations, public health, research, or substantial public interest).

9. Processing Special Category Data

The Company processes personal information classified as special category data or relating to criminal convictions only when one or more of the following legal bases apply:

- The data subject has explicitly consented to the processing of their personal data.
- Processing is necessary for fulfilling obligations or exercising specific rights of the controller or the data subject under employment, social security, or social protection law.
- Processing is necessary to protect vital interests of the data subject or another person when the data subject is physically or legally unable to give consent.
- Processing involves personal data that the data subject has manifestly made public.
- Processing is required for the establishment, exercise, or defense of legal claims, or when courts are acting in their judicial capacity.
- Processing is necessary for substantial public interest reasons.
- Processing is necessary for preventive or occupational medicine, assessment of employee working capacity, medical diagnosis, provision of health or social care, treatment, or management of health or social care systems and services.
- Processing is necessary for public health purposes in the interest of society.
- Processing is necessary for archiving in the public interest, or for scientific, historical, or statistical research, in accordance with Article 89(1) GDPR.

10. Records of Processing Activities (RoPA)

The Company maintains records of all processing activities, in compliance with Article 30 GDPR, including:

- The purposes of each processing activity
- The categories of personal data processed
- Retention periods for the data
- Recipients of the data

- Any data transfers, including transfers to third countries
- Security measures implemented to protect the data

These records are kept up to date and available for review by the Data Protection Officer (DPO) and supervisory authorities as required.

11. Third-Party Processors

The Company conducts due diligence before engaging processors, ensures data processing agreements are in place and monitors compliance. Processors must follow the Company's instructions, maintain security and support data subject rights.

12. Data Retention and Disposal

- Data is retained only as long as necessary for business, legal, or regulatory purposes.
- Customer data is generally retained for up to 10 years post-relationship, subject to exceptions (e.g., litigation).
- Prospective client data is retained for 6 months post-rejection/ withdrawal.
- Disposal is secure (shredding, deletion, wiping of IT assets).

13. Information Provided to Data Subjects (Privacy Statement)

13.1 Privacy Statement Information (Direct Collection)

- Whenever personal data is collected directly (e.g., consent forms, employees, website forms), the Company provides clear information including:
    - Identity and contact of the Company and DPO
    - Purpose and legal basis of processing
    - Details of legitimate interests (if Article 6(1)(f) applies)
    - Recipients of personal data
    - International transfers
    - Storage period
    - Rights of access, rectification, erasure, restriction, objection and data portability
    - Right to withdraw consent
    - Right to lodge complaints

  - Whether data provision is mandatory or contractual
  - Automated decision-making / profiling
- Privacy statement is available online: ecommbanx.com/privacy-statement

13.2 Indirect Collection

- When data is obtained indirectly (not directly from the subject):
  - Must inform the data subject within 30 days
  - Must include data source, categories and use for communication or third-party disclosure
  - Exceptions exist (information already known, disproportionate effort, legal/professional secrecy)

13.3 Employee Personal Data

- Employees are informed of how their data is processed through privacy statements and training.

14. Data Subject Rights Procedures

Data subjects have rights under GDPR:

- Access, rectification, erasure, restriction, objection, data portability
- Prevent processing causing distress or for marketing
- Seeking compensation for GDPR violations
- Object to automated profiling
- Request supervisory authority involvement

Also:

- Requests can be submitted via email, post, or phone to the DPO
- DPO verifies identity and processes requests with support from IT/ISO teams
- Standard response time: 1 month; extendable to 3 months for complex cases (per GDPR Article 12(3))
- All requests logged for record-keeping

14.1 Right of Access (SARs)

- Subject completes a form; DPO reviews and verifies identity

- Response in writing within 30 days
- Provided free of charge (fees for additional copies)

14.2 Right to Data Portability

- Data provided in a structured, machine-readable format
- DPO handles verification and transfer to third-party if requested

14.3 Right to Erasure ("Right to be Forgotten")

- Data erased if no longer necessary, consent withdrawn, or unlawful processing
- Exceptions: public interest, legal claims, legal/regulatory requirements
- DPO oversees deletion and informs the subject

14.4 Right to Rectification

- Incorrect or outdated data corrected in all systems, including backups and third-party recipients
- DPO logs and communicates completion

14.5 Right to Restriction

- Applied when accuracy contested, unlawful processing, legal claims, or objection under Article 21(1)
- DPO ensures only consented or legally required processing continues

14.6 Right to Object

- Object to processing based on official authority or legitimate interests
- DPO halts processing if objection is valid

15. Consent

15.1 Consent Collection

- Consent must be freely given, specific, informed, unambiguous and distinguishable from other matters
- Consent invalid if forced or under pressure
- Data subject can withdraw consent at any time

15.2 Withdrawal of Consent

- Requests accepted in writing; processing stopped per purpose
- Relevant departments informed by DPO

15.3 Child Data

- Services not provided to children directly; parental/guardian consent required for processing children's data

16. Transfers & Data Sharing

16.1 Data Sharing

- Personal data shared only with authorized third parties, under DPO approval
- Employees must exercise caution and ensure relevance and necessity

16.2 Transfers Within the EEA

- Treated as lower risk due to GDPR coverage
- Data encrypted and minimized

16.3 Transfers Outside the EEA

- Only lawful if safeguards or exceptions exist:
    - Adequacy decision by EC
    - Controller assessment (nature, purpose, destination, local laws, security)
    - Standard Contractual Clauses (SCC)
    - Exceptions: explicit consent, contract necessity, public interest, legal claims, vital interests

17. Audits & Monitoring

- Regular audits to ensure compliance and effectiveness of controls
- DPO responsible for assessing, testing and improving processes
- Focus on minimizing risks, preventing breaches and evaluating new technologies

18. Training

- All employees with responsibilities related to personal data receive training and ongoing assessments.

- DPO ensures:
    - New hires understand GDPR and data protection responsibilities.
    - Staff are updated on personal data issues.
    - Security requirements related to data protection are communicated.
- Management supports awareness programs and allocates resources.

19. Personal Data Breach Notification

19.1 Internal Reporting:

- Any employee aware of a breach completes a Data Breach Notification Form and submits it to the DPO.

19.2 Breach Notification to Supervisory Authority (Article 33):

- Notify within **72 hours** if there's likely risk to data subjects.
- DPO submits details to the Cypriot Commissioner via email: commissioner@dataprotection.gov.cy.
- Partial reporting allowed if all information is not yet available.
- Required information:
    - Nature of the breach
    - Categories and number of data subjects/records affected
    - DPO contact details
    - Consequences and mitigation measures
- Confirmation of receipt is obtained in writing.

19.3 Breach Notification to Data Subject (Article 34):

- Notify affected data subjects without undue delay, especially for high-risk breaches.
- For large volumes, public communication may be used.
- Must be in clear, plain language.
- If supervisory authority identifies high-risk breach and no notification yet, notify within 48 hours.
- Document facts, impact and remedial actions.

20. Data Protection Impact Assessment (DPIA) Procedure

- DPIA is required for processing operations likely to result in high risk to individuals' rights and freedoms.
- DPO is responsible for:
    - Assessing need for DPIA
    - Overseeing and consulting on DPIA
    - Ensuring mitigation measures are implemented
- Departments are responsible for implementing risk solutions.
- DPIA Guidelines are provided by the Compliance Unit.

21. Prior Consultation (Article 36 GDPR)

- Provide supervisory authority with:
    - Company's role as controller and other processors/joint controllers
    - Purpose of processing
    - Existing measures/controls
    - DPO contact details
    - Copy of DPIA
    - Any other requested information

22. Review of Policy

- Reviewed annually or whenever significant changes occur.
- DPO responsible for review and updates.