

## GDPR COMPLIANCE STATEMENT

Future Data Software Online Ltd

Company No.: 16728072 – Registered in England & Wales

Registered Office: 27 Old Gloucester Street, London, WC1N 3AX, United Kingdom

---

### 1. Introduction

Future Data Software Online Ltd (“Future Data”, “the Company”) is a UK-based private company limited by shares providing advanced technology services across AI, Software Engineering, Cloud Platforms, Cybersecurity, Blockchain, Smart City Systems, Medical Informatics and Enterprise Digital Solutions. The Company operates internationally across the UK, EU, Canada and Asia.

#### FUTURE DATA CORPORATE PROFILE

In carrying out its operations, Future Data is committed to ensuring the highest standards of data protection, privacy, and information security in accordance with:

- **UK General Data Protection Regulation (UK GDPR)**
- **EU General Data Protection Regulation (EU GDPR 2016/679)**
- **UK Data Protection Act 2018**
- **PECR (Privacy and Electronic Communications Regulations)**

Future Data acts as **Data Controller** as well as **Data Processor** depending on the context of each service engagement.

---

### 2. Lawful Basis for Processing

Future Data processes personal data strictly under lawful bases described in Article 6 of the GDPR:

1. **Contractual necessity** – For the performance of software development, cloud services, AI systems, IT support, consulting or professional services requested by our clients.
2. **Legitimate interest** – For business communication, service improvement, fraud detection, cybersecurity and operational monitoring.
3. **Legal obligation** – For compliance with UK/EU tax, corporate and regulatory requirements.
4. **Consent** – For optional marketing communication, newsletters or non-essential cookies.
5. **Vital interest / Public interest** – Only when explicitly applicable, particularly in health, government or public infrastructure projects.

### 3. Types of Data We Process

Future Data processes only the minimum data required for the provision of its services. This may include:

#### Client and Business Contact Data

- Name, email, phone, company details
- Communication records
- Billing and contractual information

#### Project & Technical Data

- System logs
- Platform credentials (subject to agreement)
- Source code and development data
- Cloud environment metadata

#### AI, R&D and Platform Data

- Dataset structures
- Model training datasets (only with explicit permission)
- Analytics and performance metrics

#### Sensitive Data

Processed **only** when required by the project scope and always under strict contractual, technical and legal safeguards, including encryption and access control.

---

### 4. Data Minimisation & Retention

Future Data applies strict **data minimisation** and **purpose limitation** policies.

Data retention follows:

- **Operational data:** retained only for the lifecycle of the project
- **Client datasets:** deleted upon project completion unless contractually agreed
- **Financial & legal records:** retained for statutory periods (6 years under UK regulations)
- **System logs and monitoring data:** retained for 3–12 months, depending on security policy

Upon client request, Future Data provides:

- ✓ Full data export
- ✓ Secure deletion
- ✓ Certificate of Destruction (upon deletion of client data)

---

### 5. Data Security & Technical Safeguards

As a deep-tech organisation with strong cybersecurity expertise, Future Data maintains robust protections including:

- **ISO 27001-aligned security framework**
- **Encryption in transit & at rest (TLS 1.3, AES-256)**
- **Multi-factor authentication (MFA)**
- **Zero-trust access model**
- **Network segmentation**
- **Advanced firewalls & intrusion detection systems**
- **Secure DevOps (DevSecOps) pipelines**
- **Regular penetration testing & vulnerability assessments**
- **Controlled access to AI and data-training environments**

For cloud services, Future Data uses secure infrastructures including: AWS, Azure, Google Cloud, private servers and EU-hosted environments depending on project requirements.

---

## **6. International Data Transfers**

Given Future Data's multinational operations across the UK, EU, Canada and Asia

### **FUTURE DATA CORPORATE PROFILE**

, international data transfers may occur **only under GDPR-compliant safeguards**, including:

- UK International Data Transfer Agreements (IDTA)
- Standard Contractual Clauses (SCCs)
- Adequacy decisions
- Contractual and technical protections
- Encryption of all transferred data

No data is transferred to third parties without a lawful basis and contractual guarantees.

---

## **7. Third-Party Processors**

Future Data uses carefully selected third-party service providers for specific functions (cloud hosting, email delivery, analytics, project management, cybersecurity systems), each of which is bound by:

- Data Processing Agreements (DPAs)
- Confidentiality agreements
- GDPR-compliant security and privacy controls

---

## 8. Data Subject Rights

Under UK/EU GDPR, individuals retain the right to:

- Access their data (Subject Access Request)
- Request rectification or deletion
- Request restriction of processing
- Data portability
- Object to certain processing types
- Withdraw consent at any time

Future Data responds to all subject-access requests within **one month**, as required.

---

## 9. Data Breach Notification

Future Data maintains an emergency response and breach notification protocol. In the event of a data breach involving “risk to the rights and freedoms” of individuals:

- The UK ICO (or relevant EU data authority) will be notified **within 72 hours**
- Affected individuals will be informed without undue delay
- Full incident analysis, remediation and security reinforcement actions will be undertaken

---

## 10. Governance & Accountability

Future Data's GDPR compliance is overseen by:

### **Data Protection Officer (DPO)**

Future Data Software Online Ltd

27 Old Gloucester Street, London, WC1N 3AX, United Kingdom

The Company maintains:

- Data Protection Impact Assessments (DPIA)
- Records of Processing Activities (RoPA)
- Access control logs
- Employee confidentiality obligations
- Internal GDPR training and cybersecurity awareness programmes

---

## 11. Contact for GDPR Enquiries

### **Future Data Software Online Ltd**

27 Old Gloucester Street

London WC1N 3AX

United Kingdom  
Email: [info@futuredata.com](mailto:info@futuredata.com)  
Phone: +44 0759 963 4927 / +30 694 636 6888