1. Introduction

Frontryion (“the Company”) is committed to protecting the privacy and security of personal data it processes. This Data Privacy Policy outlines the regulatory requirements applicable to the Company, the safeguarding measures used to protect information, and the rights of individuals whose data we process. This Policy applies to all who processes personal data on behalf of the Company.

---

2. Applicable Data Privacy Regulations

Frontryion adheres to the following data protection regulations, as applicable based on the jurisdiction of our operations and customers:

- **General Data Protection Regulation (GDPR) (EU) 2016/679**
- Relevant local data protection and privacy laws in countries where Frontryion operates or stores data
- Any additional regulatory or industry-specific obligations related to data handling and privacy

---

3. Safeguarding Measures

Frontryion implements administrative, technical, and physical safeguards to ensure that all personal data shared internally or with third parties is:

- Processed lawfully and securely
- Protected against unauthorized access, loss, destruction, or misuse
- Used solely for the purposes for which it was collected

Safeguards include (but are not limited to):

- Access controls based on role and least privilege principles
- Secure data storage in certified facilities
- Ongoing monitoring for security threats

---

4. Data Processing Registers

Frontryion maintains internal **Data Processing Registers** containing details of:

- Purpose and legal basis for processing
- Retention periods (including the 5-year retention period described below)

- International data transfer mechanisms
- Security measures applied

---

5. Incident Response Plan

Frontryion will apply a **Incident Response Plan** if needed, which includes:

- Procedures for detecting and assessing suspected or confirmed data breaches
- Internal reporting requirements
- Actions to contain, mitigate, and remediate the breach
- Post-incident review and corrective actions

---

6. Breach Notification Processes

If a personal data breach occurs, Frontryion will:

- **Notify applicable supervisory authorities** without undue delay and, where required, within 72 hours
- **Notify affected individuals** when the breach is likely to result in a high risk to their rights and freedoms
- Document all breaches, regardless of severity, in the Breach Register

---

7. Application of GDPR Principles

Frontryion applies the following GDPR or equivalent principles:

1. Lawfulness, Fairness, and Transparency
2. Purpose Limitation
3. Data Minimization
4. Accuracy
5. Storage Limitation
6. Integrity and Confidentiality
7. Accountability

These principles guide all data processing activities and form the foundation for privacy-by-design practices.

---

8. Third-Party Access and Compliance

Frontryion has the following third parties who have access to personal data, including:

- Service providers
- Cloud hosting partners

Third parties are permitted access only when necessary and must comply with applicable data protection laws and Frontryion's standards.

---

9. Consent Management

Frontryion ensures that:

- Consent is obtained lawfully, clearly, and explicitly when required
- Records of consent and withdrawal of consent are retained
- Individuals can withdraw consent at any time
- Consent is processed in a manner that meets GDPR and industry standards

---

10. Data Retention Period

Frontryion retains personal data for a maximum of *five (5) years*, unless:

- A longer period is legally required, or
- Retention is necessary for the establishment, exercise, or defense of legal claims

Once the retention period expires, data is securely deleted or anonymized using industry-accepted destruction methods.

---

11. Data Privacy Impact Assessments (DPIAs)

We rely on CurrencyCloud for this topic

---

12. Notification of Data Breaches

Should a data breach occur, Frontryion will notify:

- CurrencyCloud
- Affected individuals

- Applicable authorities
- Relevant internal and external stakeholders

Notifications will include the nature of the breach, likely consequences, mitigation steps, and points of contact.

---

13. Individual Rights

Individuals have the right to:

- Access their personal data
- Rectify inaccurate data
- Request data erasure
- Restrict processing
- Object to processing
- Request data portability
- Withdraw consent

Requests will be addressed within required legal timeframes.

---

14. Contact Information

For questions or requests related to this Policy, contact:

Data Protection Officer (DPO)
Bob Hadjidakis
Email: *bob@frontryion.com*
Phone: *+31 20 244 52 52*
