Flexwhere

Technical and Organisational Measures (TOM)

Art. 32 EU-GDPR
Version 1.2
Date: 07 October 2024

Introduction....2
1. Physical Access Control....2
2. Logical Access Control....2
3. Data Access Control....3
4. Data Transmission Control....3
5. Data Retention and Backup Control....3
6. Data Separation Control....4
7. Separation Control....4
8. Integrity Control....4
9. Data Minimisation and Purpose Limitation....5
10. Confidentiality Control....5
11. Incident Response and Breach Notification....5
12. Supplier and Sub-Processor Management....6
13. Regular Audits and Assessments....6
14. Employee Accountability and Training....7
15. Data Subject Rights....7
16. Supervisory Authority Cooperation....7

Introduction

Dutchview Information Technology B.V., the creator and owner of the application Flexwhere, implements a series of technical and organisational measures to ensure the security of personal data in accordance with the requirements of the General Data Protection Regulation (GDPR) and other relevant data protection laws.

1. Physical Access Control

To prevent unauthorised physical access to locations where personal data is stored, Dutchview implements the following measures:

- Secured Access: Access to data centres is controlled through electronic access control systems (keys, access cards, biometric systems).
- Surveillance Systems: Physical locations are equipped with video surveillance, alarm systems, and security personnel, where necessary.
- Visitor Management: Visitors have access only to designated areas and must be accompanied by authorised personnel when accessing other parts of the building.
- Building Security: Fire safety measures, including fire alarms and extinguishing systems, are installed to protect against environmental hazards.

2. Logical Access Control

To ensure that only authorised personnel have access to data, Dutchview implements the following logical access controls:

- Authentication: Access to systems and data is granted based on role and function. Multi-Factor Authentication (MFA) and Single Sign-On (SSO) are required wherever possible to secure access to systems.
- Password Policies: Passwords must meet minimum complexity requirements and are regularly updated. Systems enforce a password expiration policy.
- Encryption: User credentials, including passwords, are encrypted during transmission and storage to prevent unauthorised access.
- Access Reviews: User access rights are regularly reviewed, and permissions are revoked upon termination of employment or contract.

3. Data Access Control

To ensure that authorised users only access the data they are permitted to, Dutchview implements the following controls:

- Role-Based Access Control (RBAC): Permissions are granted based on the user's role and job function. No general or shared user accounts are permitted unless explicitly approved by management.
- Data Classification: Data is classified by sensitivity, and access is restricted accordingly. The more sensitive the data, the higher the level of protection required.
- Monitoring and Logging: All system and data access activities are logged and monitored to ensure accountability and traceability.

4. Data Transmission Control

To protect data during transmission, Dutchview implements the following controls:

- Encryption of Data in Transit: All personal data transmitted between Dutchview and external parties (e.g., customers, service providers) is encrypted using secure protocols (e.g., SSL/TLS).
- Secure Communication Channels: Sensitive information is never transmitted via unencrypted emails or over unsecured communication channels.
- Access Controls: Only authorised personnel are permitted to transmit or share data.

5. Data Retention and Backup Control

To ensure the availability and integrity of personal data, Dutchview implements the following measures:

- Data Backups: Customer data (Production) is backed up daily, weekly, and monthly, covering a retention period of six months. Backup data is stored in secure, geographically separate locations.
- Disaster Recovery: Dutchview has a comprehensive disaster recovery plan to restore systems and data in the event of a physical or technical incident.
- Availability Testing: Regular tests are conducted to ensure the effectiveness of backups and recovery procedures.

6. Data Separation Control

To ensure that data collected for different purposes is processed separately, Dutchview enforces the following measures:

- Separation of Environments: Development, testing, and production environments are physically and logically separated.
- Customer Data Segregation: Customer data is segregated to ensure that it is not accessible by other customers or unauthorised personnel.

7. Separation Control

To ensure that data collected for different purposes is processed separately, Dutchview implements the following separation controls:

- Logical Separation: Data for different clients or purposes is logically separated within the same systems, using access control lists, role-based access controls (RBAC), or different database schemas.
- Environment Segregation: Production, development, and testing environments are kept completely separate to prevent data from being used outside its intended environment.
- Data Anonymization and Pseudonymization: Personal data is anonymized or pseudonymized where appropriate to ensure it is not used for unintended purposes.
- Access Logging: Access to data is logged to ensure that it is only accessed for the correct purposes.

8. Integrity Control

To protect personal data from unauthorised or accidental modification or deletion, Dutchview implements the following integrity controls:

- Checksums and Hashing: Data integrity is maintained through the use of checksums and hashing algorithms to detect any unauthorised changes to data.
- Audit Trails: All modifications to critical data are logged, with audit trails maintained for forensic analysis and accountability purposes.
- Version Control: Version control systems are used to track changes to data and files, ensuring that original data can be restored if necessary.

9. Data Minimisation and Purpose Limitation

Dutchview ensures that personal data processing is limited to what is necessary for specific, legitimate purposes:

- Data Collection Policies: Only the minimum amount of personal data required for a specific purpose is collected and processed.
- Data Review: Regular reviews of data are conducted to ensure that only relevant and necessary data is retained.
- Retention Policy: Personal data is retained only for as long as necessary to fulfil its intended purpose or to comply with legal obligations. After that, it is securely deleted or anonymized.

10. Confidentiality Control

To ensure the confidentiality of personal data, Dutchview enforces the following measures:

- Non-Disclosure Agreements (NDAs): All employees and contractors are required to sign NDAs to ensure confidentiality of personal and sensitive data.
- Data Encryption: All stored personal data is encrypted using industry-standard encryption methods (AES-256 or higher) to protect it from unauthorised access.
- Employee Training: Regular training on data protection and security policies is provided to employees to ensure awareness and compliance with confidentiality requirements.

11. Incident Response and Breach Notification

Dutchview has established a comprehensive incident response plan to detect, report, and address security breaches:

- Incident Detection: Automated monitoring systems are in place to detect suspicious activity or potential security incidents.

- Incident Reporting: In the event of a data breach, Dutchview will notify the affected customers and relevant supervisory authorities in accordance with both GDPR and NIS2 requirements.
- Preventive Measures: An investigation is conducted to determine the cause of the incident, and after corrective actions are implemented, ways to prevent recurrence are determined as well.

12. Supplier and Sub-Processor Management

Dutchview ensures that all third-party suppliers and sub-processors with access to personal data comply with equivalent data protection measures:

- Due Diligence: Dutchview conducts thorough due diligence on all suppliers and sub-processors to verify their data protection practices.
- Data Processing Agreements (DPAs): All sub-processors are required to sign DPAs, committing to GDPR compliance and appropriate security measures.
- Ongoing Monitoring: Dutchview regularly monitors and audits suppliers to ensure ongoing compliance with security and data protection standards.

13. Regular Audits and Assessments

Dutchview regularly conducts internal and external audits to assess compliance with security and data protection policies:

- Internal Audits: Regular internal audits are conducted to evaluate the effectiveness of technical and organisational measures.
- External Audits: Independent third-party audits are carried out not only to ensure compliance with GDPR and other legal obligations but also to maintain our ISO certifications (ISO9001 and ISO27001).
- Penetration Testing: Periodic penetration tests are performed both internally and externally by an independent third party to identify and mitigate vulnerabilities in systems and infrastructure.

14. Employee Accountability and Training

Dutchview ensures that employees are aware of their responsibilities and are trained to handle personal data securely:

- Data Privacy Officer (DPO): A designated DPO oversees the company's data protection strategy and ensures compliance with GDPR.
- Security Training: Employees receive mandatory data protection and information security training, with updates provided as needed.
- Employee Accountability: Employees are held accountable for compliance with security and data protection policies. Non-compliance can lead to disciplinary action.

15. Data Subject Rights

Dutchview has implemented procedures to respond to data subject requests in accordance with GDPR, including:

- Right to Access: Data subjects can request access to their personal data, and Dutchview will respond within the legal timeframe.
- Right to Rectification: Data subjects can request corrections to inaccurate or incomplete personal data.
- Right to Erasure (Right to be Forgotten): Data subjects can request the deletion of their personal data, provided it is no longer needed for lawful purposes.
- Right to Restriction: Data subjects can request the restriction of data processing in certain circumstances.
- Right to Data Portability: Upon request, Dutchview will provide personal data in a structured, machine-readable format, facilitating its transfer to another data controller.

16. Supervisory Authority Cooperation

Dutchview cooperates with supervisory authorities to ensure full compliance with GDPR:

- Collaboration: Dutchview maintains open communication with relevant supervisory authorities and provides requested information promptly.
- Reporting Obligations: In the event of a data breach or other security incident, Dutchview follows the legal reporting requirements outlined by GDPR and NIS2.