White Raven IT – Data Protection Policy

Introduction

This Data Protection Policy outlines White Raven IT BV's commitment to safeguarding personal data and ensuring compliance with the General Data Protection Regulation (GDPR), ISO 27001, Digital Operational Resilience Act (DORA), and the Network and Information Security Directive 2 (NIS2). This policy applies to both internal data and customer data, ensuring the confidentiality, integrity, and availability of all information processed by the company.

As an IT advisory company, White Raven IT BV handles sensitive information and is committed to protecting personal data, minimizing risks, and ensuring compliance with all applicable laws and standards.

Scope

This policy applies to:

- All employees, contractors, and third parties working with or on behalf of White Raven IT BV.
- All personal data processed internally and on behalf of clients, including data belonging to end customers.
- The handling of data in all formats (electronic, paper, and other media).

The policy covers personal data processing, storage, transmission, and destruction within the company's operations and client engagements.

Compliance Framework

This policy is designed to meet the requirements of:

- GDPR: Regulation (EU) 2016/679 on data protection and privacy for individuals within the EU.
- ISO 27001: International standard for information security management systems (ISMS).
- DORA: Regulation (EU) 2022/2554 aimed at ensuring the digital operational resilience of financial institutions.
- NIS2: EU Directive 2022/2555 focused on strengthening the security of network and information systems across the EU.

Data Protection Principles

White Raven IT BV is committed to adhering to the following data protection principles, in accordance with GDPR, ISO 27001, DORA, and NIS2:

1. Lawfulness, Fairness, and Transparency

- All personal data will be processed lawfully, fairly, and in a transparent manner.
- Data subjects will be informed about the purposes of data processing and their rights under GDPR.

2. Purpose Limitation

- Personal data will only be collected for specified, explicit, and legitimate purposes and will not be processed further in a manner incompatible with those purposes.

3. Data Minimization

- Personal data will be adequate, relevant, and limited to what is necessary for the purposes for which it is processed.

4. Accuracy

- Personal data will be accurate and, where necessary, kept up-to-date. Inaccurate data will be rectified or erased without delay.

5. Storage Limitation

- Personal data will not be kept for longer than necessary for the purposes for which it is processed.

6. Integrity and Confidentiality

- Personal data will be processed in a manner that ensures appropriate security, including protection against unauthorized or unlawful processing, accidental loss, destruction, or damage, using appropriate technical and organizational measures.

7. Accountability

- White Raven IT BV is responsible for and will be able to demonstrate compliance with these principles.

Roles and Responsibilities

1. Data Protection Officer (DPO)

- Responsible for overseeing data protection strategy and implementation to ensure compliance with GDPR and other regulations.
- Acts as the main point of contact for data subjects and the data protection authority.

2. Information Security Manager

- Ensures compliance with ISO 27001 by managing the ISMS and performing regular audits and risk assessments.
- Oversees the implementation of technical and organizational security measures.

3. All Employees

- Must comply with this policy and complete regular data protection training.
- Responsible for reporting any suspected data breaches or vulnerabilities to the DPO immediately.

Internal Data Protection Measures

1. Data Inventory and Classification

- All personal data processed by the company will be documented in a data inventory.
- Personal data will be classified according to its sensitivity (e.g., confidential, restricted, internal, public) to ensure appropriate handling and security measures.

2. Access Control

- Access to personal data will be restricted based on the principle of least privilege. Only authorized personnel will have access to personal data necessary for their job functions.
- Multi-factor authentication (MFA) and role-based access control (RBAC) will be used to ensure secure access to sensitive systems and data.

3. Data Encryption

- Personal data will be encrypted both at rest and in transit using industry-standard encryption protocols (e.g., AES-256, TLS 1.2 or higher).

4. Data Anonymization and Pseudonymization

- Where possible, data will be anonymized or pseudonymized to reduce the risk of identifying individuals in case of a data breach.

5. Data Retention and Disposal

- Personal data will be retained only for as long as necessary to fulfill the purposes for which it was collected.
- Secure disposal methods (e.g., data wiping, shredding) will be used to destroy personal data once it is no longer needed.

6. Incident Response and Data Breach Management

- An incident response plan is in place to detect, respond to, and mitigate data breaches. This includes notifying relevant parties (e.g., data subjects, supervisory authorities) within the required 72-hour window under GDPR.
- The company will document all data breaches, their impact, and remedial actions.

Customer Data Protection Measures

1. Data Processing Agreements (DPAs)

- White Raven IT BV will enter into Data Processing Agreements with all clients and vendors who process personal data on our behalf. These agreements will outline the roles and responsibilities of each party and ensure compliance with GDPR and other relevant regulations.

2. Third-Party Vendor Management

- All third-party vendors who process personal data will undergo a rigorous vetting process to ensure they meet GDPR, ISO 27001, DORA, and NIS2 requirements.
- Vendors will be regularly monitored to ensure ongoing compliance with security and data protection standards.

3. Data Subject Rights

- Data subjects have the right to access, correct, erase, or restrict the processing of their personal data. White Raven IT BV will respond to data subject requests within the regulatory timelines (typically one month under GDPR).
- Procedures will be in place to facilitate data subject rights, including data portability and objection to processing.

4. Customer Data Encryption

- Customer data will be encrypted both at rest and during transmission. The company will ensure that customer data is processed only in secure environments.
- Regular vulnerability assessments and penetration tests will be conducted on systems that handle customer data.

5. Backup and Recovery

- Regular backups of customer data will be performed to ensure data integrity and availability. Backups will be encrypted and stored securely.
- A disaster recovery plan will be maintained and tested annually to ensure quick restoration of services in the event of a data loss or breach.

Compliance with DORA and NIS2

1. Operational Resilience (DORA)

- The company will maintain robust business continuity and disaster recovery plans to ensure digital operational resilience in line with DORA requirements. Regular testing of these plans will be conducted.
- Continuous monitoring of critical IT systems will be implemented to detect and mitigate cyber threats.

2. Network and Information Security (NIS2)

- White Raven IT BV will adopt a risk-based approach to securing its network and information systems, consistent with the NIS2 directive.
- The company will collaborate with national cybersecurity authorities and comply with incident reporting obligations within the specified timeframes.

Employee Training and Awareness

- All employees will receive mandatory data protection training during onboarding and annual refresher courses thereafter.
- Specialized training will be provided for employees handling high-risk data, such as health or financial data.

Policy Review and Updates

This policy will be reviewed annually by the DPO and Information Security Manager to ensure it remains up-to-date with the latest regulatory changes and industry best practices. Changes to the policy will be communicated to all employees and relevant stakeholders.

Contact Information

For questions, concerns, or to report a data protection issue, please contact the Data Protection Officer at dp@whiteravenit.be.

By adhering to this policy, White Raven IT BV ensures that it meets the highest standards of data protection, complies with EU regulations, and protects the privacy and rights of its employees, customers, contractors, and suppliers.

Annex – Microsoft's M365 and Hornetsecurity

Microsoft M365 and Hornetsecurity offer comprehensive solutions that can help an IT advisory company comply with GDPR, ISO 27001, DORA, and NIS2 through integrated security, data protection, and compliance features. Here's how they fit into the data protection policy and overall compliance strategy:

Microsoft M365

Microsoft M365 is a cloud-based suite that includes tools like Office 365, Microsoft Teams, OneDrive, and advanced security features. It provides a secure platform for collaboration, communication, and data storage, making it an effective tool for compliance with GDPR, ISO 27001, DORA, and NIS2.

1. Data Protection and GDPR Compliance

- Data Encryption: M365 encrypts data both at rest and in transit, using technologies such as AES-256 and TLS 1.2, ensuring personal data is securely stored and transmitted.
- Data Loss Prevention (DLP): Built-in DLP policies help prevent data breaches by identifying and blocking the unauthorized sharing of sensitive information like personal data, credit card numbers, and other confidential data.
- Access Control and Identity Management: M365 integrates with Azure Active Directory (AAD) to enforce role-based access control (RBAC) and multi-factor authentication (MFA), which are essential for limiting access to personal data in compliance with GDPR and ISO 27001.
- Data Subject Rights: Microsoft 365's compliance center helps manage and fulfill data subject requests such as the right to access, delete, or rectify personal data. Tools like Microsoft Compliance Manager assist in tracking and managing GDPR compliance.
- Audit Logs and Monitoring: M365 provides comprehensive audit logging and monitoring capabilities that help identify suspicious activities and ensure compliance with regulatory requirements.

2. ISO 27001 Compliance

- Information Security Management System (ISMS): M365 can be integrated into an organization's ISMS to maintain the confidentiality, integrity, and availability of information. It also offers templates and tools to manage risks, incidents, and compliance reports.

- Security Controls: M365 is certified for ISO 27001, meaning that Microsoft has implemented rigorous security controls to safeguard data. This simplifies the process for businesses that need to meet ISO 27001 requirements by using Microsoft's secure cloud infrastructure.

3. DORA and Operational Resilience

- Business Continuity and Disaster Recovery: M365 provides robust backup and recovery features, including the ability to recover deleted emails, files, and sites. These tools ensure operational resilience and data availability, which are critical for compliance with DORA.
- Incident Response: M365 includes tools for detecting, responding to, and managing cybersecurity incidents, including real-time alerts, automated responses, and investigation capabilities through Microsoft Defender and Sentinel.
- Regulatory Compliance: M365 provides regulatory compliance tools that assist with meeting specific DORA requirements for operational resilience, including continuous monitoring, cybersecurity frameworks, and reporting tools.

4. NIS2 Compliance

- Network and Information Security: M365's security features help ensure compliance with NIS2 by providing continuous monitoring, vulnerability management, and protection against cyber threats. Features like Conditional Access and Threat Protection help protect the company's network and information systems.
- Incident Reporting: M365 enables automated threat detection and response, which helps meet the NIS2 requirements for timely incident reporting. Microsoft Defender and Sentinel allow for real-time monitoring of networks and help meet the legal obligation to report significant incidents.

Hornetsecurity

Hornetsecurity specializes in cloud security services, particularly focusing on email security, backup, and data protection. Their solutions are designed to complement platforms like M365 by adding additional layers of security and backup, which are crucial for regulatory compliance.

1. Data Protection and GDPR Compliance

- Email Encryption: Hornetsecurity offers email encryption solutions that ensure that all email communications are protected in transit and at rest, which is vital for GDPR compliance. This prevents unauthorized access to sensitive data shared via email.

- Email Archiving: Hornetsecurity’s email archiving ensures that emails are stored securely and can be retrieved easily when necessary, supporting GDPR requirements for data retention and data subject access requests.
- Compliance Filters: Hornetsecurity provides data loss prevention and content control features for email, ensuring that confidential information is not accidentally or intentionally shared, which supports GDPR’s requirement for data protection by design.

2. ISO 27001 Compliance

- Cloud Security and Compliance: Hornetsecurity’s cloud services are compliant with ISO 27001 standards. Their secure infrastructure, encryption protocols, and operational security measures support an organization's ability to maintain an ISO 27001-certified ISMS.
- Security Controls: Hornetsecurity's solutions provide an additional layer of security for email communication, enhancing the overall security posture and helping meet the ISO 27001 controls related to communication security.

3. DORA and Operational Resilience

- Email Continuity: Hornetsecurity offers email continuity services that ensure that communication is maintained even during outages or disasters. This is critical for operational resilience and supports DORA's requirements for continuous availability and resilience in digital operations.
- Automated Backups: Hornetsecurity offers automated and encrypted backups for M365 environments, ensuring that data is regularly backed up and can be restored quickly, meeting the data integrity and availability requirements of DORA.

4. NIS2 Compliance

- Threat Detection and Response: Hornetsecurity offers advanced threat protection (ATP) for email, which includes real-time monitoring and detection of phishing, malware, and other cyber threats. These features help meet NIS2 requirements for protecting networks and systems from cyber threats.
- Incident Reporting and Management: Hornetsecurity provides detailed logging and monitoring of email security incidents, which can assist in meeting NIS2’s reporting obligations for significant incidents that affect network and information systems.

How do Microsoft M365 and Hornetsecurity Fit Into Our Data Protection Policy?

1. **Integrated Security and Compliance**: Both M365 and Hornetsecurity complement each other to create a robust security environment. M365 provides comprehensive protection for data at the application and infrastructure levels, while Hornetsecurity offers specialized email and backup security. Together, they help enforce the data protection policy and ensure compliance with GDPR, ISO 27001, DORA, and NIS2.

2. **Incident Management and Reporting**: Both solutions offer incident detection, management, and reporting features essential for complying with DORA and NIS2. Microsoft's compliance tools and Hornetsecurity's email security services help identify, report, and respond to security incidents effectively.

3. **Data Retention and Subject Rights**: M365's compliance center and Hornetsecurity's email archiving solutions help you manage data retention in line with GDPR and ISO 27001, while also facilitating the handling of data subject rights requests.

4. **Operational Resilience**: The business continuity and backup features provided by both M365 and Hornetsecurity ensure that your operations remain resilient to disruptions, fulfilling DORA's requirements for operational resilience and continuity in critical digital operations.

By leveraging both Microsoft 365 and Hornetsecurity, White Raven IT BV can build a secure and resilient IT environment that meets its regulatory and data protection obligations under GDPR, ISO 27001, DORA, and NIS2.