Technical and Organizational Measures

Governing Data Processing at PALFINGER

This document outlines the technical and organizational measures (TOMs) implemented by PALFINGER to ensure the secure, lawful, and transparent processing of personal data across all operational areas. These measures are developed in accordance with applicable data protection regulations – most notably the Gen-eral Data Protection Regulation (GDPR) – and are aligned with internationally recognized standards, includ-ing those established by the German Federal Office for Information Security (BSI). Together, they form a robust framework designed to protect confidentiality, integrity, availability, and resilience of personal data.

1. CONFIDENTIALITY

Data Encryption:

Where applicable, personal data is encrypted both in transit and at rest using industry-standard protocols (e.g., AES, TLS). Company laptops are equipped with BitLocker for hard drive encryption.

Pseudonymization:

To minimize the risk of identification, personal data is pseudonymized where appropriate. This involves re-placing identifying fields within a data record with artificial identifiers or pseudonyms, reducing the linkability of data to individuals without additional information.

Physical Access Controls:

To prevent unauthorized physical access to PALFINGER facilities, a range of protective measures are im-plemented where appropriate. These include the use of access devices such as chip cards, physical keys, and electronic door openers to restrict entry. Security personnel may be stationed at entrances to monitor and control access points. Additionally, alarm systems and continuous video surveillance (CCTV) are de-ployed to detect and deter unauthorized access attempts. Access events are logged to ensure traceability and support incident response procedures.

Electronic Access Controls:

Access to IT systems is restricted through technical controls that enforce user authentication and authoriza-tion. Role-Based Access Control (RBAC) ensures that users can only access data necessary for their job responsibilities. Multi-Factor Authentication (MFA) adds an additional layer of security by requiring multiple forms of verification before granting access to the PALFINGER network. Secure passwords are enforced, and VPN usage is required for remote access to ensure secure connections.

System Security:

Firewalls are configured to block unauthorized network traffic, while Intrusion Detection Systems (IDS) con-tinuously monitor for suspicious activity. Anti-malware tools are deployed across systems and are regularly updated to detect and prevent infections from malicious software. Additionally, advanced endpoint protec-tion platforms are used to provide real-time threat detection, behavioral analysis, and automated response capabilities across the IT environment.

Data Protection Policies:

The PALFINGER data protection policy defines responsibilities and processes to ensure the lawful, secure, and transparent handling of personal data in compliance with applicable data protection laws, including documentation of processing activities, risk assessment, breach notification, and safeguarding the rights of data subjects across all PALFINGER entities.

Handling of Sensitive Personal Data:
Sensitive personal data is identified and subject to enhanced protection measures. Access to such data is strictly limited to authorized personnel with a legitimate need, and additional safeguards such as encryption, access logging, and stricter retention policies are applied.

Employee Training:
All employees receive regular trainings on data protection principles, secure data handling, and recognizing potential security threats such as phishing. In addition, employees are contractually obliged to comply with internal data protection policies and applicable data privacy laws.

Vendor Management:
Third-party service providers who process personal data on behalf of PALFINGER are subject to strict vet-ting. Data Processing Agreements (DPAs) are in place to ensure compliance with applicable data privacy laws.

International Data Transfers:
When personal data is transferred outside the European Economic Area (EEA), PALFINGER ensures that appropriate safeguards are in place to maintain an adequate level of data protection (e.g., Standard Con-tractual Clauses (SCCs), Binding Corporate Rules (BCRs), or reliance on adequacy decisions). All cross-border transfers are documented and reviewed to ensure compliance with applicable legal requirements. Same applies to transfers from outside the EEA to the EEA.

Data Minimization:
Only the necessary personal data is collected and processed, in accordance with the principle of data mini-mization. Where feasible, privacy by design and by default principles are integrated to ensure data protec-tion is considered from the outset.

Rights of Data Subjects:
PALFINGER has established procedures to ensure that individuals can exercise their rights under applicable data protection laws. Requests are handled promptly and in accordance with applicable legal timeframes. A dedicated contact point is available for submitting and managing data subject requests.

2. INTEGRITY

Logging and Monitoring:
Where appropriate, access to systems and data is logged and monitored continuously. Logs are reviewed regularly to detect anomalies, unauthorized access attempts, or policy violations. This supports incident detection, response, and forensic investigations. To ensure effective monitoring and rapid response, PALFINGER is supported by a Security Operations Center (SOC) team, which assists in analyzing log data and managing security incidents.

Access Restrictions:
Access to personal data is governed by clearly defined roles and responsibilities. Role-Based Access Con-trol (RBAC) is implemented to ensure that only authorized individuals can view, modify, or delete data based on their job functions. The principle of least privilege is applied to ensure that users have the minimum level of access necessary for their roles.

Change Management Procedures:
Where appropriate, changes to systems that process or store personal data are subject to formal change management procedures. This includes documenting the nature and purpose of the change, assessing po-tential risks, obtaining necessary approvals, and testing changes in a

controlled environment before de-ployment. Post-implementation reviews are conducted to ensure changes do not negatively impact data security or system availability.

3. AVAILABILITY AND RESTORABILITY

Data Backup and Recovery:

Regular, automated backups of critical data are performed and stored securely. Recovery procedures are tested periodically to ensure data can be restored quickly and accurately in the event of data loss, corrup-tion, or a security incident. Backups are encrypted and stored off-site to enhance security and ensure data availability in case of local disruptions.

Cloud Infrastructure with High Availability SLAs:

Where appropriate, cloud services are used that offer high availability guarantees through formal Service Level Agreements (SLAs). These services ensure scalable and reliable access to data by leveraging redun-dant systems, load balancing, uptime guarantees and penalties for downtime.

Uninterruptible Power Supplies (UPS):

Critical systems are supported by uninterruptible power supplies to maintain operations during power outag-es. This ensures that essential hardware remains functional long enough to allow for safe shutdown proce-dures or transition to backup power sources, reducing the risk of data loss or hardware damage.

Disaster Recovery Plans:

Comprehensive disaster recovery plans are established and maintained to define the steps necessary to restore IT operations following major incidents such as natural disasters, cyberattacks, or system failures. These plans include predefined roles, communication protocols, recovery time objectives (RTOs), and regu-lar testing.

4. RESILIENCE

Incident Response Plan:

A formal incident response plan outlines procedures for identifying, reporting, and managing data breaches or security incidents. The plan includes roles and responsibilities, communication protocols, procedures for notifying the supervisory authorities and post-incident review processes. This plan is designed in accord-ance with the requirements of the European NIS2 Directive.

Distributed Architecture:

Systems are designed using a distributed architecture to eliminate single points of failure. By spreading workloads and data across multiple nodes or locations, the infrastructure ensures continued availability and resilience in the event of hardware or network failures.

Load Balancing:

Traffic and processing loads are distributed across multiple servers or services to prevent overload and maintain optimal performance. Load balancing mechanisms help ensure system responsiveness and availa-bility, especially during peak usage or unexpected spikes in demand.

Penetration Testing and Security Drills:

Regular penetration tests and simulated security incidents are conducted to identify vulnerabilities and as-sess the effectiveness of incident response procedures.

Business Continuity Planning (BCP):

A comprehensive Business Continuity Plan is maintained to ensure that critical operations can continue dur-ing and after disruptive events. The plan includes risk assessments, continuity strategies, communication protocols, and regular testing to validate its effectiveness and readiness.

5. TESTING, ASSESSMENT AND EVALUATION

Regular Testing:

Security measures are regularly tested through vulnerability assessments, penetration testing, and simulated incident scenarios.

Continuous Improvement:

PALFINGER continuously monitors technological developments, emerging threats, and regulatory changes. Security measures are updated accordingly to maintain a high level of protection and compliance.

Data Protection Impact Assessments (DPIAs):

For high-risk processing activities, Data Protection Impact Assessments are conducted to identify and miti-gate potential risks to data subjects.