TECHNICAL AND ORGANISATIONAL MEASURES FOR THE PROTECTION OF PERSONAL DATA

Computacenter Group
Information Security Management System

Group Information Systems

Document version 3.4

- Unrestricted -

DOCUMENT INFORMATION

	Document facts
Topic:	Group Data Privacy TOMs
Versions as of:	22/12/2023
Version:	3.4
Revision Cycle	1 year
Classification	Unrestricted
Document Owner	Group Chief Information Security Officer

TABLE OF CONTENTS

INTRODUCTION

This document articulates the technical and organisational security measures implemented by Computacenter to protect information and it is applicable to all systems under management by Computacenter and to its staff, partners and third parties. See Annex 1 and 2 for more information.

Computacenter fulfils the obligation established in the General Data Protection Regulation (GDPR) to safeguard processing of personal data by means of appropriate technical and organisational measures and, where possible, to anonymise or pseudonymise personal data. All measures implemented take the risk associated with the respective data processing operation into consideration. In particular, the effectiveness of the measure taking account of the protection objectives of confidentiality, availability, and integrity.

DATA PRIVACY MANAGEMENT

1 Data privacy principles

The following sets out the high-level principles that underlie Computacenter's practices for collecting, using, disclosing, storing, securing, accessing, transferring, or otherwise processing personal data.

- **Lawfulness, fairness and transparency**
  - Computacenter shall process personal data lawfully, fairly and in a transparent manner in relation to the data subject, for the legitimate business purposes only and if the processing is required in order to comply with our legal obligations.
- **Purpose limitation**
  - Computacenter shall only collect personal data for a specific, explicit, and legitimate purpose(s).
  - Any subsequent processing shall be compatible with such purpose(s), unless Computacenter has obtained the individual's consent, or the processing is otherwise permitted by law.
- **Data minimisation**
  - Computacenter shall ensure that personal data it processes is adequate, relevant and limited to what is necessary in relation to its processing purpose(s).
- **Storage limitation**
  - Computacenter shall keep personal data in a form that is personally identifiable for no longer than necessary to accomplish the purpose(s), or other permitted purpose(s), for which the personal data was obtained.
- **Accuracy**
  - Computacenter shall take reasonable steps to update or remove data that is inaccurate or incomplete. Individuals have the right to request Computacenter to erase, or to rectify, erroneous data that relates to them without delay.
- **Integrity and confidentiality**
  - Computacenter stores personal data safely and protected against unauthorised or unlawful processing and against accidental loss, destruction or damage, using appropriate technical or organisational measures.
- **Accountability**
  - Computacenter shall establish appropriate policies, processes, controls, and other measures necessary to enable it to demonstrate that its processing of personal data is in accordance with applicable data protection laws.

1.1 Information security function

- Computacenter has an established Group Information Systems function led by the Group Chief Information Security Officer (Group CISO). Group CISO is responsible for ensuring the implementation of information security elements such as framework, policies, processes, and measures of compliance;
- Group CISO is supported by a team aligned to business units and geographical areas;
- Group CISO coordinates with the Group Data Protection Officer in relation to the technical and organisational measures for the protection of personal data;
- Computacenter has established an Information Security Management System (ISMS) based on the international best practices of ISO/IEC 27001:2013 and related security standards;
- ISMS has been and continues to be assessed by auditors and receives regular attestation under ISO/IEC 270001:2013; and

- Computacenter has a comprehensive set of information security policies, approved by senior management and published to all staff.

Computacenter's main information security objectives are as follows:

- Maintain the confidentiality, integrity and availability of internal and customer data stored or processed except when authorised or otherwise legally obligated to disclose.
- Accept responsibility for preventing, detecting, and reporting a loss of data and other corporate or customer assets.
- Ensure that information security-related activities are performed in a reliable, responsible and effective manner and are sustainable through embedded processes.
- Continue to deliver secure services, solutions and products to our customers within a secure environment and integrate security into essential business processes.
- Conduct regular information security risk assessments to ensure that security risks are treated in a consistent and effective manner, reduce the likelihood of information security incidents occurring, and limit their potential business and customer impact.
- Continue to increase the level of professional skills of our employees and suppliers in terms of information security.
- Work to ensure our Information Security Management System helps us to improve efficiency and effectiveness, and promote a culture of continuous improvement in information security to enhance customer confidence in Computacenter therefore helping to win and maintain business.

2. Privacy by design and by default

2.1. Anonymisation & pseudonymisation (Article 32(1a), Article 25(1))

- Anonymisation, pseudonymisation and personal data minimisation shall be considered for new information processing activities in accordance with the principles of a privacy by design/security by design process intended to incorporate security and privacy best practices into system designs where possible; and
- Minimum measures for the use of cryptography, such as encryption, are considered based on risk assessment results according to Computacenter policies and standards.

2.2. Alignment with global standards

- Computacenter have achieved a number of security certifications; information security policies and standards have been developed to meet the needs of ISO/IEC 27001:2013; and
- Computacenter's customer-facing systems are in-scope of these certifications, along with the internal technologies used by the users, provided by its Group Information Systems team.

2.3. Security and data protection assurance

- New data processing activities are assessed internally and data minimisation and privacy by design and by default are considered within the design and development process for new applications or systems; and
- Where there are high risks for the data subject concerned with the data processing activities, a Data Protection Impact Assessment shall be completed, and issues addressed to the satisfaction of the relevant Data Protection Officer(s) or, where there remains a high risk to the data subjects associated with such processing, in consultation with the relevant supervisory authority.

2.4. Rights of data subjects

- The rights of data subjects are ensured through the Computacenter Data Protection Impact Assessment process which makes sure that Computacenter processing of personal data fulfils those rights to the extent that they are applicable.

3. Processes for regularly testing, assessing and evaluating the effectiveness (Article 32 (1d), Article 25(1) of GDPR

3.1. Internal audit

- As part of the ISO/IEC 27001:2013 certification, full internal and external audit programmes are in place to ensure non-compliances are identified and managed to resolution;
- External audits are conducted at least annually, and internal audits on an ongoing basis to ensure compliance to ISO/IEC 27001:2013; and
- Findings are delivered in the form of an audit report.

3.2. Third-party risk management programme

- Third Party suppliers that process personal data on behalf of Computacenter Group Companies are required to agree specific terms that reflect Computacenter's obligations either as a controller or a processor of that personal data;
- The security capabilities of third-party suppliers are assessed by Computacenter's Group Information Systems function based upon services provisioned by that supplier and the associated risks relating to a breach; and
- No third-party data processing is permitted without contractual agreements to make data processing compliant with the regulations.

3.3. Secure configuration

- Computacenter conducts regular checks to ensure the secure configuration of devices meet requirements in the information security policies;
- Vulnerability scans and penetration tests are used to identify non-compliance to security policies and remediated within agreed timescales;
- A scheduled operating system patching programme addresses systems defects according to the manufacture's published schedules;
- Where appropriate, the ability of users to change configuration of systems is disabled;
- Standardised servers and operating systems builds are configured in accordance with industry standards to be resistant to attacks; and
- The configuration of systems processing personal data are validated prior to release in the production environment.

Annex 1 - Technical security measures

Logical access control

- All users access Computacenter systems with a unique identifier;
- Generic accounts are prohibited unless business justification exists and exception to the policy request has been approved;
- Users must select a secure password or other means of authentication that complies with Computacenter's authentication credentials requirements defined in the Authentication Credentials Management Standard;
- Password expiry and re-use rules are pre-configured as per standards set out in the Authentication Credentials Management Standard;
- User accounts for applications are configured with an automatic logout process and operating systems are configured to lock accounts after a specified period of inactivity;
- For remote access to systems, two-factor authentication is implemented;
- Role based access control is employed in all core systems;
- Computacenter operates the 'least privilege access' model for each employee; Prior to implementation, additional access must be approved by the employee's line manager and system/service owners;
- Computacenter has a comprehensive process to deactivate users and their access when personnel leaves the company or a function; and
- All access or attempted access to systems is logged and monitored.

Implemented data separation requirements to protect confidentiality

- Environments for the shared service platforms that Computacenter provide to customers are segregated and staged in accordance with security best practice principles;
- Data processing in each environment is carried out separately for each client (logical or physical separation); and
- Access rights are controlled through appropriate groupings and associated rights management to ensure logical data separation between customers;

Data transfer controls implemented for the integrity of the systems (Article 32 (1b) of GDPR

Removable media controls

- Transfer or storage of personal data to or from mobile phone, DVD/CD or USB memory sticks is performed in accordance with Computacenter's Acceptable Use Policy and Information Classification and Handling Matrix; and
- Removal media devices to store personal data are prohibited from use for business unless case-specific exceptions are requested, and approval provided.

Transmission of web-based application data

- Electronic data transfer within the corporation (and from or to customers and suppliers where stipulated) is performed via encrypted connections (including SSL/IPSec VPNs, TLS) and dedicated circuits, assuring the integrity and confidentiality of the information in transit.

Network security

- Controls exist within Computacenter and between Computacenter and its customers and suppliers to perform data transfer using encrypted connections (TLS, SSL, IPSec) and dedicated circuits;
- Guest networks are segregated from core Computacenter networks;
- Vulnerability scanning is conducted throughout internal network scanning;
- Periodic third-party reviews of systems are conducted through penetration testing; and
- Administration of network components and devices are restricted to those who have appropriate permissions for management of those systems.

Remote working

- Computacenter employees and contractors are provided with company devices and relevant security methods to connect remotely;
- Two-factor authentication process is required to connect the company laptop to the network; and
- Users are required to comply with Computacenter's Acceptable Use Policy.

Monitoring

- Computacenter operates a Security Information and Event Monitoring (SIEM) solution which is supported 24x7 to detect security events;
- Logs and events are reviewed daily through SIEM platform with dedicated team assigned and trained for log review/analysis and alert/incident handling or escalation whether required;
- System and Network level events are monitored, logged, analysed, and incidents are raised with relevant priorities. Such incidents are managed through security incident management process; and
- Logging of user activity is undertaken in accordance with the Logging and Monitoring Policy and the Security Logging and Event Monitoring Standard .

Document classification and handling

- All data within the Computacenter Group is classified by reference to and used in accordance with Computacenter's Acceptable Use Policy and the Information Classification and Handling Matrix; and
- Personal data classified in accordance with the Acceptable Use Policy and the Information Classification and Handling Matrix based upon the risks to the data subject associated with a security breach leading to a loss of such personal data.

Availability controls implemented to protect the availability and resilience of the systems (Article 32(1b) of GDPR)

Data backup

- Computacenter shall maintain backups of core systems using virtual tape technology replicated across datacentres.

Malware prevention

- Antivirus systems are implemented for protecting the components of the infrastructure and endpoint devices;
- Real-time antivirus scanning is enabled, and regular scheduled scans are conducted across endpoint devices; and
- External emails are filtered to perform an additional level of hygiene including anti-spam, anti-phishing and anti-virus scanning.

Measures to support disaster recovery

- Computacenter's IT risk management and business continuity process ensures that programmes, configurations and data are kept available in accordance with defined processes and regulations;
- In the event of a failure (catastrophe, disaster) the latest measures are in place to guarantee recovery and continued use;
- Computacenter has localised crisis management capabilities, specified in Major Incident Management Process and Business Continuity Management procedures,
- Detailed recovery documentation are available for all core systems, ensuring a quick restoration of normal operation in the event of an incident;
- Regular individual recovery tests are carried out, at which point recovery plans are updated as necessary; and
- Recovery procedures are subjected to internal audit control. The Computacenter Group's datacentres are equipped with the latest resilient technology.

Annex 2 - Organisational Security Measures

Storage Limitation and Retention

- Personal data shall be kept in a form which permits identification of data subjects for no longer than is necessary for the purposes for which the personal data are processed;
- Determining the data retention requirements relating to personal data processed for the delivery of services are the responsibility of the customer; and
- Personal data shall be destroyed or returned to a customer after expiry of the relevant data retention period.

Information security and data privacy awareness and training

- Information security and data privacy awareness training is available to Computacenter employees via the corporate learning management system; and
- Computacenter employees are enrolled to receive mandatory training upon joining Computacenter and at regular intervals thereafter.

Employee screening

- Pre-employment checks are conducted as part of the Human Resource joiner processes; and
- Additional checks may be required for specific positions or individual customers' requirements if permitted by local laws.

Employee Joiners/Movers/Leavers processes

- The Joiners/Movers/Leavers process controls the access rights assigned to a user during their employment with the organisation;
- When an employee leaves Computacenter, the user account is deactivated immediately by an automated process.

Information security incident and data breach management

- An information security management process is established within Computacenter to identify, investigate and management of incidents through to resolution;
- Security incidents and potential privacy breaches are addressed through the security incident management process; and
- Privacy breaches are notified to the relevant data protection officer and affected customers through the security incident management process promptly and without undue delay.

Physical access controls implemented to protect confidentiality

- Computacenter has a defined physical security zones for each of its premises in order to control physical security measures;
- Each security zone is controlled by electronic entry control systems and specific premises are reinforced by security guards and personal searches on exit;
- Visitors to premises are offered a temporary ID and are always accompanied by a member of Computacenter staff;

- Computacenter datacentres have a defined and protected physical perimeter, physical controls including access control mechanisms, controlled delivery and loading areas, surveillance, and security guards;
- Access to the datacentre premises housing customer data is controlled through a security registration process requiring a photo ID; and
- Datacentre hosting customer data are protected from power failures and other disruptions and have fire detection and suppression systems implemented.

Protection of Strictly Confidential data

- Computacenter operates a need-to-know basis when handling Strictly Confidential information;
- The Acceptable Use Policy and the Information Classification and Handling Matrix in operation within Computacenter includes specific measures to handle Strictly Confidential information including document encryption requirements;
- The Acceptable Use Policy and the Information Classification and Handling Matrix sets out which personal data is deemed as Strictly Confidential;
- Exchange of Strictly Confidential information with third parties must be performed in accordance with the Computacenter's Information Classification and Handling Matrix; and
- The risk management process, in conjunction with data owners and data custodians, will evaluate and manage risks associated with data requiring special care.