WORLDLINE MERCHANT SERVICES

Technical and Organizational Measures

1. PURPOSE OF THIS DOCUMENT

This document contains a list of the technical and organizational measures which are applicable as a standard. The actual measures taken depend on the Service and the location of processing concerned for reasons that not all measures are relevant for all Services and locations. Worldline guarantees it has for all Services and locations the necessary adequate technical and organizational measures included in the list below. The measures are designed to:

- ensure the security and confidentiality of Personal Data;
- protect against any anticipated threats or hazards to the security and integrity of Personal Data;
- protect against any actual unauthorized processing, loss, use, disclosure or acquisition of or access to any Personal Data.

Worldline commits to continuous monitoring the effectiveness of its information safeguards. Worldline commits to maintaining its PCI DSS [1] compliance status.

2. TECHNICAL AND ORGANISATIONAL MEASURES

A. People, awareness and Human Resources (HR):

- All recruitments follow a screening process according to the principles of the Worldline Group background check policy, within the limits of the local laws ;
- In each contract each employee has Non-Disclosure Agreements clauses;
- Code of Ethics awareness training (including a test) is a yearly obligation for all personnel;
- Worldline staff is obliged on a yearly basis to follow the Worldline Data Protection training, the Information Security and Safety training and the PCI DSS Security training, all including a test
- Security policy statement & data protection policies are shared with all employees;
- Obligation for employees to comply with the applicable Atos, Worldline group and local security policies and data protection policies;
- Regular awareness communication on GDPR for all personnel (in addition to Worldline Data Protection policy, Information Security and Safety training);
- Additional specific trainings offered by the data protection community to select teams and employees.

B. Organization control

Worldline shall maintain its internal organization in a manner that meets the requirements of the applicable legislation and the Data controller requirements on data security. This shall be accomplished by:

- Data privacy officer appointed.
- Data privacy, security, and Business continuity organization and governance in place
- Extensive network of Atos and Worldline data protection experts
- Roles & responsibilities for all personnel related to data privacy
- Set of policies that govern data privacy & security
- Internal data processing policies ,procedures and processes for coding, testing, changes and releases, insofar as they relate to the Personal Data processed;
- Implementing a Data Protection control framework that is assessed on a regular basis for compliance
- Regular internal security audits are conducted to verify the security practices.
- Assuring the same technical & organizational measures apply to suppliers processing personal data

[1] PCI DSS: Payment Card Industry – Data Security Standard - concerning the protection of card holder data.

C. Physical Security & Safety and paper records:

All Group entities comply with the Group Worldline Physical and Environmental Security policy & Information Protection Standard:

- physical access control is implemented for all employees, and visitor management systems are implemented for all visitors/guests;
- physical access reviews as per defined periodicity;
- information, which includes paper documents, is classified, labelled, protected and handled according to the Worldline information classification policy;
- specific rules define how to store, process, display, print, transfer and destroy (both in electronic and paper form);
- CCTV surveillance to protect restricted areas;
- fire protection, water flood protection, heating, air conditioning, power supply backup systems are in place to assure integrity and availability of the data stored in the datacenters;
- controlled destruction of data media.

D. Technical Infrastructure and application security:

Worldline has implemented a defense in depth security environment, ensuring multiple layers of security. Following security measures are incorporated:

- network segregation & segmentation;
- secured transmission of data over untrusted networks;
- personal data stored on production networks which are segregated by means of firewalls;
- IDS (Intrusion Detection) and IPS (Intrusion Prevention) – and monitoring (SIEM – Security Information and Event Management System);
- security Gateways and VPN solution to connect remotely;
- vulnerability management, patching, and secure configuration;
- penetration testing for applications;
- web application Firewall;
- secure coding;
- data is only stored in the EU Data Centers and, in case of laptops, encrypted on the local device.

E. End-user devices are protected

Worldline personnel are working with laptop / desktop on Worldline secured network. Following security measures are incorporated:

- encryption of the hard disk on company assigned laptops;
- 2 Factors Authentication (PKI / Alternative) for remote working;
- centrally managed anti-virus protection, patching, firewall, host intrusion prevention system;
- management and monitoring of the software to control -unauthorized software installation;
- a secure device life cycle management.

F. Remote Access Security

2-factor authentication is used for remote access to the critical Worldline target systems. For Worldline managed systems a VPN (Virtual Private Network) solution is provided to connect to the Worldline network and for the unmanaged systems additionally, a VDI (Virtual Desktop Infrastructure) solution is in place.

Any other set up of connections needs to be upfront approved by the security department.

G. Access control to Personal Data

Personnel with access to personal data can only access the data that are necessary for the purpose of the activities under their responsibility. Access authorization is provided based on the 'least privilege basis" and is either role based or name based. Access logs & audit trails are in place and the responsibility for access control is assigned.

H. Security, confidentiality and availability of personal data

Based on a risk assessment (and if required an additional DPIA) Worldline will ensure a level of security appropriate to the risk, including inter alia as appropriate:

- the anonymization and encryption of Personal Data;
- the ability to ensure the ongoing confidentiality, integrity, availability and resilience of processing systems and services;
- the ability to restore the availability and access to Personal Data in a timely manner in the event of a physical or technical incident;
- a process for regularly testing, assessing and evaluating the effectiveness of technical and organizational measures for ensuring the security of the processing;
- ensure a logical separation of its customer data;
- set up a process to keep processed data accurate and up-to-date;
- keeps records of processing activities according to GDPR;
- unauthorized access detection measures via access log systems;
- customer Data (including back-ups and archives) will only be stored for as long as it serves the purposes for which the data was collected, according to the customers instructions, unless there is a legal or contractual obligation to retain the data for a longer period of time;
- incident management process and incident response plans;
- data breach notification procedure;
- emergency & disaster recovery plans with procedures and allocation of responsibilities in place (backup contingency plan).