Technical and Organizational Measures Worldline Financial Services (Europe) S.A.

(EU EN)

1 Purpose of this Document

This document contains a list of the technical and operational 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 operational measures included in the list below following a Data Protection Impact Assessment. 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

The page also contains a list of subcontractors used by Worldline to deliver its services. Worldline ensures that all its sub processors have provided adequate guarantees on the protection of personal data they process on our behalf by engaging on subcontracting control: there should not be any commissioned data processing within the meaning of GDPR Art. 28 without appropriate instructions from the principal, e.g., clear contract design, formalized subcontracting management, and a strict selection of processors (ISO-certification, ISMS), prior demonstration of competence, follow-up monitoring.
Worldline commits to continuous monitoring the effectiveness of its information safeguards and to a yearly compliance audit by a Third Party to provide assurance on the measures and controls in place.

2 Technical and Organisational Measures

A People, awareness, and HR:

- All recruitments follow a screening process according to the principles of Worldline background check policy;
- In each contract each employee has Non-Disclosure Agreements clauses;
- Code of Ethics awareness training (including a test) is a yearly obligation for all employees and is to be performed through a dedicated e-learning module;
- Group IT Acceptable Use policy or local version, are shared with all employees;
- Security policy statement signed by the Management is shared with all employees;
- Worldline staff is obliged on a yearly basis to follow the Worldline Data Protection policy, Information Security and Safety training (including a test);
- Regular awareness trainings on GDPR for all employees (in addition to Worldline Data Protection policy, Information Security and Safety training);
- Access to systems is provided on a 'need to have basis' taken into account segregation of duties;
- Regular internal security audits are conducted to verify the security practices.

B Physical Security and paper records:

Compliance with the Group Worldline Physical and Environmental Security policy:

- Access control and visitor management systems implemented for all visitors/guests;
- Physical access control (protection against unauthorised access to data processing or storage facilities): particularly by means of kity eys, magnetic or smart cards, electrical door openers, a doorman, security staff, alarm systems, video systems.
- Physical access reviews as per defined periodicity;
- Clean desk, clear screen and follow me printing, process implemented;
- Information, which includes paper documents, handled by the data importer is classified, labelled, protected and handled according to the Worldline information classification policy;
- Except with prior specific authorization, desktops are not taken off the site;
- CCTV surveillance to protect restricted areas;
- Fire alarm and fire-fighting systems implemented for employee safety;
- Fire evacuations drills are conducted at specified frequencies;

C Remote end user device are protected:

The remote users are working with laptop and desktop on Worldline secured network maintained by Global IT for the Worldline Group. Following security measures are incorporated in addition:

- Encryption of the hard disk on company assigned laptops;
- 2 Factors Authentication (PKI/Alternative);
- Centrally managed and anti-virus protection;
- Management and monitoring of the software to control an authorized software installation;
- Login ID and password controls are implemented to access information;
- Periodic access review is implemented;
- E-mails are automatically scanned by anti-virus and anti-spam software.

D Remote Access Security

2-factor authentication is used in general for remote access to the critical Worldline target systems. If the source of the remote connection is a Worldline controlled system then device authentication based on a certificate on the device is implemented.
Any other set up of connections needs to be upfront approved by the security department.

E Generic security measures are a.o.:

- Data is stored in the EU and CH Data Centers or in case of laptops encrypted on the local device;
- Termination of access connection in Demilitarized Zone;
- All connectivity up to the secured area (PCI zone) is encrypted;
- Access to PCI zone only possible via strong authentication via provided security client;
- Multiple layers of firewalls & intrusion detection need to be passed;
- Access managed according to Role Based Access Control principles.
- Privacy management, including regular employee training;
- Incident response management;
- Privacy-friendly default settings;

F Access control to Personal Data

Employees with access to private data can only access the data that are necessary for the purpose of the activities under their responsibility. Access authorisation is provided based on the 'need to know' and 'need to access' and is either role based or name based. Access logs are in place and the responsibility for access control is assigned.

Following measures are in place:

- Obligation for employees to comply with the applicable Worldline and local security policies and data protection policies;
- Work instructions on handling private data;
- Electronic access control (protection against unauthorised use of data processing or storage systems): particularly through passwords (including the corresponding policy), automatic lock mechanisms, two-factor authentication, encryption of data carriers;
- Internal access control (prevention of unauthorised reading, copying, modification or removal of data within Worldline): namely, by using standard-authorisation profiles on a "need to know" basis, a standard process for assigning user rights, access logging, periodic review of the assigned rights, especially of administrator accounts;
- Controlled destruction of data media;
- Procedures for Checking compliance with procedures and work instructions are in place;

G Security and confidentiality 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:

- Classification scheme for data: categorisation of personal data according to the degree of confidentiality based on legal obligations or self-assessment.
- No unauthorised reading, copying, modification or removal during electronic transmission or transport: particularly through encryption and Virtual Private Networks (VPN);
- the ability to ensure the ongoing confidentiality, integrity, availability and resilience of processing systems and services;

- Protection against accidental or intentional destruction or loss, such as backup strategy (online/offline; on-site/off-site), Uninterruptible Power Supply (UPS, diesel generator set), antivirus, firewall, alert channels and emergency plans; security checks on the infrastructure and application levels, multilevel security plan with outsourcing of backups to data backup centres, standard processes in case of change/dismissal of employees;
- 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 organisational measures for ensuring the security of the processing (Internal audit, PCI-DSS, ISO27001, national supervisory institutions).
- Process registers according GDPR requirements
- Access log systems' use with relevant for the purposes of being able to detect unauthorized access attempts
- For the main customer Data and metadate (including back-ups, archives, logfiles, etc.) will only be stored for as long as it serves the purposes for which the data was collected unless there is a legal or contractual obligation to retain the data for a longer period of time.

H Organization control

The Data Processor 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:
Internal data processing policies and procedures, guidelines, work instructions, process descriptions and regulations for programming, testing and release, insofar as they relate to the Personal Data transferred by the Controller;
Implementing a Data Protection control framework that is audited on compliance on a yearly basis;
Having an emergency plan with procedures and allocation of responsibilities in place (backup contingency plan).