Technical and Organisational Measures of Worldline Merchant Services UK Limited

(GBR EN)

1 Purpose of this Document

1.1. This document contains a list of the technical and organisational measures adopted by Worldline to protect Personal Data, which are applicable as standard in providing Acquiring Services. The actual measures taken depend on the specific service and the location of processing concerned given that not all measures are relevant for all services and locations. In any event, Worldline guarantees it has for all services and locations the necessary adequate technical and organisational measures that have been implemented 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; and
- protect against any actual unauthorised processing, loss, use, disclosure or acquisition of or access to any Personal Data.

1.2. Where Worldline uses sub-processors to provide services, Worldline ensures that such sub-processors have provided adequate guarantees on the protection of Personal Data they process on our behalf. Worldline ensures that such sub-processors are subject to a strict selection process, e.g. ISO-certification, prior demonstration of competence and ongoing monitoring through a clear and robust written subcontract.

1.3. Worldline commits to continuous monitoring of the effectiveness of its information safeguards and to an annual compliance audit by a certified third party to provide assurance on the measures and controls in place.

2. Technical and Organisational Measures

2.1. People, Awareness and HR

- All new recruits follow a screening process according to the Worldline background check policy;
- Each employee has confidentiality clauses in their employment contract;
- Code of Ethics awareness training is an annual obligation for all employees. The training and test is performed through a dedicated e-learning module;
- IT Acceptable Use policy implemented and shared with all employees;
- Security policy statement signed by management is shared with all employees;
- All employees are obliged on an annual basis to undertake the Worldline Data Protection policy, Information Security and Safety training (including a test);
- Regular awareness training on GDPR is available 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 taking into account segregation of duties; and
- Regular internal security audits are conducted to verify the security practices.

2.2. Physical Security and Paper Records

- Compliance with the Worldline Group 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 keys, 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 processes implemented;
- Information is classified, labelled, protected and handled according to the Worldline information classification policy;
- Except with prior specific authorisation, desktops are not taken off the site;
- CCTV surveillance to protect restricted areas;
- Fire alarm and fire-fighting systems implemented for employee safety; and
- Fire evacuation drills are conducted at specified frequencies.

2.3. Remote end user devices

- Remote based employees work on Worldline secured network maintained by Global IT;
- Encryption of the hard disk on company assigned laptops;
- Multi-Factor Authentication (PKI/Alternative);
- Centrally managed anti-virus protection;
- Management and monitoring of the software to control an authorised software installation;
- Login ID and password controls are implemented to access information;
- Periodic access review is implemented; and
- E-mails are automatically scanned by anti-virus and anti-spam software.

2.4. Remote access security

- Multi-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; and
- Any other set up of connections needs to be approved in advance by the security department.

2.5. Generic security measures

- Data is stored in data centres located in UK, EU or Switzerland 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 using strong authentication via provided security client;
- Multiple layers of firewalls and intrusion detection need to be passed;
- Access managed according to Role Based Access Control principles;
- Privacy management, including regular employee training;
- Incident response management; and
- Privacy-friendly default settings;

2.6. Access control to Personal Data

- Employees with access to Personal Data can only access the data that are necessary for the purpose of the activities under their responsibility. Access authorisation is provided based on a '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;
- 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, multi-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; and
- Procedures for Checking compliance with procedures and work instructions are in place.

2.7. Security and confidentiality of Personal Data

- Based on a risk assessment (and if required an additional Data Protection Impact Assessment), Worldline will ensure a level of security appropriate to the risk;
- 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 to GDPR requirements;
- Access log systems relevant for the purposes of being able to detect unauthorized access attempts; and
- 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.

2.8. Organisation control

- Worldline maintains its internal organisation in a manner that meets the requirements of the applicable legislation and the requirements on data security;
- 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 data controller;
- Implementing a data protection control framework that is audited on compliance on a yearly basis; and
- Having an emergency plan with procedures and allocation of responsibilities in place (backup contingency plan).