APPENDIX

Information Security Requirements

Contents

1 Purpose

This schedule sets out the minimum security requirements the Supplier shall adopt relevant to the scope of work being undertaken, aiming to protect VodafoneZiggo and its suppliers. Supplier is responsible to ensure ongoing compliance with these requirements and to identify and action any acts or areas of non-compliance. The parties recognize that information security techniques, and the existing threats to security are continually evolving. Therefore, Supplier shall undertake holistic and comprehensive assessments of security depending upon the circumstances and the type of data and processing to be performed in order to determine and apply an appropriate level of protection.

The Supplier shall apply the minimum requirements specified in this schedule in conjunction with any other general security requirements agreed to by the parties (such as any further security requirements as are identified in any pre or post contract security assessment).

These requirements are not intended to be specific to the processing operations undertaken by Supplier on behalf of VodafoneZiggo. Rather, Supplier shall adopt these standards as appropriate standards designed to ensure a secure operating environment generally.

These requirements also apply to all personnel, contractors, temporary employees and third parties employed either directly or indirectly by the Supplier (e.g. subcontractors) and Supplier shall procure that they comply with the requirements outlined herein.

Therefore, the SUPPLIER AGREES:

2 Definitions

In this document, the following words and expressions shall have the following meanings:

Term	**Definition**
4th party	means the Supplier's contractors and their subcontractors (of any tier)
Authorised Users	means employees, officers, directors or contractors of Supplier who have a legitimate operational need and are authorized to access Information Systems or carry out any processing of VodafoneZiggo Information.
Data Record	means any information (in whatever form) created, received and maintained as evidence and as an asset by the company or employee, in pursuit of legal obligations or in the transaction of business.
Incident	means any event which causes an interruption to, or a reduction in the provision of the Service(s) which has an actual impact to the confidentiality, integrity or availability of VodafoneZiggo Information and Information Systems.
Internet facing	means systems or applications that are reachable from the internet without needing to connect to an internal network via a VPN. Cloud assets which are accessible from the internet are to be considered internet facing.
Information Systems	means all systems used to access, store or otherwise process VodafoneZiggo Information, including temporary files.
Media	means a physical object likely to be processed in an Information System and on which data may be recorded or from which they may be retrieved.
Products and Services	means the products and services provided by the Supplier under the Agreement.
Security Breach	means the accidental, unauthorized, or unlawful destruction, loss, alteration, or disclosure of, or access to, VodafoneZiggo Information or Information Systems. For the avoidance of doubt, if any fraudulent act leads to the unauthorized access, disclosure or use of VodafoneZiggo Information or VodafoneZiggo Systems, such act will be considered a Security Breach.
User Identity	means the personal and unique identification code issued to every Authorised User

VodafoneZiggo Information	means data, such as text, audio, video or image files, provided by Supplier in connection with use of the Suppliers' solutions, and data developed at your specific request related to a statement of work or contract.
Personal Data	shall mean any information relating to an identified or identifiable natural person as defined by the Applicable Privacy Law and including the categories of data listed in the Processing Appendix together with any additional such personal data to which the Processor have access from time to time in performing the Services.

3 General

3.1 Compliance

Supplier shall

a) have a process in place to
   i. identify, document and keep up to date all requirements in this Schedule;
   ii. ensure compliance with the requirements as stated in this Schedule;
b) ensure that responsibilities for compliance with these minimum security requirements are clearly defined and documented and have been allocated to individuals with sufficient authority. The individuals shall be suitably trained and experienced in managing security, and shall be provided with appropriate resources to effectively ensure compliance.
c) upon VodafoneZiggo's request, provide independent evidence of its existing certifications as applicable (e.g. ISO27001, ISO 22301, ISAE, SOC2 or SOC3 security risk rating service etc.);
d) upon VodafoneZiggo request, use commercially reasonable endeavours to provide VodafoneZiggo with continuous access to a summary of the security reports generated by the independent security rating service, provided such discloser would not jeopardize Supplier's security posture, at Supplier's own discretion;
e) promptly (i.e. within 48 hours or as otherwise defined in agreed upon SLA's) notify VodafoneZiggo of any Incidents affecting VodafoneZiggo (e.g. business continuity, physical security) including Security Breaches. In the event of a Security Breach, the Supplier shall take responsibility for the corrective and/or mitigating actions and notifications to VodafoneZiggo. Report these to the VodafoneZiggo Security team by sending an email to CSIRT@vodafoneziggo.com.
f) define, allocate and formally document security responsibilities. This information shall be reviewed on a regular basis and updated by Supplier as required to reflect organisational and personnel changes;
g) implement appropriate security measures designed to protect VodafoneZiggo Information from loss, destruction, falsification, unauthorised access and unauthorised release;
h) review the approach to managing security and its implementation (i.e. control objectives, controls, policies, processes and procedures for security) independently at planned intervals or when significant changes occur.

3.2 Incident Response

Supplier shall

a) have a formal and documented Incident management process in place with defined roles and responsibilities;
b) log all Incidents. Supplier shall make these available to all Authorised Users who need them, and shall review them on a regular basis and update them as required in accordance with industry best practice;
c) define, document, implement and maintain a procedure for reporting, responding to and managing Incidents and Security Breaches. This shall include as a minimum:
   i. a procedure for reporting such Incidents and Security Breaches to appropriate management;
   ii. designated role(s) for managing and co-ordinating the response to an Incident or a Security Breach;

iii. a documented process for managing the response to an Incident or a Security Breach, including the requirement to keep appropriate issues and action logs to include the time at which the Incident or Security Breach occurred, the person reporting the Incident or Security Breach, to whom it was reported and the effects thereof;
iv. the requirement on the Supplier to notify VodafoneZiggo promptly (i.e. within 24 hours or as otherwise defined in agreed upon SLA's) if Personal Data was involved in the Incident or Security Breach and was impacted or affected in some way; and
v. the Supplier shall, where appropriate, use commercially reasonable efforts to work together with the VodafoneZiggo's security representatives until the Incident or Security Breach has been satisfactorily resolved.

d) test the procedure for reporting, managing, and responding to Incidents and to Security Breaches on a periodic basis, and shall provide to VodafoneZiggo with confirmation that such tests have taken place upon request.
e) provide a written post Incident/Security Breach report along with a remediation plan including a timetable and actions to be taken.
f) provide such assistance, material or information to support with investigations, as VodafoneZiggo may reasonably require, to all security investigations related to the Incident or Security Breach in connection with the services provided.

4 Organisational measures

4.1 Personnel Security

Supplier shall

a) ensure that security roles and responsibilities of all Supplier employees, contractors and sub-contractors are clearly defined and documented;
b) have a disciplinary process in place, which clearly defines what breaches of security represent misconduct and the consequences that shall be incurred;
c) carry out background verification checks on all existing and new Supplier personnel, in accordance with relevant laws and regulations, which shall be proportional to risks correlated to roles within the Supplier's organization. Supplier shall require its contractors and subcontractors who process VodafoneZiggo Information to conduct background verification checks on their own personnel;
d) inform VodafoneZiggo upon request of its employees' and contractors' responsibilities for security in their contractual agreements;
e) ensure that all Supplier personnel and, where relevant, contractors and subcontractors receive appropriate awareness and training for security policies and procedures, as relevant for their job function;
f) have a comprehensive process in place to ensure that access to VodafoneZiggo Information is revoked and any company assets in the possession of the Supplier personnel are returned back to VodafoneZiggo upon termination of the Agreement.
g) ensure all Supplier personnel performing outsourced network management tasks on behalf of VodafoneZiggo
    i. is known and administered by the organization at name level;
    ii. has undergone an appropriate background check with written confirmation prior to being granted access.

4.2 Physical Security

Supplier shall

a) ensure that responsibilities for physical security are clearly defined and documented and have been allocated to individuals with appropriate role.
b) have a clearly defined and documented physical security policy and procedures in place. The policy and procedures must be reviewed and updated on a periodic basis.
c) design and implement physical security controls to address internal and external risks to premises and information processing facilities. These controls shall be assessed on a periodic basis.

d) define and use security perimeters to protect information processing facilities and locations storing VodafoneZiggo Information;
e) have secure entry points in its premises and information processing facilities from where the services are provided, that restrict access and protect against unauthorised access. Only authorised personnel and approved visitors shall have access.
f) ensure that supplier personnel and approved visitors are issued access identification cards. Visitors' cards must be clearly distinguished from supplier personnel's access identification cards.
g) design and apply reasonable physical protection measures against malicious attack or accidents; where possible, ensure that media, equipment, information or software are not removed from the designated premises without prior approval of the appropriate role.
h) apply security to off-site assets taking into account the different risks of working outside the premises;
i) ensure that all items of equipment containing storage are verified to confirm that any VodafoneZiggo Information and licensed software has been removed or securely overwritten prior to disposal (e.g. at the end of contract, following a hardware failure) or re-use;
j) have a clear desk policy in areas where VodafoneZiggo Information is managed or stored. Any documents containing VodafoneZiggo Information must be securely stored when they are not in use;
k) have a clear screen policy for information processing facilities;
l) ensure that paper documents containing VodafoneZiggo Information are securely transferred.

4.3 Business Continuity Management

Supplier shall
a) ensure that responsibilities for business continuity are clearly defined and documented and have been allocated to individual with appropriate role;
b) have (and ensure that its subcontractors have) a business continuity management programme in place that follow industry-best practices;
c) have a business continuity plan (BCP) in place, which is reviewed and updated regularly designed to ensure the provision of services to VodafoneZiggo in case of an interruption or failure of business processes;
d) ensure that the scope of the business continuity plan encompasses all locations, personnel and information systems used to provide the contractual services to VodafoneZiggo;
e) notify VodafoneZiggo promptly in the event of an interruption which impacts the provision of services to VodafoneZiggo;

4.4 Data Management

Supplier shall
a) treat VodafoneZiggo Information according to Supplier's own information classification policies, and safe-guard it accordingly ensuring that it is not accessible for unauthorized users. .
b) not store, copy, disclose or use VodafoneZiggo Information except as necessary for the performance by the Supplier of its obligations under the Agreement or as otherwise expressly authorised in writing by VodafoneZiggo;
c) monitor the flow of data to subcontractors. If supplier subcontracts any new subcontractors who will access and / or store VodafoneZiggo information, they shall notify VodafoneZiggo in advance of such processing and obtain permission before processing.
d) ensure proper handling and disposal of such information from Supplier systems:
    i. safe disposal of data records must be conducted to ensure that relevant security measures are applied and that any restrictions on manner of destruction, for example security and confidentiality, are not breached;
    ii. physical Data Records must be destroyed in an secure manner
e) ensure that the creation of data is limited to the minimum necessary in the support of VodafoneZiggo, or to comply with legal obligations.

5 Technical Measures

5.1 Information Asset Classification & Handling

Supplier shall

a) define, document, implement and maintain rules for the acceptable use of information and of assets associated with information and information processing facilities, and shall communicate these to all users;
b) define, document, implement and maintain a policy addressing the classification of information in terms of legal requirements, value, criticality and/or sensitivity to unauthorised disclosure or modification, and shall review such policy on a regular basis and update it as required. The methodology used by Supplier to classify the information must consider the risks involved with the loss of confidentiality, integrity and availability of the information;
c) define, document, implement and maintain procedures for information labelling in accordance with the information classification scheme adopted by the Supplier and shall communicate such labelling procedures to users, and - where feasible - shall technically enforce those procedures;
d) where possible, define, document, implement and maintain information classification and labelling covering media, services and systems provided to VodafoneZiggo in accordance with the information classification scheme chosen by Supplier;
e) ensure that media containing VodafoneZiggo Information, and printed copies of this data, maintain the confidential marks, as included by VodafoneZiggo.

5.2 Information Protection

Supplier shall

a) implement appropriate measures designed to protect media containing VodafoneZiggo Information against unauthorised access, misuse or corruption at rest and during transportation;
b) define, document, implement and maintain mechanisms designed to protect equipment when unattended, e.g. through using device locks and password protected screen locks;
c) implement access controls and strong encryption designed to protect information from unauthorised access and modification;
d) implement appropriate measures designed to ensure that media containing VodafoneZiggo Information is only distributed if the data have been strongly encrypted to guarantee that it is not intelligible or is not manipulated in transit;
e) the maximum period for retaining VodafoneZiggo Information recorded shall be specified by Supplier in accordance with the industry best practice, or otherwise as agreed in the Data Processing Agreement;

5.3 Vulnerability Management, Patching and Hardening

In relation to Supplier's internal networks, Supplier shall:

a) define, document, implement and maintain security operating procedures including the management of endpoint protection, antivirus and antimalware, patching and system hardening, and where available, make such procedures available to all users who need them, review them on a regular basis and update them as required in accordance with industry best practice;
b) perform appropriate vulnerability assessments and testing prior to go live of Information Systems and make commercially reasonable efforts to remediate/mitigate any material vulnerabilities prior to go live;
c) protect endpoints, servers, storage devices, mail / web gateways and mail traffic with active anti-malware tools where technically feasible to detect and wherever possible prevent malware infections;
d) define, document, implement and maintain tools and/or processes designed to prevent the (unintended) deterioration of VodafoneZiggo Information's integrity;
e) where and as applicable to a particular Service, define, document, implement and maintain procedures for making back-up copies and for recovering VodafoneZiggo Information. These

procedures shall be intended to guarantee that data files can be reconstructed in the state they were in at the time they were lost or destroyed;

f) define, document, implement and maintain rules governing the installation of software by employees;
g) consistently enforce documented and approved security standards for desktop and laptop clients for new / newly configured client and security settings to prevent end users from changing them on their client;
h) define, document, implement and maintain standards for the secure design, configuration, hardening and management of information systems, networks and services to protect against loss of confidentiality, integrity and availability of VodafoneZiggo Information at rest and in transit;
i) define, document, implement and maintain a procedure that guarantees password confidentiality and integrity and shall store passwords in a way that makes them unintelligible while they remain valid
j) proactively provide relevant security notes and regular patches, and separately to feature releases, new product releases or additional functionalities. Define, document, implement and maintain a vulnerability and issue fixing process including identification, assessment and prioritisation of vulnerabilities. This process shall have defined resolution timelines as of the Supplier being notified. This requirement shall apply to all Products and/or Services impacted by the vulnerability, not only the original Product and/or Service for which the vulnerability was notified:
    a. Emergency (Critical AND 'Zero day' OR actively exploited)
        i. Deploy following an emergency change process jointly agreed with involved Security teams as relevant, yet never exceeding 7 calendar days.
    b. Critical (CVSS score 9.0-10.0):
        i. Deploy without undue delay, yet never exceeding 30 calendar days.
    c. High risk (CVSS score 7.0-8.9):
        i. Internet-facing systems*: 30 calendar days
        ii. Other systems: 90 calendar days
    d. Medium risk (CVSS score 4.0-6.9):
        i. Internet-facing systems*: 90 calendar days
        ii. Other systems: 180 days
    e. Low risk (CVSS score 0.1-3.9): remediation by software updates; next lifecycle software update or release.

    * Definition internet facing: 'means systems or applications that are reachable from the internet without needing to connect to an internal network via a VPN. Cloud assets which are accessible from the internet are to be considered internet facing'.

5.4 Identity & Access Management

Supplier shall:

a) define, document, implement and maintain a process covering the formal registration of users with a unique identity as prerequisite for granting any access to the user, and de-registration of users in order to support the timely revocation of access rights;
b) define, document, implement and maintain a formal process for where the use of functional accounts (used by systems / applications) or shared accounts (used by multiple individuals) are necessary for business or operational reasons to supply services, and shall maintain the documentation and assignment of a responsible owner;
c) define, document, implement and maintain a formal process for granting, modifying and revoking user access rights;
d) implement appropriate measures designed to ensure that all access rights and identities of all staff, contractors and external party users shall be reviewed by responsible management upon change of their role, adjusted / removed as required and are locked or removed upon termination of their employment, contract or agreement in a timely manner;
e) monitor accounts remaining inactive or dormant and these may be suspended as a result of Supplier's account review process, review user identities and user access rights on a regular basis, to confirm that they continue to be still required;

f) control the process of granting and provisioning privileged access and assign it only to an administrative account or a separate account different from that used for regular business activities;
g) keep an up-to-date record of Authorised Users, and the authorised access available to each, and shall establish identification and authentication procedures for all access to Information Systems or for carrying out any processing of VodafoneZiggo Information;
h) implement appropriate measures designed to restrict access to VodafoneZiggo Information and application system functions by a secure log-on procedure which meets at minimum the following requirements:
    i. the use of passwords which are compliant with Supplier's password policies is enforced by Supplier;
    ii. passwords shall consist of at least eight characters, or, if this is not technically permitted by the relevant Information System, a password shall consist of the maximum permitted number of characters.
    iii. passwords shall be modified by the Authorised User to a secret value known only to the Authorised User when it is first used;
    iv. passwords aren't displayed while being entered and aren't transmitted in clear text over a network;
    v. log-on information is validated only on completion of all input data;
    vi. accounts are actively monitored and where appropriate locked or blocked for a period of time after a number of successive unsuccessful log-on attempts;
    vii. unsuccessful and successful attempts are being logged and security events are raised if a potential attempt or successful breach of log-on controls is detected;
    viii. inactive sessions are terminated or locked after a defined period of inactivity.

5.5 Software Development

Supplier shall
a) implement appropriate measures designed to ensure software development is executed in line with a best practice Secure Software Development Life-Cycle (SSDLC). It is ensured that development, test, and production environments are separated to reduce the risks of unauthorised access or changes to production data.
b) undertake any testing in non-production environments for services supplied to VodafoneZiggo. Supplier shall not use VodafoneZiggo Information for testing purposes. If such use is necessary and there is no reasonable alternative, Supplier shall obtain VodafoneZiggo's prior written consent for testing with VodafoneZiggo Information, and such use shall be limited to the extent necessary for the purposes of testing and Supplier guarantees the level of security corresponding to the type of VodafoneZiggo Information processed;
c) implement appropriate measures designed to ensure that information security related requirements are included in the requirements for new Information Systems or enhancements to existing Information Systems;
d) control changes to systems within the development lifecycle by formal change control procedures;

5.6 Network Security

Where and as applicable, Supplier shall
a) define, document, implement and maintain strong encryption and security configuration standards to secure communication over the network across the relevant network elements;
b) implement appropriate measures designed to ensure that changes to firewall rule bases are controlled through a formal request / approval process;
c) restrict access to the organisation's networks to authorised devices and control this using digital certificates;
d) define, document, implement and maintain a policy and supporting security measures to protect information accessed, processed or stored at teleworking sites;
e) define, document, implement and maintain two factor authentication on endpoints / mobile devices which can be used to access services, systems and networks from the Internet as well as for the Internet facing services;

5.7 Security Logging & Monitoring

Supplier shall

a) define, document, implement and maintain security operating procedures including but not limited to the management of security event logging and monitoring.
b) make relevant logs available to users who need them, and shall review them on a regular basis in accordance with industry best practice;

6 Supplier & External Party Security

Supplier shall
a) define, document, implement and maintain information security requirements for mitigating the risks associated with Supplier's own external supplier's access to processing or hosting assets or provision of IT infrastructure;
b) include information security requirements in agreements with its suppliers;
c) include an obligation of prompt notification of Security Breach(es) in agreements with its suppliers;
d) Include the right to monitor, review and audit its suppliers' service delivery on a regular basis, in agreements with its suppliers;
e) manage the changes to the provision of services by Suppliers' suppliers, taking account of the criticality of business information, systems and processes involved and re-assessment of risks.

7 End of Services / Change of Contract

a) When the Services include processing of, access to or hosting of VodafoneZiggo Information and are due to cease as a result of a contract expiring or change of service Supplier shall, as a matter of course or upon VodafoneZiggo's written request;
    i. agree on the arrangements for the secure return, destruction or retention of the VodafoneZiggo Information, hardware and media;
    ii. provide evidence that each of these actions was completed as required.

8 Right to Audit

a) Supplier shall permit VodafoneZiggo or a mutually agreed upon independent auditor (each an "Auditing Party") the right to perform an (on-site) audit at a Supplier facility, at VodafoneZiggo's sole expense, to check that Supplier is complying with the security requirements under this schedule. Except for audits by a government agency, VodafoneZiggo must provide at least 6 weeks advice written notice and such on-site audit will be limited to a maximum of once per year. Before the commencement of such audit, the parties will agree on the scope, location, date, duration and manner of such audit.
b) Any audit in accordance with this paragraph shall not require the review of any third party data and the Auditing Party may be required to enter into a confidentiality agreement with Supplier as may be reasonably necessary to respect the confidentiality of the information of which the Auditing Party may become aware in the course of undertaking the audit. Each Party shall bear its own costs in relation to such audit, unless the audit reveals a material non-compliance with Supplier's obligations under this schedule, in which case Supplier shall reimburse VodafoneZiggo for all third party auditor fees incurred by VodafoneZiggo.

End of document.