Data Privacy Framework

Table of Contents

Terms and Terminologies

The following terms and terminologies shall help you read this document better

DPO: Data Privacy Officer

CITS: Corporate IT Services

Information Processor: The person who processes the data or has authorized the processing of the data

ISSC - Information Security Steering Committee

ISSD: Information Systems Security Department

CDU / CFU – Client Delivery Units / Client Facing Units

User or Users: Indicates all people who come under the coverage of this policy including employees, contractors, 3rd party workers

Introduction

Onmobile understands the importance of protecting the personal data from possible events or causes and maintain the privacy of such personal data. Taking into consideration the international nature of Onmobile's business activities, Onmobile has decided to have a framework to be compliant with the provisions of the Spanish Data Protection Laws

The ISMS at OnMObile consists of a system of internal controls to safeguard these information assets, including personal data covered under the relevant Data Privacy laws. The Information Security Steering Committee coordinates the Information Systems Security Department (ISSD), responsible for devising policies and overseeing the implementation of the ISMS for the protection of these information assets. The responsibility for ensuring the continued viability of business by protecting these business critical assets is shared by all the employees.

The ISMS manual explains the structure, phases and functions within these phases of the ISMS along with the associated mandatory procedures, documents and records.

2. Scope & Definitions

2.1 Scope of the Data Privacy Framework

Scope of Data Privacy Framework is limited to Onmobile Global Espana SL offices located in Spain.

2.2 Definitions

Terms which are used in the relevant Spanish Data Privacy Laws are used here, the definitions provided in such Data Privacy laws are applied.

In particular, the Data Privacy Framework is defined as the part (which includes organisational structure, policies, planning activities, plans, responsibilities, working practices, procedures, processes and resources) of Onmobile's overall management system which, based on operational risk approach, enables leadership to establish, implement, operate, monitor, review, maintain and improve Data Privacy measures within the Organization.

3. Security Organization & Responsibilities

3.1 Security Organization

Data Privacy is a business responsibility shared by all members of the management team. Senior management shall see to it that there is a clear direction and visible management support for Data Privacy initiatives at Onmobile. It is the responsibility of Onmobile senior management to

- Ensure that data privacy is practiced across the organisation
- Establish a strong security organisation structure with clear roles and responsibilities

- Provide adequate resources for establishing, implementing and reviewing the security practices at Onmobile
- Identify and appoint Data Privacy Officer, accountable to the senior management and to co-ordinate the implementation of the data privacy controls

ISSC shall ensure that, DPO shall be responsible for ensuring that, all the employees in the organisation are well aware about the importance / security of the personal information they are handling and or communicating. Any employee can raise a security incident on data privacy security threat and weakness and the same is forwarded to Information Security Incident Management Team (ISIMT) / Information Systems Security Department to initiate the corrective action to eliminate the problem.

Other dynamic / virtual teams like business continuity (BCP) implementation team, Emergency Response team and Information Security Incident Management Team will be formulated on a need basis and will be reporting to DPO.

3.2 ISSC (Information Security Steering Committee)

The responsibility of Information Security Steering Committee (ISSC) follows:

- Help in reviewing and publishing Data Privacy Policy;
- Oversee the implementation of security controls and classification mechanisms;
- Appoint one or more individuals to be in charge of coordinating and controlling compliance with the measures specified in the security brief.
- Support organization-wide data privacy initiatives;
- Reviewing data privacy incidents;
- Help ISSD in data privacy policy implementation;
- Coordinate with ISSD for conducting periodic data privacy awareness trainings;
- Co-ordinate with various departments to develop and implement data privacy policies and solutions;
- Closely work with senior management, users and external agencies to ensure suitable level of protection for personal data.
- Ensure the importance of Data Privacy is well penetrated into the organization by spearheading training and awareness initiatives.
- Identification and appointment of one or more security officers responsible for the implementation of security measures.
- Periodic Control of compliance with Security Protocol.
- Description of measures to be adopted in the event of re-use or destruction of physical file support.
- Prepare a document containing Scope, Measures, norms, security procedures, rules and security standards in accordance with the provisions of Royal Decree, Tasks and obligations of personnel processing data, Structure and description of files and IT systems, Notification procedures, incident management and incident response protocols, Back up procedures, copy and recovery protocols, Identification of data processor
- The ISSC will approve and endorse all data privacy initiatives in the organization.

- To define procedures and processes for updating the list of users and authorised access to database, ID and verification of ID protocols, access criteria, assignment of passwords and their periodic replacement, encrypted storage of passwords.
- Record any incident (type, time, person notifying the incident, persons receiving communication of the incident and consequences of the incident) relating to data privacy.
- Permits and obligations are clearly defined and supported by documents.
- Closely work with senior management (Onmobile Global Ltd.), users and external agencies to ensure suitable level of protection for information security objectives & Information assets.

3.3 GNOC Operations Enablement Department

The GNOC Operations Enablement Department is responsible for the Data Privacy initiative for the Client Facing Units in Onmobile. Broadly it has the following responsibilities:

- Define, implement & evangelize organizational security policy
- On a periodic basis, and at least once in two years, audit and review vulnerabilities pertaining to data privacy security measures, identify causes or events and evaluate the level of risk if the causes or events affect the business objectives and communicate the same to the Data Controller.
- Ensure that the level of security for accesss through networks is equivalent to that applicable to local access.
- Conduct Data Privacy tests periodically to ensure that level of security adequate for the type of file subject to test is not impaired.
- Verify the definition and implementation of the recovery and copy protocols every 6 months.
- Identify the nature of the information stored held.
- Ensure that no recovery of data is done without data controller authorization.

- Ensure that every user accesses data and resources which are strictly necessary to perform that user's function and this shall be kept through a record and also implement mechanisms for the prevention of access to databases or sources which are not authorised.
- Ensure that only authorised personnel appointed in the security document can grant and/or alter access rights of staff.
- Ensure that even external contractors are bound by the protocol at par with internal employees.
- Setting up procedures to allow for the unequivocal and personalized identification of every user and for ID verification and only limited number of attempts for non-authorised access.
- Prepare a Security document in line with the requirements of the relevant data privacy laws.
- Documenting and recording of data recovery procedures, person implementing such procedures, registration of data restored and data manually stored.
- Written authorisation of the person responsible for the file to implement file recovery.
- Ensure that procedures and processes including those for updating the list of users and authorised access to database, ID and verification of ID protocols, access criteria, assignment of passwords and their periodic replacement, encrypted storage of passwords set by the ISSC are adhered to.
- Educating personnel on the required norms and of the consequences of the failure to comply with them.

- Evaluate implementation of new systems and processes towards improving Information Security
- Work with various departments for an effective business continuity plan in the event of a disaster.
- Monitor and review the progress of Data Privacy on a periodic basis and suggest improvements
- Managing Data Privacy related incidents and communicate with all the relevant stake holders including BU Heads, Directors etc.

3.4 DPO (Data Privacy Officer)

Apart from the below functions as a Data Privacy Officer, the DPO shall also be responsible for the functions and responsibilities of GNOC Operations Enablement Department mentioned above with respect to personal data concerning the Corporate functions at OnMobile: -

- Data Privacy Officer (DPO) is to provide technology vision and leadership for developing and implementing Information Security initiatives that create and maintain leadership for the enterprise in a constantly changing and intensely competitive marketplace. CISO has overall responsibility for information security matters.
- The DPO should ensure the reconstruction of data in the same status as it was when the loss or destruction occurred.
- The DPO shall ensure that at least one back up copy of the personal data is made per week and the storage of all personal data has restricted access to the authorised individuals only.
- The DPO shall be responsible for maintaining inventory of systems, including recording the details of the incoming and outgoing data storage devices, and any outgoing data storage devices should be authorised only by the person responsible for the storage device.
- The DPO shall be further responsible for ensuring that the transfer of systems should be planned to avoid security breaches and unauthorised access and where a storage device which is going to be rejected or recycled necessary measures are implemented to prevent recovery of information from.
- The DPO shall ensure that the physical access to the location where data are stored is controlled and restricted.
- Ensure that procedures and processes including those for updating the list of users and authorised access to database, ID and verification of ID protocols, access criteria, assignment of passwords and their periodic replacement, encrypted storage of passwords set by the ISSC are adhered to.
- The DPO role in information security is to communicate to the ISSC and the senior management the business risks of implementing new and distributed technology and the necessity for developing the appropriate security infrastructure.
- Co-ordinate with various groups & departments to develop and implement information security policies and solutions.
- Ensure the importance of Data Privacy is well penetrated into the organization by spearheading training and awareness Initiatives.
- Representing Onmobile with respect to inquiries from customers, partners, and the general public regarding the organizations security strategy.
- Representing Onmobile when dealing with law enforcement agencies while pursuing the sources of network attacks and information theft by employees.

- Balancing security needs with the organizations strategic business plan, identify risk factors, and determine solutions to both.
- Ensure that security policies and procedures provide adequate business protection without interfering with core business requirements.

3.5 Business Continuity & Emergency Response Team

Mentioned below are the responsibilities of the BC & ERT members:

- Actively participate in all phases of the BCP project from requirements gathering to implementation and sign off.
- Assist business functions in conducting the business impact analysis
- Assist in implementing recovery strategies and options, and assist with the implementation of recovery solutions.
- Coordinate in BCP testing exercises
- Report the BCP status of business functions to CISO/BCMS Manager
- Provide expertise and support to management and business functional areas, as requested, during disruptions
- Initiate initial response actions if they are the first person on the scene
- Restrict access to the incident scene and surrounding area as the situation demands

3.6 Security Incident Response Team

Mentioned below are some of the responsibilities of Security Incident Response Team:

- The team comprises of the personnel from ISSD and ISSC. One or more team members, depending on the magnitude of the incidents and availability of personnel, will then handle the incidents
- Information Security Incident Management Team should be available for contact by anyone who discovers or suspects that an incident has occurred
- Information Security Incident Management Team will be reporting to DPO
- Responsible for Receive, Filter, Validate, Register, Assign, Resolve and Close the incidents

3.7 Internal Audit Team

Major roles and responsibilities of internal audit team are summarized as below:

- Evaluates and provides reasonable assurance that risk management, control, and governance systems are functioning as intended and will enable the organization's objectives and goals to be met
- Reports risk management issues and internal controls deficiencies identified directly to the senior management and provides recommendations for improving the organization's operations, in terms of both efficient and effective performance
- Evaluates information security and associated risk exposures
- Evaluates regulatory compliance program with consultation from legal counsel
- Evaluates the organization's readiness in case of business interruption

- Maintains open communication with management and the audit committee
- Teams with other internal and external resources as appropriate
- Engages in continuous education and staff development
- Provides support to the company's anti-fraud programs.

4. Documentation

Onmobile's Data Privacy documentation consists of various groups or 'Levels' or levels as it is generally called in the document:

- The grouping of documents in levels is relative to their degree of importance in Data Privacy framework and is coined for their easy maintenance and handling. The numerical representation depicts the level of importance of the document.
- The scope of Data Privacy framework & manual, Data Privacy policies, risk management methodology and the SOA (separate, version controlled documents). These documents are the Level-1 Data Privacy documentation for Onmobile. The control objectives described in SOA are achieved by controls that include policies and procedures.
- The separate, version controlled risk assessment and risk treatment plan, whose preparation follows the methodology described in Risk Assessment Methodology.
- Those procedures, which describe how the policies are implemented, are the Level 2 documents.
- Work Instructions or technical procedures which set out specific requirements for the performance or execution of specific tasks, including for the measurement of the effectiveness of the controls, in Onmobile generally and in the operations and CITS specifically, and which are identified in procedures, and similar documents, such as Backup & Restore, user access management, and job descriptions, are Level 3 documentation.
- Records of the Onmobile's control of its Data Privacy processes, including details of audits, security incidents and management reviews, are the fourth level of documentation.

4.1 Authorization Levels

- By approving this document, the ISSC confirms their approval on the said document authorization levels ownership of which cannot be delegated.
- The Information Security Steering Committee (ISSC) has ultimate authority over the Data Privacy policy and approves and authorises all changes to the policy, the Statement of Applicability, the manual and any separate policy statements (level 1 documents).
- The Data Privacy Officer (DPO) has lead executive authority for information security and works with the ISSC to approve, authorise and issue all level 2 documents.
- The DPO and respective BU heads approve and authorize level 3 documents owned by individuals or entities in their areas of responsibility. Any data privacy documents personally owned by business functions have to be approved and authorised by the DPO.
- Access rights are specified in access control procedures. Access rights are personal, are set out in individual User Agreements and cannot be delegated.

Onmobile has a documented record control procedure which defines the controls for identification, storage, protection, retention time and disposal of records. Documents are available to those who need and are authorised to access them in line with these requirements.

5. Risk Management

Onmobile's approach to risk, which has been specifically approved and authorised by management, is contained in a separate, version controlled, Risk Management Methodology which it applies to its overall ISMS planning process. The risk management procedure is designed to identify and assess Data Privacy risk, to identify and evaluate options for the treatment of those risks, and to select control objectives and controls that will reduce those risks to acceptable levels within the context of organization.

5.1 Information security risk management

- Controls which are required to meet contractual, legal or regulatory requirements are identified at the point of identifying requirements of interested parties, and these controls are implemented.
- Onmobile has established and maintains its ISMS, and identifies and assesses information related risks, and evaluates options for their treatment, within the context of the risk management framework and performs risk assessments in line with Risk Management Methodology, using the customised Risk Assessment spread sheets.
- All control objectives and controls adopted are documented in the Statement of Applicability.
- A consolidated risk treatment plan is formulated to implement selected controls.
- The implementation is reviewed for effectiveness and, where possible, improvements are identified and these, within the context of the overall ISMS, are implemented, using a process of continual improvement.
- This process is followed irrespective of whether a single risk is being considered, or multiple risks.

5.2 Risk assessment

Onmobile's method for risk assessment is via customized risk assessment spread sheet and procedure document. This is suitable for the scope of Onmobile's ISMS, the objectives, the security, contractual obligations, legal and regulatory requirements and risk management framework that were identified earlier. The selection criteria are set out in Risk Assessment Tool.

5.3 Systematic approach to risk assessment

- Onmobile has documented its framework, tool and methodology for risk assessment.

5.4 Preparing Statement of Applicability

- The control objectives and controls selected as a result of carrying out risk management procedures are documented in a Statement of Applicability, which is made available as a separate, stand-alone document in support of the ISO27001 compliance certificate.
- Controls or control objectives in Annex A of ISO27001:2013 are documented, whether included or excluded on the basis of the risk assessment, together with the justification for their inclusion or exclusion.
- The remaining residual risks are highlighted in the risk treatment plan as required by Risk Management Framework, approved by the risk owners, and management authorisation is obtained for implementation of the ISMS.

- Any changes to the risk treatment plan, which lead to a change in the ISMS, are subject to authorisation by ISSC.

6. Management Reviews

The commitment to Data Privacy is further demonstrated and strengthened by periodic senior management reviews. Reviews shall be conducted at least once in 3 months, formally, or informally with the objective of ensuring the suitability, adequacy and effectiveness of the ISMS. This review shall include assessing opportunities for improvement and the need for changes to the ISMS also including data privacy. The inputs to the review shall cover the following: (wherever applicable)

The management review shall include consideration of:

a) The status of actions from previous management reviews;
b) Changes in external and internal issues that are relevant to the information security management system;
c) feedback on the information security performance, including trends in:
    a. nonconformities and corrective actions;
    b. monitoring and measurement results;
    c. audit results; and
    d. fulfilment of information security objectives;
d) feedback from interested parties;
e) results of risk assessment and status of risk treatment plan; and
f) Opportunities for continual improvement;
g) Recommendations for improvement;
h) Audit calendar for the next cycle, including any new functions to be added in scope.

The outputs of the management review shall include decisions related to continual improvement opportunities and any needs for changes to the information security management system.

The output of the senior management reviews shall include any decisions and actions related to the following:

a) Up dated risk assessment and risk treatment plan
b) Improvement of the effectiveness of the ISMS
c) Modification of procedures and controls that affect information security, as necessary, to respond to internal or external events that may impact on the ISMS, including changes to:
    a. Security requirements
    b. Business requirements
    c. Business processes that have an effect on existing business requirements
    d. Regulatory or legal requirements
    e. Contractual obligations; and
    f. Levels of risks and /or criteria for accepting risks.
d) Resource needs
e) Improvement to how the effectiveness of controls is being measured.