Information Security, Privacy and Personal Data Protection Policy

Revision History

Version	Reference	Author	Date	Comments
1.0		Luis Rodeia	01-08-2018	First Version

Know the unknown

Contents

1. Introduction

This document describes WeDo Technologies' Information Security Management System.

Nowadays the benefits of using Information Technologies (IT) in the organizations are undeniable. Their use makes it possible to accelerate the business strategies through new services, processes and costs optimization. However, there are also associated risks, in particular related to information security, that need to be managed.

2. Information Security Policy

Information is one of the most critical assets of an organization. With the generalization of information technologies and, in particular, of the Internet the volume of digital information has been increasing in an exponentially way over the last years.

The protection of information is therefore of vital importance, so that the trust among the several business partners may be maintained and solidified.

The availability, integrity and confidentiality of information, in a rigorous and expedite way, to support business decisions has become a competitive advantage for organizations.

If the information of an organization, including Personal Data, is disclosed, manipulated or made unavailable, the consequences can be serious and create an impact in the organization´s reputation and performance.

WeDo top management is committed to maintain the continual improvement of the information security management system. The information security should be monitored as a dynamic process, so that it is possible to predict and react to information security threats.

Information Security Policy can be defined as the preservation of:

1. Confidentiality: assure that information is accessible to authorized personnel only;
2. Integrity: safeguard the correctness and completeness of information and processing methods;
3. Availability: assure that authorized users have access to information and associated assets when required.

WeDo defined four objectives to ensure that all information assets have the required protection and specifies the control objectives that should be seen as a regulatory requirement:

Objective 1:
Integrate Information Security in the business objectives of WeDo, as a distinguishable and competitive factor;

Objective 2:
Ensure compliance with industry and legal requirements in all countries where WeDo develops business;

Objective 3:
Ensure business continuity always keeping the highest levels of service quality;

Objective 4:

Promote within staff members a culture of responsibility and accountability for Information Security;

WeDo follows security best practices as defined in the General Data Protection Regulation.

This Security Policy applies to WEDO, in all of its organization. Therefore, WEDO defined a general set of policies, which assures information security, including personal data:

- Backups Policy;
- Acceptable Use of Assets;
- Cryptography;
- Information Transfer;
- Clear Desk and Screen Policy;
- Passwords Policy;
- IT_Helpdesk_Facilities_Policy;
- WeDo Site Data Protection, Privacy and Cookies Policy.

WeDo Technologies is ISO 27001 certified for a subset of our services, which scope is:

The Information Security System for Managed Services Process related with WeDo Braga and Wedo Madrid and SaaS CLOUD in WeDo Braga.

3. Privacy and Personal Data Protection Policy

The protection of privacy and personal data of all persons who somehow relate to WeDo (clients, users of the services, employees, partners and others) is a fundamental commitment of our Company. Personal data is essential for the activity of WeDo, in particular, for the marketing of its products and services, for the provision, monitoring and improvement of the quality of the services made available by WeDo, for the management of WeDo's human resources and for the fulfilment of legal obligations, with the challenges that are associated to the processing of personal data for the said purposes being very strongly influenced by the technological, economic and social developments.

Our commitment is to work every day in order to ensure the privacy and protection of personal data for which we are responsible in compliance with the applicable legislation, regulations and guidelines on such matters.

This commitment is executed, namely, by the adoption and implementation of policies and standards of privacy, including, for that purpose, the Privacy Policy of the Company, as well as our Information Security Policy.

In order to better carry out our commitment, we have appointed a Data Protection Officer (DPO), which is responsible for advising WeDo, monitoring WeDo's compliance of the personal data processing with the said policies and standards, as well as applicable law, and is the point of contact for the Data Subject and the relevant Supervisory Authority.
In addition, WeDo have a security team within the organization responsible for, among other aspects, the maintenance, development and supervision of information security, policies and standards, as well as security awareness through training and communication.
With this Statement of Commitment, we want to make clear WeDo's commitment to privacy, security and personal data protection and ensure that all those processing personal data under their relationship with WeDo are bound and act in accordance with the underlying principles.

Personal Data Processing Principles and Data Subjects Rights

The processing of personal data by our Company complies with the following fundamental principles:

- Lawfulness principle
- Purpose limitation principle
- Transparency principle
- Adequacy and data minimisation principle
- Need to know principle
- Integrity and confidentiality principle
- Privacy by design and by default principle

In addition to complying with the said applicable principles, WeDo is committed to ensure the respect of Data Subjects rights, in particular, the right of access and information to personal data being processed by WeDo, the right to rectification, the right to erasure ("right to be forgotten"), the right to data portability, the right to restriction of processing, the right to withdraw consent, the right to object, the right not to be subject to a decision based solely on automated processing, including profiling, and the right to lodge a complaint.

A) Lawfulness principle

The personal data will be processed only if and to the extent that it is grounded on one of the conditions laid down for lawfulness, namely (i) when consent is given by the Data Subject or when the processing is necessary for (ii) the performance of a contract to which the Data Subject is a party, (iii) compliance with a legal obligation, or (iv) the purposes of the legitimate interests pursued by WeDo or by a third party.

B) Purpose limitation principle

The personal data will be processed exclusively for the purposes that determined its collection and will only be processed when legally permitted and by providing the due information to the corresponding Data Subject.

C) Transparency principle

Data subjects will be informed in a clear and concise way of the relevant aspects related to the processing of their personal data, namely, regarding the processing purposes and possible transmission to third parties.

D) Adequacy and data minimisation principle

Only personal data that is adequate, relevant and limited to the necessary personal data for the relevant purposes will be processed and for the time strictly necessary.

E) Need to know principle

Only employees and partners of WeDo whose functions require it will have access to the relevant personal data processed.

F) Integrity and confidentiality principle

The personal data will be processed in such a way as to guarantee its security, namely, (i) protected against unlawful or unauthorized access or disclosure, (ii) protected against unauthorized modification, loss or destruction of personal data or accidental loss of such personal data, and (iii) ensured that personal data will be available when necessary and permitted, without undue delay.

G) Privacy by design and by default principle

WeDo's products and services, their support systems, and their procedures will be developed with the concern of protecting your privacy and personal data.

Personal Data Protection

WeDo respects best practices in the field of protection of personal data and information, and has adopted a program of policies and standards to ensure confidentiality, integrity and availability of the information it is dealing with and that is under its responsibility, which is known to all employees and partners of WeDo.
Wedo's Information Security Policy establishes a wide range of set of technical and organizational measures, organized in several security areas, including:

(i) **Logical security measures**, such as the use of firewalls and detection of intrusion, the existence of a policy of access to information and logging;

(ii) **Physical/organizational security measures**, among which a strict access control to the physical installations of our Company, by employees, partners and visitors, as well as very restricted access, permanently monitored, to the essential technological infrastructures of our Company;

(iii) **Other measures** such as masking, encryption, pseudonymization and anonymization of personal data, as well as a set of measures which aim to execute the principle of privacy by design and by default. Where WeDo uses subcontractors or third parties, WeDo will assure that its subcontractors and third parties are be bound by obligations in order to comply with the applicable legislation and security measures considered necessary by WeDo for the relevant purposes, as well as to ensure that: (i) the sharing of personal data obeys the applicable laws as amended from time to time, (ii) the transmission is securely made, and that (iii) the subcontractors or third parties are contractually obliged to observe confidentiality duties and to ensure the security of personal data, which, to that end, may

be transmitted to them, with the restriction not to be able to use such data for any other purpose, for their own benefit or that of third parties, nor to correlate them with other data that is in the said subcontractors and third parties possession.

Compliance with information security policies, security standards and protection of personal data is subject to periodical scrutiny, audit and control, complemented by a demanding program of information and training of WeDo's employees and partners.