

## PRIVACY AND DATA SECURITY POLICY

The **MULTISOFT Information Technology Services Limited Liability Company** (seat: 1115 Budapest, Bartók Béla út 105-113.; whose records are held at the Budapest Municipal Court as Court of Registration under No. 01-09-161858) – hereinafter: **Company** – under Section (6)(1) of Act CXIX of 1995 on the Use of Names and Addresses for Purposes of Research and Direct Marketing, as well as for the purposes of ensuring protection and security of client data collected during its software development activity formulated the following internal data protection and data security policy - hereinafter: Data Privacy Policy - forming the unseparable **Schedule 1** of the Company's Data Processing Policy (hereinafter: **Data Processing Policy**).

### I. GENERAL PROVISIONS

1. The Company provides among others direct marketing within the framework of activities, - including promotional activities (sending newsletters and advertisement newsletters, calls to participate in giveaways, offering products/services) and telemarketing/telesales activities - to that end handling company names and residential address data (contact details), as well as personal data.

2. Computer programming (software development) is also an activity of the Company, during which client data may be transferred to the Company in relation to carrying out this activity.

3. Data processing is carried out in compliance with the General Data Protection Rule No. (EU) 679/2016 of the European Parliament and the Council, Act CXII of 2011 on the Informational Self-determination and Freedom of Information (hereinafter: **Info Act**), as well as the provisions of Act CXIX of 1995 on the Use of Name and Address Information Serving the Purposes of Research and Direct Marketing, in addition to this Privacy Policy and Data Processing policy established within the framework of these regulations

4. Pursuant to the Data Privacy Policy **data** shall mean exclusively personal information, and **Client Data** shall mean data information forwarded by the contractual partners of the company in the course and for the purposes of the software development activity to the Company. Terms not defined in the data privacy policy should be interpreted according to the provisions of the regulations referred to in above Section I (3).

5. The Company ensures that data are collected and used in a fair and lawful manner.

6. The Company shall process such data

- for the purpose specified in the Data Processing Policy, thus for marketing or direct marketing activities,
- and the Client Data in the course of their software development activity performed for their contractual partners exclusively in the interest of carrying out software development activity (hereinafter jointly: **activity or activities**) in accordance with them, in addition to be allowed to process only data, which are required and suitable for such respective activities. Data processing is allowed exclusively to the extent required for the purposes of carrying out the respective activity and in the case of Client Data with respect to the software development activity

specified in the respective contract for the duration necessary for performing the software development activity under the respective contract.

7. The Company will ensure that no unauthorized persons have access to the data. The Company will handle the data confidentially, - with regard to Client Data not including the contractual partners in the respective contract concluded in the subject matter of the software development activity -, may not divulge any details of or allow them to be seen by third persons, furthermore they can make copies of them exclusively under the provisions of this privacy policy.

8. Access to data will be granted by the Company exclusively to employees, or persons working under any other arrangement who by virtue of their duties are authorized and obligated to

- carry out activities, and/or
- operate the server hosting data.

9. During data handling attention should be paid to data integrity.

10. In the event the process of activities changes or otherwise warranted by circumstances influencing the performance of activities, the company will - as required - amend this data protection and the data processing policy accordingly.

## **II. TECHNICAL MEASURES FOR DATA PROTECTION**

1. The Company shall store data on password protected servers or also in password protected CRM databases ensuring that they are displayed only on password protected work stations.

2./a. The Company shall provide for the physical protection of the data-hosting server by using premises equipped with security locks (server rooms). The entrance of the premise dedicated to safeguard the server (server room) can only be accessed after entering the building of the company's seat, any other doors and windows will prevent forced entry using generally accepted methods. The seat of the company is located in an office building with 24-hour concierge and equipped with an alarm system. There is one designated person at the company authorized to use the keys to the server room. At the same time, the Company designates a substitute person to use the keys should the person in care of the keys be unable to perform this duty for any reason. The keys can be handed over exclusively in this latter case, to the identified substitute person with the purpose of handling the keys.

2. b. In addition to this, the Company uses cloud services to store data, where access is also password-protected.

3. To prevent any unauthorized person from accessing the IT assets storing data accessible through networks all IT/information technology tools available at all times should be utilized.

4. Data may only be accessed or displayed by the persons specified in above Section 1(8) of this data privacy policy using the IT devices provided for their personal use by the company.

5. The Company shall provide the conditions of anti-virus protection regarding the IT assets referred to in Section II (4) of this data privacy policy. The persons identified in above Section I (8) of this data privacy policy are obligated to continuously take care of the anti-virus protection of the IT devices for their personal use.

6. The Company by sustaining and maintaining the actually available IT asset park shall ensure their availability and load capacity required for the software development activity as per contract.

7. The erasure of electronically stored data will be performed by final deletion.

### **III. ORGANISATIONAL MEASURES FOR DATA PROTECTION AND SECURITY**

1. The Company will grant data access exclusively for employees, or who work for them under any other arrangement and who due to their duties are authorized and obligated to have access to such data

- to perform their respective activities, they need to have access to data pertaining to given activity, as well as to persons, who
- operate the server hosting data.

2. Persons specified under Section I (8) of this data privacy policy are obligated to take all expectable measures to ensure data security.

3. Persons specified under Section I (8) of the data privacy policy are obligated to take all expectable measures to prevent any unauthorized person accessing the devices listed under Section II (4) above. Within this framework the protection of these devices should be specifically ensured with password, furthermore these assets should be stored in a safe, closed place. It is expressly forbidden to leave such devices in an unattended vehicle even in case the vehicle is securely locked.

4. Displaying data is only allowed during the work when such activity is performed and only for that purpose, only for the time period necessary to carry out given activity.

5. Furthermore, it is expressly forbidden to print or display the data by any other physical means (hard copy) for any other purpose than performing the activity, or to take the hard copy of the document from the premises designated to carry out such tasks. It should also be ensured that while displaying data, no such data is lost, damaged or destroyed and their content does not become known to, or accessed by any unauthorized person. Should the storage of the hard copy of data become inevitable, it should be kept for the time period absolutely necessary to normally carry out the activity and only in closed premises and in lockable filing cabinets. Any hard copy of the data, when the purpose of printing the hard copy ceased to exist, should be immediately destroyed.

6. In addition to complying with the provisions of this data privacy policy and apart from taking other aspects into account for data protection considerations, the rooms and the premises, where IT devices suitable for producing hard copies are operated (computer, work stations), should be used in accordance with the data protection and IT security requirements.

7. Client Data forwarding is only permitted strictly in accordance with the provisions of the software development contract, unless otherwise stated in the relevant contract exclusively for the contractual partners under the respective contract of the Company.

8. By making the persons specified under Section I (8) of this Data Privacy Policy available, the Company ensures the completion of the services required to perform the software development as per the relevant contract.

9. The persons specified under Section I (8) of this Data Privacy Policy shall immediately notify their superiors about any data protection issue encountered in their duties, especially about security breaches resulting in accidental or unlawful destruction, loss, change, unauthorised disclosure or access (**data protection incident**) of the forwarded, stored or otherwise processed data.

10. The Company keeps records of the data handled ensuring control over data handling, as well as over the provisions on data protection and data security, and to trace the database path. The records include the name of the database, the date of each phase and the end of data handling, as well as the name and signature of persons handling the data along with their superiors.

#### **IV. MISCELLANEOUS PROVISIONS**

1. The Company shall inform its employees along with all other workers providing services in a different employment status about this data privacy policy and data processing policy prior to starting their activities that would affect data handling, furthermore advising them about the ramifications of the respective regulations, the procedures specified in the provisions of such regulations, as well as the mandatory compliance therewith.

2. The scope of this data privacy policy applies to all Company employees and those employed under any other legal relationship.

3. The Company reserves the right to unilaterally amend this data privacy policy.

Budapest, 29 November 2019

**MULTISOFT Information Technology Services Limited Liability Company**