MICROSEC

Microsec zrt.

Privacy policy

Version: 1.6

7 September 2020

Versioning

Publication	Entry in Force	Amendment / Comment
1.0	2016-05-31	New document
1.1	2017-11-30	Minor clarifications
1.2	2018-02-26	Annual review
1.3	2018-08-14	Update due to legislative changes.
1.4	2019-04-05	Restructuring and consolidating privacy policies and privacy notices.
1.5	2019-06-13	Amendments necessary due to legislative changes (with respect to the GDPR).
1.6	2020-09-07	Review.

Contents

1. Introduction

1.1 About the company

Name:	Microsec zrt.
Registered seat:	1033 Budapest, Ángel Sanz Briz út 13.
Company registration number:	01-10-047218
Phone number:	+36 (1) 505-4444 Telefax: +36 (1) 505-4445
Website:	www.microsec.hu, www.e-szigno.hu

1.2 Purpose of the document

The purpose of the public Privacy Policy (hereinafter: **Privacy Policy**) of Microsec zrt. (hereinafter: the **Company**) is to ensure that during all data processing activities carried out by the Company the data processing is performed in a regulated form and that the protection of the data can be ensured.

Further purpose of this Privacy Policy is to exclude unauthorized use during the processing of data, and to reduce or prevent disadvantages arising from unauthorized use.

It is not the purpose of the Privacy Policy to present the data processing situations and to inform the persons concerned with the data processing, for this please see the Privacy Notice which is continuously available on the Company's website (https://e-szigno.hu/en/privacynotice.html) (hereinafter: ***Privacy Notice***).

1.3 Personal and territorial scope

The personal scope of the Privacy Policy covers all employees of the Company, as well as all persons who participate in the provision of the Company's services within the framework of a contract concluded with the Company or in another legally regulated way.

The territorial scope of the Privacy Policy covers all premises and offices of the Company, as well as all locations where the Company carries out any activity in connection with its services.

The data controller is responsible for the lawful data processing. Where data processing is carried out by more than one person, the responsible person shall be clearly defined, including in the case of joint data controllers.

1.4 Legal background of the Privacy policy

- Act CXII. of 2011 on Informational Self-Determination and the Freedom of Information (***Act on Information***);
- Act CCXXII. of 2015 on the general rules of electronic administration and trust services (***Act on E-Administration***);

- Regulation 2016/679 of the European Parliament and of the Council on the protection of natural persons with regard to the processing of personal data and on the free movement of such data (***General Data Protection Regulation*** or ***GDPR***).

1.5 Definitions and principles

1.5.1 Definitions

Processing: any operation or set of operations which is performed on personal data or on sets of personal data, whether or not by automated means, such as collection, recording, organisation, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction; (point 2 of article 4 of the GDPR)

Processor: a natural or legal person, public authority, agency or other body which processes personal data on behalf of the controller; (point 8 of article 4 of the GDPR)

Controller: the natural or legal person, public authority, agency or other body which, alone or jointly with others, determines the purposes and means of the processing of personal data; where the purposes and means of such processing are determined by Union or Member State law, the controller or the specific criteria for its nomination may be provided for by Union or Member State law; (point 7 of article 4 of the GDPR)

Personal data breach: a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data transmitted, stored or otherwise processed; (point 12 of article 4 of the GDPR)

Pseudonymization: the processing of personal data in such a manner that the personal data can no longer be attributed to a specific data subject without the use of additional information, provided that such additional information is kept separately and is subject to technical and organisational measures to ensure that the personal data are not attributed to an identified or identifiable natural person; (point 5 of article 4 of the GDPR)

Recipient: a natural or legal person, public authority, agency or another body, to which the personal data are disclosed, whether a third party or not. However, public authorities which may receive personal data in the framework of a particular inquiry in accordance with Union or Member State law shall not be regarded as recipients; the processing of those data by those public authorities shall be in compliance with the applicable data protection rules according to the purposes of the processing; (point 9 of article 4 of the GDPR)

Consent: any freely given, specific, informed and unambiguous indication of the data subject's wishes by which he or she, by a statement or by a clear affirmative action, signifies agreement to the processing of personal data relating to him or her; (point 11 of article 4 of the GDPR)

NADP: National Authority for Data Protection and Freedom of Information;

Personal data: any information relating to an identified or identifiable natural person (‘data subject’); an identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person (point 1 of article 4 of the GDPR).

1.5.2 Principles of data protection

In compliance with the GDPR, personal data shall be:

a) accessed lawfully, fairly and in a transparent manner in relation to the data subject **(‘lawfulness, fairness and transparency’);**
b) collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes; further processing for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes shall not be considered to be incompatible with the initial purposes (‘pur**pose limitation**’);
c) adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed (‘**data minimisation’**”);
d) accurate and, where necessary, kept up to date; every reasonable step must be taken to ensure that personal data that are inaccurate, having regard to the purposes for which they are processed, are erased or rectified without delay (‘**accuracy’**);
e) kept in a form which permits identification of data subjects for no longer than is necessary for the purposes for which the personal data are processed; personal data may be stored for longer periods insofar as the personal data will be processed solely for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes, subject to implementation of the appropriate technical and organisational measures required by the GDPR in order to safeguard the rights and freedoms of the data subject (‘**storage limitation’**);
f) processed in a manner that ensures appropriate security of the personal data, including protection against unauthorised or unlawful processing and against accidental loss, destruction or damage, using appropriate technical or organisational measures (‘**integrity and confidentiality’**).

In all data processing carried out by the Company, the Company acts in accordance with the above principles and takes the necessary measures to be able to demonstrate compliance with the principles of data processing ("accountability") (article 5 of the GDPR)

1.5.3 Protection of business secrets

Persons subject to this Privacy Policy shall keep all information obtained in connection with

the performance of the service provided by the Company as a business secret, strictly confidential.

Business secrets are any facts, information, other data related to the economic activity and the compilations thereof which are not well-known or hardly available to persons carrying out the respective economic activity, the acquisition, exploitation by unauthorised persons, disclosure with others or publication of which would prejudice or jeopardise the entitled party's legitimate financial, economic or market interests, provided that the party who has the right to lawfully dispose of it is not liable in relation to the retention of the secret.

The information thus obtained may be made available to external third parties in any way only based on the express and prior written authorisation of the other party. Provided that the persons under the scope of this Privacy Policy violate their obligation to keep the business secrets confidential, they are obliged to reimburse the Company for all resulting damages.

2 Data processing

2.1 Tasks and responsibilities within the organization

2.1.1 Data protection officer

The data controller's authorized director appoints the data protection officer to enforce this Privacy Policy. The Company shall ensure that the data protection officer is involved in all issues which relate to the protection of personal data properly and in a timely manner.

The Company shall support the data protection officer in performing his / her tasks by providing resources necessary to carry out those tasks and access to personal data and processing operations, and to maintain his or her expert knowledge.

The Company shall ensure that the data protection officer does not accept any instructions in connection with performing his / her tasks. He or she shall not be dismissed or penalised by the Company for performing his or her tasks. The data protection officer shall directly report to the highest management level of the Company.

2.1.2 Tasks of the data protection officer

The data protection officer shall:

a) prepare the Privacy Policy and synchronize it with other regulations, review other policies from a data protection point of view before publishing;

b) maintain the records of data processing activities (Article 30 of the GDPR) (hereinafter referred to as the ***"Records of Processing Activities"***);

c) inform and advise the Company and the employees who carry out processing of their obligations pursuant to the data protection laws;

d) provide professional assistance to the management of the Company for taking the organizational measures necessary for ensuring data security, in establishing

procedural rules;

e) monitor compliance with the data protection laws, and with the policies of the Company in relation to the protection of personal data, including the assignment of responsibilities, awareness-raising and training of staff involved in processing operations, and the related audits;

f) provide advice if requested as regards the data protection impact assessment and monitor the implementation of such impact assessment;

g) receive and investigate reports and initiate measures before the Company's management;

h) act as the contact point for the NADP on issues relating to processing, and to consult, where appropriate, with regard to any other matter.

The data protection officer shall conduct his / her duties with proper consideration of the risks associated with processing operations, taking into account the nature, scope, context and purposes of processing.

2.1.2.1 Maintaining the Records of Processing Activities

The Records of Processing Activities is the central register of certain personal data processing activities carried out by the Company, which contains the information indicated in Article 30 of the GDPR. In the Records of Processing Activities, all existing and new data processing activities introduced by an organizational unit shall be recorded without delay, together with the changes in the previous data processing activities, while the discontinued data processing must be deleted from the records.

The Records of Processing Activities shall include the followings:

a) the name and contact details of the data controller and, when applicable, the joint controller, the controller's representative and the data protection officer;

(b) the purposes of data processing;

(c) a description of the categories of data subjects and of the categories of personal data;

(d) the categories of recipients to whom the personal data have been or will be disclosed including recipients in third countries or international organisations;

(e) where applicable, transfers of personal data to a third country or an international organisation, including the identification of that third country or international organisation and, the documentation of suitable safeguards;

(f) where possible, the envisaged time limits for erasure of the different categories of data;

(g) where possible, a general description of the technical and organisational security measures necessary for the data security.

2.1.2. Heads of the departments

Heads of the departments specified in the Organizational and Operational Regulations of the Company

(a) are responsible for the compliance of the data management of the organizational unit under their control with the law, the present Privacy Policy and other related regulations;

(b) are responsible for ensuring that the data security requirements established in the present Privacy Policy are fully complied with during the data management of the organizational unit under their control;

c) shall monitor compliance with data protection regulations, in particular the provisions of the present Privacy Policy;

(d) shall request the assistance of the Data Protection Officer if they have any questions regarding the processing of personal data, business secrets or data of public interest;

(e) shall cooperate with the Data Protection Officer in order to enforce data protection regulations;

(f) shall ensure that their subordinates may participate in the data protection trainings organized or carried out by the Data Protection Officer.

If an organizational unit decides to carry out a new activity affecting personal data, or if it wishes to modify or delete its existing data management activities recorded in the Privacy Notice and the Data Management Register, the head of the organizational unit shall inform the Data Protection Officer in order to consult on compliance with data protection legislation. and to modify the Privacy Notice and the Data Protection Register.

2.1.3 The person carrying out the data processing

The person carrying out the data processing within the Company's organization is responsible for the processing, modification, deletion, transmission and disclosure of data within the scope of his / her activities, as well as for the accurate, traceable documentation of the data. During his / her activities, the person carrying out the data processing shall:

(a) manage and preserve data obtained in course of performing his / her duties;

(b) ensure that registries containing personal data are handled and stored in a secure way;

(c) ensure that no unauthorized person has access to the data which he or she processes;

(d) comply with data processing laws and internal instructions;

(e) immediately inform his / her superior if he / she needs the assistance of his / her superior or the Data Protection Officer in a data protection matter;

f) participate in trainings related to data processing and data protection.

A person becoming aware of business secrets or personal data is obliged to keep such secret without a time limit. Business secrets and personal data may not be misused, so it is especially

prohibited to use them outside the scope of the Company's duties for the employee's own or other personal or business purposes, gaining direct or indirect benefits, and to the detriment of the Company or its customers.

2.2 Protection of data generated during the provision of services

2.2.1 The Company as a data controller

The Company performs the activities outlined in its Privacy Notice as data controller. Chapter 5 of the Privacy Notice contains the mandatory data processing activities prescribed for the Company as trust service provider by the applicable laws.

2.2.2 The Company as data processor

The Company may perform data processing activities in the cases indicated in its Privacy Notice or on the basis of an agreement concluded with the Data Controller for data processing activities. If the Company acts as a Processor, it concludes data processing agreement with the Data Controller on the basis of the GDPR (in the case of archiving services this happens by accepting the Company's General Terms and Conditions). Pursuant to Article 28 (3) of the GDPR, the Controller and the Processor have to include in their agreement the followings: (i) the subject, (ii) the duration, (iii) the nature and purpose of the data processing (iv) the type of personal data processed, (v) the categories of data subjects and (vi) and the rights obligations of the Controller.

2.3 Personal data of the Company's employees

The rules of processing of the personal data of Company’s employees are included in the Privacy Notice prepared for the employees.

3 Data security

Taking into account the state of the art, the costs of implementation and the nature, scope, context and purposes of processing as well as the risk of varying likelihood and severity for the rights and freedoms of natural persons, the Company shall implement appropriate technical and organisational measures to ensure a level of security appropriate to the risk, including inter alia as appropriate: (a) the pseudonymisation and encryption of personal data; (b) the ability to ensure the ongoing confidentiality, integrity, availability and resilience of processing systems and services; (c) the ability to restore the availability and access to personal data in a timely manner in the event of a physical or technical incident; (d) a process for regularly testing, assessing and evaluating the effectiveness of technical and organisational measures for ensuring the security of the processing (point 1 of article 32 of the GDPR).

In assessing the appropriate level of security account, the Company takes into account in particular the risks that are presented by processing, in particular from accidental or unlawful

destruction, loss, alteration, unauthorised disclosure of, or access to personal data transmitted, stored or otherwise processed. (point 2 of article 32 of the GDPR)

The controller and processor shall take steps to ensure that any natural person acting under the authority of the controller or the processor who has access to personal data does not process them except on instructions from the controller, unless he or she is required to do so by Union or Member State law. (point 4 of article 32 of the GDPR)

The Company undertakes that only such persons may access and operate its IT systems that handle personal data, who have the appropriate level of access rights. Such access shall be considered an appropriate level of access rights, the scope of which is adapted to the so-called "need to know" principle, the essence of which is that access should only be granted to the extent strictly necessary for the performance of the work and only to such person whose official task is the data management /processing. The Company reviews the access rights and their use at regular intervals.

Within the scope of its tasks related to IT security, the Company ensures:

- protection against unauthorized access (protection of hardware, software devices)
- regular backups,
- protection of data files against viruses,
- the physical protection of data files and media.

The Company shall take the necessary measures to protect the paper-based records, especially with regard to physical security and fire protection. Employees and persons acting on behalf of the Company are required to securely store and protect the personal information they use or possess.

Additional rules related to data security are defined in the Company's Security Policy.

4 Data transfer

In all cases, data transfer may only take place on the appropriate legal basis set out in the GDPR, after informing the data subjects. The Company provides data regularly to bodies specified by law, at intervals specified by law.

In all cases, the data transfer must be documented in such a way that its procedure and lawfulness may be demonstrated.

Data transfer to abroad:

Data transfer to a Member State of the European Economic Area (EEA) shall be deemed to take place within the territory of Hungary. If data is transferred to a third country outside the EEA, the Company complies with the requirements set out in Chapter V of the GDPR (thus it shall notify the persons concerned prior to the transfer and shall comply with the relevant legal guarantees (Standard Contractual Clauses of the European Commission, Privacy Shield, etc.).

5 Supervision, monitoring

The heads of the organizational units processing data shall continuously monitor compliance with legal regulations and internal regulatory documents related to data protection.

The inspections carried out by the Company must cover in particular:

- the up-to-dateness of employees' access, inspection and access rights,
- enforcement of physical security regulations (electronic access control system, alarm, camera)
- compliance with fire safety rules,
- periodical change of passwords,
- random inspection of scrapping and destruction.

The person authorized to inspect may, subject to the purpose of the inspection, enter any premises where data are processed, in order to carry out the inspection. The person authorized to inspect may request information from the persons carry out the data processing in all such issues which are related to the data processing activities of the audited body, including getting to know all data processing activities and inspection of the concerned data carriers.

6 Procedures to be followed in the event of a breach of data protection provisions

If a person becomes aware that the data protection and data security provisions prescribed by law or the present Privacy Policy have been violated or there is danger of doing so, he / she shall immediately inform the Chairman of the Board of Directors of the Company.

The Chairman of the Board of Directors of the Company shall immediately take measures:

- to restore the protection of personal data,
- to reveal the causes of the violation and the circumstances facilitating it,
- to establish the liability of the person responsible for the omission,
- based on the obtained data, to initiate disciplinary proceedings in case the violation falls within the liability of an employee of the Company, in other cases, to take the sanction applicable on the basis of the contract or legislation governing the given legal relationship.

In the event of a personal data breach, the Company applies the procedure described in the Privacy Notice.

7 Final provisions

The provisions of this Privacy Policy shall be communicated to the employees of the Company who also manage or process personal data.