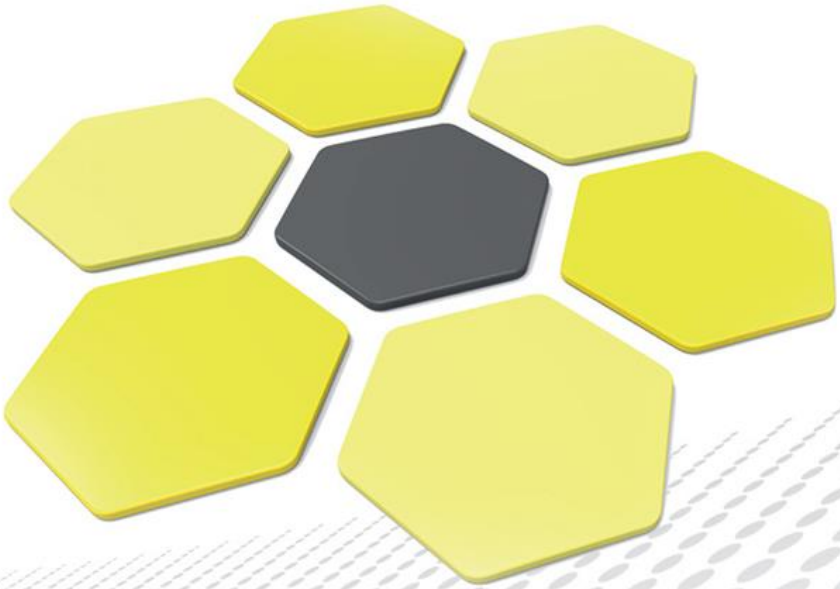
MICROSEC

Microsec zrt.

Privacy Policy

May 25, 2018



Track Changes

Publication	Entry in Force	Amendment / Comment
1.	May 25, 2018	New document

Contents

1 General Terms and Contact Details 5

2 Updates of the Policy and Accessibility 5

3 Reading and Accepting this Policy 5

4 Scope of Processed Data, Applicable Law, Purpose of the Data Processing 5

4.1 Personal Data Processed as a Data Processor 6

4.2 Applicable Law 6

4.3 Purpose of the Data Processing, Data Transfer, Information on the Rights of the Subject 7

5 Our obligations Related to Trust Services 7

5.1 Identification Obligation in relation to Certificates 8

5.2 Obligation to Store Data in Connection with the Certificates Issued Within the Framework of Trust Services 9

5.3 Logging Obligation of the Trust Service Provider 9

6 Personal Data in Archived Documents 10

7 Data Processing by Microsec 11

7.1 Issuing of certificates related to signature, website authentication and code signing for natural persons 12

7.2 Issuing of certificates related to signature, website authentication and code signing for legal entities 15

7.3 Issuing of Authentication and Encryption Certificates 18

7.4 Archiving 21

7.5 Time stamp 23

7.6 Data Processing Related to Accounting Documents 25

7.7 Processing of the Administrator's Data 25

7.8 Obligation to Log Data Pursuant to the Provisions of Law 27

7.9 Data Processing in Connection with the MicroSigner services 28

7.10 Electronic Billing Services 29

7.11 PassBy[ME] mobile electronic signature services 29

7.12 e-Szignó Registration Database and Software Development Kit (SDK); Operating the

Downloading Page. 31

7.13 Company Register Services 32

7.14 Operating the System for Electronic Delivery of Judicial Execution Documents (VIEKR) 36

7.15 Operation of the Electronic Asset Evaluation System of the Registry Court (CEVR) 38

7.16 Data Processing of Contact Persons of Clients and Potential Clients in case of Individual Agreements and Interested Parties 39

7.17 Operating the Call Center 40

7.18 Staff Recruitment 41

7.19 Data Processing for Marketing Purposes 42

8 People Entitled to Process Data 43

9 Newsletters 43

10 Information on CCTV Recordings at our Office Building 43

11 Placing Anonymous Visitor Identification (cookie) on Our Website 44

12 Securing Data Privacy 45

13 Managing Data Breaches 46

13.1 Our Internal Procedures in case of a Suspicion of a Data Breach 46

13.2 Reporting the Data Breach to the Supervising Authority 47

13.3 Informing the Persons Affected by the Data Breach 47

14 Activities Conducted as Data Processor 48

15 Personal Data Pertaining to Children and Third Persons 49

16 The Rights of the Affected Person and Legal Remedies Available 49

16.1 Your Right of Access 49

16.2 Right to Rectification and Erasure (the "Right to be Forgotten") 50

16.3 Right to Restriction of Processing 50

16.4 Right to Data Portability 51

16.5 Right to Object 51

16.6 Right of Complaint Before the Supervisory Authority 52

16.7 Effective Legal Remedies Against the Supervisory Authority 52

16.8 Effective Legal Remedy Against the Data Controller or the Data Processor 52

1 General Terms and Contact Details

This privacy policy (***Policy***) applies to personal data that are or may be processed in relation to you by Microsec Számítástechnikai Fejlesztő zártkörűen működő Részvénytársaság (1031 Budapest, Záhony utca 7. D., company registry No.: 01-10-047218, Tax ID No.: 23584497-2-41, hereinafter: ***Microsec***).

In case you have any questions or comments in relation to this Policy, please contact our client service desk at the below contact points before using any of the websites at https://www.microsec.hu or https://e-szigno.hu/ or before providing any data under this Policy to Microsec.

Telefon: (+36-1) 505 – 4444

Fax: (+36-1) 505 – 4445

E-mail: info@microsec.hu

If you have any questions, complaints or comments specific to data protection, please contact our Data Protection Officer (DPO) at adatvedelmitisztviselo@microsec.hu.

2 Updates of the Policy and Accessibility

Microsec is entitled to unilaterally amend this Policy with effect after said amendment. With respect to the foregoing, we kindly ask you to regularly visit our websites at https://www.microsec.hu or https://e-szigno.hu/ so that you are aware of any such amendments.

3 Reading and Accepting this Policy

If you provide us with personal data through our websites, or by communicating with our client desk or otherwise under the term of your agreement with Microsec, you thereby declare to have read the provisions of this Policy effective at the time of providing such data to us.

Special privacy provisions may be applicable in relation to acquiring certain services, of which you will be informed prior to using such services.

4 Scope of Processed Data, Applicable Law, Purpose of the Data Processing

We may ask you to provide us with certain data related to you on our websites, or such may be asked of you when communicating with our client desk or our sales representatives, in order for you to acquire or acquaint our services (e.g request a certification, download the beta version of our e-Szignó software etc.) or certain data may be provided or disclosed by you voluntarily through our correspondences. In addition to the foregoing, by using our services (e.g electronic signature with signature certificate, time stamping documents) new data are created which often contain personal data (e.g. the log files related to the use of certificates). This Policy also applies to the processing of such personal data.

4.1 Personal Data Processed as Data Processor

Some of our services (e.g. archiving, electronic billing software) imply that we process the personal data of third persons as data processors (e.g. the personal data contained in the archived documents or electronic bills). In such cases, Microsec assumes that its client providing the data (being the data controller) disposes of adequate legal grounds to process such personal data. Microsec, as data processor will not investigate the legal basis for data processing (as in many cases Microsec does not even have access to the personal data) and shall not be liable in connection therewith.

The data processor is not under obligation to provide information about the data processing in relation to such persons whose personal data it processes, this is the obligation of the data controller of the personal data in question. In some cases, this Policy mentions that Microsec acts as data processor, however does not contain all information in relation thereto. Consequently, it may happen that Microsec processes your personal data as data processor even in cases not mentioned in this Policy.

4.2 Applicable Law

When we process personal data, the legal basis and the duration of the data processing is often laid down in the applicable laws. Therefore, this Policy refers to various pieces of legislation as follows.

- Act CXII. of 2011 on Informational Self-Determination and the Freedom of Information (***Act on Information***);
- 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***);
- Regulation 910/2014 of the European Parliament and of the Council on electronic identification and trust services for electronic transactions in the internal market (***eIDAS Regulation***);
- Act CCXXII. of 2015 on the general rules of electronic transaction and trust services (***Act on E-Administration***);
- Decree of the Interior Minister No. 24/2016. (VI. 30.) on the specific requirements of trust services and service providers (***BM Decree***);
- Act V of 2013 on the Civil Code (***Civil Code***);
- Act C f 2000 on Accounting (***Act on Accounting***);
- Act CVIII of 2001 on electronic commercial services and services related to informational societies (***Act on Commercial Services***);
- Act V of 2006 on public company information, company registration and winding-up proceedings (***Company Registry Act***);
- Act LIII of 1994 on judicial execution (***Act on Judicial Execution***);
- Decree of the Minister of Administrative Matters and Justice No. 40/2012. (VIII. 30.) on the rules pertaining to the operation of the electronic delivery system employed in judicial execution (***KIM Decree***)
- Act CXXXIII of 2005 on the rules of the protection of property and personnel and private investigator activities (***Act on Property Protection***)

4.3 Purpose of the Data Processing, Data Transfer, Information on the Rights of the Subject

We generally ask you to provide us with data because we are obligated by law to do so (such as asking for the data to be included in the certificate we issue), or because it is needed for providing the services requested (in particular contact details, telephone numbers, e-mail addresses). Pursuant to Section 3(2) of the Act on Information, and Article 4. 1. of the GDPR, some of the data we ask you to provide or that are provided by you qualify as "personal data".

The information set out in Articles 13 and 14 of the GDPR and the information on your rights related to your data as per Articles 15-22 and 34 are provided to you by Microsec in this Policy.

Microsec does not transfer your personal data to third countries outside the European Economic Area or to any international organizations and furthermore does not conduct any automated decision making processes based on your personal data (including any profiling).

Based on the General Data Protection regulation you are entitled to ask the correction and deletion of your data processed by Microsec and we are also obligated to hand these data over to you on a data carrier. Information related to your rights are detailed in Section 16 herein.

5 Our obligations Related to Trust Services

The main activities of Microsec are providing trust services and issuing other certificates that are not subject to the law (e.g authentication, encryption). The notion of "trust services" is defined by the eIDAS Regulation under which trust services are:

(i) the creation, verification, and validation of electronic signatures, electronic seals or electronic time stamps, electronic registered delivery services and certificates related to those services,
(ii) the creation, verification and validation of certificates for website authentication; or
(iii) the preservation of electronic signatures, seals or certificates related to those services (archiving);

A higher level of transactional and IT security is attached to the "qualified" version of the above services and therefore the legislator generally accords a higher level of probative force thereto. The service providers who provide such qualified trust services must comply with much stricter requirements than a service provider who does not provide such qualified trust services.

Microsec provides the following services as qualified trust service provider:

- issuing e-Szignó qualified signature certificates;
- issuing e-Szignó qualified seal certificates;
- e-Szignó qualified time stamp services;
- e-Szignó qualified archiving services.

Under Hungarian law, documents signed by way of a qualified signature and sealed with a qualified time stamp prove with full probative force that such document has been signed by the natural person having attached the electronic signature to the document at the time indicated on the time stamp.

By way of a **qualified seal,** legal entities (such as governmental entities and companies) are enabled to create a seal certifying a procedure completed in the name of such entity, which proves with full probative force that the document sealed with the qualified seal is the legal statement of the entity indicated in the certification.

With the use of **qualified archives,** one can ensure that the documents placed in the archive remain authentic until the end of the archiving period and preserve their probative force, therefore it is assumed until proven to the contrary that the electronic signature, the electronic seal or time stamp and the pertaining certificates placed on the electronic document were valid at the time of placing such signature, seal or time stamp.

By using trust services, our clients create proofs that may only need to be used years later. In order to ensure that (i) the certificates can only be linked to the person indicated in the certificate, (ii) the evidence created with the help of the trust services are safeguarded for a long time, and (iii) there is no unauthorized access, the applicable European and Hungarian legislation (including the eIDAS regulation and the Act on E-Administration) prescribe stringent rules to the providers of trust services.

If you use our trust services, several pieces of legislation oblige us to process your data.

5.1 Identification Obligation in relation to Certificates

One of the most important of these rules is that once we issue a certificate for you or your organization or for your website (in other words if you become a certificate-subject or you file such request on behalf of your organization or in connection with your website so that you qualify as a "applicantapplicant") we as trust service provider are obligated under Section 82(1) of the Act on E-Administration to verify the data to be indicated in the certificate as well as the identity and representation rights of the applicant, in particular and based on the content of the certificate, the following:

- your identity,
- the authenticity of the data used to identify you (such as the data indicated in the personally presented or photocopied ID card, driver's license, passport) and, if public or central databases are available, the fact whether your identification data matches the contained in such database (in other words the data provided by you will be compared to the data contained by the central personal data and address register),
- your representation rights in case you proceeded on behalf of a legal entity
- the existence of the right of representation which will be indicated in the certificate,
- the right to dispose over the domain verified by the certificate,
- the right to dispose over the IP address indicated in the certificate,
- the existence of the organizational unit contained in the certificate,
- the right to exercise a certain regulated profession in case the certificate will indicate such profession (such as attorney of public notary).

This not only means that we will ask the person requesting the certificate to provide us with certain personal data during the application, but also that we will verify the data so provided in the central personal data and address register kept by the Ministry of the Interior (***Ministry***

of Interior register), the company registry, the registry for non-governmental organizations, the register kept by the bar association and the bar for public notaries, the domain registry, in case of schools in the registry for information on public education kept by the Office for Education (in Hungarian: Oktatási Hivatal), the registry of the budgetary authorities kept by the Hungarian State Treasury, the registry for individual entrepreneurs etc. The findings of such comparison with the data in public registers will be stored in connection with the given certificate. These data arerelated to the certificate and therefore will be stored in accordance with the provisions of Section 7.1 of this Policy.

5.2 Obligation to Store Data in Connection with the Certificates Issued Within the Framework of Trust Services

Section 84(1) of the Act on E-Administration prescribes trust service providers to store the information available to them in connection with the certificates, including those which they became aware of during the creation of the certificate and all personal data related thereto for a period of ten years as of the expiry of the validity of the given certificate. If the trust service provider is notified by any client, authority or court about a dispute relating to the accuracy of the data included in the certificate or the validity of a certificate, the trust service provider continues to be obliged to store said data until the dispute is closed with a final and binding decision even if such time is beyond the ten years following the expiry of the validity of the certificate.

With respect to the above, if you provided us with personal data in the course of requesting and the issuing of a certificate (certificates include: certificates for digital signature, seal and website authentication, encryption signature certificates, qualified or non-qualified), such data may not be deleted upon the expiry of the validity of the certificate or with the termination of the underlying service agreement, because we as trust service providers are under obligation to store the data attached to the certificates for a period of 10 years (in order to ensure subsequent traceability and the probative force).

5.3 Logging Obligation of the Trust Service Provider

The BM Decree prescribes numerous further rules related to the operation of trust services, which apply to the so called qualified service providers providing qualified trust services. Microsec is the first qualified (trust) service provider registered in Hungary , thus we must comply with these rules.

Based on Section 33 of the BM Decree, Microsec as a qualified service provider, logs all events related to its IT system and to the providing of the qualified services, to ensure the continuity of the operation and to avoid data loss. The recorded data must cover the entire process of providing the qualified service and must be suitable to enable reconstruction of all events connected to the qualified service to the extent necessary to assess real situations. According to Section 34(1) of the BM Decree, "*The logged data shall contain the calendar day and the exact time of the occurrence of the event subject to the logging and all data necessary for the traceability and reconstruction of the event, and also the name of the user or other persons who triggered the occurrence of said event*." (…) Based on Subsection (4) of the same Section of the BM Decree "*the qualified service provider ensures the continuous evaluation and monitoring of the logs*."

Pursuant to Section 35(1) of the BM Decree, the qualified service provider is obliged to store the data related to the certificates for the time period prescribed by law E-Administration (which is 10 years as of the expiry of the validity of the certificate, pursuant to Section 84(1) of the Act on E-Administration). The service provider is obliged to store or ensure that data are stored for 10 years as of the date of recording in case of further data recorded in the logs, and in case of the service policy and its amendments, for 10 years as of the date of the

version of the policy being repealed.

Consequently, if you use our qualified services, we are obligated to continuously log the service provided to you and to regularly make backup copies thereof. These log files and their backups may contain your personal data. Under the respective legislation, the aim of this is to (i) avoid the loss of data; (ii) ensure IT security; and (iii) reconstruct the events related to qualified services. Therefore, these logs and backups are prepared so that we may provide you with secured services in accordance with the law, where the subsequent traceability of the evidences is ensured.

6 Personal Data in Archived Documents

If you use our qualified archiving services, the documents intended to be archived will be uploaded into our archiving system. The documents uploaded by clients in the qualified archives operated by Microsec are stored in an encrypted format, the content of these documents is not known to the staff of Microsec.

In special cases you are entitled to request the decryption of the archived documents from the service provider (for example if you request the termination of the archiving services and you intend to remove the archived documents from the archives). In such event, the decryption is completed by an archiving officer of Microsec (holding a regulated position within the organization of the trust service provider) under documented circumstances and double control and the requested documents are handed over to you in a format determined by you. This process is handled pursuant to Section 14 of the BM Decree according to which the content of the archived electronic document may only be accessed by the archiving service provider and its staff or any person appointed by it with the written authorization of the client of the trust services.

It is possible that the documents uploaded by you in the archives contain personal data of third parties who are in no legal relation with Microsec. In relation to these personal data, Microsec qualifies as data processor and you qualify as the data controller. By using our qualified archiving services, you represent and warrant that you have adequate legal basis to process the data contained in the archived documents. Microsec, as data processor carrying out technical tasks is not aware of the personal data which may be contained in the documents archived by you, as Microsec does not have access to the archived documents. In relation to the personal data contained in the archived documents, you undertake to have obtained the consent of the concerned data subjects for the data processing or you declare that you otherwise have a legal basis for the data processing.

7 Data Processing by Microsec

In order that you may review in a clear and comprehensible manner the (i) purpose of the data processing; (ii) the legal basis of the data processing; (iii) the personal data retention time; (iv) the categories of the personal data subjects; (v) the group of persons with authorized access within the organization of the data controller in relation to the personal data processed by Microsec, we have summarized the respective information in the below table. As a principle rule, we do not transfer your personal data to third parties. If however, such special case occurs, it is duly indicated in the column listing the persons with access to the concerned personal data.

In case of services provided by Microsec, the subject of the certificate (typically a natural person) is usually different from the Subscriber responsible to pay the service fee and complete the related administrative tasks (typically a legal entity: company, law firm, governmental organization, hereinafter the ***Subscriber***). Our services are effectively used by the "subjects" (so for example they create the electronic signature), however using such services is necessary for proceeding on behalf of their employer or other organization. This is not always the case, as it is possible that the Subscriber is also a natural person, and we issue our invoice to this person as a private citizen. Therefore, the data pertaining to the Subscriber and to the natural person proceeding on its behalf is handled separately in the below table from the data of the certificate-subject

Type and purpose of the data processing	Legal basis of the data processing	Categories of the processed data	Term of the data processing	Who has authorized access to the data within Microsec?
7.1 Issuing certificates related to signature, website authentication and code signing for natural persons				
Issuing qualified certificates (or non-qualified but issued based on personal identification) to create electronic signature, for website authentication and code signing, to natural persons	Upon requesting the certificate: Section 5(1) a) of the Act on Information // Article 6 (1) a) of the of the General Data Protection Regulation – consent of the data subject which is first provided electronically on the Microsec website when submitting the request for the certificate and then on paper, by signing the document called Request for Certificate before a public notary or a Microsec colleague responsible for registration. In relation to data reconciliation necessary for issuing the certificate: Section 5(1)	The following data is requested for identification of the applicant (in case of signature certificates: **certificate-subject**): name, birth name, mother's name, place and date of birth, type and number of the identification document. In order to keep contact with our client, we ask for his/her telephone number and e-mail address during the application. The signature certificate will indicate the data of the applicant, which may be supplemented – if requested – with the e-mail address of the applicant as well as the name of the applicant's organization (e.g employer) and the name of the country where the organization operates. If you request a website authentication certificate through our website and you are a natural person, your name will not necessarily appear, but the IP address and domain name provided in your application will be indicated in the certificate which also qualifies as personal data. Furthermore, we also record your registration and	10 years as of the expiry of the certificate pursuant to Section 84(1) of the Act on E-Administration.	• registration officers (the job description of the position is set out in Section 2 of the BM Decree: it means the scope of work of the person responsible for approving the creation, issuance, withdrawal and suspension of certificates – access is required for handling the application and carry out the personal identification) • application operators • system administrator • key account managers to administer the special requests of clients with individual agreements

	b) of the Act on Information // Article 6. (1) c) of the of the General Data Protection Regulation – fulfillment of the legal obligation of the data controller : the trust service provider is obligated to verify the data to be indicated in the certificate in accordance with Section 82(1) of the Act on E-Administration which consists of the verification of the authenticity of the data used for personal identification and comparison with the data contained in the Ministry of Interior register	suspension password so that you can effectively use and eventually suspend your certificates. The personal identification data provided during your application for a certificate will be compared to the data indicated in the Ministry of Interior register thereby complying with our legal obligation. In case of website authentication certificate requests, your right to dispose over the domain name and IP address provided during f requesting the certificate will also be verified in the respective registers.		
Issuing non-qualified signature certificates (without personal identification) to natural persons (such as the signature certificates issued to examination officers and school staff)	Upon request of the certificate: Section 5(1) a) of the Act in Information // Article 6. (1) a) of the of the General Data Protection Regulation - consent of the data subject which is first provided electronically on the	Microsec offers such signature certificates for natural persons, which are issued without an intelligent card and operate with a software. These certificates are issued remotely in a simplified procedure without personal identification. A lower level of security applies to theseh certificates than to those which require personal presence, so these "non-qualified" (enhanced	10 years as of the expiry of the certificate pursuant to Section 84(1) of the Act on E-Administration. as this retention period is not only prescribed to qualified certificates but to all	• registration officers • application operators • system administrator • key account managers to administer the special requests of clients with individual agreements

	Microsec website when submitting the request for the services and then on paper, by signing the document entitled Request for Certificate and sending it to Microsec. In relation to data reconciliation necessary for issuing the certificate: Section 5(1) b) of the Act on Information // Article 6. (1) c) of the of the General Data Protection Regulation – fulfillment of the legal obligation of the data processor: the trust service provider is obligated to verify the data to be indicated in the certificate in accordance with Section 82(1) of the Act on E-Administration based on the photocopy of personal identification documentation / the personal identification documents demonstrated in person and comparing these data with the data in the Ministry of Interior register	security) certificates and the signatures created with such certificates are not accepted in every situation. Notwithstanding, the advantage of these certificates is that these can be issued without the personal presence of the certificate-subject before our client service desk or a public notary. However Microsec is required even in case of these certificates to check the identity of the applicant certificate-subject. In order to complete this identification obligation, we ask the certificate-subject placing the request to send us by post the photocopy of his/her personal ID card, passport or driver's license or in case he/she does not wish to send us such photocopy, to present it personally to our client service desk at a time previously scheduled, in which case the presented identification document is not photocopied. The following information is requested for remote identity check of the certificate-subject in case of non-qualified certificates: name, birth name, place and date of birth, mother's name, type of identification and the ID number. These data will be compared to the data contained by the Ministry of Interior register pursuant to our legal obligation.	certificates issued as a trust service provider.	

		If the applicant sent us the photocopy of the identification documents, we will retain these as well. We also record the certificate-subject's registration and suspension passwords to enable the use and suspension of the certificates. In order to keep contact with our client, we ask for a telephone number and an e-mail address.		
7.2 Issuing certificates related to signature, website authentication and code signing for legal entities				
Qualified (and non-qualified but issued based on personal identification) services related to seals (signature certificated issued to legal entities), and issuing of website authentication and code signing certificates for legal entities	Upon requesting the certificate: Section 5 (1) a) of the Act in Information // Article 6 (1) a) of the of the General Data Protection Regulation – consent of the data subject which is first provided electronically on the Microsec website when submitting the request for the services and then on paper, by signing the document entitled Request for Certificate before a public notary or a Microsec colleague responsible for registration.	When a legal entity applies for a certificate, a natural person proceeds on their behalf as the person placing the request. Microsec is obligated to verify the identity of the natural person proceeding in case of such certificates and also the right of representation of such persons. The following data is requested for the verification of the identity of the natural person proceeding on behalf of the legal entity: name, birth name, mother's name, place and date of birth, type and number of the identification documentation. These data provided will be compared to the data indicated in the Ministry of	10 years as of the expiry of the certificate pursuant to Section 84(1) of the Act on E-Administration.	• registration officers (for handling the applications and carrying out the identification procedure) • application operators • system administrator • key account managers to administer the special requests of clients with individual agreements

	In relation to data reconciliation necessary for issuing the certificate: Section 5(1) b) of the Act on Information // Article 6. (1) c) of the of the General Data Protection Regulation – fulfillment of the legal obligation of the data controller: the trust service provider is obligated to verify the data to be indicated in the certificate in accordance with Section 82(1) of the Act on E-Administration; in case you proceed on behalf of a legal entity (so you are requesting the certificate for an organization), your authorization to represent the entity (and your personal identification in relation thereto) will be verified.	Interior register thereby complying with our legal obligation. We also keep record of your registration and suspension password so that you can effectively use and eventually suspend your certificates. In order to ensure contact with our client, we ask for the telephone number and e-mail address during the application. If you request website authentication the right to dispose over the domain name and IP address provided by you in the course of requesting the certificate will also be verified in the respective registers.		
Non-qualified seal services (signature certificates issued to legal entities)	Upon requesting the certificate: Section 5(1) a) of the Act in Information // Article 6(1) a) of the of the	Non-qualified seals (signature certificates) are such certificates issued to legal entities, which are issued without an intelligent card and operate with a software. These are	10 years as of the expiry of the certificate pursuant to Section 84(1) of the	• registration officers (for handling the applications and carrying out the identification procedure)

(without personal identification)	General Data Protection Regulation – consent of the data subject which is first provided electronically on the Microsec website when submitting the request for the services and then on paper, by signing the document entitled Request for Certificate before a public notary or a Microsec colleague responsible for registration. In relation to data reconciliation necessary for issuing the certificate: Section 5(1) b) of the Act on Information // Article 6. (1) c) of the of the General Data Protection Regulation – fulfillment of the legal obligation of the data processor: the trust service provider is obligated to verify the data to be indicated in the certificate in accordance with Section 82(1) of the Act on E-Administration; in case you proceed on behalf of a legal entity (so you request the certificate for an organization),	issued remotely in a simplified procedure without personal identification. A lower level of security applies to such certificates than to those which require personal presence, so the natural person applying for the certificate is not required to appear personally before our client service desk or a public notary. However, Microsec is required even in the case of these certificates to check the identity of the certificate-subject placing the request and also the authorization of these persons to represent the legal entity applying for the certificate. In order to fulfill this obligation, we ask the applicant placing the request to send us by post the photocopy of his/her personal ID card, passport or driver's license or in case he/she does not wish to send us such photocopy,, to appear before our client service desk at a time previously scheduled, in which case the presented identification document is not photocopied. . The following information is requested for remote identity check of the natural person proceeding on behalf of the legal entity in case of non-qualified certificates: name, birth name, place and date of birth, mother's name, type of identification and the ID number. These data will be compared to the data contained in the Ministry of	Act on E-Administration.	• application operators • system administrator • key account managers to administer the special requests of clients with individual agreements

	your authorization to represent the entity (and your personal identification in relation thereto) will be verified.	Interior register pursuant to our legal obligation. If the person placing the request sent us the photocopy of the identification documents, we will retain these as well. We also record the registration and suspension passwords of the applicant to enable the use and suspension of the certificates. In order to keep contact with our client, we ask for a telephone number and an e-mail address.		
7.3 Issuing Authentication and Encryption Certificates				
Issuing authentication and encryption certificates to natural persons or legal entities – with personal identification	If it is a legal entity requesting the certificate, in respect of the natural person proceeding on behalf of the legal entity: Section 5(1) a) of the Act on Information // Article 6. (1) a) of the of the General Data Protection Regulation – consent of the data subject which is first provided electronically on the Microsec website when submitting the request for the services and then on paper, by signing the	The authentication and encryption certificates issued upon the personal identification of the applicant provide a higher level of security as those issued without personal identification. These certificates may be issued to natural persons as well as legal entities. In case of certificates issued to legal entities, the application process is also managed by a natural person. . With regard to the applicant, the following information is requested: : name, birth name, place and date of birth, mother's name, type and number of identification document.	We erase the data 5 years after as of the expiry of the validity of the certificate, so if there is a claim or dispute related to the certificate which arises within the statutory limitationperiod , we may dispose of the necessary evidence in respect of the request.	• registration officers (for handling the applications and carrying out the identification procedure) • application operators • system administrator • key account managers to administer the special requests of clients with individual agreements

	document entitled Request for Certificate before a public notary or a Microsec colleague responsible for registration. If the certificate is requested by a natural person, Article 6(1) b) of the General Data Protection Regulation – processing is necessary for the performance of a contract to which you are a party or in order to take steps at your request prior to entering into a contract	The certificate will indicate the applicant's data, and in case the applicant is a natural person, the certificate may contain – upon request – the e-mail address of the applicant as well as the name of his/her organization (e.g employer), the country and city where the organization operates. It is also possible to indicate the function and title of the applicant within that organization. In order to keep contact with our client, we ask for a telephone number and an e-mail address. The personal identification data provided during applying for the certificate will be compared – in accordance with our service policy - to the data indicated in the Ministry of Interior register since this certificate is issued based on personal identification. When a legal entity is the subject of the certificate, the natural person proceeding on its behalf is required to be identified. The applicant shall provide the same data when the certificate-subject is a natural person (see above). We also record the registration and suspension passwords of the applicant to enable the use and suspension of the certificates.		

Issuing authentication and encryption certificates to natural persons or legal entities – without personal identification **e.g. for accessing the company registry database free of charge (with chip card)**	If thee applicant is a legal entity requesting the certificate, in respect of the natural person proceeding on behalf of the legal entity: Section 5(1) a) of the Act in Information // Article 6 (1) a) of the of the General Data Protection Regulation – consent of the data subject which is first provided electronically on the Microsec website when submitting the request for the services and then on paper, by signing the document called Request for Certificate before a public notary or a Microsec colleague responsible for registration. If the certificate is requested by a natural person, Article 6 (1) b) of the General Data Protection Regulation – processing is necessary for the performance of a contract to which you are a party or in order to take steps at your request prior to entering into a contract	Microsec offers also such authentication and encryption certificates, which are issued remotely in a simplified procedure without personal identification. A lower level of security applies to such certificates than those which require personal presence. However, Microsec is required even in case of these certificates to check the identity of the applicant (certificate-subject or the person representing the organization). In order to fulfill this obligation, we ask the natural person (being the certificate-subject or the representative of the organization) to send us by post the photocopy of his/her personal ID card, passport or driver's license or in case he/she does not wish to send us such photocopy, to appear before our client service desk at a time previously scheduled, in which case the presented identification document is not photocopied. The following information is requested for remote identity check of the natural person (certificate-subject or representative of the organization): name, birth name, place and date of birth, mother's name, type of	We erase the data after 5 years as of the expiry of the validity of the certificate, so if there is a claim or dispute related to the certificate which arises within the statutory limitation period, we dispose of the necessary evidence in respect of the request.	• registration officers (for handling the applications and carrying out the identification procedure) • application operators • system administrator • key account managers to administer the special requests of clients with individual agreements

		identification and the ID number. The certificate will indicate the applicant's data, and in case the applicant is a natural person, the certificate may contain – upon request – the e-mail address of the applicant as well as the name of his/her organization (e.g employer), the country and city where the organization conducts operation. It is also possible to indicate the function and title of the applicant within that organization. The personal identification data provided during application for the certificate will be compared – in accordance with our service policy - to the data indicated in the Ministry of Interior register since this certificate is based personal identification. If the applicant sent us the photocopy of his/her identification documents, we will retain these as well. We also record the registration and suspension passwords of the applicant to enable the use and suspension of the certificates. In order to keep contact with our client, we ask for a telephone number and an e-mail address.		
7.4 Archiving				

Providing archiving services	Article 6 (1) b) of the General Data Protection Regulation – processing is necessary for the performance of a contract to which you are a party or in order to take steps at your request prior to entering into a contract Following the termination of the respective service agreement: Section 6(1) (b) of the Act on Information / Article 6. (1) f) of the General Data Protection Regulation – legitimate interest of Microsec	Only such clients may order our archiving services, who already dispose of an authentication certificate, hence the existence of the authentication certificate is the pre-requisite of accessing the archives. Consequently, in relation to this service, we store the data of to the certificate with which the client requested the services (and with which the client will be authenticated when downloading and uploading documents to and from the archives). We do not have access to the personal data contained in the uploaded documents, we only store them as processor.	The term of the data processing is identical to the term of the agreement we have in place with the Subscriber which is 50 years as a principle rule in case of archiving services, or the time period for which the client requested the archiving services. Following the termination of the agreement, the 5-year period set forth in Section 6:22 of the Act V of 2013 on the Civil Code (***Civil Code***) applies (statutory limitation) so as to ensure that if a legal dispute arises in connection with the archiving services after the termination of the agreement. Microsec is enabled to provide evidence that the communication with the client was in accordance with the agreement via the channels determined by the client and that Microsec had not	• registration officers (for handling the applications and carrying out the identification procedure) • application operators • system administrator • key account managers to administer the special requests of clients with individual agreements

			breached the provisions of the agreement in place. In relation to the logged personal data related to the qualified archiving services, Microsec applies the 10-year retention term prescribed by the BM Decree (see above in Section 5.3).	
Data Processing in relation to the personal data contained in the archived documents of our clients We do not have access to the stored data as a result of the applied encryption procedure employed. Decryption is only possible upon the written request of the Subscriber.	The consent of the individual data subjects, obtained by the Subscriber as controller. Microsec stores the archived documents as data processor.	We do not have information on the types of personal data contained in the archived documents as we do not have access to them. Considering, however that archiving services are typically used by attorneys and public notaries, it can be assumed that the documents contain numerous personal data.	Term of the agreement concluded with the Subscriber. Upon expiry thereof, we destroy the archived documents from our system.	• archiving officer, only upon written request of the client
7.5 Time stamp				
Providing time stamp services	Article 6 (1) b) of the General Data Protection Regulation – processing is necessary for the	In order to acquire the services, a user ID and a password is required which are stored by our system.	The term of the data processing is identical to the term of the agreement we have	• registration colleagues • application operators • system administrator • sales staff

	performance of a contract to which you are a party or in order to take steps at your request prior to entering into a contract Following the termination of the respective service agreement: Section 6(1) (b) of the Act on Information / Article 6(1) f) of the General Data Protection Regulation – Microsec legitimate interest of Microsec		in place with the Subscriber. Following the termination of the agreement, the 5-year period set forth in Section 6:22 of the Civil Code applies (statutory limitation) so as to ensure that if a legal dispute arises in connection with the time stamp services after the termination of the agreement, Microsec is able to provide evidence that the communication with the client was in accordance with the agreement, it was made via the channels determined by the client and that Microsec had not breached the provisions of the agreement in place. In relation to the logged personal data related to the qualified stamp services, Microsec applies the 10-year retention term prescribed by the BM Decree (see above in Section 5.3).	

7.6 Data Processing Related to Accounting Documents				
Invoicing of our services, retaining the underlying accounting documentation	Section 5(1) b) // Article 6(1) c) of the General Data Protection Regulation –fulfilment of the legal obligation of the data controller : Section 169(2) of the Act C of 2000 on Accounting (***Act on Accounting***)	The agreement (service order) serving as a basis for providing our services and the invoice issued in respect thereof qualify as accounting documents and therefore shall be stored by Microsec for a period of 8 years pursuant to Section 169(2) of the Act on Accounting. The processed data are the data contained in the invoice, the underlying agreement and the service order.	The retention period applicable for invoices starts on the date of their issuance and for agreements, on the date when the last invoice is issued based on the agreement (termination of the agreement). In this case, the data (so the document containing the data) may only be destroyed by Microsec upon the expiry of the 8-year period irrespective of the data subject's consent.	• colleagues of the finance department • sales staff • client service desk in case of agreements
7.7 Processing the data of an organization's administrator				
The Subscriber as organization may appoint an administrator entitled to proceed on its behalf before Microsec in connection with the	Section 5(1) a) // Article 6(1) a) of the General Data Protection Regulation – consent of the data subject, which is first provided via the website of Microsec	When requesting certificates, the certificate-subject (typically a natural person in case of signature certificates) and the person paying for the services, which is frequently an organization (the Subscriber), are often not the same. Considering that in addition to	We process the personal data of administrators in connection with certificates as these persons are entitled to make statements	• registration officers • application operators • system administrator • sales staff

services provided to the Subscriber in case of change of data, withdrawal and suspension of certificates, reinstating, replacement and the modification of the list of subjects and signatories	electronically, followed by signing the form called " Administrator Appointment Form" on paper format.	the certificate-subject, the Subscriber is also entitled to make statements in connection with the certificates (e.g. withdrawal of certificates or request for suspension), in order to facilitate the administration on behalf of the Subscriber, a contact person as **administrator** may be appointed in course of the application or such administrator may get involved in the application process himself/herself. This administrator is entitled to make legally binding statements in connection with certain certificates on behalf of the organization. Microsec must identify the administrator in order to verify the identity of the person making a statement on behalf of the given organization (so for example in order to ensure that the request for withdrawal or suspension of the certificate was made effectively by the person authorized to make such statement on behalf of the organization). Such administrators may be appointed on one hand on the electronic platform on Microsec's website where the administrator can provide his/her personal data requesting a certificate in order to be able to proceed with regard to the requested certificate. An administrator may be appointed by filing the applicable form signed by the authorized representative of the Subscriber, whereby the administrator – by signing the form - consents to	in connection therewith. As a result, we delete the data of the administrators from our registries 10 years after the expiry of the organization's certificates (Section 84(1) of the Act on E-Administration)	

		processing his/her personal data by Microsec, in connection with the certificates pertaining to the organization. The personal data processed in connection with administrators: name as displayed in ID document, birth place and date, mother's name (these are the data based on which we are able to identify the administrator), telephone number and e-mail address in order that Microsec may contact the administrator e.g. may notify the administrator of changes in the status of the certificates (e.g completion of withdrawal).		
7.8 Obligation to Log Data Pursuant to the Provisions of Law				
Logging qualified services (IT environment, pertaining events)	Section 5(1) b) // Article 6(1) c) of the General Data Protection Regulation – fulfilment of the legal obligation of the data controller - Decree of the Interior Minister No. 24/2016. (VI. 30.) on the specific requirements of trust services and service providers	The log files contain the events pertaining to the use of qualified services (issuing signature and seal certificates, time stamp, archiving), which may contain personal data. Fundamentally, the log files record events (e.g. upon creation of a time stamp, we record the client's specific identifier and the public IP address of the device with which the client used the service, in case of archiving, the data pertaining to the certificate by which the client was authenticated and the public IP address of the device with which the client used the service and the calendar day and exact time of the	Pursuant to Section 35(1) of the BM Decree referenced before, the qualified service provider shall store the logged data pertaining to events other than certificates for a period of 10 years as of their occurrence date.	• system administrators (the job description of the position is set out in Section 2 of the BM Decree: the staff responsible for the installation, configuration and maintenance of the IT systems) • independent system auditors (the job description of the position is set out in Section 2

		occurrence of the event, the data necessary for the traceability and reconstruction of the event and the name of the user or any other person who enabled the occurrence of the event.		of the BM Decree: the person responsible for the audits of the logged and archived data of the service provider, for the inspection of the controlling measures taken by the service provider to ensure compliant operation, for the continuous control and monitoring of the existent procedures)
7.9 Data Processing in Connection with the MicroSigner services				
Providing MicroSigner services	Article 6 (1) b) of the General Data Protection Regulation – the data processing is necessary for the performance of a contract to which you are a party or in order to take steps at your request prior to entering into a contract.	To run a trial version of the MicroSigner services, an operational e-mail address is required which is provided by the interested party. The system generates a user name and a password which enables the client to access the test version. If you are using MicroSigner as an end-user, you need to install it on your computer. Upon installation, you agree to the terms and conditions of the MicroSigner software license, whereby you also consent to Microsec storing the data of the signature certificate, which enables you to use the MicroSigner service, for the purposes of improving the service.	The e-mail address, user name and password are stored for as long as the client requires access to the pilot version- We delete annually the statistics comprising the data of the certificate used for MicroSigner services and the frequency of use.	• colleagues of the technical support department; • application operator, • system operator

		Consequently, we store the data included in your signature certificate, which may differ according to the type of certificate, but typically means the name, title, organization name and e-mail address.		
7.10 Electronic Billing Services				
Providing electronic billing services	Article 6 (1) b) of the General Data Protection Regulation – the data processing is necessary for the performance of a contract to which you are a party or in order to take steps at your request prior to entering into a contract. Microsec qualifies as data processor in respect of the personal data contained in the uploaded invoices, Microsec processes the data on the basis of the agreement concluded with the Subscriber.	Name, address, e-mail address, telephone number. We do not have access to the personal data contained in the invoices uploaded to our billing system, we only store these as data processors. In case our clients issued invoices to natural persons as well, then the name, address and the goods purchased or the services acquired will be the stored as personal data.	The term of the agreement concluded with the Subscriber. We destroy the stored invoices upon termination of the agreement.	• application operator, • system operator
7.11 PassBy[ME] mobile electronic signature services				

Providing PassBy[ME] mobile signature services **PassBy[ME] Mobile ID is a mobile application downloadable from application stores (AppStore, GooglePlay) providing signature solutions on smart devices. Only such end users may use the PassBy[ME] Mobile ID , whose organization (as Subscriber) registered on passbyme.com.**	Section 5(1) a) // Article 6. (1) a) of the General Data Protection Regulation – consent of the data subject Authorization by law: Section 13/A of the E-commerce Act: Following the termination of the respective service agreement: Section 6(1) (b) of the Act on Information / Article 6. (1) f) of the General Data Protection Regulation – legitimate interest of Microsec PassBy[ME] mobile signature services enable the user to upload documents to our system for the purposes of electronic signature. The system stores the document for 24 hours and then irrevocably deletes it. The user is liable to acquire an adequate legal basis in respect of the personal data contained in the uploaded documents;	Microsec provides the PassBy[ME] mobile signature services directly only to organizations. . The organization's administrator must register the organization on the passbyme.com website. The administrator provides Microsec with his/her data directly (name, e-mail address, telephone number) on the registration platform on the passbyme.com website. The data of further users are recorded by the initial administrator, other administrators authorized by the initial administrator and other users of pertaining IT systems. Providing these data is necessary for the registered users of the Subscriber to use the PassBy[Me] services and for Microsec to invoice the Subscriber (the service fee is determined on the basis of the number of users). Microsec assumes that the administrator obtained the consent of the users on behalf of the Subscriber in order that the Subscriber as an organization may register them for the PassBy[ME] Mobile ID services, thus, the Subscriber is liable to obtain such consent. Consequently, the consent of the end-users to the processing of their data is granted by the Subscriber as a representative. In order to provide the PassBy[ME] mobile signature services, beyond the name, e-mail adresse and telephone number of the users, we need to register the individual identifier of the user (OID) within the global user	Until the withdrawal of the data subject's consent. We consider the consent withdrawn if the agreement concluded with the organization using the services is terminated (the organization does not have an active registration on the passbyme.com website or the agreement concluded separately with the organization is terminated), considering that the administrator provided us with his/her personal data and that of other user so that the organization may use the PassBy[ME] mobile signature services. Therefore, the term of the data processing is the term of the agreement concluded with the organization and 5 years thereafter pursuant to Section 6:22 of the Civil Code	• colleagues of the technical support department; • application operator, • system operator

	with respect to these personal data, Microsec qualifies as data processor.	system, the individual identifier of the user within the organization (PassBy[ME] ID), the identifier of the mobile device of the user specific to the system (vendorid) and furthermore, the end-user certificates necessary for the creation of the electronic signatures (name, e-mail, vendroid, public key). We provide a demo version of the PassBy[ME] mobile signature services for trial where only one operating e-mail address is required from the interested party. We expressly ask the interested party not to provide any personal data upon registration other than an e-mail address.	(statutory limitation period), so that if a legal dispute arises in connection with the services rendered after the termination of the agreement, Microsec is able to prove to have duly rendered the transaction authentication, signature or messaging services to the end-users registered by the administrator(s) and that it did not breach the provisions of the agreement. With respect to the fact that the end-users typically approve financial transactions with the help of the PassBy[ME] mobile signature services, Microsec has a special interest to store the data within the statutory limitation period.	
7.12 Operating the download page for the e-Szignó Registration Database and Software Development Kit (SDK);.				
Operating the downloading page for	Article 6 (1) b) of the General Data Protection	Name of the client or the person interested in our services in case of	In respect of people showing interest in	• sales staff

the e-Szignó Registration Database and Software Development Kit (SDK); We provide online access (download website) to certain software products of Microsec: these are the e-Szignó Automat and the VHKIR communication module (providing communication channels for the participants of the legal enforcement system). Access is granted to contracted clients, interested persons running a trial version of the software and and clients already having an end-user e-Szignó license.	Regulation – processing is necessary for the performance of a contract to which you are a party or in order to take steps at your request prior to entering into a contract. Following the termination of the respective service agreement: Section 6(1) (b) of the Act on Information / Article 6 (1) f) of the General Data Protection Regulation – the legitimate interest of Microsec .	natural persons. In case of legal entities, name of the representative, name of the organization and e-mail address. A user name and an individual registration key belonging to the user is necessary for the use of the developer package of the e-Szignó Automat and the VHKIR communication module software.	our software products (so potential clients contacting us with the intention to enter into an agreement), we delete the data from our database 6 months after sending the registration e-mail necessary to run the test version of the software / the date of the one-time extension of the registration period upon request of the client, provided that the conclusion of an agreement does not take place.	• colleagues of the technical support department; • system operator
7.13 Company Register Services				
Operation of the National Company Register and Company Information Services (OCCSZ) (company information services containing up-to-date data) to the subscribers (in	In respect of the subscriber: Article 6 (1) b) of the General Data Protection Regulation – processing is necessary for the performance of a contract to which you	Pursuant to the agreement concluded with the predecessor of the Ministry of Justice, the Ministry of Public Administration and Justice (***Ministry Agreement***), Microsec is obliged to technically operate the the National Company Register and Company	The term of the data processing is identical to the term of the agreement we have in place with the subscriber. Following the termination of the agreement, the 5-year period set forth	• system operator, • application operator • client service desk • technical support department;

exchange of a service fee) **The service is accessible on the https://occsz.e-cegjegyzek.hu/ website.** **The processed data: data pertaining to the persons using the services**	are a party or in order to take steps at your request prior to entering into a contract The subscriber is entitled to appoint a contact person in relation to the services and to allow access to the OCCR system to its own clients (further users). These users are registered by the subscriber in the system operated by Microsec, therefore Microsec assumes in relation to these users - just like in the case of the appointed contact persons - that the subscriber previously obtained consent from the persons affected for processing their data, as the subscriber proceeds on their behalf. Consequently, the legal basis is Section 5(1) a) of the Act on Information // Article 6. (1) a) of the General Data Protection Regulation – consent of the data subject which is	Information System (***OCCR***) in accordance with the applicable laws. Pursuant to Section 15(2) of the Company Registry Act, fee is payable for company information not accessible in the free version of the company register for data requested in the form of a public deed. A part of this fee is payable to Microsec for the use of the OCCR system. Microsec and the client paying the fee (subscriber) enters into an agreement for the use of the OCCR system. We record the personal data of the subscriber concluding the agreement with Microsec (name, address, mother's name, place of birth, type and number of ID) in the agreement on the use of services. The subscriber may also appoint a contact person in the agreement in order to facilitate the services provided by Microsec. If the subscriber appoints a contact person, a name, telephone number, e-mail address, fax number and post address may be indicated. Our subscribers are also entitled to provide further users access to the OCCR system. The data pertaining to these users (full name, user name, password, e-mail address, place of work, address, contact person on behalf of user and the name, address, e-mail, telephone number of the latter) are directly recorded in the IT system.	in Section 6:22 Civil Code applies (statutory limitation) so as to ensure that if a legal dispute arises in connection with the services after the termination of the agreement, Microsec is able to verify that communication with the client was in accordance with the agreement via the channels determined by the client and that Microsec did not breach the provisions of such agreement. In respect of the users registered by the subscriber, we retain data for a period of 5 years as of the termination of the right to access.	

	provided by the subscriber as representative.			
Operation of the National Company Register and Company Information Services (OCCSZ) (company information services containing up-to-date data) to organizations and persons charged with public duty (free of charge) **The service is accessible at the https://gov.e-cegjegyzek.hu (https://cert.e-cegjegyzek.hu) website.** **The processed data: data pertaining to the persons using the services**	Based on Section 15(3) of the Company Registry Act, the company information service shall supply company information (regarding the entirety of the company register) free of charge to the court, the prosecutor's office, an investigative authority or other administrative body, notary public, court bailiff, liquidator, to chambers of commerce and trade associations to the extent required for discharging their duties conferred upon them by law. These entities and persons may not be charged either for the information, or for the transfer of data, unless otherwise provided by law. . Pursuant to the Ministry Agreement, Microsec is obligated to fulfill all requests regarding free company information, including	The organization charged with public duty who is entitled to free access acting as data controller transfers to Microsec the name, place and date of birth and mother's name of the natural person intended to have access to the OCCR system via the document called "employer's certificate". An authentication certificate is necessary to access the OCCR system so if the given person intended to have access already disposes of such certificate, the employer shall also transfer the data pertaining thereto. (In the absence thereof, an authentication certificate must be required before using the OCCR system. Data processing issues related to authentication certificates are set out in the respective line of this Policy.) Organizations charged with public duty, who are entitled to free access, shall also register themselves with Microsec, as entities entitled to issue the above mentioned "employer's certificate". The registration shall be carried out via a form, signed by the authorized representative of the given organization. When filling out the form, the entity as data controller may also provide contact details (name of the	We retain the registered data of the user and the pertaining data traffic during the term of active access to the OCCR system and 5 years thereafter (within the statutory limitation period) in order that if the user made use of the free services for purposes not allowed by law, we may enforce indemnity claims against the organization charged with public duty (the liability for such indemnity vis-á-vis Microsec is undertaken by the organization's representative on the registration form).	• system operator, • application operator • client service desk • technical support department

	the requests of the organizations set forth in Section 15(3) of the Company Registry Act. Microsec receives the personal data of the natural persons entitled to request information from the OCCR system free of charge from the organizations granted free access. The natural persons granted with free access (typically government officials, judges, prosecutors etc) may use the service with an authentication certificate. Microsec assumes that the organizations charged with public duty entitled to free access previously obtained the consent of these persons for processing their data, as the organization proceeds as their representative when transferring their data. Therefore, the legal basis is Section 5(1) a) of the Act on Information // Article 6. (1) a) of the General Data Protection Regulation – consent of	contact person, title, e-mail, telephone number), which are processed by Microsec on the basis of the contact person's consent, given by way of their representative (the employer charged with public duty), just like in the case of individual users. The user data (individual user name, organization and the amount of requests made in a given month) is transferred to the Ministry of Justice pursuant to the Agreement.		

	the data subject which is provided on behalf of the data subject by the employer being the organization charged with public duty.			
7.14 Operating the System for Electronic Delivery of Judicial Execution Documents (VIEKR)				
Operating the System for Electronic Delivery of Judicial Execution Documents (VIEKR) VIEKR is an electronic delivery system created to comply with the provisions of the Act LIII of 1994 on Judicial Execution (***Act on Judicial Execution***). Microsec operates the IT infrastructure of the system pursuant to an agreement concluded with the Hungarian Association of Court Enforcement Officers	Only organizations may be registered to the VIEKR system. The organization may appoint a general and a technical contact person in relation to the services and may also provide access to the system for users within its own organization. The data of these users is transferred to Microsec by the organization to ensure the use of the VIEKR system by said users. Microsec assumes in relation to the data of the users as well as in relation to the data of the contact persons appointed, that the organization had previously obtained their consent to process their data, as the organization acts as the	In case of registered organizations, the VIEKR system keeps record of the contact details of the general and technical contact persons of the registered organizations (name, e-mail address, telephone number). Microsec uses these data for the purposes of resolving eventual problems arising in connection with sending messages in the VIEKR system. The system retains the data indicated in the signature, encryption and authentication certificates necessary for the use of the VIEKR system, in case of users of an organization, the data indicated in their certificate. . (The user of the organization may be a natural person or the automatism of the organization.) The VIEKR system must store the meta data, the deposit slip and the receipt slip of the deliveries for a period of 10 years as of their creation, pursuant to the Act on Judicial Execution and the Decree of the Minister of Public Administration and Justice on the detailed rules of the operation of the	The data pertaining to the organization (so the data of the general and technical contact persons) are retained in the system in the period between the approved registration of the given organization and the completion of the approved request to delete such organization from the system. VIEKR backup files contain the above data for a period of one year. The log files are also stored for one year. Pursuant to Section 43(1) of the Decree of the Minister of Public Administration and Justice No. 40/2012.	• system operator • application operator

	representative of these individuals in order to grant them access to the VIEKR system. Therefore, the legal basis is Section 5(1) a) of the Act on Information // Article 6 (1) a) of the General Data Protection Regulation – consent of the data subject which is provided on behalf of the data subject by the organization registered in the VIEKR system.	electronic delivery system employed by independent court enforcement officials No. 40/2012. (VIII. 30.). These contain data that are suitable to determine the identity of the sender and the addressee of the given delivery. The messages forwarded via the system may contain personal data. However, these are coded with end-to-end encryption, so the content thereof is not accessible to Microsec and therefore Microsec does not qualify either as data controller or as data processor in this relation.	(VIII. 30.) , the VIEKR system automatically deletes from the inbox of the user all deliveries and all receipts, notices and confirmations of sending and receiving such deliveries 30 days after the date of delivery or the date when the legal presumption of a successful delivery came into force. Subsection (2) of the same Section states however, that continuous access to the receipts, notices and confirmations of sending and receiving deliveries and to the meta data of the deliveries must be ensured by the VIEKR system after the expiry of the above 30 days period for a period of 10 years. The same applies to technology necessary for reading the retained data. After the 10 year retention period, these data shall be destroyed.	

7.15 Operation of the Electronic Asset Evaluation System of the Registry Court (CEVR)				
Operation of the Electronic Asset Evaluation System of the Registry Court (CEVR) In accordance with Section 117 of the Company Registry Act and Sections 10/C-F of the pertaining Decree of the Minister of Justice No. 24/2006 (V.18.), the electronic evaluation of the assets of companies subject to involuntary dissolution is carried out by the registry courts. The primary aim of the CEVR system is that organizations requested by the registry courts to provide information in course of the involuntary dissolution process, are enabled to provide the requested information by way of electronic documents.	Only organizations may be registered in the CEVR system. The organization may appoint a general and a technical contact person in relation to the services and can also provide access to the system for users within its own organization. The data of these users is transferred to Microsec by the organization to ensure the use of the CEVR system by said users. Microsec assumes in relation to the data of the users as well as in relation to the data of the contact persons appointed that the organization had previously obtained their consent to process their data, as the organization acts as the representative of these individuals in order to grant access to them to the CEVR system. Therefore, the legal basis is Section 5(1) a)	In case of registered organizations, the CEVR system keeps record of the contact details of the general and technical contact persons of the registered organizations (name, e-mail address, telephone number). Microsec uses these data for the purposes of resolving eventual problems arising in connection with sending messages within the VIEKR system. The system retains the data indicated in the signature, encryption and authentication certificates necessary for the use of the CEVR system, in case of users of an organization, the data indicated in their certificate. (The user of the organizations may be a natural person or the automatism of the organization.) The CEVR system must store the meta data, the deposit slip and the receipt slip of the deliveries for a period of 1 year as of the date of their creation. These contain data that are suitable to determine the identity of the sender and the addressee of the given delivery. The messages forwarded via the system may contain personal data. However, these are coded with end-to-end encryption, so the content thereof is not accessible to Microsec and therefore Microsec does not qualified	The data pertaining to the organization are retained in the system in the period between the approved registration of the given organization and the completion of the approved request to delete such organization from the system. CEVR backup files contain the above data for a period of one year. The log files are also stored for one year. The system stores the meta data of the deliveries and the deposit and receipt slips for a period of 1 year to ensure traceability.	• system operator • application operators

	of the Act on Information // Article 6 (1) a) of the General Data Protection Regulation – consent of the data subject which is provided on behalf of the data subject by the organization registered in the CEVR system.	neither as data controller nor data processor in this relation.		
7.16 Processing the Data of Contact Persons of Clients and Potential Clients in case of Individual Agreements and Interested Parties				
Conclusion and performance of individual agreements with clients entered – including participation on tenders (giving offers) and responding to the queries of potential clients interested in our services	Section 6(1) (b) of the Act on Information / Article 6 (1) f) of the General Data Protection Regulation – Microsec rightful interest In case we receive (e.g recorded in an agreement) the contact details from our client / potential client (typically the employer), we assume that the employer is authorized to disclose the given data. In this case, the legal basis for data processing is the data subject's consent as per	In the course of the conclusion and performance of client agreements based individual orders, offers made in relation to the conclusion of such agreements, request of information about our services, Microsec comes into contact with the individuals representing the partner, so for example the interested parties fill out on our website the contact form (name, e-mail address, telephone number, and the services, which are subject to the interest of the partner), the person proceeding on behalf of the client sends an e-mail to Microsec staff with the intention of entering into an agreement or the performance thereof. These emails are typically signed by an automatic signature. Therefore, the processed data are typically the contact details of the individual	After receipt of the result of a tender process, the responsible colleague of our sales department erases such parts of the offer made by Microsec that contain personal data. In the event that the tender is successful, the personal data indicated in the respective agreement is erased after 5 years as of the completion of the services as set forth in Section 6:22 of the Civil Code (after the lapse of the	• sales staff

	Section 5(1) a) of the Act on Information // Article 6. (1) a) of the General Data Protection Regulation which is provided by the client (typically the employer) concluding or intending to conclude the agreement with Microsec.	proceeding on behalf of the partner in connection with the agreement (name, address, telephone number, e-mail) and also the his/her activity in relation to the preparation and performance of the agreement.	statutory limitation period) in order to ensure that if a legal dispute arises Microsec is able to verify that the communication with the client was in accordance with the agreement via the channels determined by the client and that it had not breached the provisions thereof (e.g the information or the payment notice was sent to the appropriate e-mail address etc.).	
7.17 Operating the Call Center				
Call Center and handling complaints Accurate documentation of your contact details and the conversations with our call center in order to ensure that the requests and comments in connection with the activity of Microsec are available in the case of any subsequent question or dispute in their original form and also that we	Section 5(1) a) of the Act on Information // Article 6 (1) a) of the of the General Data Protection Regulation – consent of the data subject, which is provided by the client by way of using our call center.	When you contact our call center, we record your telephone number, first and last name, voice, the organization which you represent, in case of queries related to certificates, the number of the card affected, the data of the certificate-subject, in case of certificate suspension: the following data of the certificate subject: name as displayed in his/her identification document, birth name, mother's name, place and date of birth, number of the ID card or the suspension password. Furthermore, we record all personal data in addition to the above	Until withdrawal of the data subject's consent and in the absence thereof, 4 months after the telephone conversation took place.	• employee of the client service desk participating in the call • department leader of the client service desk • employee of the technical support department participating in the call • leader of the technical support department

may contact you in relation to any of the above, if necessary. Further purposes of the data processing is the identification of the client in course of performing our contractual obligations (e.g suspension of certificates) and the quality assurance of our call center, to guarantee client satisfaction by evaluating and monitoring of the work of our call center colleagues.		which you may disclose during the telephone conversation, including especially the circumstances of the matter in respect of which you contacted the call center.		colleague responsible for quality assurance
7.18 Recruitment				
Recruitment	Section 5(1) a) of the Act on Information // Article 6 (1) a) of the of the General Data Protection Regulation – consent of the data subject which is provided by sending the job application-related documents	Name, telephone number, e-mail address (potentially date of birth), qualification, professional experience, language skills (as provided in the CV or resumé of the applicant).	The job applications we receive via our website, job portals or other sources are stored for a period of 1 year as of receipt considering that in case the selection process is extended or unsuccessful, we often contact applicants who submitted their application to us months before we contact them.	• HR manager • Board of directors • future supervisor of the applicant

7.19 Data Processing for Marketing Purposes				
Sending advertising materials by e-mail and advertising by telephone	Section 6(1) of the Act XLVIII of 2008 on the essential conditions and certain limitations of business advertising activity (***Act on Advertisement***) – the previous, unambiguous and express consent of the targeted person	The name of the possible recipient, name of organization, title, e-mail address (telephone number if shared), scope of products, which falls within the recipient's field of interest.	Upon the withdrawal of consent, the personal data must be deleted.	• colleague responsible for marketing • colleagues responsible for sales
Promotions, campaigns and media appearances (as per the conditions applicable to the promotion)	Section 5(1) a) of the Act on Information // Article 6 (1) a) of the of the General Data Protection Regulation – consent of the data subject which is provided by participating in the promotion or campaign or attending the media appearances (pursuant to the conditions applicable to participating in the promotion)	The scope of the personal data is determined on a case-by-case basis, as per the conditions applicable to participating in the promotion.	The term of the data processing is determined on a case-by-case basis as per the conditions applicable to participating in the promotion.	The scope of the affected persons is determined on a case-by-case basis, as per the conditions applicable to participating in the promotion. In the absence thereof, the persons carrying out tasks in connection with the promotion.

8 Authorized Data Processors

Microsec does not employ data processors for the completion of technical tasks pertaining to the data processing operations. If, however this is to occur, the person of the data processor and the fact of data transfer will be indicated with regard to each data processing activity set out in Section 7 of this Policy.

9 Newsletters

You have the right to unsubscribe from our newsletters at any time without limitation and justification, free of charge, at any of the following contact points: info@microsec.hu, Microsec zrt. 1031 Budapest, Záhony utca 7/D; client service desk: (+36-1) 505 – 4444.

Furthermore, if you receive advertising from us in an e-mail, we will remind you in each of these e-mails that you have the right to unsubscribe at any time, without limitation and justification, free of charge.

10 Information on CCTV Recordings at our Office Building

We operate a CCTV system at our client service desk for the protection of our property pursuant to Act CXXXIII of 2005 on the rules of the protection of property and personnel and private investigator activities (***Act on Property Protection***). The notice prepared pursuant to Section 28(2) d) of the Act on Property Protection is displayed in our client helpdesk office, while detailed information on the recordings, as recommended by the guidelines of the Hungarian National Authority for Data Protection and Freedom of Information, is set out in this Policy.

The legal basis for the CCTV recordings operated by Microsec is Section 6(1) b) of the Act on Information and Article 6 (1) f) of the General Data Protection Regulation - the rightful interest of Microsec.

For the sake of property protection, three cameras are installed in the client service area of Microsec located at the ground floor of 1031 Budapest, Záhony utca 7/D, which the clients typically enter in order to receive their cards (personal identification). The areas covered by each of the cameras are as follows:

1. Camera: entrance of the client service area, the door leading to the premise designated for our clients to receive the cards
2. Camera: the edge of the reception desk of the client service area (the receptionist colleague and the client are not visible in this angle), a large sized sliding door
3. Camera: the sliding door and the parking area visible through the door

Microsec monitors the events through the recordings made by these three cameras and stores the recordings at its registered seat located at 1031 Budapest, Záhony utca 7/D, the place of the recordings are made. Microsec stores the recordings in a secure location, closed off from the public, on the hard drive of its own hub computer, accessible only with a user name and password.

The recordings may be viewed only in case there is a security breach; otherwise, the system deletes the recordings after 72 hours. The management is entitled to review the recordings in case of a security breach, while the employees of the Operational Department may review the recordings for the purposes of maintenance. Microsec does not transfer the fixed recordings except if the crime investigation authorities require so for the investigation of a security breach.

In case you visit our client service desk in person, it is possible that you will appear in the recordings made by our CCTV system, therefore your movements and image (which qualify as personal data) may be recorded. As it is possible that your image qualifying as personal data is processed by us, you are hereby kindly notified that you have certain rights in relation to this data processing as set out in Chapter 15 of this Policy (in particular you have the right to ask for information as to whether data processing is in progress, you may request erasure of your data, you may object against the data processing). Chapter 15 also contains the legal remedies available to you.

11 Placing Anonymous Visitor Identification (cookie) on Our Website

As most companies, Microsec also uses cookies when operating its websites (www.e-szigno.hu, www.microsec.hu, hereinafter: the website). When visiting our website, there is a pop-up sign at the bottom of the screen informing you about the fact that Microsec uses cookies for operating certain functions of its website, and there is also a link indicated which leads you to this Policy. By clicking on the "I agree" button on the right-hand side of the pop-up window, you accept the use of cookies.

Microsec places small data packages (cookies) on your computer and then reads them with the help of your browser in the interest of analyzing the use of our website and thereby improving our services. This is necessary because if your browser returns a cookie previously saved, the operator processing the cookie can link your current visit with previous ones, but only in connection with the content of the website.

You can erase the cookies from your computer at any time and you can also block the application of cookies in your browser. Usually the 'Tools/Settings' menu provides the options to manage cookies, under the 'Privacy' settings, under the name "cookies". You can find more detailed guidelines at the following websites on secure online communication:

European Interactive Digital Advertising Alliance (http://www.youronlinechoices.com/hu/)

Hungarian Civil Liberties Union (http://www.nopara.org/blank-bvzk2)

The websites use cookies exclusively for the following purposes:

1.) *to check that the information notice indicated in the pop-up window has been accepted (if the user clicked on the acceptance button, the information never pops up again – this serves the comfort of the user)*

The legal basis of using these cookies is Article 5 (3) of Directive 2002/58/EC concerning the processing of personal data and the protection of privacy in the electronic communications sector and additionally, your consent which you provide or withdraw by the adequate setting of your browser functions.

Identification	Data content, description	Life span
cookiebar	Remembering the pop-up window containing the notice on cookies	1 year

2.) *remembering the individual setting of the website's user (such individual setting may be turning on the visually impaired settings on the website)*

The legal basis of using these cookies is Article 5 (3) of Directive 2002/58/EC concerning the processing of personal data and the protection of privacy in the electronic communications

sector and additionally, your consent which you provide or withdraw by the adequate setting of your browser functions.

Identification	Data content, description	Life span
blind_people	Remembering that the visually impaired settings are turned on	1 year

3.) Google Analytics services

The independent evaluation of visitation frequency data and other web-analytical statistics is assisted by Google as service provider by a built-in Google Analytics tracking code.

The legal basis for processing Google Analytics cookies is Article 5(3) of Directive 2002/58/EC concerning the processing of personal data and the protection of privacy in the electronic communications sector and additionally, your consent which you provide or withdraw by the adequate setting of your browser functions.

Identification	Data content, description	Life span
_ga	distinction of users	2 years
_gat	distinction of users	24 hours
_gid	Used to throttle request rate. I	1 minute

The function of Google Analytics cookies: Google Analytics cookies help the website operator to receive to most important information of the use of the website and to draw certain conclusions therefrom to further improve the website. These cookies gather information anonymously (e.g. the number of visit, which website lead the user to our website and which websites this user visited), without the identification of the user.

Detailed information on data procession in relation to Google Analytics cookies can be found at the below websites:

Google Privacy Guidelines (https://www.google.com/intl/hu/policies/privacy/)

Google Analytics Information for developers (https://developers.google.com/analytics/devguides/collection/analyticsjs/cookie-usage)

12 Measurements to Secure Data Privacy

For Microsec, data and information security are high priority issues, as it is an organization certified under ISO 27001 standard since 2003. ISO 27001 is an information security standard, which applies a process-driven approach to the establishment, introduction,

operation, monitoring, maintenance and development of the entire information security management system of an organization.

To ensure compliance with the standard, Microsec is audited yearly, in the course of which our entire data processing procedure is reviewed. By complying with the ISO 27001 standard, it is certified by an independent, external certifying body that Microsec has an information security system that is suitable to ensure the safeguarding of the confidentiality, integrity and availability of the data retained by us.

The ISO 27001 standard prescribes clearly: "All applicable legal, regulatory, contractual requirements and the organization's respective approach to comply with these requirements must be clearly identified, documented and updated in respect of all information systems and organization". As a result, our ISO 27001 certification means that the information systems of Microsec comply with the information security requirements set forth by law.

The security of your information is ensured by the following measures, with special attention to Article 32 of the General Data Protection Regulation as well:

- encryption of the personal data provided by the user, especially the passwords;
- regular risk assessment in accordance with the ISO 27001 standard (in order to identify the threats ad vulnerability which my impact our information system);
- stringent internal policies regarding the handling of IT equipment containing data and data carriers;
- ensuring continuous operation which is also required of us as trust service providers, which helps preventing data loss even if an unforeseen event occurs;
- communication through an encrypted SSL channel; and
- limitation of the access to information (only those members of staff are authorized to access the personal data we process, whose access is necessary in order to achieve any of the above purposes)

Please help us keeping information safe by not using obvious passwords and by regularly changing your password. We kindly ask you not to disclose your password to other persons.

13 Managing Data Breaches

According to the General Data Protection Regulation, "data breach" means a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorized disclosure of, or access to, personal data transmitted, stored or otherwise processed.

13.1 Our Internal Procedures in case of a Suspicion of a Personal Data Breach

Microsec employees must report immediately to the leader of their department and the DPO by e-mail all security incidents which may qualify as a personal data breach, by describing the underlying security breach and briefly presenting the pertaining evidence.

The department leader is obliged to have the incident reported investigated within 72 hours, to a degree depending on the severity of the breach.

In case there is a probable suspicion of a data breach, so for example the personal data in question are not accessible or the unauthorized access to the data is evident, the department leader shall inform the board of directors in writing (by e-mail) within 24 hours after becoming aware thereof and shall initiate the investigation of the incident.

13.2 Reporting the Personal Data Breach to the Supervisory Authority

If the board of directors of Microsec receives a notification on the probable suspicion of the occurrence of a personal data breach, the board of directors shall determine based on the notification and the pertaining investigation and after consultation with the DPO whether the personal data breach is likely to jeopardize the rights and freedoms of individuals.

When determining whether the personal data breach jeopardizes the rights and freedoms of natural persons, the following shall be taken into consideration:

- type of incident (e.g unauthorized access; alteration of erasure);
- nature of the personal data, their sensitivity and volume;
- how easy it is to identify the individual affected by the personal data breach;
- probability of the consequences regarding the individual and their materiality;
- number of affected individuals.

If the board of directors determines based on the above that the personal data breach in question is likely to carry risks in respect of the rights and freedoms of natural persons, then the Hungarian National Authority for Data Protection and Freedom of Information must be notified within 72 hours after becoming aware thereof.

This notice is given electronically and contains the following information:

- The nature of the personal data breach including - if possible - the categories of the data subjects and an estimate of the number of individuals affected, furthermore the categories of data affected by the breach and the volume of the such data;
- name and contact details of the DPO;
- the probable consequences which may arise from the personal data breach;
- the measures taken or planned by Microsec to remedy the personal data breach including – if applicable - the measures aimed at the mitigation of the detrimental consequences of the data breach.

Microsec keeps a registry of the data breaches indicating the facts, effects of the data breach and the measures made to remedy these breaches.

13.3 Informing the Persons Affected by the Personal Data Breach

If – based on the report received and after consultation with the DPO – the board of directors of Microsec determines that the occurred personal data breach is likely to carry a high risk to the rights and freedoms of individuals (for example, the breach results in identity theft or fraud, discrimination, financial loss, damage to the reputation, loss of confidentiality of personal data protected by professional secrecy, economic or social disadvantage), the individuals affected by the personal data breach shall be informed without undue delay.

The individuals affected are notified by e-mail to the address provided by them to Microsec as contact information, provided that Microsec is able to exactly identifythe individuals affected and this does not imply a disproportionate effort for Microsec. If notification via sending individual e-mails would require a disproportionate effort or the group of affected persons cannot be accurately determined, the affected individuals are informed of the occurrence of the personal data breach by a notice published on the opening page of the website of Microsec at www.e-szigno.hu.

Under Article 34(3) of the General Data Protection Regulation, Microsec is not obliged to provide the above notification regarding the data breach to the individuals affected, if any of the following conditions are met:

- Microsec implemented appropriate technical and organizational protection measures regarding the personal data affected by the personal data breach (such as encryption), which rendered the affected personal data unreadable to any person who is not authorized to access it,;

- Microsec took such measures after the personal data breach that ensure that the personal data breach no longer constitutes high risk to the rights and freedoms of data subjects

14 Activities Conducted as Data Processor

If you did not provide us directly with your personal data (e.g your data is contained by documents archived by a Subscriber, your contact details have been provided by your employer in an individual agreement or you applied for one of our job openings which you became aware of from a source other than our website), Microsec may qualify as data processor in your regard. In such cases, the person who handles your data based on your consent or a contract or other legal basis and who transferred your data to us is the data controller (e.g the Subscriber).

If Microsec processes personal data as data processor pursuant to an engagement of another data controller, Microsec still complies with the provisions of this Policy and processes the relevant data in accordance with the applicable law and the obligations undertaken vis-á-vis the data controller.

In the event that the Subscriber or any other processor acting as data controller engages Microsec as data processor to process personal data on behalf of the Subscriber or an other data controller, Microsec undertakes pursuant to Article 28 of the General Data Protection Regulation:

- to process the personal data only based on the written instructions of the controller, with the exception that the data processing is obligatory pursuant to the applicable European Union or Member State law; in such a case, the data processor shall inform the data controller of that legal requirement before processing,
- that the purpose and means of the data processing shall be determined by the data controller,
- to take all security measures prescribed Article 32 of the General Data Protection Regulation,
- to engage another data processor only as allowed under the provisions of the General Data Protection Regulation,
- to assist the data controller in the fulfilment of the data controller's obligation to respond to requests concerning exercising the data subject's rights,
- after the data processor no longer provides the services involving data processing, to delete or return all personal data to the data controller, depending on the choice of the data controller, to , and to delete all existing copies, unless the laws of the European Union or a Member State require the storage of the respective personal data,
- to make available to the data controller all information necessary to demonstrate compliance with the obligations laid down in Article 28 of the General Data Protection Regulation and allow for and contribute to audits, including inspections, conducted by the controller or another auditor mandated by the controller, including on-site audits.

Notwithstanding the above, Microsec excludes any and all liability as data processor in respect of such obligations, which shall be complied with by the data controller, therefore Microsec will not investigate whether the controller disposes of the consent or other legal basis in relation to the transferred personal data, other than requesting a respective statement of the controller.

It is the liability of the controller to immediately notify Microsec if the legal basis of the data processing in relation to the transferred data had ceased to exist.

In case Microsec processes the affected personal data exclusively pursuant to the agreement concluded with the controller, the data shall be destroyed or returned to the controller upon the termination of said agreement.

15 Personal Data Pertaining to Children and Third Persons

Persons under the age of 16 may not provide Microsec with personal data pertaining to them unless they obtained consent from their legal guardian.

By providing your personal data, you represent and warrant that you proceeded in compliance with the above, that your legal capacity in connection with providing your personal data is not limited.

In case your legal capacity to provide personal data is limited in any way, you are obliged to obtain the consent of concerned third parties (e.g. legal guardian, legal representatives or other persons). In this regard you shall consider whether the consent of any third person is required for providing the given personal data, therefore, the compliance with the foregoing Section is your responsibility. By providing your personal data to Microsec without the consent of third parties, you represent that your legal capacity to provide such data is not limited.

16 The Rights of the Affected Person and Legal Remedies Available

Following May 25, 2018 your privacy rights and the pertaining legal remedies are governed by EU legislation, in particular the General Data Protection Regulation (including in particular Articles 15., 16., 17., 18., 19., 20., 21., 22., 77., 78., 79. and 82.). Below is a summary of the most important provisions.

In case you wish to enforce the below rights, please contact our DPO, dr. Lilla Lovas legal counsel at adatvedelmitisztviselo@microsec.hu e-mail address, and at the telephone number (+36-1) 505 – 4444.

16.1 Your Right of Access

You have the right to receive information from us as to whether your personal data are being processed. If yes, you have the right to access your personal data and to gain access to the following information:

a) purpose of the data processing;

b) categories of the processed personal data;

c) the recipients or the category of recipients receiving or intended to receive your personal data including in particular any recipients in third countries or international organizations;

d) if applicable, the planned period of the retention of the personal data or if such is not possible, the criteria used for determining such period;

e) you have the right to request from us the rectification or erasure or restriction of processing of personal data and you are entitled to object against the processing of your personal data;

f) the right to lodge a complaint with a supervisory authority; and

g) if the data was not collected from you, all information available on the source thereof;

h) the existence of automated decision-making, including profiling, and at least in those cases, meaningful information about the logic involved, as well as the significance and the envisaged consequences of such processing for the data subject.

The above information is provided to you within the framework of this Policy. If you require, we will provide you with a copy of your personal data being processed by us. If you filed your request with us electronically, the information must be provided in an electronic format which is widely used unless you request otherwise.

If this Policy does not contain the information you require and you contact Microsec with a request relating to individual data processing or to be provided with a copy of your personal data, Microsec shall respond to your request within the shortest time after filing your request, but in all cases within 25 days, in an easy-to-understand written format.

16.2 Right to Rectification and Erasure (the "Right to be Forgotten")

You have the right to request the rectification of your inaccurate personal data which we shall respond without undue delay.

You the right to have your incomplete personal data completed, including by means of providing a supplementary statement.

You have the right to obtain the erasure of personal data concerning you without undue delay where one of the following grounds applies:

a) the personal data are no longer necessary in relation to the purposes for which they were collected or otherwise processed;

b) you withdraw consent on which the processing is based and there is no other legal ground for the processing;

c) you object to the processing pursuant to Article 21(1) and there are no overriding legitimate grounds for the processing;

d) the personal data have been unlawfully processed;

e) the personal data have to be erased for compliance with a legal obligation in Union or Member State law; or

f) the personal data have been collected in relation to the offer of information society services

We cannot comply with your request of erasure in case we are obligated to continue processing your data pursuant to the applicable law (such as for example before the expiry of the 10-year retention period in relation to certificates), or in order to ensure that we can present, enforce and defend our legal claims.

16.3 Right to Restriction of Processing

You have the right to request that we restrict the processing of your data in the following case:

a) the accuracy of the personal data is contested by you, for a period enabling us to verify the accuracy of the personal data;

b) the processing is unlawful and you oppose the erasure of the personal data and request the restriction of their use instead;

c) we no longer need the personal data for the purposes of the processing, but you require them for the establishment, exercise or defense of legal claims;

d) you have objected to processing, pending the verification whether the legitimate grounds of Microsec override yours.

Where processing has been restricted as per the above, such personal data shall, with the exception of storage, only be processed with your consent or for the establishment, exercise or defense of legal claims or for the protection of the rights of another natural or legal person or for reasons of important public interest of the Union or of a Member State.,

We will inform you before the restriction of processing is lifted.

16.4 Right to Data Portability

You have the right to receive the personal data concerning you, which has been provided to us, in a structured, commonly used and machine-readable format and have the right to transmit those data to another controller if Microsec (i) processes your data pursuant to your consent or an agreement; and (ii) the data processing is carried out by automated means.

In exercising your right to data portability, you shall have the right to have your personal data transmitted directly from one controller to another, where technically feasible.

16.5 Right to Object

You have the right to object, on grounds relating to your particular situation, at any time to processing of personal data concerning you. In such case, we shall no longer process your personal data unless we demonstrate compelling legitimate grounds for the processing which override your interests, rights and freedoms or for the establishment, exercise or defense of legal claims.

Where personal data are processed for direct marketing purposes, you have the right to object at any time to processing of personal data concerning you for such marketing to the extent that it is related to such direct marketing. Where you object to processing for direct marketing purposes, the personal data shall no longer be processed for such purposes.

In the context of the use of information society services, and notwithstanding Directive 2002/58/EC, you may exercise your right to object by automated means using technical specifications.

You also have the right to object to data processing of your personal data pursuant to Section 21 of the Act on Information. Microsec shall review the objections within the shortest time possible as of receipt of the request but no later than within 15 days and shall adopt a decision on the grounds thereof and shall inform you of the result in writing.

16.6 Right of Complaint Before the Supervisory Authority

You have the right to file a complaint with the supervisory authority - in particular the authority competent in the Member State according to your place of residence, employment or the suspected infringement – if you deem that the processing of your personal data infringes the General Data Protection Regulation. In Hungary, the competent authority is the Hungarian National Authority for Data Protection and Freedom of Information (http://naih.hu/; 1530 Budapest, Pf.: 5.; telephone: +36-1-391-1400; fax: +36-1-391-1410; e-mail: ugyfelszolgalat@naih.hu).

16.7 Effective Legal Remedies Against the Supervisory Authority

You have the right for effective legal remedies against the binding decision adopted by the supervisory authority concerning you and also if the competent supervisory authority does not deal with your complaint or it does not inform you within three months regarding the developments or results of the procedure pertaining to the complaint filed. The procedure against the supervisory authority shall be lodged in the Member State's court competent according to the registered seat of the authority.

16.8 Effective Legal Remedy Against the Data Controller or the Data Processor

In case of breach of your rights ensured by the General Data Protection Regulation, you have the right to seek remedy from a court of law. The litigation may be lodged – depending on your choice – before a court competent according to your address or residence.