MICROSEC

Microsec zrt.

Privacy Notice

Identifier: 1.3.6.1.4.1.21528.1.2.1.2.3

Version: 2.0

7 March 2025

Track Changes

Publication	Entry in Force	Amendment / Comment
1.	25-05-2018	New document.
1.1	05-04-2019	Extending data management roles, changes in the video system regarding the office move.
1.2	13-06-2019	Amendments necessary due to legislative changes (with respect to the GDPR).
1.3	22-08-2019	Information about outdoor cameras.
1.4	08-05-2020	Amendments due to new data processor, updating the provisions for the data protection officer and extending the cases of data processing.
1.5	26-05-2020	Extending the cases of data processing (introduction of paperless service application), small clarifications.
1.6	04-12-2020	Amendments due to new data processor, extending the cases of data processing (introduction of online video identification).
1.7	14-12-2020	Reference to legal requirement (laid down in Section 82/A of the Act CCXXII. of 2015 on the general rules of electronic transaction and trust services). Further amendments and clarifications for GDPR compliance.
1.8	26-11-2021	Data processing related to the personal data of operators registered in frame of the V2X PKI Service.
1.9	07-04-2022	Modifications and additions made as a result of the annual legal review.
1.10	13-09-2022	Introduction of additional data processor, expanding the scope of data processing (introduction of non real-time online video identification).
1.11	19-09-2023	Updating the list of data processors, transferring data to third parties, changing the legal basis for processing the data of an organization's administrator, revising data processing in connection with V2X, using of telephone number for authentication purposes
1.12	19-02-2024	Extending the cases of data processing (inclusion of new Root CA to the V2X PKI trust list managed by Microsec)
1.13	15-05-2024	Addition to the scope of data processing (provision of remote assistance services), minor clarifications.
1.14	1-09-2024	Amendment required due to the entry into force of Act CIII. of 2023 on the Digital State
2.0	07-03-2025	Restructuring of document, clarification and modification of certain data processing cases

Contents

1. General Terms and Contact Details

This privacy notice (***Privacy Notice***) applies to personal data that are or may be processed in relation to you by Microsec Micro Software Engineering & Consulting Private Company Limited by Shares (1033 Budapest, 13 Ángel Sanz Briz Road, 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 Privacy Notice, 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/ furthermore, https://v2x-pki.com/ before providing any data under this Privacy Notice to Microsec.

Phone: (+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 dpo@microsec.hu.

2. Updates of the Privacy Notice 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/ furthermore, https://v2x-pki.com/

so that you are aware of any such amendments.

3. Reading and Accepting this Privacy Notice

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 Privacy Notice 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, web-Szignó) 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, or the personal data uploaded to web-Szignó). 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 Privacy Notice 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 Privacy Notice.

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 Privacy Notice 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 CIII of 2023 on the Digital State and Certain Rules for the Provision of Digital Services (hereinafter: ***Digital State Act***);
- 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***);
- Government decree No. 541/2020. (XII. 2.) on the other methods of identification which provide equivalent safeguard to personal presence and are recognized at national level in case of trust services.

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 we request further personal data necessary to comply with our identification obligation), 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 Privacy Notice.

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 (among others) 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 authentica-tion; 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 *Digital State* Act) 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 an "applicant") we as trust service provider are obligated under Section 85(1) of the *Digital State* Act 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 image (photo) of your face,
- in case of identification using video technical means: the photo and video taken of you and the declarations you made during such video call,
- the photo of your ID card,
- 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 / presented via identification using video technical means) 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 or 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 are related to the certificate and therefore will be stored in accordance with the provisions set out in Annex 1 of this Privacy Notice.

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

Section 88(1) of the *Digital State* Act 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, authentication and encryption certificates), 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).

Based on 86 (2) of the *Digital State* Act, in case of identification by video technical means provided in accordance with Government Decree No. 541/2020. (XII. 2.) on the other methods of identification which provide equivalent safeguard to personal presence and are recognized at national level in case of trust services, trust services providers shall record and preserve for 10 years from the expiry date of the certificate the entire communication between the trust service provider and the applicant during the identification by video technical means, the detailed information provided to the applicant in relation to the identification by video technical means and the applicant's express consent to it, in a retrievable mode, in a way which prevents the image and sound recording from deterioration. Based on 86 (3) of the *Digital State* Act, the trust service provider is entitled to preserve the image record taken of the identity card of the natural person for 10 years as of the expiry date of the certificate.

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 (which is 10 years as of the expiry of the validity of the certificate, pursuant to Section 88(1) of the *Digital State* Act). 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, legal bases

7.1 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) in case of data processing based on the legitimate interests of the data controller or a third party, the respective legitimate interests of the controller or the third party; (iv) the personal data retention time; (v) the categories of the personal data subjects; (vi) 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 table contained in Section 7.2 and Annex 1. 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.

7.2 According to Article 6 (1) of the GDPR, processing of personal data shall be lawful only if and to the extent that at least one of the following applies:

a) the data subject has given consent to the processing of his or her personal data for one or more specific purposes;

b) processing is necessary for the performance of a contract to which the data subject is party or in order to take steps at the request of the data subject prior to entering into a contract;

c) processing is necessary for compliance with a legal obligation to which the controller is subject;

d) processing is necessary in order to protect the vital interests of the data subject or of another natural person;

e) processing is necessary for the performance of a task carried out in the public interest or in the exercise of official authority vested in the controller;

f) processing is necessary for the purposes of the legitimate interests pursued by the controller or by a third party, except where such interests are overridden by the interests or fundamental rights and freedoms of the data subject which require protection of personal data, in particular where the data subject is a child.

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. In such cases, the employer or other organization (in the interest of whom certificates are applied for) may initiate the certificate application process by submitting the personal data of all certificate subjects (employees or other persons acting on behalf of the organization) simultaneously, via the organization's administrator (hereinafter: ***Mass Application***).

If the certificate-subject is also a signatory to the contract, then in all cases Article 6(1)(b) of the GDPR is the legal basis for the data processing, i.e. the performance of a contract to which the data subject is a party. This is the case when the "subject" is entitled to represent the Subscriber, for example, when the electronic signature certificate is requested by a person who is entitled to represent the Subscriber that is a legal person or when the Subscriber is also a natural person who is billed as a private individual (i.e. the Subscriber and the Subject are the same person). Furthermore, the Subject always signs a contract in case of requesting electronic signature certificates, as in these cases the Subject shall sign the document called "Annex to the Service Contract regarding the Subject" at all times.

However, since a contract is not always concluded directly with the certificate subjects, Article 6(1)(b) GDPR may not always be applicable as a legal basis.

In those cases, the processing of the personal data of the "subjects" by Microsec as data controller cannot be based on Article 6(1)(b) GDPR, since the data subject, whose data are processed by the data controller would have to be one of the contracting parties, which is not the case (except in the cases detailed above).

In such cases, the data processing is based on Article 6(1)(f) of the GDPR, the legitimate interest of Microsec. The legitimate interest of Microsec is based on the performance of the service contract between Microsec and the Subscriber, for which purpose it is necessary to process the personal data of the "subjects" who actually use the service.

If Microsec bases the processing of personal data on the legitimate interests of the controller or a third party pursuant to Article 6(1)(f) of the GDPR, a balancing test is prepared each case, comparing the interests of the controller with the fundamental rights of the data subject and deciding on this basis whether the processing is lawful. If the certificates are requested by way of a Mass Application by the organization's administrator, from the point of time when the organization's administrator provides the personal data of the subjects to Microsec until the subject signs the document called "Annex to the Service Contract regarding the Subject" the legal basis of the data processing is also Article 6(1)(f) of the GDPR. At this time, Microsec has not yet been able to obtain the necessary consent from the certificate subjects for the data processing, so the personal data of the certificate subjects provided by the organization's administrator are processed by Microsec on the basis of the legitimate interests of the employer or other third party (the contracted partner of Microsec) providing the data. 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 from the data of the certificate-subject in the table contained in Annex 1.

8. Authorized Data Processors

In connection with some technical tasks pertaining to the data processing activities, Microsec employs data processors. Microsec informs you on the person of the data processors in this section. Should Microsec employ further data processors, this section shall be updated accordingly and Microsec shall inform the data subjects as set out in the Privacy Policy (the internal data protection rules and regulations applied at Microsec, in Hungarian: Adatkezelési Szabályzat) of Microsec.

Microsec currently applies the following data processors:

1. *Arenim Technologies Fejlesztő és Szolgáltató Korlátolt Felelősségű Társaság (Company registration number: 01-09-330669, Registered seat: 1117 Budapest, Infopark sétány 1. I. ép.)*

The phone calls conducted by the customer service are being recorded, therefore, both the data of employees and clients (their voices and other personal data that may be shared throughout the phone call) are processed by Arenim.

2. *Pipedrive OÜ Registered seat: Mustamäe tee 3a, Tallinn 10615, Estonia)*

The documents, e-mails prepared 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 are recorded by Pipedrive OÜ. The processed data are typically the contact details of the individual proceeding on behalf of the partner in connection with the agreement (name, address, telephone number, e-mail) and also his/her activity in relation to the preparation and performance of the agreement.

3. *SIGNICAT SLU (Registered Seat: Avenida Ciudad de Barcelona 81 - 4ª floor, C.P. 28007 Madrid, Spain, Registration number: B-86681533)*

The data necessary for carrying out the video identification: photo of the identity card of the applicant and all data indicated therein, photo of the applicant, image and sound (video) recording and the declarations of the applicant made during the video technological identification.

4. *FaceKom limited liability company (Company registration number: 01-09-962028, Registered seat: 1015 Budapest, Szabó Ilonka street 9.)*

In connection with the software package necessary for non-real-time online video identification provides software tracking, incident management and remote monitoring services and provides a service to fix the bugs of the software package. In course of providing the service, the data processor has access to the following data necessary for the video identification: the

image of the applicant's identity documents and the data contained therein, the photograph, image and sound recording (video) of the customer and the statements made by the customer in course of the video identification.

5. Google Ireland Limited (Registered seat: Gordon House, Barrow Street, Dublin 4, Ireland)

In connection with the potential crushes of the e-Szignó mobile application, the application version, operating system version of the User's mobile device, device type, language, the circumstances in which the crush occurred, the user's OID or, in the absence of an OID, e-mail address, and the unique identifier (vendor) within the operating system.

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. 1033 Budapest, Ángel Sanz briz út 13.; 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 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 Privacy Notice.

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 legitimate interest of Microsec, therefore the CCTV is mainly used for the protection of Microsec's assets, to prevent crime and obtain proof of crime if necessary, to ensure the integrity and undisturbed operation of trust services. Through this means detection of such crimes and identifying the perpetrator is easier. Prevention of such crimes cannot be achieved through other means, and the application of CCTV does not exceed the necessary measures, therefore it does not restrict the right of informational self-determination of the data subjects. Microsec has conducted the balance of interests test with respect to the data processing activity and has documented it properly.

For the sake of property protection, two cameras are installed in the client service area of Microsec located at the ground floor of 1033 Budapest, Ángel Sanz Briz út 13., which the clients typically enter in order to receive their cards (personal identification). The cameras in the client service area are directed to the waiting area and the entrance. Further areas where clients or potential clients might enter are also covered by cameras are as follows:

First floor: one camera covers the entrance door, another one covers the entrance of the

meeting room and the adjacent corridor.

Third floor: one camera covers the waiting area, two further cameras are directed to the corridors leading to the elevators

In addition, six outdoor cameras have been installed that focus on the facade of the Microsec building and serve security purposes.

Microsec monitors the events through the recordings made by these thirteen cameras and stores the recordings at its registered seat located at 1033 Budapest, Ángel Sanz Briz út 13., 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 username and password.

The recordings may be viewed only in case there is a security breach; otherwise, the system deletes the recordings after 7 days. 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 16 of this Privacy Notice (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 with the exception of certain cases as outlined in the present Privacy Notice, you may object against the data processing). Chapter 16 also contains the legal remedies available to you. In addition to the rights set out in Chapter 16 you are also entitled to request to access (i.e. to look into) the recordings concerning you from the DPO, provided that you justify the reason for requesting access to the footages and that you determine the time of preparation of the recording with at least 30 minutes of accuracy (so that finding the footage would not mean a disproportionate burden for Microsec). Microsec shall keep reports on the reason and time of accessing the recordings and the name of the person making the request. We hereby inform you that you cannot request erasure of the recordings before the expiration of the retention period, otherwise the purpose of applying CCTV cannot be ensured.

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, portal.e-szigno.hu, web-szigno.com, hereinafter: the website).

Microsec places small data packages (cookies) on your computer and then reads them with the help of your browser in the interest of operating and 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.

When you visit our websites, a notice will pop up at the bottom of the screen informing you that Microsec uses cookies to improve the functionality of the website and enhance your browsing experience. The notice also contains a link to this Privacy Notice. The cookies used on our website are distinguished between cookies that are essential for the functioning of the website and comfort cookies that enhance your browsing experience. You give consent to the use of cookies by clicking on one of the following buttons on the right of the pop-up cookie bar:

"I accept the cookies essential for the functionality of the website" or

"I accept all cookies".

Please note that the use of cookies essential for the functionality of the website does not involve the processing of personal data, so consent to the use of these cookies is not required from a data protection perspective.

Without the use of these cookies, our websites cannot be displayed, therefore it is obligatory to download them in order to browse our websites.

Comfort cookies to enhance your browsing experience may only be used upon your explicit consent (as personal data may be processed if you download them).

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: Please note that erasing the cookies or rejecting the cookies on our website as outlined above may negatively impact your browsing experience.

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

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

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.

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 anony-

mously (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)

The websites of Microsec use the following cookies:

www.microsec.hu

1. Name of cookie: has_js

Cookie lifetime: session
Purpose of cookie: Stores the existence of JavaScript, for a more convenient browsing experience.
When: when loading website
Personal data storage: no
Essential for functionality: yes

2. Name of cookie: cookie-agreed-version

Cookie lifetime: 3 months 8 days
Purpose of cookie: It records the acceptance of the use of cookies.
When: when loading website
Personal data storage: no
Essential for functionality: yes

3. Name of cookie: _gat

Cookie lifetime: 1 year
Purpose of cookie: Google Analytics cookie. It is used to control the speed of requests.
When: when loading website
Personal data storage: yes
Essential for functionality: no

4. Name of cookie: _gid

Cookie lifetime: 1 day
Purpose of cookie: Google Analytics cookie. It is used to distinguish between users.
When: when loading website
Personal data storage: yes
Essential for functionality: no

5. Name of cookie: _ga

Cookie lifetime: 2 years
Purpose of cookie: Google Analytics cookie. It is used to distinguish between users.
When: when loading website

Personal data storage: yes
Essential for functionality: no

www.e-szigno.hu

1. Name of cookie: cookie:accepted
Site: e-szigno.hu
Cookie lifetime: 1 year
Purpose of cookie: It records the ac-ceptance of the use of cookies.
When: when loading website
Personal data storage: no
Essential for functionality: yes

2. Name of cookie: eszigno_locale
Site: e-szigno.hu
Cookie lifetime: session
Purpose of cookie: It records the lan-guage chosen or preferred by the user.
When: when loading website
Personal data storage: no
Essential for functionality: yes

3. Name of cookie: csrf_token
Site: e-szigno.hu
Cookie lifetime: session
Purpose of cookie: The visitor's own unique identifier that his/her browser sends to the web-site (prevents an un-wanted command from being sent to the site on behalf of the user)
When: when loading website
Personal data storage: no
Essential for functionality: yes

4. Name of cookie: PHPSESSID
Site: e-szigno.hu
Cookie lifetime: session
Purpose of cookie: Identification of PHP session
When: when loading website
Personal data storage: no
Essential for functionality: yes

5. Name of cookie: _ga
Site: e-szigno.hu
Cookie lifetime: 2 years
Purpose of cookie: Google Analytics cookie. It is used to distinguish between users.
When: when loading website
Personal data storage: yes
Essential for functionality: no

6. Name of cookie: PREF

Site: e-szigno.hu / youtube.com
Cookie lifetime: 2 years
Purpose of cookie: Google uses this cookie to record the user's language preference.
When: when loading website
Personal data storage: yes
Essential for functionality: no

7. Name of cookie: VISITOR_INFO1_LIVE

Site: e-szigno.hu / youtube.com
Cookie lifetime: 6 months
Purpose of cookie: This cookie is used as a unique identifi-er to track the viewing of videos.
When: when loading website
Personal data storage: yes
Essential for functionality: no

8. Name of cookie: CONSENT

Site: e-szigno.hu / youtube.com
Cookie lifetime: 2 years
Purpose of cookie: This cookie is nec-essary to view vid-eo content embed-ded in the site.
When: when loading website
Personal data storage: yes
Essential for functionality: no

9. Name of cookie: YSC

Site: e-szigno.hu / youtube.com
Cookie lifetime: session
Purpose of cookie: This cookie is set by the YouTube video service on websites containing embedded YouTube video.
When: when loading website
Personal data storage: yes
Essential for functionality: no

www.portal.e-szigno.hu

1. Name of cookie: PHP-SESSID

Cookie lifetime: session
Purpose of cookie: Identifies the PHP session (identifies the session, no user settings are lost, text entered in a form is kept within the session)
When: when loading website
Personal data storage: no, but the session itself might contain personal data
Essential for functionality: yes

2. Name of cookie: cookieconsent_status

Cookie lifetime: 1 year
Purpose of cookie: It records the acceptance of the use of cookies.
When: upon acceptance of cookie

Personal data storage: no
Essential for functionality: yes

3. Name of cookie: x-cdn

Cookie lifetime: session
Purpose of cookie: Required for PayPal
When: after login
Personal data storage: yes
Essential for functionality: yes

4. Name of cookie: x-pp-s

Cookie lifetime: session
Purpose of cookie: Required for PayPal
When: after login
Personal data storage: yes
Essential for functionality: yes

5. Name of cookie: nsid

Cookie lifetime: session
Purpose of cookie: Required for PayPal
When: after login
Personal data storage: yes
Essential for functionality: yes

6. Name of cookie: X-PP-L7

Cookie lifetime: session
Purpose of cookie: Required for PayPal
When: after login
Personal data storage: yes
Essential for functionality: yes

7. Name of cookie: akavpau_ppsd

Cookie lifetime: session
Purpose of cookie: Required for PayPal
When: after login
Personal data storage: yes
Essential for functionality: yes

8. Name of cookie: enforce_policy

Cookie lifetime: 6 months
Purpose of cookie: Required for PayPal (GDPR)
When: after login
Personal data storage: yes
Essential for functionality: yes

9. Name of cookie: ts

Cookie lifetime: 3 years

Purpose of cookie: Required for PayPal
When: after login
Personal data storage: yes
Essential for functionality: yes

10. Name of cookie: ts_c

Cookie lifetime: 3 years
Purpose of cookie: Required for PayPal
When: after login
Personal data storage: yes
Essential for functionality: yes

11. Name of cookie: KHcl0EuY7AKSMgfvHl7J5E7hPtK

Cookie lifetime: 19 years 2 months
Purpose of cookie: Required for PayPal
When: after login
Personal data storage: yes
Essential for functionality: yes

www.web-szigno.com

1. Name of cookie: G_AUTHUSER_H

Cookie lifetime: While the session is active (until the browser is closed)
Purpose of cookie: Necessary to login via a Google account
When: when loading website
Personal data storage: yes
Essential for functionality: no (but it is necessary to login via a Google account)

2. Name of cookie: G_ENABLED_IDPS

Cookie lifetime: Unlimited
Purpose of cookie: Necessary to login via a Google account
When: when loading website
Personal data storage: yes
Essential for functionality: no (but it is necessary to login via a Google account)

3. Name of cookie: _gid

Cookie lifetime: 1 day
Purpose of cookie: Google Analytics cookie. It is used to control the speed of requests.
When: when loading website
Personal data storage: yes
Essential for functionality: no

4. Name of cookie: _gat

Cookie lifetime: 1 hour
Purpose of cookie: Google Analytics cookie. It is used to control the speed of requests.
When: when loading website
Personal data storage: yes

Essential for functionality: no

5. Name of cookie: _ga

Cookie lifetime: 1 year
Purpose of cookie: Google Analytics cookie. It is used to distinguish between users.
When: when loading website
Personal data storage: yes
Essential for functionality: no

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.

In case there is a probable suspicion of a data breach, in line with the relevant provisions of the Privacy Policy and the GDPR, the data protection officer and the members of management shall initiate the investigation of the incident and, if necessary, shall report it to the supervisory authority and inform the concerned 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 Privacy Notice 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 another 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 at adatvedelmitiszt-viselo@microsec.hu e-mail address, and at the telephone number (+36-1) 505 – 4477.

17. 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 Privacy Notice. 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 Privacy Notice 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.

18. 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.

19. 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.

20. 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.

21. 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.

22. 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).

23. 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.

24. 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.

1. Annex

1.1 Data processing related to issuing signature certificates and code signing certificates for natural persons

1.1.1 Qualified certificates

Type and purpose of the data processing

Issuing qualified certificates (or non-qualified but issued based on personal identification) to create electronic signature, for code signing, to natural persons, enforcing claims if necessary

Legal basis of the data processing

Upon requesting the certificate: in case of certificates for code signing 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 the case of a request for a signatory certificate, Article 6(1)(b) of the General Data Protection Regulation - the performance of a contract to which the data subject is a party, the scope of which is detailed in point 7. In this case, the subscriber will sign the "Annex to the Service Contract regarding the Subject".

In relation to data reconciliation necessary for issuing the certificate: Article 6. (1) c) 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 85(1) of the *Digital State* Act 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.

If issuing the certificate requires such data or information that is not contained in the Ministry of Interior register (especially a title, the existence of membership, appearing in a database or other identifier), the trust service provider issues the certificate after having requested the organization entitled to verify the required data or information, or after comparing it with other - if available, public - registers. Pursuant to Article 18 (3) of Act LXXVIII of 2017 on the Activities of Lawyers, the trust service provider shall provide information on the issuance of the certificate to the bar associations. Pursuant to Article 23/A (3) of Act LXXV of 2007 on the Hungarian Chamber of Auditors, Auditing Activities and Public Oversight of Auditing, the trust service provider shall immediately provide the Chamber with information on the issuance of the electronic signature of the auditor who is a member of the Chamber, and on its revocation.

Article 6(1)(a) of the General Data Protection Regulation - the data subject's consent in relation to the display in the certificate store after the issuance of a signatory certificate, which the data subject gives when applying for the certificate.

Categories of the processed data

If the subject of the certificate (typically a natural person) and the subscriber who pays the service fee and performs the administrative tasks related to the service are different persons, we will collect the billing data of the Subscriber, which, if the Subscriber is a natural person, will be processed in accordance with point 8 of this Annex. 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 case of representative of the company: tax number. 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. In the case of applications for code-signing certificates for natural persons, the municipality of residence of the applicant will also be indicated on the certificate, therefore the applicant shall present his/her address verification document.

Furthermore, we also record your registration and 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 addition to the data provided, the data retrieved from the Ministry of Interior register contains the sex of the applicant, which is compared with the data on the provided ID document as part of the identity check.

If data or information not included in the Ministry of Interior Register is required for the issuance of the certificate, in connection with the verification of such data or the issuance of the required certificate, the trust service provider must identify without any doubt the person from whom the data, information or verification (in particular the verification pursuant to Section 18 (2) of Act LXXVIII of 2017 on Legal Practice) is requested. Therefore, if the data or information cannot be verified in a public database or if the public database does not contain the amount of personal identification data necessary to identify the person concerned beyond reasonable doubt, the trust service provider shall provide the following data of the person concerned to the body managing the register and issuing the verification: name, place of birth, date of birth.

The certificate store contains the personal data contained in the certificate.

Term of the data processing

At least 10 years as of the expiry of the certificate pursuant to Section 88(1) of the *Digital State* Act. If the trust service provider is notified by a claimant, public authority or court of a dispute concerning the authenticity or validity of the data contained in the certificate, the trust service provider shall comply with the obligation to preserve the data until the dispute is finally settled, even if the ten-year period from the expiry of the certificate has already expired.

Who has authorized access to the data within Microsec?

- 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

1.1.2 Non-qualified certificates

Type and purpose of the data processing

Issuing non-qualified signature certificates (without personal identification) to natural persons (such as the signature certificates is-sued to examination officers and school staff), enforcing claims if necessary

Legal basis of the data processing

Upon request of the certificate: the performance of a contract to which the data subject is a party, the scope of which is detailed in point 7. In this case, the subscriber will sign the "Annex to the Service Contract regarding the Subject".

In relation to data reconciliation necessary for issuing the certificate: 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 85(1) of the *Digital State* Act 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

Article 6(1)(a) of the General Data Protection Regulation - the data subject's consent in relation to the display in the certificate store after the issuance of a signature certificate, which the data subject gives when applying for the certificate.

Categories of the processed data

Microsec offers such signature certificates for natural persons that operate with a software and that are issued remotely in a simplified procedure without personal identification. A lower level of security applies to these certificates than to those which require personal presence, so these "non-qualified" (enhanced 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.

If the subject of the certificate (typically a natural person) and the subscriber who pays the service fee and performs the administrative tasks related to the service are different persons, we will collect the billing data of the Subscriber, which, if the Subscriber is a natural person,

will be processed in accordance with point 8 of the Annex.

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, or electronically via our application platform 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, in case of representative of the company: tax number. These data will be compared to the data contained by the Ministry of Interior register pursuant to our legal obligation. In addition to the data provided, the data retrieved from the Ministry of Interior register contains the sex of the applicant, which is compared with the data on the provided ID document as part of the identity check.

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.

The certificate store contains the personal data contained in the certificate.

Term of the data processing

At least 10 years as of the expiry of the certificate pursuant to Section 88(1) of the *Digital State* Act as this retention period is not only prescribed to qualified certificates but to all certificates issued as a trust service provider. If the trust service provider is notified by a claimant, public authority or court of a dispute concerning the authenticity or validity of the data contained in the certificate, the trust service provider shall comply with the obligation to preserve the data until the dispute is finally settled, even if the ten-year period from the expiry of the certificate has already expired.

Who has authorized access to the data within Microsec?

- registration officers
- application operators
- system administrator key account managers to administer the special requests of clients with individual agreements

The certificate store is public, so the data contained therein can be accessed by third parties.

1.2 Data processing related to the issuing signature certificates, web-site authentication and code signing certificates for legal entities

1.2.1 Qualified certificates

Type and purpose of the data processing

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, enforcing claims if necessary.

Legal basis of the data processing

Upon requesting the certificate: 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.

In relation to data reconciliation necessary for issuing the certificate: 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 85(1) of the *Digital State* Act; 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.

Categories of the processed data

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 Interior register thereby complying with our legal obligation. In addition to the data provided, the data retrieved from the Ministry of Interior register contains the sex of the applicant, which is compared with the data on the provided ID document as part of the identity check.

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.

Term of the data processing

At least 10 years as of the expiry of the certificate pursuant to Section 88(1) of the *Digital State* Act. If the trust service provider is notified by a claimant, public authority or court of a dispute concerning the authenticity or validity of the data contained in the certificate, the trust service provider shall comply with the obligation to preserve the data until the dispute is finally settled, even if the ten-year period from the expiry of the certificate has already expired.

Who has authorized access to the data within Microsec?

- 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

1.2.2 Non-qualified certificates

Type and purpose of the data processing

Non-qualified seal services (signature certificates issued to legal entities) (without personal identification)

Legal basis of the data processing

Upon requesting the certificate: 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.

In relation to data reconciliation necessary for issuing the certificate: 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 85(1) of the *Digital State* Act; in case you proceed on behalf of a legal entity (so you request the certificate for an organization), your authorization to represent the entity (and your personal identification in relation thereto) will be verified.

Categories of the processed data

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 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 Interior register pursuant to our legal obligation. In addition to the data provided, the data retrieved from the Ministry of Interior register contains the sex of the applicant, which is compared with the data on the provided ID document as part of the identity check.

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.

Term of the data processing

At least 10 years as of the expiry of the certificate pursuant to Section 88(1) of the *Digital State* Act. If the trust service provider is notified by a claimant, public authority or court of a dispute concerning the authenticity or validity of the data contained in the certificate, the trust service provider shall comply with the obligation to preserve the data until the dispute is finally settled, even if the ten-year period from the expiry of the certificate has already expired.

Who has authorized access to the data within Microsec?

- registration officers (for handling the applications and carrying out the identification procedure)
- application operators
- system administrator
- key account managers to administer the special re-quests of clients with individual agreements

1.3 Data processing related to the issuing Authentication and Encryption

Certificates

1.3.1 Certificates issued with personal identification

Type and purpose of the data processing

Issuing authentication and encryption certificates to natural persons or legal entities – with personal identification.

Legal basis of the data processing

If it is a legal entity requesting the certificate, in respect of the natural person proceeding on behalf of the legal entity: Article 6. (1) a) of the of the General Data Protection Regulation – consent of the data subject which is provided electronically on the Microsec website 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.

In relation to data reconciliation necessary for issuing the certificate: 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 85(1) of the *Digital State* Act; in case you proceed on behalf of a legal entity (so you request the certificate for an organization), your authorization to represent the entity (and your personal identification in relation thereto) will be verified.

Categories of the processed data

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, in case of representative of the company: tax 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 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. In addition to the data provided, the data retrieved from the Ministry of Interior register contains the sex of the applicant, which is compared with the data on the provided ID document as part of the identity check.

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.

Term of the data processing

Since Section 88 (1) of the *Digital State* Act applies to all certificates issued as trust service provider, the period of data retention is at least 10 years from the expiry of the certificate's validity. If the trust service provider is notified by a claimant, public authority or court of a dispute concerning the authenticity or validity of the data contained in the certificate, the trust service provider shall comply with the obligation to preserve the data until the dispute is finally settled, even if the ten-year period from the expiry of the certificate has already expired.

Who has authorized access to the data within Microsec?

- 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

1.3.2 Certificates issued without personal identification

Type and purpose of the data processing

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)

Legal basis of the data processing

If the applicant is a legal entity requesting the certificate, in respect of the natural person proceeding on behalf of the legal entity Article 6 (1) a) of the of the General Data Protection Regulation – consent of the data subject which is provided electronically on the Microsec website 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.

In relation to data reconciliation necessary for issuing the certificate: 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 85(1) of the *Digital State* Act; in case you proceed on behalf of a legal entity (so you request the certificate for an organization), your authorization to represent the entity (and your personal identification in relation thereto) will be verified.

Categories of the processed data

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 or electronically, via our application platform 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 identification and the ID number, in case of representative of the company: tax 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. In addition to the data provided, the data retrieved from the Ministry of Interior register contains the sex of the applicant, which is compared with the data on the provided ID document as part of the identity check.

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.

Term of the data processing

Since Section 88 (1) of the *Digital State* Act applies to all certificates issued as trust service provider, the period of data retention is at least 10 years from the expiry of the certificate's validity. If the trust service provider is notified by a claimant, public authority or court of a dispute concerning the authenticity or validity of the data contained in the certificate, the trust service provider shall comply with the obligation to preserve the data until the dispute is finally settled, even if the ten-year period from the expiry of the certificate has already expired.

Who has authorized access to the data within Microsec?

- 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

1.4 Data processing in case of paperless service application

Type and purpose of the data processing

In case of certain services, the entire procedure of the application can be managed electronically (it is the so-called paperless application).

The purpose of the data processing is to issue qualified, non-qualified signature certificates authentication and encryption certificates, and enforcing claims if necessary.

Legal basis of the data processing

Upon requesting the certificate: 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 the case of a request for signature certificates or authentication and encryption certificates issued for private persons, Article 6(1)(b) of the General Data Protection Regulation - the performance of a contract to which the data subject is a party, the scope of which is detailed in point 7. In this case, the subscriber will sign the "Annex to the Service Contract regarding the Subject".

In relation to data reconciliation necessary for issuing the certificate 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 85(1) of the Digital State Act 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.

Categories of the processed data

We process the following data during the paperless application: in each case we process the data pertaining to the requested certificate (as described above), and in addition, as in case of paperless application we request a photo of the applicant for identification purposes, we process his/her photo as well.

In the event you request qualified certificate in a paperless way, we do not request you to provide us with your photo but the data processing rules for online video identification detailed

under section 5 of this chapter are applicable.

Term of the data processing

At least 10 years as of the expiry of the certificate pursuant to Section 88(1) of the *Digital State* Act. If the trust service provider is notified by a claimant, public authority or court of a dispute concerning the authenticity or validity of the data contained in the certificate, the trust service provider shall comply with the obligation to preserve the data until the dispute is finally settled, even if the ten-year period from the expiry of the certificate has already expired.

Who has authorized access to the data within Microsec?

- registration officers
- application operators
- system administrator
- key account managers to administer the special requests of clients with individual agreements

1.5 Data processing in case of identification by video technical means (for the issuance of qualified certificates)

Type and purpose of the data processing

In accordance with the Government Decree No. 541/2020. (XII. 2.) on the other methods of identification which provide equivalent safeguard to personal presence and are recognized at national level in case of trust services, Microsec, as a trust service provider, can also verify the applicant's identity by means of an electronic communication device providing video technology (identification by video technical means).

Microsec uses both real-time and non-real-time video identification. The purpose of the data processing is to issue qualified signature certificates and qualified seal services, also enforcing claims if necessary.

Legal basis of the data processing

When requesting the certificate: the General Data Protection Regulation Article 6 (1) c) - fulfilment of the legal obligation of the controller: once the data subject has given his/her consent to identification by video technical means, the data controller is obliged to comply with the provisions of Section 86 of the *Digital State* Act, thus Microsec is entitled to process the personal data. In relation to data reconciliation necessary for issuing the certificate: 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 85(1) of the *Digital State* Act 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.

Categories of the processed data

In addition to the data detailed in the relevant certificate (see above), in case of identification by video technical means, we process the following further data: photo of the identity card (and the attorney's license) and all data indicated therein, image and sound (video) record, the declarations made by the applicant and photo taken of the applicant during the video recording, recording of the entire communication.

Term of the data processing

Microsec records via video recording, and preserves for 10 years from the expiry date of the certificate pursuant to Section 86 (2)-(3) of the *Digital State* Act: the entire communication between Microsec and the applicant during the identification by video technical means, the detailed information provided to the applicant in relation to the identification by video technical means and the applicant's express consent to it, in a retrievable mode, and in way which prevent the image and sound recording from deterioration.

Who has authorized access to the data within Microsec?

- registration officers
- application operators
- system administrator
- key account managers to administer the special requests of clients with individual agreements

In case of real-time video identification, SIGNICAT SLU acts as data processor.

In case of non-real-time video identification FaceKom Limited Liability Company acts as data processor.

1.6 Data processing related to KASZ identification (for the issuance of qualified certificates)

Type and purpose of the data processing

In the case of trust services, Microsec as a trust service provider may verify identity by means of KASZ identification in accordance with the provisions of Government Decree 541/2020 (XII. 2.) on other nationally recognized methods of identification providing equivalent assurance to personal presence. The purpose of the data processing is to fulfil the trust service provider's obligation to identify the person.

Legal basis of the data processing

In relation to data reconciliation necessary for issuing the certificate 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 85(1) of the Digital State Act 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.

Categories of the processed data

In addition to the data contained in the certificate request (see above), the following additional data are processed in the case of KASZ identification: electronic data read from the identity document: identity document data (type, document number, issuing country, expiry date, date of issue), name, birth name, nationality, mother's name, place of birth, date of birth, in the case of a company representative: tax identification number. In case of KASZ identification, if the document type allows it, the following data of the applicant are read out from the document using NFC (near field communication): photo, signature picture, name, name at birth, name at birth, mother's name, sex, place of birth, date of birth, type, number and validity of the identity document.

Term of the data processing

Microsec will retain the data recorded during the KASZ-identification for 10 years from the expiry date of the certificate.

Who has authorized access to the data within Microsec?

- registration officers
- application operators
- system administrator
- key account managers to administer the special requests of clients with individual agreements

1.7 Data processing related to archiving as data controller and as data processor

1.7.1 Data processing related to archiving as data controller

Type and purpose of the data management

Providing archiving services

Legal basis of the data *processing*

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: Article 6. (1) f) of the General Data Protection Regulation – legitimate interest of Microsec

Categories of the *processed* data

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).

The following personal data are available in the archiving systems: the unique ID of the certificate (OID), the name displayed in the certificate and the e-mail address provided for the aim of archiving.

Upon erasure of the documents uploaded to the archives (which mostly occurs in case of termination of the contract), the service provider shall make a registry of the erased folders, containing the size of the erased folders, the time of upload, the title and category of folders (hereinafter: Registry of Erased Folders).

We do not have access to the personal data contained in the uploaded documents, we only store them as processor.

Term of the data processing

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 (i) the communication with the Subscriber was in accordance with the agreement via the channels determined by the Subscriber and that (ii) Microsec had not breached the provisions of the agreement in place, furthermore that (iii) based on the Registry of Erased Folders the amount of payment obligation towards the Service Provider can be established (in order to claim payment). This is the basis for Microsec's legitimate interest for the data retention after the termination of the service contract.

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).

Who has authorized access to the data within Microsec?

- 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

1.7.2 Data processing related to archiving as data processor

Type and purpose of the data processing

Processing of personal data contained in documents archived by our customers. The data stored is not accessible to us due to the encryption procedure used. The encryption can only be lifted if the Subscriber requests it in writing.

Legal basis of the data processing

Microsec will store the archived documents as a data processor in accordance with the data processing agreement set out in Annex 1 of the e-Signature Authentication Service Provider Terms and Conditions.

Categories of the processed data

We do not know what personal data is contained in the archived documents, as we do not have access to it. However, given that our archiving services are typically used by lawyers and notaries, it can be assumed that the documents contain a large amount of personal data.

Term of the data processing

The duration of the contract with the Subscriber. At the end of the term, the archived documents will be deleted from our system.

Who has authorized access to the data within Microsec?

- archiving officer, only if requested in writing by the client

1.8 Data processing related to time stamp service

Type and purpose of the data processing

Providing time stamp services

Legal basis of the data processing

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: Article 6(1) f) of the General Data Protection Regulation – Microsec legitimate interest of Microsec.

Categories of the processed data

The time stamping service is sold by Microsec primarily as part of electronic signature packages. In order to acquire the services, a user ID and a password is required which are stored by our system. If the services are obtained by private persons, the user ID and password are linked to the private person (for example, in the case of signature packages or if the time stamp service is ordered by a private person).

In case the service is provided to a legal entity, the user ID and password are not linked to a private person (since they are used to identify the entity and Microsec has no information about who is using them on behalf of the entity), so in this case they are not considered personal data.

Term of the data processing

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 (statutory limitation) set forth in Section 6:22 of the Civil Code applies with respect to the user ID and

password 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 (i) the communication with the subscriber was in accordance with the agreement, it was made via the channels determined by the client (ii) that Microsec had not breached the provisions of the agreement in place furthermore, Microsec also needs to have the time stamp consumption data relating to the subscriber.

(In the Timestamp Consumption Registry database, the data will continue to be stored after 5 years, but then this will be done anonymously, so that the data can no longer be linked to the natural person.)

This is the basis for Microsec's legitimate interest for the data retention after the termination of the service contract.

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).

Who has authorized access to the data within Microsec?

- registration colleagues
- application operators
- system administrator
- sales colleagues

1.9 Data Processing Related to Accounting Documents

1.9.1 Invoicing our services, keeping receipts

Type and purpose of the data processing

Invoicing of our services, retaining the underlying accounting documentation.

Legal basis of the data processing

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).

Categories of the processed data

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, especially the name and the invoicing address.

Term of the data processing

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.

Who has authorized access to the data within Microsec?

- colleagues of the finance department
- sales colleagues
- client service desk in case of agreements

1.9.2 Indication of the subject of the certificate

Type and purpose of the data processing

Indication of the subject of the certificate on the accounting document. Given the fact that a Subscriber is billed for several certificates, Microsec and the Subscriber have a legitimate interest in ensuring that the invoices issued are easily identifiable and that the certificate subject is indicated on the invoice.

Legal basis of the data processing

The indication of the subject of the certificate is necessary for the legitimate interest of Microsec and the Subscriber as a third party, for the easier identification of the account, and therefore the legal basis is Article 6 (1) f) of the General Data Protection Regulation - legitimate interest of Microsec or a third party.

Categories of the processed data

The data processed are, in addition to the data referred to in point 1.9.1, the name of the subject of the certificate.

Term of the data processing

The retention period starts when the invoice is generated, in the case of an invoice, and when the contract is concluded, when the last invoice is issued (the contract is terminated). In this case, Microsec may only retain the data (containing the document) after 8 years from the end of the service provision, regardless of the consent of the data subject.

Who has authorized access to the data within Microsec?

- staff in the finance department
- sales staff
- customer service for contracts

1.10 Processing the data of an organization's administrator

Type and purpose of the data processing

The Subscriber as organization may appoint an administrator entitled to proceed on its behalf before Microsec in connection with the 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.

Legal basis of the data processing

Article 6(1) c) of the General Data Protection Regulation – the legitimate interests of Microsec as data controller and the Subscriber as a third party. The Organization's Administrator is appointed by the Subscriber to coordinate the certificate application process, thereby simplifying the administrative tasks of both the Subscriber and Microsec in connection with certificate application and maintenance, especially in the case of Mass Application.

Categories of the processed data

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 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).

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 - acknowledges that Microsec processes his/her personal data 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).

If any person (not only the organization's administrator) entitled to make the legal declaration requests the revocation or suspension of the certificate by SMS, then his / her telephone number is also included in the managed data.

Term of the data processing

We process the personal data of administrators in connection with certificates as these persons are entitled to make statements in connection therewith. As a result, we delete the data of the administrators from our registries at least 10 years after the expiry of the organization's certificates (Section 88(1) of the *Digital State* Act).

Who has authorized access to the data within Microsec?

- registration colleagues
- application operators

- system administrator
- sales colleagues

1.11 Data Processing Related to obligation to Log Data Pursuant to the Provisions of Law

Type and purpose of the data processing

Logging qualified services (IT environment, pertaining events).

Legal basis of the data processing

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.

Categories of the processed data

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 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.

Term of the data processing

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.

Who has authorized access to the data within Microsec?

- 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 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)

1.12 Data Processing in Connection with the MicroSigner services

Type and purpose of the data processing

Providing MicroSigner services.

Legal basis of the data processing

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.

Categories of the processed data

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 username 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. 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.

Term of the data processing

The email address, username and password will be stored for as long as the customer requests access to the trial version.

The statistics containing the details of the certificate with which you use the MicroSig-ner service and the frequency of use will be deleted annually.

Who has authorized access to the data within Microsec?

- colleagues of the technical support department
- application operator
- system operator

1.13 Data Processing Related to PassByME mobile electronic signature services

Type and purpose of the data processing

Providing PassByME mobile signature services, PassByME Mobile ID is a mobile application downloadable from application stores (AppStore, Google Play) providing signature solutions on smart devices. Only such end users may use the PassByME Mobile ID, whose organization (as Subscriber) registered on passbyme.com.

Legal basis of the data processing

Regarding the administrator of the organization: the legitimate interest of a third party, i.e. the organization receiving the service, Article 6(1)(f) of the General Data Protection Regulation.

Regarding further end-users: Article 6 (1) (b) of the General Data Protection Regulation -

performance of the contract with the end-user.

Following the termination of the respective service agreement: Article 6. (1) f) of the General Data Protection Regulation – legitimate interest of Microsec.

PassByME 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; with respect to these personal data, Microsec qualifies as data processor.

Categories of the processed data

Microsec provides the PassByME 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 PassByME services. Microsec enters into an end user license agreement with these end users, when the end users install the application on their phones. These data are also necessary to enable Microsec to invoice the Subscriber (the service fee is determined on the basis of the number of users). Microsec assumes that the administrator has an appropriate legal basis to forward these further users' data to Microsec.

In order to provide the PassByME mobile signature services, beyond the name, e-mail addressee and telephone number of the users, we need to register the individual identifier of the user (OID) within the global user system, the individual identifier of the user within the organization (PassByME ID), the type and operation system of and 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, vendoroid, public key).

Certificate subjects using the remote key management signature service provided by Microsec shall download the e-Szignó mobile application to use the remote key management signature service. By downloading the e-Szigno mobile application, these certificate subjects become users of the PassByME mobile signature service and the data processing operations set out in this clause will be performed in respect of them.

Term of the data processing

The data processing terminates 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 PassByME mobile signature services. The

processing of the administrator's data during the term of the service agreement is therefore in the legitimate interest of the respective organization, the Subscriber, as described above. 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 (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.

This is the basis for Microsec's legitimate interest for the data retention after the termination of the service contract.

With respect to the fact that the end-users typically approve financial transactions with the help of the PassByME mobile signature services, Microsec has a legitimate interest to store the data within the statutory limitation period.

Who has authorized access to the data within Microsec?

- colleagues of the technical support department
- application operator
- system operator

1.14 Data Processing Related to operating the download page for the e-Szignó Registration Database and Software Development Kit (SDK)

Type and purpose of the data processing

Operating the downloading page for 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 clients already having an end-user e-Szignó license.

Legal basis of the data processing

Regarding persons acting on behalf of contracted customers (organizations) - Article 6 (1) f) of the General Data Protection Regulation - the legitimate interest of Microsec and third parties, i.e. the organizations using the service.

Regarding persons interested in our software products - Article 6 (1) (b) of the General Data Protection Regulation – data processing is necessary for the performance of a contract to which you are a party, or - processing is necessary for the purposes of taking steps on your behalf prior to the conclusion of the contract.

Regarding individual customers who purchased the client side e-Szignó software product or other software products- 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. Following the

termination of the respective service agreement: Article 6 (1) f) of the General Data Protection Regulation – the legitimate interest of Microsec.

Categories of the processed data

Name of the client or the person interested in our services in case of natural persons. In case of legal entities, name of the representative, name of the organization and e-mail address. A username 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.

Term of the data processing

In respect of persons showing interest in 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.

The performance of the contract concluded between Microsec and the respective organization is in the legitimate interest of both parties. It is in Microsec's legitimate interest to identify the contracting party when using the service and in the customer's interest to be able to download the software purchased.

In the case of a software license agreement, the period of data processing is 5 years after the termination of the agreement in accordance with the Act V of 2013 on the Civil Code (Civil Code) 6:22. § (general limitation period), in order to enable Microsec to prove that (i) it has communicated with the subscriber of the service through the channels indicated by the subscriber in accordance with the contract (ii) it has not acted in breach of contract and (iii) the subscriber was obligated to pay service fees towards the service provider (for the purpose of debt recovery).

Who has authorized access to the data within Microsec?

- sales colleagues
- colleagues of the technical support department
- system operator

1.15 Data Processing Related to previously provi company Register Services

1.15.1 Previous provision of the OCCSZ Service for Subscribers

Type and purpose of the data processing

The operation of the OCCSZ Service (company information service containing data in force) for subscribers (subject to a fee) was provided by Microsec until 1 March 2025, after this the date the service provided by the Hungarian Company Data Service Ltd. After the transfer,

Microsec keeps a copy of the contracts under which it had provided the company information services for the 5 years preceding the transfer.

Legal basis of the data processing

In respect of the subscriber (if the subscriber was a natural person):

Article 6 (1) b) of the General Data Protection Regulation – processing is necessary for the performance of a contract to which the subscriber is a party or in order to take steps at the request of the subscriber prior to entering into a contract.

The subscriber was entitled to appoint a contact person in relation to the services in the contract The legal basis is Article 6. (1) f) of the General Data Protection Regulation – data processing is necessary for the purposes of the legitimate interests pursued by the controller or a third party. The legitimate interest lasts for 5 years from the date of transfer of the service, i.e. from 1 March 2025.

Categories of the processed data

The processed data: personal date of the persons indicated in the retained contracts.

Pursuant to the agreement concluded with the predecessor of the Ministry of Justice, the Ministry of Public Administration and Justice (Ministry Agreement), Microsec was obliged to technically operate the National Company Register and Company 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) entered 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.

Term of the data processing

The term of the data processing is identical to the term of the agreement we have in place with the subscriber. Following 1 March 2025 the 5-year period set forth 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 delivery of the service, Microsec is able to verify that (i) communication with the client was in accordance with the agreement via the channels determined by the client and that (ii) Microsec did not breach the provisions of such agreement.

Who has authorized access to the data within Microsec?

- system operator
- client service desk

1.15.2 Previous operation of the OCCSZ Service for public bodies and persons

Type and purpose of the data processing

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) was provided by Microsec until 1 March 2025, after which the service was transferred to Hungarian Company Data Service Ltd.

Legal basis of the data processing

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 was obligated to fulfill all requests regarding free company information, including the requests of the organizations set forth in Section 15(3) of the Company Registry Act.

Microsec received 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.) have used the service with an authentication certificate. Microsec assumes that the organizations charged with public duty entitled to free access possessed appropriate legal basis for the transferring the data of these private persons. Therefore, the legal basis is Article 6. (1) f) of the General Data Protection Regulation – data processing is necessary for the purposes of the legitimate interests pursued by the controller or a third party. The legitimate interest lasts for 5 years from the date of transfer of the service, i.e. from 1 March 2025.

Categories of the processed data

The data processed: personal data contained in the retained document called "employer's certificate".

The organization charged with public duty who is entitled to free access acting as data controller transfered 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 disposed of such certificate, the employer also transfered the data pertaining thereto. (In the absence thereof, an authentication certificate had to be required before using the OCCR system. Data processing issues related to

authentication certificates are set out in the respective line of this Privacy Notice.)

Organizations charged with public duty, who are entitled to free access, have also registered themselves with Microsec, as entities entitled to issue the above mentioned "employer's certificate". The registration was done through a form, signed by the authorized representative of the given organization. When filling out the form, the entity as data controller may have also provided contact details (name of the contact person, title, e-mail, telephone number), which are processed by Microsec on the basis of legitimate interest.

Term of the data processing

We retain the "employer's certificate" documents for 5 years after 1 March 2025 (within the statutory limitation period) in order to prove that the users did not make use of the free services unlawfully.

Who has authorized access to the data within Microsec?

- system operator
- client service desk

1.16 Data Processing Related to operating the System for Electronic Delivery of Judicial Execution Documents (VIEKR)

Type and purpose of the data processing

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.

Legal basis of the data processing

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. Therefore, the legal basis is Article 6. (1) f) of the General Data Protection Regulation – data processing is necessary for the purposes of the legitimate interests pursued by the controller or a third party.

Categories of the processed data

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 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.

Term of the data processing

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. (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.

Who has authorized access to the data within Microsec?

- system operator
- application operator

1.17 Processing the Data of Contact Persons of Clients and Potential Clients in case of Individual Agreements and Interested Parties

Type and purpose of the data processing

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. Maintaining a company calendar (recording meetings, discussions). Purpose

of data processing: more efficient work organization.

Legal basis of the data processing

Article 6 (1) f) of the General Data Protection Regulation – Microsec legitimate 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 has appropriate legal basis to disclose the given data.

Categories of the processed data

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 e-mails are typically signed by an automatic signature. Therefore, the processed data are typically the contact details of the individual 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.

Microsec conducts meetings and negotiations with external partners and other natural persons. These meetings are organized by using the company calendar. Typical data processed: partner's name, contact details (phone number, e-mail address).

Term of the data processing

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 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.).

We delete the contents of the company calendar once a year and store the data contained therein for a period of maximum one year.

Who has authorized access to the data within Microsec?

- sales colleagues
- Pipedrive OÜ is a data processor in this case

Public entries in the calendar are accessible to all colleagues.

Private and confidential events can only be viewed by the employee.

1.18 Data Processing Related to finding Potential Clients, building customer relationships

Type and purpose of the data processing

To build and maintain a customer relationship, to conclude individual customer contracts with Microsec.

Legal basis of the data processing

Article 6 (1) f) of the General Data Protection Regulation – the legitimate interest of Microsec.

Categories of the processed data

Inquiries from Microsec are made through the professional (and not private) contact details (name, e-mail address, telephone number) made publicly available by potential partners and interested parties.

Term of the data processing

The data will be deleted when it becomes clear and certain that business cooperation with the potential partner or interested party cannot be established for any reason. The data of the partners will be deleted after the existence of the partnership when it becomes certain that another, different type of business cooperation can no longer take place between them and Microsec.

Who has authorized access to the data within Microsec?

- V2X PKI team members,
- Employees working in the sales department

1.19 Data Processing Related to operating the Call Center and complaint handling

Type and purpose of the data processing

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 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). The purpose of recording telephone conversations is also to the quality assurance of our call center, to guarantee client satisfaction by evaluating and monitoring of the work of our call center colleagues. In order to evaluate the work of the customer service colleagues, after the call, the call taker can rate the conversation on a scale of 1 to 4, where 1 is dissatisfied and 4 is satisfied.

Legal basis of the data processing

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 or, after the interview, by rating on a scale of 1 to 4.

Categories of the processed data

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 which you may disclose during the telephone conversation, including especially the circumstances of the matter in respect of which you contacted the call center.

Term of the data processing

Until withdrawal of the data subject's consent and in the absence thereof, 90 days after the telephone conversation took place. If you rate the quality of your telephone conversation with us on a scale of 1 to 4 after the conversation, we will keep this rating.

Who has authorized access to the data within Microsec?

- 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 colleague responsible for quality assurance
- Arenim Technologies Developer and Service Provider Limited Liability Company is a data processor in this case
- with the permission of the head of customer service, a new colleague may listen to old recordings for learning purposes within the framework of a mentoring program, or the mentor can listen to his / her mentee's conversations for monitoring purposes

1.20 Data Processing Related to recruitment

Type and purpose of the data processing

Processing of data of natural persons applying to Microsec for the purpose of employment.

Legal basis of the data processing

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.

Categories of the processed data

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).

Term of the data processing

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.

Who has authorized access to the data within Microsec?

- HR generalist
- Board of directors
- future supervisor of the applicant

1.21 Data Processing for Marketing Purposes

1.21.1 Sending promotional material

Type and purpose of the data processing

Sending advertising materials by e-mail and advertising by telephone.

Legal basis of the data processing

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.

Categories of the processed data

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.

Term of the data processing

Upon the withdrawal of consent, the personal data must be deleted.

Who has authorized access to the data within Microsec?

- colleague responsible for marketing
- colleagues responsible for sales

1.21.2 Promotions, campaigns and media coverage

Type and purpose of the data processing

Promotions, campaigns and media appearances (as per the conditions applicable to the promotion).

Legal basis of the data processing

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).

Categories of the processed data

The scope of the personal data is determined on a case-by-case basis, as per the conditions applicable to participating in the promotion.

Term of the data processing

The term of the data processing is determined on a case-by-case basis as per the conditions applicable to participating in the promotion. If the data subject withdraws his / her consent, the pertaining data shall be erased.

Who has authorized access to the data within Microsec?

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.

1.22 Data processing related to the operation of the V2X User Portal

Type and purpose of the data processing

Use of certain menu items of the V2X User Portal available through the website https://portal.v2x-pki.com/. Upon registration, the user accepts a separate Terms of Use.

Legal basis of the data processing

General Data Protection Regulation Article 6 (1) (b) performance of a contract – by way of accepting the Terms of Use, the user enters into a contract with Microsec at the time of registration, the execution of which requires Microsec to process the portal login data.

Categories of the processed data

E-mail address (password) for registration.

Term of the data processing

User cannot delete the V2X User Portal account. If the user has not logged in to the V2X User Portal for at least one year, the account will be deleted by Microsec, together with the login data associated with the account.

Who has authorized access to the data within Microsec?

- customer service staff, sales representatives
- developers
- for debugging purposes, system administrators, developers

1.23 Data Processing related to registering for V2X PKI test certificates

1.23.1 Data provided before using the test version

Type and purpose of the data processing

Personal data disclosed before registering for the **V2X Public Key Instrastructure ("PKI") service, used for marketing purposes and sending newsletters**.

The Microsec V2X PKI is a PKI-based certification test system required for proper secure and standard communication between communicating vehicles, road users, and transportation infrastructure. In the system it is possible to register (user, organization, devices), then to request different test certificates - developed for vehicles, road users and transport infrastructure units - to use the functions necessary for testing.

Legal basis of the data processing

Based on Section 6 (1) of Act XLVIII of 2008 on the conditions and restrictions of commercial advertising activities (Advertisement Act) – the explicit and unambiguous prior consent of the data subject.

Categories of the processed data

The name, IP address, e-mail address, name of the employer, position of the person registering for the test certificates.

Term of the data processing

Users are entitled to withdraw their consent at any time on the same platform, furthermore, at the end of each e-mail, Microsec informs the data subjects on how to unsubscribe and indicates the link where they can perform it. Upon withdrawal of the consent, Microsec erases the personal data immediately.

Who has authorized access to the data within Microsec?

- the operators and developer of the application
- marketing and sales department employees

1.23.2 Contact details

Type and purpose of the data processing

There is an opportunity to contact the operators of the application through the V2X PKI Test service. Any personal data provided in the course of contacting the operators shall only be used for keeping in contact with the users.

Legal basis of the data processing

Article 6 (1) a) of the of the General Data Protection Regulation – consent of the data subject which is provided by ticking the appropriate box on the website.

Categories of the processed data

Name, e-mail address, IP address, name of the employer, position.

Term of the data processing

Contact details shall be processed as long as the consent of the data subject is withdrawn, in the lack of such withdrawal as long as there is relevant communication with the interested person, in the topic indicated by them.

Who has authorized access to the data within Microsec?

- the operators and developers of the application
- marketing and sales department employees

1.24 Data processing related to V2X PKI certificate requests

Type and purpose of the data processing

Data processing of the operator manager appointed by the client and the operators registered by the operator manager in course of using the live version of the V2X PKI service.

The Microsec V2X PKI is a PKI-based certification system required for secure and standard communication between communicating vehicles, road users, and transportation infrastructure. Only operators registered by the operator manager and the operator manager appointed by the client may login to the system and the operators may request different certificates - developed for vehicles, road users and transport infrastructure units.

Microsec cannot fulfill the registration requests of the clients using the V2X PKI service, (i) if Microsec cannot verify that the operators have been registered by such operator managers who were appointed by the client (ii) if Microsec cannot verify that such persons registered the devices who had been authorized by the operator managers of the client to do so as operators (iii) if Microsec cannot notify the operator of the client when a registration is unsuccessful / an anomaly occurs related to the registration.

In order for Microsec to be able to perform the above verification process, it is necessary that the operator managers and operators can only access the V2X PKI service platform after having provided the username and password and the additional information required to use PassByMe as described in this notice.

Legal basis of the data processing

The clients of the V2X PKI service (mainly organizations) appoint such operator managers, who are entitled to register operators who will then proceed in the matter of registration (requesting certificates for devices) and revocation of devices.

To authenticate the V2X device registration and revocation requests and to enter the device management platform, the appointed persons shall be identified, which occurs based on username and password, and via the PassByME application.

The data necessary for such identification (which are the data of the employees of Microsec's client) are sent to Microsec by the client. in order to enable Microsec's client to securely use the V2X PKI service provided by Microsec. Therefore, the legal basis is Article 6 (1) f) of the General Data Protection Regulation – the data processing is necessary for pursuing the lawful interest of Microsec as data processor and its client as third party. The legitimate interest of Microsec is that it may fulfill its obligations arising out of the contract concluded with the client. The legitimate interest of Microsec’s client as third party is using the V2X service in the most secure way possible.

Categories of the processed data

The name, e-mail address, phone number of the operators announced by the operator manager and the operator manager appointed by the client, name of the employer, username and password and the information required to use PassByME in accordance with this Privacy Notice. In case of the operator manager, the type and number of the identity document is also required, because the relevant EU-level regulation requires that the PKI service provider shall use an identity document as basis for identification (EU Certificate Policy, 13 March 2019 [2], Section 3.2.3.).

Term of the data processing

Active data management terminates when the contract with the client using the service is terminated, since if the client does not have an active service, processing the data of the operator manager and the operators appointed by the client are no longer necessary. The activity logs of the operator manager and the operators are stored in the system for 5 years after the termination of the contract, in accordance with Section 6:22 of the Civil Code (general limitation period), in order to ensure that, in the event of a dispute arising in connection with the provided service after the termination of the contract, Microsec can prove that the system has performed its functions properly and that Microsec has not acted in breach of contract. This is the basis for Microsec's legitimate interest in data processing after the termination of the service contract.

Who has authorized access to the data within Microsec?

- registration officers
- the operators of the application
- system administrators

1.25 Data processing related to V2X Root CA inclusion

Type and purpose of the data processing

If a V2X PKI service provider wants to apply for the inclusion of its Root CA certificate in the V2X PKI Trust List operated by Microsec, then based on the Microsec V2X TLM CPS and the relevant EU regulations, the service provider’s authorized representative person must provide Microsec with his/her personal data (e.g. name, place and time of birth) and contact information (e.g. company e-mail), so that Microsec can identify this authorized representative person and check his/her data, in order to accept the application and perform the Root CA certificate inclusion.

Legal basis of the data processing

General Data Protection Regulation Article 6 (1) (f) legitimate interest of Microsec or a third party – by way of filling out a special application form with the requested information, signing this form, and sending it to Microsec, the authorized representative initiates a contractual agreement with Microsec. By way of accepting the application and including the Root CA certificate into the Microsec Certificate Trust List, a contractual agreement is established between

Microsec and the authorized representative person's organization. The creation of this contractual agreement is the legitimate interest of both parties.

Categories of the processed data

The following data of the authorized representative person are processed: name, time and place of birth, company phone and company e-mail address of the person as well as his/her position within the company, and any other data included in the Certificate Authorization issued by the V2X PKI service provider applying for its Root CA inclusion (based on the EU C-ITS Certificate Policy, 13 March 2019 [2], Section 3.2.3.1).

Term of the data processing

Active data management terminates when the included Root CA certificate is deleted form the Microsec Certificate Trust List.

The Certificate Authorization document (containing the data of the authorized representative) is stored for 5 years after the termination of the contract, in order to ensure that in the event of a dispute, Microsec may prove that it has properly verified the identity and representation rights of the authorized representative. The minimum 5 years long data retention period is prescribed by Section 5.5 of the EU C-ITS Certificate Policy.

Who has authorized access to the data within Microsec?

- registration officers
- colleague responsible for quality assurance
- board member responsible for V2X PKI services

1.26 Data processing related to web-Szignó services

Type and purpose of the data processing

With web-Szignó service users can create electronic folders on the web platform and insert documents into the folders, download documents from the folders or to place electronic signatures on the PDF files or folders and forward it to a certain addressee.

The purposes of processing personal data given at the registration is the providing of services and concluding an agreement with the data subject. In case the data subject obtains services that are subject to fees and therefore an invoice needs to be issued, we also process such personal data of the data subject that are necessary for invoicing purposes.

Legal basis of the data processing

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.

After the termination of the service contract: General Data Protection Regulation Article 6 (1) f) Microsec's legitimate interest.

Categories of the processed data

In order to provide the service and conclude the agreement we request the following personal data: e-mail address.

In order to issue our invoice we store especially the following personal data: the name and address of the addressee of the invoice, based on Point 8 of the present chart.

Term of the data processing

Personal data provided upon registration are erased after 5 years from the completion of the services as set forth in Section 6:22 of the Civil Code (after the lapse of the statutory limitation period) if no legal dispute has been initiated between the data subject and the Service Provider pertaining to the services.

Personal data related to billing shall be processed as set out in Point 8 of this Annex, for the period prescribed for the processing of accounting data.

Who has authorized access to the data within Microsec?

The system administrators can access the data provided upon registration.

1.27 Data processing related to Client Portal / Account

Type and purpose of the data processing

Use of the services of the Client Portal / Account available via the website https://portal.e-szigno.hu/. Upon registration, the User shall accept the Terms of Use.

Legal basis of the data processing

Article 6 (1) b) of the General Data Protection Regulation – Accepting the Terms of Use.

Categories of the processed data

The e - mail address (password) for registration, the certificate user ID (OID) and the type of document uploaded depend on the personal data we handle (eg personal data on the invoice, uploaded documents related to the application, etc.)

For information security reasons, access to the Client Portal / Account is via two-factor authentication. The first factor is e-mail address and password, then the user shall either present a code received in SMS code or approve the login in the e-Szignó application (second factor). If Microsec sends the user an SMS as the second factor for authentication, the sms is sent to the phone number provided when the certificate was applied for, and Microsec uses this phone number to contact the certificate holder for this purpose as well. The user has the possibility to use the e-Szignó mobile application for second factor authentication if the application had been previously installed in order to use the remote key management service. In this case, Microsec already has access to such data in connection with the user's mobile phone that the present Privacy Notice outlines with regard to the PassByME mobile signature service. If the user has installed the e-Szognó mobile application on more than one mobile device, Microsec will display to the user, at login, the identification information (type of mobile device, operating system) of the different devices, in order to allow the user to choose the application

installed on his mobile device in which he wishes to receive the messages for the purpose of second factor authentication.

Term of the data processing

Uploaded documents will be deleted after 30 days. The account cannot be deleted by the User. If Microsec sets the User to "not our customer" status (meaning that there is no valid service contract existing at Microsec regarding the Customer), the User's account will be deleted 1 month later. The account of such User to whom Microsec does not assign a Certificate User ID (OID) will be deleted 1 year after registration.

The data stored for the purpose of two-factor authentication (telephone number, data of the mobile phone used for the e-Szigno mobile app) is stored as long as the two-factor authentication method is set or the account is terminated.

Who has authorized access to the data within Microsec?

Customer Service representatives, members of the Sales Team, Troubleshooting Administrator, Developer - Access is set by the IT Operations Department to the person whose department head requested access because it is required to serve customers.

1.28 Data processing related to processing external requests

Type and purpose of the data processing

Processing of e-mails / inquiries / written complaints from customers / interested parties.

Legal basis of the data processing

Article 6 (1) a) of the General Data Protection Regulation – consent of the data subject. By sending an e-mail to a contact e-mail address or contact interface provided by Microsec, you expressly consent to the processing of your personal information.

Categories of the processed data

All personal data provided by the Customer / Interested Party in the given e-mail / other request.

Term of the data processing

5 years from receipt (statutory limitation period) is the retention period of requests.

Who has authorized access to the data within Microsec?

The internal administration and ticket management systems may be accessible to all Microsec employees. The request is handled by the department and its staff responsible for the subject of the request.

1.29 Data processing related to Test Certificates

Type and purpose of the data processing

https://srv.e-szig-no.hu/index.php?lap=szoftve-res_teszt_igenyles

Legal basis of the data processing

Article 6 (1) a) of the General Data Protection Regulation – consent of the data subject.

Categories of the processed data

Only the contact e-mail address is real data managed as part of the service.

Otherwise, non-real data is included in the test certificates, the attention of the users of the service is explicitly warned not to provide real data when applying for the test certificate. If the user of the service still provides real data, we consider that he / she also contributes to the processing of his/her real data at the same time.

Term of the data processing

By the withdrawal of the consent, Microsec deletes the personal data without any undue delay.

Who has authorized access to the data within Microsec?

The test certificate registry is public. https://srv.e-szigno.hu/teszt_tan_kereses

1.30 Data processing related to transfer of data processed by Microsec to a third party cost bearer

Type and purpose of the data processing

Microsec may transfer to a third party cost bearer personal data provided to Microsec in course of applying for a certificate, in case the service is entirely or partially not financed by the Subscriber or the subject of the certificate, but by a third party cost bearer (hereinafter referred to as ***Cost Bearer***). The purpose of the data transfer is to verify that only such persons applied for a certificate indicating the Cost Bearer, with whom the Cost-Bearer had previously agreed in this respect and therefore, the Cost Bearer only finances the certificates of such entitled persons. If the certificate is financed in order that it is used by the subject in a system operated by the Cost Bearer, Microsec may also transfer data to the Cost Bearer for the purpose of facilitating the use of the certificates in its own system (verifying registration, technical assistance).

Legal basis of the data processing

Article 6 (1) f) of the General Data Protection Regulation - legitimate interest of Microsec or a third party. It is the legitimate interest of the Coast Bearer that the service provided by Microsec is financed by the Cost Bearer exclusively for persons or organizations entitled to it, or that the financed certificates are actually used by the subjects in the system operated by the Cost Bearer.

Categories of the processed data

The minimum possible amount of personal data obtained by Microsec during the certificate application that enables the Cost Bearer to identify the person or entity for whom the service is financed or who is benefiting from the discount without any doubt, in particular the name and tax number of the person (certificate subject) or entity (Subscriber). If the Cost Bearer

pays the costs related to the certificates in order to ensure that the certificates are used by the subjects in the Cost Bearer's system, Microsec may also provide data necessary for the identification of the certificate and contact information (telephone number, e-mail address) in order to enable the Cost Bearer to verify whether the requested certificates have already been registered in the Cost Bearer's system for creating electronic signatures and, if not, to contact the certificate subject to facilitate the registration.

Microsec informs the certificate subjects concerned of the exact type of data transferred and the details of the data processing carried out by the Cost Bearer on the certificate application platform.

Term of the data processing

The processing (in relation to the transfer) ceases when the data is transferred to a third party.

If the transferred data are processed by Microsec for other data processing purposes, Microsec shall continue to process them in accordance with the provisions of this Privacy Notice after the transfer.

Who has authorized access to the data within Microsec?

- the sales representative who provides the data to the Cost Bearer
- the developers of the customer record system, application operators and system administrator
- customer service staff

1.31 Data processing related to Providing Remote Assistance Services to Microsec Customers

Type and purpose of the data processing

Provision of remote assistance service free of charge at the Customer's request

Legal basis of the data processing

Article 6(1)(a) of the General Data Protection Regulation - the consent of the data subject, the Customer gives Microsec access to his/her device for viewing and control purposes, his/her consent is given by expressing his/her explicit consent when requesting the Remote Assistance service during the telephone conversation and by maintaining the session while personal data is potentially disclosed.

Categories of the processed data

When providing the Remote Assistance Service, Microsec is entitled to access information to be found on the device of the Customer and to modify the settings of the device only to the extent necessary to resolve the problem identified by the Customer.

When providing the Remote Assistance Service, Microsec has access to the following personal

data: name, telephone number. Microsec already processes these data for other data processing purposes.

By default, during providing the Remote Assistance Service, Microsec may not access documents containing personal data on the Customer's device, however, it cannot be excluded that the support colleague of Microsec providing the Remote Assistance Service may access information available on the device of the Customer (e.g. on the 'Desktop') that qualifies as personal data.

During the provision of the Remote Assistance Service, the Customer will continuously monitor and control the provision of the Remote Assistance Service and may take back control of his/her device and interrupt the session at any time. If the Customer does not interrupt the provision of the Remote Assistance Service, the Customer shall be deemed to have agreed to the changes made on his/her device and to the support colleague of Microsec having access to his/her personal data potentially disclosed during the Remote Assistance Service.

If, during the provision of the Remote Assistance Service, Microsec does indeed access the personal data on the device and the Customer does not interrupt the session, the Customer shall be deemed to have considered the access to be indispensable for the provision of the Remote Assistance Service, to have given its express consent to the data processing and to have an adequate legal basis for processing the data and making them available to Microsec.

Term of the data processing

Microsec does not record any data during the provision of the Remote Assistance Service and does not have access to the data on the Customer's device after the session has ended. Microsec will not process any personal data of the Customer requesting the Service, after the Remote Assistance has been completed (with regard to this data processing purpose).

Who has authorized access to the data within Microsec?

The support colleague of Microsec providing the Remote Assistance Service.

1.32 Data processing related to e-Szignó Mobile application crash monitoring

Type and purpose of the data processing

Monitoring of possible crashes of the e-Szignó mobile app with the Firebase Crashlytics crash reporting solution, which notifies the developers when a user's mobile device crashes during using the e-Szignó mobile app and provides analysis of the crashes

The purpose of the data processing is to correct the user's error, maintain the software quality of the mobile application, and to fulfill customer requests.

Legal basis of the data processing

General Data Protection Article 6 (1) b) - the processing is necessary for the performance of a contract to which the data subject is a party.

Under the end-user license agreement of the e-Szignó Mobile application, Microsec must ensure that certain features of the application work on the end-user's mobile device.

Categories of the processed data

If the e-Szignó Mobile Application crashes on the user's device, Microsec will not be able to fulfil its contractual obligations in relation to the features of the application (e.g. creation of an electronic signature).

In order for Microsec to prevent further errors and to be informed of the crash of the application (even if the user does not file a complaint), Microsec collects the following data through the Firebase Crashlytics application: the version of the application running on the end-user's device, the operating system version, the type of device, the language, the circumstances of the crash, the user's OID or, in the absence of an OID, the user's e-mail address, and the unique identifier of the user within the operating system (vendorid). The OID is required so that, if a user reports a crash, information about the crash on his or her specific device is available for troubleshooting purposes.

Term of the data processing

Microsec retains the data collected through the Firebase Crashlytics application for each crash for 90 days after the app crash.

Who has authorized access to the data within Microsec?

- the developers of mobile app
- support mun-companions