PRIVACY POLICY
FOR PARTNERS, CLIENTS AND REGISTERING PARTIES

NETLOCK Informatics and Network Security Services Limited Liability Company

Document name in Hungarian:	Adatkezelési Tájékoztató
Document name in English:	Data Privacy Policy
Document short name:	PP-EN
Version:	220907
Object identifier (OID):	1.3.6.1.4.1.3555.1.6.1.0.220907
Date approved:	05/09/2022
Date published:	07/09/2022
Valid from:	07/09/2022
Number of pages:	19 pages, including cover
Approved by:	**dr. Dorottya Vey** Head of Compliance

TABLE OF CONTENTS

1 INTRODUCTION ..... - 4 -

1.1 DATA OF THE DATA CONTROLLER ..... - 4 -
1.2 GETTING ACQUAINTED WITH AND ACCEPTANCE OF THIS PRIVACY POLICY ..... - 4 -
1.3 REVISION, AMENDMENT ..... - 4 -
1.3.1 Revisions of the Document ..... - 5 -

2 PROVISIONS REGARDING DATA PROCESSING ..... - 5 -

2.1 GOVERNING LEGAL ACTS ..... - 5 -
2.2 PLACE OF THE DATA PROCESSING ..... - 6 -
2.3 THE SCOPE OF DATA SUBJECTS ..... - 6 -
2.4 THE SCOPE OF DATA PROCESSED ..... - 6 -
2.5 AUTOMATED DECISION-MAKING AND PROFILING, DATA TRANSFER ..... - 6 -
2.6 THE PURPOSE OF DATA PROCESSING ..... - 7 -
2.7 CATEGORIES OF RECIPIENTS ..... - 7 -

3 DATA PROCESSING ASSOCIATED WITH TRUST SERVICES ..... - 7 -

3.1 IDENTIFICATION OF IDENTITY ..... - 7 -
3.1.1 Establishment of the identity by identification by using video technology ..... - 8 -
3.1.2 Establishment of the identity on the basis of personal presence ..... - 8 -
3.2 REVOCATION, SUSPENSION AND RE-ACTIVATION ..... - 9 -

4 OTHER DATA PROCESSING OPERATIONS ..... - 9 -

4.1 SIGNATURE IMAGE MANAGEMENT ..... - 9 -
4.2 LINKING USER ACCOUNTS ..... - 10 -
4.3 PUSH MESSAGES ..... - 10 -
4.4 NEWSLETTER, SYSTEM NOTIFICATION ..... - 10 -
4.5 DATA PROCESSING IN RELATION TO OPERATING THE WEBSITE ..... - 11 -
4.5.1 Setting cookies in browsers ..... - 11 -
4.5.2 Summary ..... - 12 -
4.6 DATA PROCESSING IN RELATION TO SAFEGUARDING OF PROPERTY ..... - 12 -
4.7 CUSTOMER SERVICE ..... - 13 -
4.7.1 Telephone Customer Service ..... - 13 -
4.8 PUBLIC CERTIFICATE STORE ..... - 13 -
4.9 PERMANENT ID ..... - 13 -
4.10 PROCESSING OF THE DATA OF CONTRACTUAL CONTACT PERSONS ..... - 13 -
4.11 STORAGE OF LOG FILES ..... - 13 -
4.12 LABOUR RECRUITMENT ..... - 14 -
4.13 ENFORCEMENT OF LEGAL CLAIMS, REQUEST FOR PAYMENT ..... - 14 -

5 PERSONAL DATA PROCESSED AS DATA PROCESSOR ..... - 14 -

6 LEGAL BASES, PRINCIPLES OF DATA PROCESSING ..... - 15 -

7 YOUR RIGHTS ..... - 15 -

7.1 INFORMATION ..... - 15 -
7.2 RIGHT OF ACCESS TO THE DATA ..... - 16 -
7.3 RIGHT TO RECTIFICATION ..... - 16 -
7.4 RIGHT TO ERASURE ..... - 16 -
7.5 RIGHT TO RESTRICT THE PROCESSING OF PERSONAL DATA ..... - 16 -
7.6 RIGHT TO DATA PORTABILITY ..... - 17 -
7.7 RIGHT TO OBJECT ..... - 17 -

8 FRAMEWORK FOR EXERCISING YOUR RIGHTS ..... - 17 -

8.1 METHOD OF EXERCISING YOUR RIGHTS ..... - 17 -
8.2 RULES RELEVANT TO THE ARRANGEMENT OF THE REQUEST ..... - 18 -
8.2.1 Content of the request of the data subject ..... - 18 -

9 ENGAGEMENT OF DATA PROCESSORS ..... - 18 -

10 DATA SECURITY MEASURES ..... - 19 -

11 LEGAL REMEDIES ..... - 19 -

11.1 RIGHT TO COMPLAIN WITH THE SUPERVISORY AUTHORITY ..... - 19 -

11.2 RIGHT TO AN EFFECTIVE JUDICIAL REMEDY AGAINST THE SUPERVISORYAUTHORITY ..... - 19 -

1 INTRODUCTION

The purpose of this Privacy Policy (hereinafter referred to as: Privacy Policy) is to provide sufficient information for those entering into contact or in a contractual relationship with NETLOCK Kft. on the scope and source of data processed by NETLOCK Kft. as Data Controller (hereinafter: Service Provider) or by other data processors or data controllers in a contractual relationship with NETLOCK Kft., on the principles, purpose, legal basis and duration of the data processing, the rights of the data subjects, and on the data processors involved in the data processing and on other activities related to the data processing, as well as, if the personal data of the data subject are transferred or transmitted, on the legal basis and recipients of the data transfer.

1.1 DATA OF THE DATA CONTROLLER

Name of the data controller: NETLOCK Informatics and Network Security Services Limited Liability Company
Seat: H-1101 Budapest, Expo tér 5–7., Hungary
Website: https://netlock.hu/
Postal address: H-1439 Budapest, Pf. 663, Hungary
Electronic address: info@netlock.hu
E-mail address of the Data Protection Officer: dpo@netlock.hu

Should you have any questions or observations to pose or make in relation to this Privacy Policy or the data processing activity carried out by the Service Provider, please contact our Customer Service Centre using the following contact data:

Telephone: +36 1 437 6655
E-mail: info@netlock.hu

If you have a complaint or question specifically related to data privacy, you can contact the Service Provider's Data Protection Officer at the following e-mail address:

E-mail: dpo@netlock.hu

This Privacy Policy shall be construed in accordance and harmony with the requirements laid down in the Service Provider's other Policies and Privacy Policy. Should there be any conflict or controversy regarding the protection of personal data between the provisions included in this Privacy Policy and the requirements laid down in any other Policy that entered into force prior to the entry into force of this Privacy Policy, the provisions of this Privacy Policy shall be governing.

1.2 GETTING ACQUAINTED WITH AND ACCEPTANCE OF THIS PRIVACY POLICY

If you provide personal data to us in using our services, communicating with our Customer Service Centre or using our website, you will make a declaration by providing the personal data that you have become acquainted with and accepted our Data Privacy Policy effective at any time.

1.3 REVISION, AMENDMENT

The Service Provider is entitled to unilaterally amend this Privacy Policy at any time. You will find the currently effective version of our Data Privacy Policy on our website at the following address: https://netlock.hu/.

1.3.1 Revisions of the Document

OID	Effective from to	Description of change	Created by
1.3.6.1.4.1.3555.1.67.20180525	26/05/2018-11/05/2020	Document creation	Docler Services Ltd.
1.3.6.1.4.1.3555.1.67.20200506	12/05/2020-17/06/2020	The rights of the data subjects, the ways of exercising them, more detailed explanation of data security measures, data processing related to trust services	Dr Dóra Káli
1.3.6.1.4.1.3555.1.67.20200618	18/06/2020-17/12/2020	Amendments related to the phasing out of the identification by video technology (Government Decree no. 132/2020)	Éva Varga-Szabó
1.3.6.1.4.1.3555.1.67.20201214	18/12/2020-15/09/2021	Amendments related to the introduction of identification by video technology (Government Decree no. 541/2020. (XII. 2.)), explanation in detail of data protection roles in relation to archiving, the NETLOCK SIGN and "NETLOCK" cloud service, presentation of the relevant legal acts, presentation of the rules concerning data processors and joint controllers in detail, precision on data processing.	Dr Dóra Káli
1.3.6.1.4.1.3555.1.6.1.0.210916	16/09/2021-25/08/2022	Restructuring the Policy for ease of understanding, information about linking user accounts, other clarifications to comply with the GDPR as well as updating cookie information. Document OID change.	NETLOCK Ltd.
1.3.6.1.4.1.3555.1.6.1.0.220826	26/08/2022-06/09/2022	Adding Signature image management (4.1) to the policy and deletion of Chapter 5 (Personal data processed in the quality as joint controllers).	NETLOCK Ltd.
1.3.6.1.4.1.3555.1.6.1.0.220907	07/09/2022 until withdrawn or a new version is issued	Modifying chapter 4.1 Signature image management (multiple images can be uploaded).	NETLOCK Ltd.

2 PROVISIONS REGARDING DATA PROCESSING

2.1 GOVERNING LEGAL ACTS

The legal basis of processing personal data by the Service Provider is often based on a legal act, which may be as follows:

- Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 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, hereinafter: GDPR);
- Regulation (EU) No 910/2014 of the European Parliament and of the Council of 23 July 2014 on electronic identification and trust services for electronic transactions in the internal market (hereinafter: eIDAS);
- Act CXII of 2011 on informational self-determination and freedom of information;

- Act CCXXII of 2015 on the general rules for electronic administration and trust services (hereinafter: Electronic Administration Act);
- Act V of 2013 promulgating the Civil Code (hereinafter: Civil Code);
- Act C of 2000 on accounting (Accounting Act);
- Decree no. 24/2016. (VI. 30.) of the Ministry of Interior (hereinafter: Decree of the Ministry of Interior) on detailed requirements for trust services and their providers;
- Government Decree no. 541/2020. (XII. 2.) (hereinafter: Government Decree) on other identification methods recognized at a national level and providing a guarantee equivalent to being physically present in the case of trust services.

2.2 PLACE OF THE DATA PROCESSING

Processing of personal data will take place at the Service Provider's registered seat or site, or at the registered seat or site or branch office of a data processor commissioned by the Service Provider or a joint controller with the Service Provider.

If you wish to obtain information about the geographical place where the data made available by you to the Service Provider will be processed or whether they will be transferred to a data processor/other data controller, please contact our Data Protection Officer as specified in Chapter 8.

2.3 THE SCOPE OF DATA SUBJECTS

The Service Provider processes and controls the data of the following persons:

- Applicant for the Service,
- Subscriber for the Service,
- Person representing the Applicant/Subscriber (e.g., proxy, representative of the organisation, etc.),
- Person subscribing to the Newsletter,
- and any other person that contacts but is not in a contractual relationship with the Service Provider (e.g., those requesting information about a service).

2.4 THE SCOPE OF DATA PROCESSED

The Service Provider describes the scope of data processed in the relevant section.

2.5 AUTOMATED DECISION-MAKING AND PROFILING, DATA TRANSFER

The Service Provider does not use automated decision-making and profiling.

The Service Provider uses service providers based outside the European Economic Area (hereinafter: EEA) for providing the services offered by it and for performing day-to-day administration tasks. Data transfer to countries located outside the EEA will take place on the basis of an adequacy decision or Standard Data Protection Clauses approved by the European Commission.

Should you need further information regarding the data transfer, you may request further information in the manner specified in Chapter 8.

2.6 THE PURPOSE OF DATA PROCESSING

The purpose of data processing is to identify your person, perform the ordered service, provide support for the service, if required, in order to provide the service you intend to use, as well as to fulfil payment and invoicing obligations associated with the service and to exercise rights and fulfil obligations stemming from the legal relationship established as a result of your use of the service.

From among the data provided by you, the Service Provider will process your name and e-mail address in order to send you system notification. More detailed information regarding the sending of system notification are available in Section **Hiba! A hivatkozási forrás nem található.**.

The Service Provider is entitled to use the data for statistical purposes in a way unsuitable for identifying the person.

2.7 CATEGORIES OF RECIPIENTS

In order to provide the service you intend to use, the Service Provider will communicate your data both to the organisational units involved in the service provision within its own organisation (e.g., to the Finance Department, in order to issue the invoice), and to the data processors/joint data controllers – in a contractual relationship with the Service Provider – as far as is necessary to provide the specific service.

You can find more detailed information about the data processors of the Service Provider in Chapter 9, and about the entities in a joint controller relationship with it in Section 3.2.

The Service Provider will communicate any rectification or erasure of personal data or restriction of processing to each recipient to whom the personal data have been disclosed, unless this proves impossible or involves disproportionate effort.

3 DATA PROCESSING ASSOCIATED WITH TRUST SERVICES

3.1 IDENTIFICATION OF IDENTITY

In respect to the Service Provider's activity of providing trust services as well as qualified trust services, the Service Provider is bound by an identity identification obligation pursuant to Article 82 *of Act CCXXII of 2015 on the general rules of electronic administration and trust services.* Identification of identity may be carried out by being physically present, and without it by way of identification using video technology.

In fulfilling the identification of identity obligation, the Service Provider must ascertain precluding any doubt about the following:

- the identity of the person included on the certificate,
- genuineness of the personal identity documents/data used for establishing the identity of that person,
- should a legal entity be represented, the authorisation and entitlement to represent the legal entity,
- whether the organisation/organisational unit indicated in the certificate really exists,
- in the case of a lawyer's/judge's/public notary's certificate, the authorisation and entitlement to exercise that profession.

Pursuant to Article 84 (1) of the Electronic Administration Act, the Service Provider will retain the pieces of information available in relation to the individual certificates – including those related to their

production – and the personal data associated with them ***for 10 (ten) years from the date of expiry of the validity of the certificate*** for the purpose of fulfilling its legal obligations.

The Service Provider is obliged to verify – if possible – the data included in the personal identity document used as a basis for establishing the identity in legally authentic records. Pursuant to Article 84 (1) of the Electronic Administration Act, the Service Provider will retain the result of such verification ***for 10 (ten) years from the date of expiry of the validity of the certificate*** for the purpose of fulfilling its legal obligations.

If the Service Provider is notified by a user, authority or court that a litigation has been initiated concerning the genuineness or validity of any data included in the certificate, the Service is obliged to fulfil its the retention obligation ***by the final and binding conclusion of the litigation*** pursuant to Article 84 (1) of the Electronic Administration Act, even if the 10-year time period from the expiry of the certificate has already expired.

Information on the retention time period for any other data not related to certification services are available in Annex 1.

3.1.1 Establishment of the identity by identification by using video technology

The Service Provider may carry out identification through a system providing video technology certified as a reliable IT system (hereinafter: VideoRA). The establishment of identity is carried out ***on-line, on the basis of a recorded (not live) video recording.*** The precise process of identification by video technology is described in detail in Section iv. Video technology identification of Section 3.2.3 Authentication of individual identity of Service Policy for Qualified Certificate Services of "NETLOCK".

The Service Provider processes the following data in the course of identification by using video technology:

- Picture of the front and back page of the personal identity document and the data included in it;
- The image and voice recording (hereinafter: video recording) made of you in the course of the identification by using video technology, including the entire communication established between you and the Service Provider;
- The photo made during the video recording;
- The statements made by you during the video recording;

Pursuant to Article 82/A. (2) of Act CCXXII of 2015 on the general rules for electronic administration and trust services, the Service Provider will record ***the entire communication established between you and the Service Provider*** during identification by using video technology, as well as the provision of detailed information to you in relation to the identification by video technology and the natural person's express and specific consent to it, on image and voice recording, in a retrievable way and in a manner that precludes deterioration of the quality of the image and voice recording and ***will retain it for 10 (ten) years from the date of the recording.***

The provisions of Section 3.1. are governing for the retention time period for any other information available in relation to the individual certificates.

3.1.2 Establishment of the identity on the basis of personal presence

In addition to identification by using video technology, the Service Provider also ensures the opportunity for identification by being physically present.

Identification will be carried out on the basis of your personal identity document presented by you in person, by using a Data Validation Form to be filled out by the Service Provider's employee:

The data content of the Data Validation Form is as follows:

- Type of the document;
- Nationality;
- Surname and first name;
- Mother's maiden name;
- Place and date of birth;
- Document ID;
- Validity;
- Date of issue;
- Issuing authority;
- Country and name of the settlement as per the home address card;
- Signature of the applicant.

The provisions of Section 3.1. are governing for the retention time period for the Data Validation Form.

3.2 REVOCATION, SUSPENSION AND RE-ACTIVATION

You have the option to request a change in the certificate status within the validity period of your certificate. The purpose of the status change can be suspension, re-activation or revocation of the certificate, which you can request by phone and e-mail.

The request for revocation, suspension and activation shall contain at least the following information:

- serial number of the certificate,
- name of the entity (natural person and, where applicable, legal entity) requesting the revocation / suspension,
- contact details of the person requesting revocation / suspension,
- date of revocation / suspension (if not immediate).

Pursuant to Article 84 (1) of the Electronic Administration Act, Service Provider will control your personal data – including the telephone number or e-mail address through which you submitted the request for status change – for 10 (ten) years from the date of expiry of the validity of the certificate for the purpose of fulfilling its legal obligations.

4 OTHER DATA PROCESSING OPERATIONS

The following section describes the data processing not related to the trust service, however performed by the Service Provider.

4.1 SIGNATURE IMAGE MANAGEMENT

You have the option to upload an image of your manual (handwritten) signature to the certificate profile and place it on the documents simultaneously with your electronic signature. The management of the image of the manual signature according to this section (uploading, storage, deletion, etc.) does not apply to the processing of the data of the electronic signature or other (e.g., personal identity) data associated with trust certificate services.

The Service Provider does not check the adequacy, correctness, or other characteristics of the manual signature, it only provides the opportunity to upload, change, store, place on documents and delete the image of the manual signature. In the event of any copyright infringement related to the uploaded image,

the uploader of the image shall bear the consequences; moreover, the Service Provider does not assume responsibility for the truthfulness and authenticity of the data. All clients are entitled to upload images to their profile data at their own risk. The Service Provider is entitled to suspend the client's profile with immediate effect or to delete the uploaded image if its content is contrary to legal, moral or other provisions (e.g., content infringing copyrights, erotic content), as well as infringes or endangers the rights or legitimate interests of third parties (for example: content that endangers the good reputation of the Service Provider or the Customer, offends public taste or the religious, ethnic, political or other sensitivities of others; content that is classified as a business secret [confidential, internal use information]).

The user can change (replace) the image of the manual signature at any time or delete it from his/her certificate profile without uploading a new version during the validity period of the certificate. Multiple images of the manual signature can be stored in the certificate profile.

The legal basis for storing the image of the signature is the consent of the data subject, which is given by uploading the image of the signature to the certificate profile. If the data subject deletes the image of the signature from the certificate profile without uploading a new version, it is considered a withdrawal of consent to data processing. The duration of the signature image management lasts until the image is deleted, or, in the lack of it, until the validity period of the certificate.

4.2 LINKING USER ACCOUNTS

If you already have a user account in the "NETLOCK" cloud service, when you create another user account, the user accounts will be linked based on the personal information you provided during registration. The purpose of linking the accounts is, among others, to strengthen protection against certificate abuse and to enhance the customer experience.

The legal basis for the data processing during the linking of the accounts is Article 6 (1) f) of the GDPR; i.e., the legitimate interest of the Service Provider, against which you may object as defined in point 9 of this Policy.

The duration of data processing is the time needed to link the accounts.

4.3 PUSH MESSAGES

If you use the "NETLOCK" cloud service through a mobile application, you must subscribe to the so-called push messages (or push notifications) from the "NETLOCK" mobile application. The "NETLOCK" mobile application displays the so-called TOTP (Time-based One-Time Password), a second factor required to identify the initiator of the signing transaction, as a push message. Push messages are sent by the "NETLOCK" cloud service using the Firebase Cloud Messaging service of Google (see https://firebase.google.com/docs/cloud-messaging). When subscribing to the push messages, the "NETLOCK" mobile application sends the unique ID of the mobile device running the mobile app to the Firebase Cloud Messaging service of Google, which is required to "address" push messages.

4.4 NEWSLETTER, SYSTEM NOTIFICATION

The Service Provider will regularly contact you in an electronic way so that you can learn about our latest products (hereinafter: Newsletter) and obtain the necessary information about the services you use (hereinafter: System notification).

The Service Provider will process and use the ***name*** and ***e-mail address*** you have provided when subscribing to the newsletter or when creating your user account, for sending newsletters or system notification.

The Service Provider will use the data made available to it in a way limited to the purpose, exclusively for sending marketing messages and system notification (e.g., expiry of a certificate, occurrence of a security incident, etc.).

The Service Provider sends system notification based on its legitimate interest, and newsletters on the basis of your freely given consent. The Service Provider will make the interest assessment test certifying its legitimate interest available to you at any time upon your request.

The Service Provider will process the name and e-mail address provided by you for sending news-letters until you unsubscribe from the newsletter. If the Service Provider uses those data for other purposes as well; e.g., for providing a certification service, those data will be processed further for that purpose.

You can indicate your intention to unsubscribe from the newsletter to the Service Provider free of charge and at any time by sending a notification to the e-mail address specified in this section or at the bottom of the Newsletter. Upon unsubscribing, the Service Provider will not process your e-mail address and other personal data for the purpose of sending newsletters any longer.

You can unsubscribe from the newsletter at the following e-mail address: leiratkozas@netlock.hu

If you have sent system notification, you have the right to object (see Section 7.7) and you may exercise this in the manner described in Chapter 7.

4.5 DATA PROCESSING IN RELATION TO OPERATING THE WEBSITE

The Service Provider operates its website at the following address: https://netlock.hu/. The website collects information on visits on an anonymous basis by using ***cookies)*** for operating certain functions, the use of which is based on your ***consent*** **(**by clicking on the Accept button in the pop-up window on the website).

The Service Provider measures the number and characteristics of the visitors to the website, by using the ***Google Analytics*** web analytics service.

The data stored in Google Analytics are not suitable for identifying you by name, however, it is able to recognize, should you re-visit our website, that the website has already been visited before by a specific computer by using a specific browser.

Google uses the above information for ***assessing and analysing*** your use of this website, ***as well as for compiling reports on the activities carried out on the website and for providing other services associated with the use of the Internet.*** Your attention is kindly drawn to the fact that you can reject the use of cookies by selecting the appropriate settings in your browser. You are hereby informed that by accepting the use of the cookies on the website you grant your consent to the processing of your data on an anonymous basis, in the way and for the purposes specified above.

You can access the Data Privacy Policy of Google Analytics at the following link:
https://policies.google.com/privacy?hl=hu

4.5.1 Setting cookies in browsers

Please note that browsers allow the use of cookies by default. If you do not want us to collect information about you as described above, you may disable the use of cookies in part or in full in your Internet browser settings.

For the most commonly used browsers, you will find a guide here:

Google Chrome

Mozilla Firefox
Microsoft Internet Explorer
Microsoft Edge
Apple Safari

Please note that when using an **ad-blocker**, information about the use of cookies may not always be displayed. If you would like to view cookie information, please deactivate the ad-blocker!

4.5.2 Summary

Affected domain	Controlled data set	Cookie type	Purpose of data management	Duration of data management
sign-auth.hu.netlock.com	AUTH_SESSION_ID	session cookie	ID of the current authentication session to ensure the proper functioning of the website	The period until the end of the relevant visitor session
sign-auth.hu.netlock.com	KC_RESTART	session cookie	To ensure the proper functioning of the website	The period until the end of the relevant visitor session
sign-auth.hu.netlock.com	KEYCLOAK_LOCALE	session cookie	To ensure the setting of the language of the website	The period until the end of the relevant visitor session
sign-auth.hu.netlock.com	KEYCLOAK_IDENTITY	session cookie	To ensure the proper functioning of the website	The period until the end of the relevant visitor session
sign-auth.hu.netlock.com	KEYCLOAK_SESSION	session cookie	ID of the current browser session to ensure the proper functioning of the website	40 days
sign-auth.hu.netlock.com	KEYCLOAK_REMEMBER_ME	session cookie	To ensure the proper functioning of the website	The period until the end of the relevant visitor session

4.6 DATA PROCESSING IN RELATION TO SAFEGUARDING OF PROPERTY

A video camera surveillance and access system is operated at the registered seat and site of the Service Provider, with the sole purpose of safeguarding the property and interests of the Service Provider and other companies based in the building. The system is operated by Docler Office Building at the registered seat, while at the site of the Service Provider the camera surveillance system is operated by the responsible Security Service of OTP Ingatlan Befektetési Alapkezelő Zrt.

The Service Provider does not perform data processing activities concerning data recorded in association with the operation of the system.

Details of data processing related to the safeguarding of property are laid down in the relevant regulations of the Security Services on the safeguarding of property and data privacy.

4.7 CUSTOMER SERVICE

You can contact the Service Provider in person, in writing, by phone, or by using the messaging interface or chat window on the website.

4.7.1 Telephone Customer Service

We would like to inform you that the voice recording on your conversation with one of our colleagues upon the occasion of your contacting our Customer Service Centre by phone will be recorded and stored ***for 5 (five) years*** from the date of your call, on the basis of the ***Company's legitimate interest***. Should you have any questions regarding the storage and use of the voice recording, you can request information in the way specified in Section 7.1.1

4.8 PUBLIC CERTIFICATE STORE

The Service Provider operates a public certificate store on its website, through which such certificates can be searched and downloaded by anyone, for the publication in the certificate store of which the Client has granted their consent. You are hereby informed that ***you can withdraw your consent at any time,*** however, such withdrawal will not affect the lawfulness of data processing based on your consent and performed prior to the withdrawal.

The public certificate store contains the data included in the specific certificate, together with the status of the certificate.

4.9 PERMANENT ID

The subject of each certificate issued by the Service Provider must be unique in order to be able to unequivocally identify it. To that end, the Service Provider assigns to each person a unique ID; i.e., a ***permanent ID*** managed in its records. This ID identifies the natural person involved in the certificate in a unique manner.

Since the Permanent ID is a piece of data included in a certificate the Service Provider will retain it ***for 10 (ten) years from the date of expiry of the validity of the certificate.***

4.10 PROCESSING OF THE DATA OF CONTRACTUAL CONTACT PERSONS

To facilitate the concluding and performing of individual contracts and making any communication run smoothly between the Parties to a contractual relationship, the Service Provider will process, based on its legitimate interest, ***the name, e-mail address and phone number*** of the natural person acting on behalf of the contractual partner ***for 5 (five) years,*** in accordance with Article 6:22 of the Civil Code.

In the case of contracts for pecuniary interest, the time period during which the data must be retained is ***8 (eight) years*** pursuant to Article 169 (2)–(3) of the Accounting Act.

4.11 STORAGE OF LOG FILES

Article 33 of the Decree of the Ministry of the Interior sets forth that "*The qualified service provider shall log each event related to its IT system and the provision of a qualified service continuously, in order to ensure continuity of the operating procedure, avoid data loss and guarantee IT security. The logged data file shall cover the entire process of the provision of the qualified service and shall be suitable for reconstructing any event related to the qualified service to a degree necessary for assessing the real situations*".

The logged data file must contain the following data:

- the calendar date and precise time of the occurrence of the logged event;

- the data necessary for tracking and reconstructing the event;
- the name of the user or other person that triggered the event.

The Service Provider is obliged to retain or provide for the retention of the data related to the certificate ***for 10 (ten) years*** from the date of expiry of the validity of the certificate, the data logged outside the scope of the certificate for ***10 (ten) years*** counted from their occurrence, while the Service Practice Statement and its amendments for ***10 (ten) years*** from the date on which they are repealed.

In respect to the above statutory provisions, if you use any of our qualified services the Service Provider as a provider of trust services will log each event related to its IT system and the provision of the qualified service in order to ensure proper security of the service provision and such saved data may contain your personal data as well.

4.12 LABOUR RECRUITMENT

We would like to inform you that if you apply for a job advertised by the Service Provider, we will process the following data based on your voluntary, informed ***consent***:

- Name;
- E-mail address;
- Telephone number;
- Photo;
- Education;
- Professional experience;
- Language skills;
- In addition, all the information you include in your CV.

Please note that application materials will be kept for ***6 (six) months*** from the date of receipt, given that the selection process may take longer. If you withdraw your consent to data processing, the data will be deleted.

4.13 ENFORCEMENT OF LEGAL CLAIMS, REQUEST FOR PAYMENT

If a payment reminder is sent during the contractual relationship between the Service Provider and you, the Service Provider will process the data required for sending the payment request, such as ***name***, ***address/e-mail address*** in accordance with Article 6 b) of the GDPR; i.e., on the basis of the performance of the contract.

We would like to inform you that if the Service Provider has a claim against you after the termination of the contract, the Service Provider will process the data necessary for the enforcement of the claim in accordance with Article 6 f) of the GDPR, i.e., on the basis of its legitimate interest. In order to substantiate its legitimate interest, the Service Provider will have an interest assessment test prepared, which is available to you at any time upon request. We inform you that you may object to such processing of your personal data at any time in the manner set out in Chapter 9.

The duration of data processing is the duration of claim enforcement.

5 PERSONAL DATA PROCESSED AS DATA PROCESSOR

When you use certain services of the Service Provider (e.g., qualified archiving, NETLOCK SIGN or "NETLOCK" cloud services), the Service Provider acts as a Data Processor, while the Customer using the service is considered to be a Data Controller.

During the data processing activity, the Service Provider does not examine the legal basis of the data processing, especially with regard to the fact that the Service Provider does not get acquainted with the documents subject to data processing as a general rule. The Service Provider assumes and stipulates in

the data processing contract with the Data Controller that the Data Controller has the appropriate legal basis for data controlling.

The Service Provider stipulates that it shall immediately forward the requests of the data subjects related to the data processing activity to the Data Controller and it is the responsibility of the Data Controller to address them.

The Service Provider stipulates that, with regard to Article 28 (3) of the GDPR, it concludes a data processing contract with the Data Controller for the data processing activity performed by it, which contract is specified in Section 8.1 of the General Terms and Conditions.

The Service Provider informs you that this Chapter cannot be considered as complete information on the data processing activity, so if you have any questions, please contact the Data Controller.

6 LEGAL BASES, PRINCIPLES OF DATA PROCESSING

The Service Provider will process personal data only and exclusively in the following cases:

a) the data subject has given consent for 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 Service Provider 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 purposes of the legitimate interests pursued by the Service Provider 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.

The Service Provider will process the personal data to an extent appropriate, relevant and necessary for achieving the purpose. After the purpose of the data processing has expired, the Service Provider will erase the personal data definitively and in an unrecoverable way.

During the data processing the Service Provider will do its utmost using appropriate technical or organisational measures in order to ensure the appropriate security of the personal data, including protection against unauthorised or unlawful processing and against accidental loss, destruction or damage.

The Service Provider has carried out interest assessment tests in relation to data processing based on its legitimate interest.

7 YOUR RIGHTS

In the section below, you will find all the rights you have during data controlling.

7.1 INFORMATION

The Service Provider as the Data Controller is obliged to provide information on the purpose, legal basis of the data processing, duration of the retention of the data, designation and contact details of the Service Provider as the Data Controller, on the contact details of its Data Protection Officer, and on the recipients or categories of recipients of the personal data, if the processing is based on a legitimate interest, about the legitimate interest of the Service Provider or a third party, about data transfer, if any, about your right to request access from the Service Provider to your personal data, to rectify, erase or limit the

processing of such data, your right to object to the processing of such personal data or to transfer the data to another data controller and about the legal remedy opportunities.

The Service Provider intends to fulfil this information provision obligation by issuing this Privacy Policy.

If you are not the source of the data and do not have the above-mentioned information yet, the Service Provider is obliged, in addition to the obligations listed above, to provide information to you about the source of the personal data and the categories of the personal data concerned.

Should you have any more questions in relation to the processing of your data besides the scope of information provided in this Privacy Policy, you may request further information from the Service Provider by submitting a request to the e-mail address specified in Section 1.1.

7.2 RIGHT OF ACCESS TO THE DATA

You have the right to request feedback from the Service Provider whether the processing of your personal data is on course, and if yes, to request information on the issues mentioned in Section 7.1.

7.3 RIGHT TO RECTIFICATION

If the personal data recorded by the Service Provider are inaccurate, you have the right to ask the Service Provider to rectify them without delay or to complement them, if the data are incomplete.

7.4 RIGHT TO ERASURE

You have the right to ask the Service Provider to ***erase your data processed by it***, at any time, and the Service Provider must satisfy your request ***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 your consent on which the processing is based and there are no other legal grounds for the processing;
c) you object to the processing 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 to which the Service Provider is subject.

Satisfying your request for erasure of your data will not be obligatory if the processing is necessary:

a) for exercising the right of freedom of expression and information;
b) for compliance with a legal obligation which requires processing by Union or Member State law to which the Service Provider is subject;
c) for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes, in so far as the fulfilment of your request is likely to render impossible or seriously impair the achievement of the objectives of that processing; or
d) for the establishment, exercise or defence of legal claims.

7.5 RIGHT TO RESTRICT THE PROCESSING OF PERSONAL DATA

If one of the following applies, you will have the right to request the Service Provider to ***temporarily cease to process your personal data,*** if:

a) you contest the accuracy of the personal data; in such a case the restriction will last for a period enabling the Service Provider 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) the Service Provider no longer needs the personal data for the purposes of the processing, but you require them for the establishment, exercise or defence of legal claims; or
d) you have objected to processing; in such a case the restriction will last pending the verification whether the legitimate grounds of the Service Provider override yours.

Where processing has been restricted under one of the following grounds, such personal data may, with the exception of storage, be processed by the Service Provider only with your consent or for the establishment, exercise or defence 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.

If the restriction of the processing is lifted you will be informed before this is carried out.

7.6 RIGHT TO DATA PORTABILITY

You have the right to receive the personal data concerning you, which you have provided to the Service Provider, ***in a structured, commonly used and machine-readable format*** (e.g., xml), and ***you have the right to transmit those data to another data controller, if the following conditions apply***:

a) the processing is based on your consent or on a contract; and
b) the processing is carried out by automated means (e.g., the processing is not paper-based).

If the above conditions are fulfilled, you will have the right to have the personal data transmitted directly from one controller to another, where technically feasible.

When exercising the above-mentioned right, it shall not adversely affect the rights and freedoms of others.

7.7 RIGHT TO OBJECT

You have the right to object, ***on grounds relating to your particular situation, at any time to the processing of your personal data which is based on the Service Provider's legitimate interest.***

In such a case the Service Provider shall no longer process the personal data unless the Service Provider demonstrates compelling legitimate grounds for the processing that override your interests, rights and freedoms or for the establishment, exercise or defence of legal claims.

Where personal data are processed to object at any time ***for direct marketing purposes*** (e.g., sending newsletters), you will have the right ***to object at any time*** to the processing of personal data concerning you for such marketing. If you object to the processing for direct marketing purposes, the personal data shall no longer be processed for such purposes.

8 FRAMEWORK FOR EXERCISING YOUR RIGHTS

8.1 METHOD OF EXERCISING YOUR RIGHTS

We wish to inform you that you can exercise your above-mentioned rights by submitting a request to the Service Provider or directly to the Data Protection Officer of the Service Provider. The request can be submitted by postal mail or electronically to the following addresses:

Postal address: H-1439 Budapest, Pf. 663, Hungary
E-mail: info@netlock.hu

If you wish to turn directly to the Data Protection Officer, you can do so at the following e-mail address or by a letter sent to the Service Provider but marked as for the attention of the Data Protection Officer.

E-mail: dpo@netlock.hu

8.2 RULES RELEVANT TO THE ARRANGEMENT OF THE REQUEST

The Service Provider is obliged to inform you of the measures taken in pursuance of the request submitted by you, without undue delay but by no means later than ***within a month*** from the date of receipt of the request.
If necessary, this deadline ***may be extended by a further two months,*** by taking the complexity of the request and the number of pending requests into account. The Service Provider will inform you of the extension of the deadline, by specifying the reasons for the delay, within a month from receipt of the request. If the request submitted by you has been received electronically, the information shall also be provided in an electronic way, if possible, except if you request it in another manner.

If the Service Provider does not take any action upon receipt of your request, it shall inform you without delay but not later than within a month from receipt of the request about the reasons for failing to take measures and about the fact that you can lodge a complaint with the competent data protection supervisory authority. The Service Provider may decline the request only in writing, by providing justifications.

We will provide the information and the measure requested by you ***free of charge*** to you, except if your request is manifestly unfounded or excessive – especially if it is made in a recurring manner.

Taking into account the ***administrative costs*** of providing the information or communication or taking the action requested, the Service Provider may either:

- charge a reasonable fee, or
- refuse to act on the request.

8.2.1 Content of the request of the data subject

In order to accelerate the processing of the request of a data subject, the request should include at least the following:

- Name and contact details of the applicant;
- Designation of the right of the data subject you want to be enforced;
- Name of the service you use.

We inform you that if the Service Provider has reasonable doubts about the identity of the applicant, it is entitled to request additional information necessary to establish the identity.

9 ENGAGEMENT OF DATA PROCESSORS

The Service Provider employs only and exclusively Data Processors who comply with the provisions of the GDPR and other relevant legal provisions. Furthermore, the Service Provider requires the data processors in a contractual relationship with it to observe and enforce the provisions and requirements laid down in this Privacy Policy and in its internal Data Protection and Data Security Policy.

The Service Provider transmits personal data to its data processors, solely on the basis of a written agreement and to the extent and for the purpose(s) specified in that agreement.

The list of the Data Processors is included in Annex 1 to this Privacy Policy.

10 DATA SECURITY MEASURES

The Service Provider takes the measures specified in this Privacy Policy and in its internal Data Protection and Data Security Policy during data processing according to this Privacy Policy, in order to prevent unauthorised persons' access to the processed personal data.

The Service Provider has elaborated ***different levels of right*** of electronic or physical access to the personal data, the technical details of which and a detailed specification of the IT data security requirements are contained in the Service Provider's internal regulations.

The Service Provider takes the necessary action in order to enable ***its employees to obtain access*** to personal data processed by the Service Provider ***only to the extent and in the scope required for carrying out their work.***

In addition, the Service Provider is an organisation certified according to the ***ISO 27001 standard*** (hereinafter: Standard) and in order to comply with that Standard, the Service Provider is audited each year by an independent external certification body. The Standard applies a process-focused information security approach that covers the architecture, the introduction, operation, review, monitoring, maintenance and development of the entire information security management system of the organisation. In the course of certification under the Standard, the Service Provider's entire data management process is also reviewed.

11 LEGAL REMEDIES

If you believe that the Service Provider has violated the requirements relevant to the processing of personal data concerning you, you have the following remedies available to you in accordance with the present Chapter.

11.1 RIGHT TO COMPLAIN WITH THE SUPERVISORY AUTHORITY

You have the right to lodge a complaint with the competent supervisory authority, in particular in the Member State of your habitual residence, place of work or place of the presumed infringement, if you consider that the processing of personal data concerning you infringes provisions of the GDPR.

Competent supervisory authority in Hungary:

Name: Hungarian National Authority for Data Protection and Freedom of Information
Seat: H-1055 Budapest, Falk Miksa u. 9–11., Hungary
Postal address: H-1363 Budapest, Pf.: 9., Hungary
E-mail: ugyfelszolgalat@naih.hu

11.2 RIGHT TO AN EFFECTIVE JUDICIAL REMEDY AGAINST THE SUPERVISORYAUTHORITY

We would like to inform you that you can appeal to a court against a legally binding decision of the supervisory authority concerning you, or even if the authority does not deal with your complaint or does not inform you of the handling of your complaint within three months.

You are hereby informed that should the requirements regarding the processing of your personal data be violated, you can take the case before a court of law, in addition to turning to the competent supervisory authority. The procedure may be initiated at a court with jurisdiction over the location of your domicile or place of residence.