PRIVACY POLICY

FOR PARTNERS, CUSTOMERS AND REGISTERING PARTIES

Hungarian name of the document: Adatkezelési Tájékoztató

English name of the document: Privacy Policy

Short name of the document: PP-HU

Version: 261112

Identification number (OID): 1.3.6.1.4.1.3555.1.6.1.0.261112

Date of approval: 13/10/2026

Date of publication: 13/10/2026

Effective date: 12/11/2026.

Number of pages: 18 pages including cover page

Approved by: NETLOCK Kft.

© COPYRIGHT, NETLOCK Kft. – ALL RIGHTS RESERVED

1. INTRODUCTION

The purpose of this Privacy Policy (hereinafter: the "Policy") is to provide those who contact NETLOCK Kft. and those who are in a contractual relationship with it with appropriate information about the data processed by NETLOCK Kft., as the controller (hereinafter: the "Provider"), and by the processors and other controllers in a contractual relationship with the Provider, including the scope and source of such data, the principles, purpose, legal basis and duration of the processing, the rights of data subjects, the processors that may be involved in the processing, and other activities related to the processing, as well as – where the data subject's personal data are transferred – the legal basis for, and recipient of, such transfer.

1.1 Details of the Controller

Name of the Controller: NETLOCK Informatikai és Hálózatbiztonsági Szolgáltató Korlátolt Felelősségű Társaság (NETLOCK Information Technology and Network Security Services Limited Liability Company)

Registered seat: 1143 Budapest, Hungária körút 17-19.

Company registration number: 01-09-563961

Tax number: 12201521-2-42

Website: https://netlock.com/

Electronic contact: trust@netlock.com

Contact details of the Data Protection Officer: dpo@netlock.hu

Details of the hosting service provider: Amazon Web Services EMEA SARL (38 avenue John F. Kennedy, L-1855 Luxembourg)

If you have any questions or comments regarding this Policy or the Provider's processing of personal data, you may contact our Customer Service at the following details:

Phone: +36 1 255 0792

E-mail: trust@netlock.com

If you have a complaint or question specifically relating to data protection, you may contact the Provider's Data Protection Officer at the following details:

E-mail: dpo@netlock.hu

This Policy must be interpreted in accordance with the provisions of the Provider's other policies and notices. If any contradiction arises, in relation to the protection of personal data, between the provisions of this Policy and the provisions of any other policy that entered into force before this Policy took effect, the provisions of this Policy shall prevail.

1.2 Acknowledgement and Acceptance of the Policy

You accept this Policy when using our services available on the netlock.com website, in the course of concluding the service agreement, by ticking the separate checkbox provided after the link to download the Policy (placing a tick in the checkbox). By ticking the checkbox, you declare that you have read and accepted our Privacy Policy in effect at the time of acceptance.

1.3 Review and Amendment

The Provider is entitled to update this Policy in line with applicable legal requirements and changes in data processing practice. The version of the Privacy Policy in effect at any given time can be found on our website at https://netlock.com/.

If the amendment materially affects the purpose or legal basis of the processing, the recipients of any data transfer or the transfer to a third country, or the rights of data subjects, the Provider shall also notify data subjects thereof

– within a reasonable time before the amendment takes effect – by means of a notice displayed on the user interface of the service.

If the amendment affects the scope or content of a consent previously given by the data subject, the data subject shall be informed whether a new consent is required for further processing.

1.3.1 Document Revisions

OID	Period of validity	Description of change	Prepared by
1.3.6.1.4.1.3555.1.67.20180525	2018.05.26.– 2020.05.11.	Creation of the document	Docler Services Kft.
1.3.6.1.4.1.3555.1.67.20200506	2020.05.12.– 2020.06.17.	More detailed explanation of data subjects' rights and the manner of exercising them, and of data security measures, as well as of the processing related to trust services	dr. Káli Dóra
1.3.6.1.4.1.3555.1.67.20200618	2020.06.18.– 2020.12.17.	Amendments relating to the phasing-out of video-technology identification (Government Decree 132/2020)	Varga-Szabó Éva
1.3.6.1.4.1.3555.1.67.20201214	2020.12.18.– 2021.09.15.	Amendments relating to the introduction of video-technology identification (Government Decree 541/2020 (XII. 2.)), a more detailed description of the data protection roles relating to archiving and the NETLOCK SIGN and "NETLOCK" cloud service, presentation of the applicable legislation, a more detailed description of the rules applicable to processors and joint controllers, and clarification of the processing operations.	dr. Káli Dóra
1.3.6.1.4.1.3555.1.6.1.0.210916	2021.09.16.– 2022.08.25.	Restructuring of the Policy for easier comprehension, inclusion of information on account linking, other clarifications made to ensure compliance with the GDPR, and an update of the cookie notice. Change of the document's identification number.	NETLOCK Kft.
1.3.6.1.4.1.3555.1.6.1.0.220826	2022.08.26.– 2022.09.06.	Supplementing the Policy with the management of the handwritten signature image (4.1), and deletion of Chapter 5 (Personal data processed as joint controllers).	NETLOCK Kft.
1.3.6.1.4.1.3555.1.6.1.0.220907	2022.09.07.– 2026.02.17.	Amendment of Chapter 4.1 on the management of the signature image (multiple signature images may be uploaded).	NETLOCK Kft.
1.3.6.1.4.1.3555.1.6.1.0.260218	2026.02.18. – 2026.09.08.	Annual review of the Policy. – Amendment of the referenced legislation, – Change of the Provider's registered seat, – Deletion of the Provider's PO box address, – Other minor amendments.	NETLOCK Kft.
1.3.6.1.4.1.3555.1.6.1.0.260810	2026.09.09.- 2026.11.11.	Inclusion of automated decision-making in the Policy; removal from the Policy of identification through personal presence; changes to the video-technology identification process; AI-supported solutions in relation to identification and uploaded documents; changes in the use of cookies; clarification of retention periods in line with legislation	NETLOCK Kft.
1.3.6.1.4.1.3555.1.6.1.0.261112	From 12/11/2026 until withdrawal or the entry into force of a new version	Modification of the Service Provider's contact details	NETLOCK Kft

2. PROVISIONS RELATING TO THE PROCESSING OF PERSONAL DATA

2.1 Applicable Legislation

In many cases, the legal basis for the processing of personal data by the Provider is based on legislation, which may include the following:

- Regulation (EU) 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 (hereinafter: the "GDPR");
- Regulation (EU) No 910/2014 on electronic identification and trust services for electronic transactions in the internal market (hereinafter: "eIDAS");
- Regulation (EU) 2024/1183 amending Regulation (EU) No 910/2014 as regards establishing a European Digital Identity Framework (hereinafter: "eIDAS 2.0");

- Act CXII of 2011 on the Right of Informational Self-Determination and Freedom of Information (the "Infotv.", i.e. the Hungarian Privacy Act);
- Act CIII of 2023 on the Digital State and Certain Rules for the Provision of Digital Services (hereinafter: the "Digital State Act")
- Act V of 2013 on the Civil Code (hereinafter: the "Civil Code");
- Act C of 2000 on Accounting (hereinafter: the "Accounting Act");
- Decree No. 24/2016 (VI. 30.) of the Ministry of Interior on the detailed requirements for trust services and their providers (hereinafter: the "BM Decree");
- Government Decree No. 541/2020 (XII. 2.) on other nationally recognised identification methods providing a guarantee equivalent to personal presence in the case of trust services (hereinafter: the "Government Decree").

2.2 Place of Processing

The processing of personal data takes place at the registered seat or premises of the Provider, or at the registered seat, premises or branch office of a processor engaged by the Provider.

If you would like information on where geographically the data you have provided to the Provider are processed, or whether they are transferred to a processor/other controller, please contact our Data Protection Officer in the manner set out in point 8.

2.3 Scope of Data Subjects

The Provider processes the personal data of the following persons:

- Applicants for the Service,
- Subscribers to the Service,
- Payers of the fee for the Service,
- Persons representing the Applicant/Subscriber (e.g. an authorised agent, an organisational representative, etc.),
- Persons subscribing to the Newsletter,
- and any other person who comes into contact with the Provider without being in a contractual relationship with it (e.g. a person requesting information about a service, a visitor to the website, an applicant for a job vacancy, or a contact person of a contractual partner).

2.4 Scope of the Data Processed

The Provider describes the scope and source of the data processed, the legal basis for the processing, whether the provision of the data is mandatory or voluntary, and the legal consequences of failing to provide the data, in the relevant chapter and in Annex 1 to this Policy.

2.5 Automated Decision-Making, Profiling and Data Transfers

The Provider may apply automated decision-making in the course of identity verification, but does not carry out profiling. In supporting identity verification, the Provider also uses artificial intelligence-based solutions, details of which can be found in point 3.1.1.

In order to provide the services it offers and to carry out its day-to-day administration, the Provider also uses service providers located outside the European Economic Area (hereinafter: the "EEA"). Transfers of data to countries outside the EEA are carried out on the basis of an adequacy decision or standard data protection clauses approved by the European Commission.

If you require further information regarding the transfer of data, you may request additional information in the manner set out in point 8.

2.6 Purpose of the Processing

The purpose of the processing is to identify you in order to provide the service you wish to use, to perform the ordered service, to provide service support where necessary, to fulfil the payment and invoicing obligations related to the service, and to exercise the rights and fulfil the obligations arising from the legal relationship created by the use of our service.

Of the data provided by you, the Provider also processes your name, telephone number and e-mail address for the purpose of sending system messages. More detailed information on the sending of system messages can be found in point 4.4. The Provider is entitled to use the data for statistical purposes in a form that does not permit identification of the individual.

2.7 Categories of Recipients

In order to provide the service you have made use of, the Provider discloses your data both to the relevant organisational units within its own organisation (e.g. to the finance department for the purpose of issuing an invoice) and to the processors – in a contractual relationship with the Provider – necessary for the provision of the given service.

More detailed information on the Company's processors can be found in point 9.

The Provider informs every recipient to whom personal data have been disclosed of any rectification, erasure or restriction of processing, unless this proves impossible or involves disproportionate effort.

3. PROCESSING RELATED TO TRUST SERVICES

3.1 Identity Verification

In view of its trust and qualified trust service activities, the Provider is subject to an identity verification obligation under Section 85 of the Digital State Act. Identity verification takes place exclusively by means of remote video-technology identification, or, in the case of identification via the mobile application, by means of identification using an identity card containing a storage element (chip).

In the course of the identity verification obligation, the Provider must ascertain, beyond any doubt, the following:

- the identity of the person named in the certificate,
- the authenticity of the identity documents/data used to establish identity,
- in the case of representation of a legal person, the authority to represent it,
- the existence of the organisation/organisational unit indicated in the certificate,
- in the case of an attorney's/judicial/notarial certificate, the entitlement to practise in that capacity.

The provision of the data necessary for identity verification is a statutory requirement; without such data, identity verification cannot be carried out and the certificate cannot be issued.

Pursuant to Section 88(1) of the Digital State Act, on the ground of compliance with a legal obligation, the Provider retains the information available to it in connection with each certificate – including information related to their issuance – and the personal data connected thereto, for 10 years from the expiry of the certificate's validity.

Where possible, the Provider is required to verify, in an authentic public register, the data contained in the identity document forming the basis of the identity verification. Pursuant to Section 88(1) of the Digital State Act, on the ground of compliance with a legal obligation, the Provider retains the result of this verification for 10 years from the expiry of the certificate's validity.

If the Provider is notified by a user, an authority or a court of a legal dispute that has commenced regarding the authenticity or validity of data contained in the certificate (hereinafter: "notified dispute"), the Provider must, pursuant to Section 88(1) of the Digital State Act, comply with its retention obligation until the final and binding conclusion of the dispute, even if the ten-year period calculated from the expiry of the certificate has already elapsed.

Annex 1 sets out the retention period for personal data provided in connection with certificates that become invalid due to revocation, and for applications closed without the issuance of a certificate.

Information on the retention period of any other data not related to certificate services can be found in Annex 1.

3.1.1 Identity Verification by Means of Video-Technology Identification

Identity verification is carried out by the Provider in a reliable system providing video technology certified as an IT system (hereinafter: "video-technology identification" or "VRA"). In the course of identity verification, the customer's facial image is recorded via a live video telecommunications connection, within the Provider's system, in the manner and at the time determined by the Provider. The Provider examines the conditions of identification online, on the basis of recorded (not live) video material (not in real time), by automated means, following the termination of the telecommunications connection; the process does not require the real-time involvement of a customer service representative. The precise process of video-technology identification is set out in detail in point iv. "Video-technology identity verification" of subsection 3.2.3 "Authentication of the identity of a natural person" of the Service Policy applicable to Qualified Certificate Services.

In the course of video-technology identification, the Provider processes the following data:

- in the case of a card-format identity document, an image of its front and back, together with the data shown thereon; in the case of a book-format identity document, an image of the page containing the photograph and identity data, together with the data shown thereon;
- the image and sound recording made of you during video-technology identification (hereinafter: "video recording"), including the entire communication between the Provider and you;
- the photograph taken during the video recording;
- the statements made by you during the video recording.

Pursuant to Section 86(2) of the Digital State Act, the Provider records, in a retrievable manner, on an image and sound recording – in a way that precludes deterioration of the quality of the image and sound recording – the entire communication between the Provider and you in the course of video-technology identification, the detailed information provided to you regarding video-technology identification, and the natural person's express consent thereto, and retains it for the period specified in Annex 1 to this Policy. In the event of a notified dispute, the Provider must comply with its retention obligation until the final and binding conclusion of the dispute, even if the ten-year period calculated from the expiry of the certificate has already elapsed.

To support video-technology identification and the related automated decision-making, the Provider applies artificial intelligence-based solutions that are run exclusively within the Provider's own system (locally, i.e. on-premise). These solutions serve facial recognition and face matching, liveness detection (in order to filter out manipulation or deception), recognition and authentication of the document, optical character recognition (OCR) of the data contained on the document, and voice-based verification. The data processed by these solutions (in particular the video recording, the photograph, the sound recording, and the data contained on the document) are not transferred to any external, third-party artificial intelligence service provider. The artificial intelligence-based system supports the identification; the result of the identification may be reviewed by an authorised employee of the Provider, which is particularly warranted where an error, inconsistency or uncertainty has arisen during identification (e.g. the authenticity check of the document was unsuccessful, or the person to be identified appears on a sanctions list). In such a case, the decision is not based on automated decision-making (Article 22 of the GDPR).

If you are unable to complete the video-technology identification process on your own and identification therefore fails, you may, in the course of the identification process, request that identification be carried out by an authorised employee of the Provider, and you are also entitled to submit such a request – together with the related provision of information – directly by contacting our customer service. In such a case, the decision is not based on automated decision-making.

Please be informed that, in the course of video-technology identification – in particular during verification based on facial recognition and face matching – the Provider also processes and verifies your biometric data qualifying as a special category of personal data under the GDPR (biometric characteristics derived from your facial image that are suitable for unique identification).

The provision of the personal data given during video-technology identification is necessary for compliance with a statutory obligation, while the provision of special category data is based on the data subject's prior, explicit consent.

For the purposes of identity verification, the related sanctions list check, and quality assurance tasks, the Provider transfers your data (in particular your name, date of birth, address, document number and telephone number) to an external service provider. Detailed information on the data transfer can be found in point 9, and the list of processors/recipients can be found in Annex 1.

3.1.2 Identity Verification Using an Identity Card Containing a Storage Element (Chip)

In the case of registration via the mobile application, and identity verification within it, the Provider carries out identity verification on the basis of the content of the storage element (chip) placed on the identity document.

Of the data stored in the storage element of the identity card, the Provider verifies the following data:

- data readable from the MRZ (Machine-Readable Zone): type and number of the document, its expiry date, the issuing country, and the holder's name, date of birth and sex
- the image and sound recording made of you (hereinafter: "video recording"), including the entire communication between the Provider and you;
- the photograph taken during the video recording;
- the statements made by you during the video recording.

Pursuant to Section 86(2) of the Digital State Act, in the course of identification based on the content of the storage element placed on the identity document, the Provider records, in a retrievable manner, on an image and sound recording – in a way that precludes deterioration of the quality of the image and sound recording – the entire communication between the Provider and you, the detailed information provided to you regarding the identification, and the natural person's express consent thereto, and retains it for the period specified in Annex 1 to this Policy. In the event of a notified dispute, the Provider must comply with its retention obligation until the final and binding conclusion of the dispute, even if the ten-year period calculated from the expiry of the certificate has already elapsed.

To support identification based on the content of the storage element placed on the identity document and the related automated decision-making, the Provider applies artificial intelligence-based solutions that are run exclusively within the Provider's own system (locally, i.e. on-premise). These solutions serve facial recognition and face matching, liveness detection (in order to filter out manipulation or deception), recognition and authentication of the document, optical character recognition (OCR) of the data contained on the document, and voice-based verification. The data processed by these solutions (in particular the video recording, the photograph, the sound recording, and the data contained on the document) are not transferred to any external, third-party artificial intelligence service provider. The artificial intelligence-based system supports the identification; the result of the identification may be reviewed by an authorised employee of the Provider, which is particularly warranted where an error, inconsistency or uncertainty has arisen during identification (e.g. the authenticity check of the document was unsuccessful, or the person to be identified appears on a sanctions list). In such a case, the decision is not based on automated decision-making (Article 22 of the GDPR).

Please be informed that, in the course of identification based on the content of the storage element placed on the identity document, the Provider also processes and verifies your biometric data qualifying as a special category of personal data under the GDPR (biometric characteristics derived from your facial image that are suitable for unique identification).

The provision of the personal data given during identification based on the content of the storage element placed on the identity document is necessary for compliance with a statutory obligation, while the provision of special category data is based on the data subject's prior, explicit consent.

For the purposes of identity verification, the related sanctions list check, and quality assurance tasks, the Provider transfers your data (in particular your name, date of birth, address, document number and telephone number) to an external service provider. Detailed information on the data transfer can be found in point 9, and the list of processors/recipients can be found in Annex 1.

The provisions of point 3.1 govern the retention period of any other information available in connection with each certificate.

3.2 Revocation, Suspension and Reactivation

You may request a change to the status of your certificate within its period of validity. A request for a change of status may relate to the suspension, reactivation or revocation of the certificate, and may be requested by telephone or e-mail.

A request for revocation, suspension or reactivation must contain at least the following data:

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

Pursuant to Section 88(1) of the Digital State Act, on the ground of compliance with a statutory obligation, the Provider processes your personal data – including the telephone number or e-mail address through which you submitted the request for a change of status – for 10 years from the expiry of the certificate's validity. In the event of a notified dispute, the Provider must comply with its retention obligation until the final and binding conclusion of the dispute, even if the ten-year period calculated from the expiry of the certificate has already elapsed.

4. OTHER PROCESSING

This chapter describes the processing carried out by the Provider that is not related to trust services.

4.1 Management of the Signature Image

You have the option to upload an image of your handwritten signature to your certificate profile, which you may place on documents together with your electronic signature. The processing of the image of the handwritten signature under this point (uploading, storage, deletion, etc.) does not extend to the processing of the electronic signature or other data (e.g. identification data) related to the trust service of the certificate.

The Provider does not verify the adequacy, correctness or other characteristics of the handwritten signature; it only provides the possibility to upload, change, store, place on documents, and delete the image of the handwritten signature. The uploader of the image is responsible for the consequences of any infringement of copyright relating to the uploaded image, and the Provider assumes no liability for the truthfulness or authenticity of the data. Each Customer is entitled to upload images to their profile data at their own risk. The Provider is entitled to suspend the customer's profile with immediate effect, or to delete the uploaded image, if its content is contrary to legal, moral or other rules (for example, content infringing copyright, or content of an erotic nature), or infringes or endangers the rights or legitimate interests of a third person (for example: content that endangers the good reputation of the Provider or the Customer, offends public morals, or offends the religious, ethnic, political or other sensitivities of others, or content qualifying as a business secret (for internal use, confidential)).

The user may change (replace) the image of the handwritten signature at any time, or may delete it from the certificate profile without uploading a new version, during the period of validity of the certificate. Several images of the handwritten signature may be stored in the certificate profile at the same time.

The legal basis for the storage of the image of the signature is the data subject's consent, 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, this shall qualify as withdrawal of consent to the processing. The duration of the processing of the image or images of the signature lasts until the deletion of the uploaded image, or, in the absence thereof, until the expiry of the certificate's validity.

4.2 Account Linking

If you already have a user account in the "NETLOCK" cloud service, user accounts will not be linked upon the creation of a further user account.

4.3 Push Messages

The NETLOCK mobile application processes a push identifier for the delivery of transactional and security push messages necessary for the operation of the service. The legal basis and duration of the processing, the service provider involved, and the conditions of any transfer of data outside the EEA are set out in Annex 1..

4.4 Newsletter and System Messages

In order for you to learn about our latest products (hereinafter: "Newsletter"), and to receive the necessary information relating to the service you use (hereinafter: "System Message"), the Provider contacts you electronically at regular intervals or on an ad hoc basis.

In sending the Newsletter and the System Message, the Provider processes and uses the name, telephone number and e-mail address provided by you when subscribing to the Newsletter or when creating your user account.

4.4.1. System Message

In order for you to receive the necessary information relating to the service you use (hereinafter: "System Message"), the Provider may send notifications electronically on a regular or ad hoc basis.

In sending the System Message, the Provider processes and uses your name, telephone number and e-mail address provided when your user account was created.

The Provider uses your data for the purpose of sending System Messages, in particular in the event of the expiry of the certificate's validity, the occurrence of a security incident, or any other event affecting the use of the service.

The Provider sends the System Message on the basis of its legitimate interest, which is aimed at avoiding a situation where the Customer's electronic signatures become invalid due to the expiry of the certificate's validity, or where the Customer's processes relating to the use of the NETLOCK service are interrupted, as well as at satisfying the need for information identified on the basis of customers' previous feedback.

The retention period of the data processed for the purpose of sending System Messages is set out in Annex 1.

You have the right to object (see 7.7) in respect of the sending of the System Message, which you may exercise in the manner set out in Chapter 8.

4.4.2. Newsletter

In order for you to learn about our latest products, and to inform you about the Provider's business activities and related developments, the Provider may send you electronic notifications (hereinafter: "Newsletter") based on your voluntary consent.

You have the option to subscribe separately to Newsletters about new developments, products and services, and to Newsletters about the Provider's business activities, related developments and professional information. You may unsubscribe from the two types of Newsletter separately.

In sending the Newsletter, the Provider processes and uses your name and e-mail address provided when you subscribed to the newsletter, until you unsubscribe from the Newsletter. If the Provider also uses this data for another purpose, e.g. for the provision of certificate services, this data will continue to be processed by the Provider for that purpose.

You may notify the Provider of your intention to unsubscribe from the Newsletter at any time and free of charge, at the e-mail address or via the link provided in this point or at the bottom of the Newsletter. Following unsubscription, the Provider will no longer process your e-mail address or other personal data for the purpose of sending the Newsletter.

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

4.5 Processing Related to the Operation of the Website

The Provider operates its website at https://netlock.com/. For certain functions to work, the website collects anonymous visitor information using cookies. The types of cookies used, the data processed by them, and the purpose and duration of the processing are set out in point 4.5.2. Some cookies are necessary for the proper functioning of the website and do not process personal data.

Please be informed that the Provider's website – only with your separate consent – also uses cookies for analytical purposes (Analytical Cookies), provided by a web analytics service called PostHog, operating in a cloud within the European Union (EU-cloud). You give your consent to the use of Analytical Cookies by clicking the "Accept" button on the information window displayed on the website; you may decline to give consent by clicking the Reject button, and you may withdraw your consent at any time thereafter.

The Provider uses the PostHog web analytics service to measure the number and characteristics of visitors to the website. The Provider uses the so-called EU-cloud package of PostHog, under which the storage and processing of your data takes place exclusively within the territory of the European Union, using servers located in the Amazon Web Services Frankfurt (eu-central-1) region.

PostHog's privacy notice is available at the following address: https://posthog.com/privacy

The data stored by PostHog are not suitable for identifying you by name; however, when you visit our website again, it is able to recognise that our website has previously been visited from a given computer using a given browser. In view of this, it may be suitable for identifying you personally, and therefore the use of Analytical Cookies is only possible with your consent.

PostHog uses the above information to assess and analyse your use of this website, to compile reports on the activities carried out on the website, and to provide other services related to the activities carried out on the website and to internet use in general. Please note that you may refuse the use of cookies by selecting the appropriate settings in your browser. Please be informed that by enabling cookies on the website, you consent to the processing of your data in the manner and for the purposes set out in this point.

If you refuse the use of Analytical Cookies, the Provider will still record the number of visits in this case as well, but only in an aggregated form that does not permit individual identification, generated using a one-way hash function.

Please note that, in respect of the processing described above in connection with Analytical Cookies, the Provider is also the controller.

4.5.1 Setting Cookies in Browsers

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

Please note that if you use an ad-blocker, the information on the use of cookies may not always be displayed. If you wish to view the information on cookies, please deactivate the ad-blocker!

4.5.2 Summary

Domain concerned	Data processed	Type of cookie	Purpose of processing	Duration of processing
sign-auth.hu.netlock.com	AUTH_SESSION_ID	session cookie	Identifier of the current authentication session, to ensure the proper functioning of the website	Period until the closure of the relevant visitor session
sign-auth.hu.netlock.com	KC_RESTART	session cookie	Ensuring the proper functioning of the website	Period until the closure of the relevant visitor session
sign-auth.hu.netlock.com	KEYCLOAK_LOCALE	session cookie	Ensuring the website's language setting	Period until the closure of the relevant visitor session
sign-auth.hu.netlock.com	KEYCLOAK_IDENTITY	session cookie	Ensuring the proper functioning of the website	Period until the closure of the relevant visitor session
sign-auth.hu.netlock.com	KEYCLOAK_SESSION	persistent cookie	Identifier of the current browser session, to ensure the proper functioning of the website	40 days
sign-auth.hu.netlock.com	KC_AUTH_SESSION_HASH	session cookie	Ensuring the integrity and proper functioning of the login process	60 seconds
sign-auth.hu.netlock.com	KEYCLOAK_REMEMBER_ME	persistent cookie	Remembers the login identifier (username) for the "Stay logged in" function. It is only created if the user ticks the "stay logged in" option, which is available on the login page.	365 days, which is a value hard-coded in the Keycloak source code (CookieMaxAge.YEAR) and is not configurable
sign-auth.hu.netlock.com	KC_ROUTE	session cookie	Routing of requests to the same server (load balancing), to ensure the proper functioning of the website	Period until the closure of the relevant visitor session
sign-auth.hu.netlock.com	ph_*_posthog	third-party, persistent cookie (PostHog, EU-	Analysis of website use, statistical identification of visitors (only with your consent)	1 year

Domain concerned	Data processed	Type of cookie	Purpose of processing	Duration of processing
		cloud), only with consent		

4.6 Processing Related to Asset Protection

A camera surveillance system and an access control system operate at the Provider's registered seat, the sole purpose of which is to protect the assets and interests of the Provider and other companies located in the building. The system at the registered seat is operated by the Security Service of OTP Ingatlan Befektetési Alapkezelő Zrt., as applicable from time to time.

The Provider does not carry out any processing activity in respect of the data recorded in connection with the operation of the system.

Details of the processing related to asset protection are set out in the Security Service's policies on asset protection and data protection.

4.7 Customer Service

The Provider may be contacted in person, in writing, or by telephone.

4.7.1 Telephone Customer Service

Please be informed that, in the course of contact with our telephone Customer Service, we record the entire audio recording of the conversation with the customer service representative on the basis of the Company's legitimate interest, and store it for 5 years from the date of the call. An exception applies to telephone calls relating to the suspension, reactivation and revocation of a certificate, to which the retention period set out in point 3.2 applies. If you have any questions regarding the storage or use of the audio recording, you may request information in the manner set out in Chapter 8.1.

4.8 Public Certificate Repository

The Provider operates a so-called public certificate repository on the netlock.com website, through which certificates whose publication in the repository the Customer has consented to may be searched and downloaded by anyone. Please be informed that you may withdraw your consent at any time; however, withdrawal of consent does not affect the lawfulness of processing based on consent before its withdrawal. In the absence of withdrawal of consent, the Provider processes the data for this purpose until the certificate expires.

The public certificate repository contains the data included in the given certificate, together with the status of the certificate.

4.9 Permanent ID

The subject of every certificate issued by the Provider must be unique, so that they can be unambiguously identified. To this end, the Provider assigns to each person a unique identifier maintained in the Provider's records, i.e. a Permanent ID. This identifier uniquely identifies the natural person named in the certificate.

Given that the Permanent ID is data included in the certificate, the Provider retains it for 10 years from the expiry of the certificate's validity. In the event of a notified dispute, the Provider must comply with its retention obligation until the final and binding conclusion of the dispute, even if the ten-year period calculated from the expiry of the certificate has already elapsed.

4.10 Processing of the Data of Contractual Contact Persons

In order to conclude and perform individual contracts, and to facilitate any communication between the Parties to the contractual relationship, the Provider processes the name, e-mail address and telephone number of the natural person acting on behalf of the contractual partner, on the basis of the Provider's legitimate interest, pursuant to Section 6:22 of the Civil Code, for 5 years.

In the case of contracts for consideration, the retention period of the data is 8 years, pursuant to Section 169(2)–(3) of Act C of 2000 on Accounting.

4.11 Storage of Log Files

Section 33 of the BM Decree provides that "the qualified service provider shall continuously log every event related to its IT system and the provision of the qualified service – in order to ensure business continuity, avoid data loss, and ensure IT security. The logged data set must cover the entire process of providing the qualified service and must be suitable for reconstructing every event related to the qualified service to the extent necessary for assessing the actual situations."

The logged data set must contain the following:

- the calendar date and exact time of the occurrence of the logged event;
- the data necessary for tracing and reconstructing the event;
- the name of the user or other person who caused the event.

The Provider is required to retain, or arrange for the retention of, data related to the certificate for 10 years from the expiry of the certificate's validity, data logged outside of this for 10 years from their creation, and the service policy and its amendments for 10 years from their repeal. In the event of a notified dispute, the Provider must comply with its retention obligation until the final and binding conclusion of the dispute, even if the ten-year period calculated from the expiry of the certificate has already elapsed.

In view of the above statutory provision, if you make use of our qualified service, the Provider, as a qualified trust service provider, logs every event related to its IT system and the provision of the qualified service, in the interest of the appropriate security of the provision of the service, and such logs/backups may also contain your personal data.

4.12 Recruitment

Please be informed that if you apply for a position advertised by the Provider, we will process the following data on the basis of your voluntary, informed consent:

- Name;
- E-mail address;
- Telephone number;
- Photograph;
- Education/qualifications;
- Professional experience;
- Language skills;
- As well as any other data that the applicant includes in their curriculum vitae.

Please be informed that we retain application materials for 6 months from their receipt, given that the selection process may take longer. If you withdraw your consent to the processing, the data will be deleted.

4.13 Enforcement of Legal Claims, Payment Reminders

If a payment reminder is sent in the course of the contractual relationship between the Provider and you, the Provider processes the data necessary for sending the payment reminder, such as name and address/e-mail address, on the basis of Article 6(1)(b) of the GDPR, i.e. the performance of a contract.

Please be informed that if, following the termination of the contract, the Provider has a claim against you, the Provider processes the data necessary for enforcing the claim on the basis of Article 6(1)(f) of the GDPR, i.e. the Provider's legitimate interest. The Provider has prepared a legitimate interest balancing test to support its legitimate interest, which it will make available to the authority upon request at any time. Please be informed that you may object at any time to this processing of your personal data, in the manner set out in Chapter 8.

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

4.14 Data Transfer Related to Invoicing and Payment

The Provider uses an external payment service provider for invoicing and processing online payments. The legal basis for the processing is Article 6(1)(b) of the GDPR. Transfers of data outside the EEA are carried out exclusively under the conditions set out in Chapter V of the GDPR. The payment service provider, the scope of data concerned, and the data transfer mechanism applied are set out in Annex 1.

4.15. Analysis of Uploaded Documents

Please be informed that documents uploaded to the NETLOCK service for signature are subjected, by the Provider's system, to automated, artificial intelligence-based analysis as part of the operation of the service. The purpose of the analysis is to determine the type of the document, to recognise signature positions, and to prepare a summary of the document's content. During the analysis, the entire text of the document is processed – without redaction.

The analysis takes place in a segregated cloud environment operated by the Provider, using the Amazon Bedrock service provided by the processor Amazon Web Services EMEA SARL, in data centres located within the European Economic Area; no transfer of data to a third country takes place. The content of the document is not transferred to any further third party – including the developer of the language model used – and is not used to train artificial intelligence models.

The legal basis for the processing is the pursuit of a legitimate interest under Article 6(1)(f) of the GDPR.

The Provider processes the result of the analysis for the same period as the document concerned, in accordance with the retention period set out in Annex 1 to this Policy.

This processing does not qualify as processing related to trust services.

The analysis is carried out in an automated manner; it does not qualify as automated decision-making under Article 22 of the GDPR, and it is not to be regarded as legal advice and does not replace consultation with a legal expert.

5. PERSONAL DATA PROCESSED AS PROCESSOR

In the provision of certain services, the Provider also acts as a Processor, while the Customer using the service qualifies as the Controller.

In the course of its processing activities, the Provider does not examine the legal basis of the processing, in particular given that the Provider only becomes aware of the documents that are the subject of the processing in the manner and subject to the restrictions set out in point 4.15. The Provider assumes, and records as a requirement in the data processing agreement between it and the Controller, that the Controller has the appropriate legal basis necessary for the processing.

The Provider records that it forwards, without delay, to the Controller any data subject requests relating to its processing activities, and that answering such requests is the responsibility of the Controller.

The Provider records that, having regard to Article 28(3) of the GDPR, it concludes a data processing agreement with the Controller in respect of the processing activity it carries out, which agreement is set out in point 8.1 of the General Terms and Conditions.

The Provider informs you that this chapter does not constitute complete information regarding the processing activity; therefore, if you have any questions, please contact the Controller.

6. LEGAL BASES AND PRINCIPLES OF PROCESSING

The Provider processes personal data exclusively in the following cases:

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

- the processing is necessary for compliance with a legal obligation to which the Provider is subject;
- the processing is necessary in order to protect the vital interests of the data subject or of another natural person;
- the processing is necessary for the purposes of the legitimate interests pursued by the 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 Provider processes personal data to the extent that is adequate, relevant and necessary for achieving the purpose. Once the purpose of the processing has ceased to exist, the Provider deletes the personal data permanently and irretrievably.

In the course of processing, the Provider does everything within its power to ensure the security of personal data by applying appropriate technical or organisational measures, including protection against unauthorised or unlawful processing and against accidental loss, destruction or damage.

The Provider has carried out a legitimate interest balancing test in connection with processing based on legitimate interest.

7. YOUR RIGHTS

This chapter sets out all the rights to which you are entitled in connection with the processing.

7.1 Right to Information

The Provider, as Controller, is required to provide information on the purpose, legal basis and duration of storage of the processing, the name and contact details of the Provider as Controller, the contact details of the data protection officer, the recipients of the personal data or the categories of recipients, and – where the processing is based on legitimate interest – on the legitimate interest of the Provider or a third party, on the fact of any data transfer, on the data subject's right to request from the Provider access to, rectification, erasure or restriction of processing of personal data concerning him or her, and to object to such processing, on the right to have the data transferred to another controller, and on the available remedies.

The Provider intends to fulfil this information obligation through this Policy.

If you are not the source of the data, and do not yet have the information described above, the Provider is also required, in addition to the above, to provide information on the source of the personal data and on the categories of personal data concerned.

If you have any questions regarding the processing of your data beyond what is set out in this Policy, you may request further information from the Provider by submitting a request to the e-mail address specified in point 1.1.

7.2 Right of Access

You have the right to request confirmation from the Provider as to whether or not personal data concerning you are being processed, and, if so, to request the information set out in point 7.1.

7.3 Right to Rectification

If the personal data recorded by the Provider are inaccurate, you have the right to request that the Provider rectify the personal data without undue delay, or, in the case of incomplete data, that it be completed.

7.4 Right to Erasure

You have the right to request, at any time, the erasure of your data processed by the Provider, which request the Provider must fulfil without undue delay in the following cases:

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

- you withdraw the consent on which the processing is based, and there is no other legal basis for the processing;
- you object to the processing of your data and there are no overriding legitimate grounds for the processing,
- the personal data have been unlawfully processed;
- the personal data must be erased for compliance with a legal obligation under Union or Member State law to which the Provider is subject.

Compliance with a request for erasure is not mandatory where the processing is necessary:

- for exercising the right of freedom of expression and information;
- for compliance with an obligation under Union or Member State law applicable to the Provider that requires processing of the personal data;
- for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes, insofar as compliance with the request is likely to render impossible or seriously impair the achievement of the objectives of that processing; or
- for the establishment, exercise or defence of legal claims.

7.5 Right to Restriction of Processing

If any of the following applies, you have the right to request that the Provider temporarily suspend the processing of your personal data, if:

- you contest the accuracy of the personal data, in which case the restriction shall apply for a period enabling the Provider to verify the accuracy of the personal data;
- the processing is unlawful and you oppose the erasure of the personal data and request the restriction of their use instead;
- the 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
- you have objected to the processing; in this case, the restriction shall apply for the period until it is established whether the Provider's legitimate grounds override your legitimate grounds.

Where processing is restricted under the above, such personal data may, with the exception of storage, only be processed by the Provider 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 processing is lifted, you will be informed of this in advance.

7.6 Right to Data Portability

You have the right to receive the data you have provided to the Provider in a structured, commonly used, machine-readable format (e.g. XML), and to have such data transmitted to another controller, provided that the following conditions are met:

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

Where the above conditions are met, you have the right to request that the personal data be transmitted directly between controllers, where technically feasible.

The exercise of the above right must 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 where such processing is based on the Provider's legitimate interest.

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

Where personal data are processed for direct marketing purposes (e.g. the sending of a newsletter), you have the right to object at any time to the processing of personal data concerning you for such purposes. If you object to the processing of personal data for the purposes of direct marketing, the personal data may no longer be processed for that purpose.

8. FRAMEWORK FOR THE EXERCISE OF YOUR RIGHTS

8.1 Manner of Exercising Your Rights

Please be informed that you may exercise the rights described above by submitting a request to the Provider or directly to the Provider's Data Protection Officer. The request may be submitted by post or electronically, at the following addresses:

Postal address: 1143 Budapest, Hungária körút 17-19.

E-mail address: trust@netlock.com

If you wish to contact the Data Protection Officer directly, you may do so at the contact details below, or in a letter sent to the Provider but addressed to the Data Protection Officer:

E-mail address: dpo@netlock.hu

8.2 Rules for Handling the Request

The Provider must inform you, without undue delay and in any event within one month of receipt of the request, of the measures taken in response to your request. Where necessary, taking into account the complexity and number of requests, this period may be extended by a further two months. The Provider shall inform you of any such extension, together with the reasons for the delay, within one month of receipt of the request. If your request was submitted electronically, the information shall, where possible, be provided electronically, unless you request otherwise.

If the Provider does not take action on your request, it must inform you without delay, and at the latest within one month of receipt of the request, of the reasons for not taking action, and that you may lodge a complaint with the competent supervisory authority. The Provider may only refuse a request in writing, stating its reasons.

The information and the requested measure shall be provided to you free of charge, unless your request is manifestly unfounded or excessive, in particular because of its repetitive character.

Having regard to the administrative costs involved in providing the requested information or notification, or in taking the requested measure, the Provider:

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

8.2.1 Content of a Data Subject Request

In order to ensure the faster handling of data subject requests, please ensure that the request contains at least the following:

- The name and contact details of the person submitting the request;
- The designation of the data subject right you wish to exercise;
- The designation of the service you have used.

Please be informed that if the Provider has reasonable doubts concerning the identity of the person submitting the request, it is entitled to request further information necessary to establish that person's identity.

9. ENGAGEMENT OF PROCESSORS

The Provider only engages Processors that comply with the provisions of the GDPR and other relevant legal requirements. The Provider also requires its processors, with whom it is in a contractual relationship, to comply with and enforce the provisions of this Policy and of its internal Data Protection and Data Security Policy.

The Provider transfers personal data to its processors solely on the basis of a written agreement, and only to the extent and for the purposes set out therein.

The list of Processors is set out in Annex 1 to this Policy.

10. DATA SECURITY MEASURES

In the course of processing under this Policy, the Provider implements the measures set out in this Policy and in its internal Data Protection and Data Security Policy in order to ensure that unauthorised persons do not gain access to the personal data processed.

The Provider has developed access levels to regulate electronic and physical access to personal data, the technical details of which, and the detailed IT data security requirements, are set out in its internal Policies.

The Provider takes measures to ensure that employees have access to the personal data processed by the Provider only to the extent necessary for the performance of their duties.

In addition to the above, the Provider is an organisation certified in accordance with the ISO 27001 standard (hereinafter: the "Standard"), and, in order to comply with this standard, the Provider is audited every year by an external, independent certification body. The Standard applies a process-based approach to information security that covers the establishment, implementation, operation, review, monitoring, maintenance and improvement of the organisation's entire information security management system. In the course of certification against the Standard, the Provider's entire data processing operations are also reviewed.

11. REMEDIES

If, in your view, the Provider has infringed the processing of personal data concerning you, you are entitled to the following remedies, in accordance with this chapter.

11.1 Right to Lodge a Complaint with a Supervisory Authority

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

The competent supervisory authority in Hungary:

Name: National Authority for Data Protection and Freedom of Information

Registered seat: 1055 Budapest, Falk Miksa u. 9-11.

Postal address: 1363 Budapest, P.O. Box 9.

E-mail: ugyfelszolgalat@naih.hu

11.2 Right to an Effective Judicial Remedy Against a Supervisory Authority

Please be informed that you may go to court against a legally binding decision of the supervisory authority concerning you, and also where the authority does not handle your complaint or does not inform you within three months of the progress or outcome of the complaint lodged.

Please be informed that, in addition to the competent supervisory authority, you may also go to court in the event of an infringement of the processing of your personal data. Proceedings may also be brought before the court of the place of your residence or habitual residence.

This Privacy Policy was originally drafted in Hungarian. This English-language version is provided solely for the convenience of users and does not constitute a substitute for the Hungarian original. In the event of any discrepancy, inconsistency, or conflict between the Hungarian and English versions, the Hungarian version shall prevail.