General Terms and Conditions (GTC)

for Certificate, Timestamp and Signature services and related optional services

NETLOCK Informatics and Network Security Services Limited Liability Company

Document name in Hungarian:	Általános Szerződési Feltételek
Document name in English:	General Terms and Conditions (GTC)
Version:	251215~~0625~~
Object identifier (OID):	1.3.6.1.4.1.3555.1.1.1.0.251206~~25~~15
Date approved:	14~~26~~.11~~05~~.2025.
Date published:	14~~26~~.11~~05~~.2025.
Valid from:	15~~25~~.12~~06~~.2025.
Number of pages:	36 pages, including cover

Approved by: **Dorottya dr. Vey**,
Head of Compliance of Netlock Ltd.

Table of Contents

1 Introduction 6
1.1 Overview 6
1.2 Service provider 6
1.3 Definitions 7
2 Purpose, scope and management of GTC 9
2.1 Purpose of GTC 9
2.2 Scope of GTC 9
2.2.1 Material Scope 9
2.2.2 Personal scope 9
2.2.3 Territorial scope 10
2.2.4 Temporal scope 10
2.3 Revision of GTC 10
2.4 Disclosure, notification and acceptance 10
2.5 Document versions 10
3 Services 13
3.1 Service Packages 13
3.2 Technical conditions of using the services 13
3.3 Availability of Services 13
3.4 ECC Transition 14
4 Service Agreement 16
4.1 Concluding the Standard Service Agreement 16
4.2 Term of the Service Agreement 18
4.3 Termination of the Service Agreement 18
4.4 Ceasing of the Service Agreement 19
4.5 Cases of material breach 20
4.6 Amendment of the service agreement 20
4.7 Website authentication online SSL certificate 20
5 Application and payment for Services 21
5.1 Application for periodic services 21
5.2 Application for optional and other services 22
5.3 Fees 22
5.4 Payment and invoicing 23
5.5 Complaints related to invoices 24
6 Contracting parties' rights and obligations 24
6.1 Service Provider's obligations, liability and rights 24
6.2 Customers' obligations, liability and rights 25
7 "NETLOCK" cloud service 27
7.1 "NETLOCK" cloud service for private purposes 27

7.2 NETLOCK Mobile Application 27
7.3 Concluding the licence agreement 27
7.4 Rules applicable to the use of the Mobile Application 27
7.5 Rights and obligations of the user of the Mobile Application 27
7.6 Service Provider's liability 28
7.7 Copyrights 28
8 Logfile retention 29
9 Protection of personal data 30
9.1 Provisions related to data processing 30
9.1.1 Content of the data processing relationship 30
9.1.2 Data Controller's rights and obligations 31
9.1.3 Data Processor's rights and obligations 31
9.1.4 Data security 32
9.1.5 Use of additional data processor 32
9.1.6 Exercising the data subject's rights 33
9.1.7 Personal data breach 33
9.1.8 Register of data processing activities 34
9.1.9 Audits and inspections 34
9.1.10 Technical and organisational measures 34
10 Suggested verification procedure for Certificate status 35
11 Other conditions and important information 35
11.1 Communication and complaint management 35
11.2 Obligation of confidentiality 36
11.3 Procedure to be applied in the event of disputes 38
11.4 Other conditions 38
11.5 Security Requirements in Contracts with Third Parties 38
~~1 Introduction ..... 4~~
~~1.1 Overview ..... 4~~
~~1.2 Service provider ..... 4~~
~~1.3 Definitions ..... 5~~
~~2 Purpose, scope and management of GTC ..... 7~~
~~2.1 Purpose of GTC ..... 7~~
~~2.2 Scope of GTC ..... 7~~
~~2.2.1 Material Scope 7~~
~~2.2.2 Personal scope 7~~

2.2.3Territorial scope 8
2.2.4Temporal scope 8
2.3 Revision of GTC 8
2.4 Disclosure, notification and acceptance 8
2.5 Document versions 8
3 Services 11
3.1 Service Packages 11
3.2 Technical conditions of using the services 11
3.3 Availability of Services 11
3.4 ECC Transition 12
3.5 Fulfillment of certificate requests based on Bit4ID cards 13
4 Service Agreement 13
4.1 Concluding the Standard Service Agreement 14
4.2 Term of the Service Agreement 16
4.3 Termination of the Service Agreement 16
4.4 Ceasing of the Service Agreement 17
4.5 Cases of material breach 18
4.6 Amendment of the service agreement 18
4.7 Website authentication online SSL certificate 18
5 Application and payment for Services 18
5.1 Application for periodic services 19
5.2 Application for optional and other services 20
5.3 Fees 20
5.4 Payment and invoicing 21
5.5 Complaints related to invoices 21
6 Contracting parties' rights and obligations 22
6.1 Service Provider's obligations, liability and rights 22
6.2 Customers' obligations, liability and rights 23
7 "NETLOCK" cloud service 24
7.1 "NETLOCK" cloud service for private purposes 24
7.2 NETLOCK Mobile Application 25
7.3 Concluding the licence agreement 25
7.4 Rules applicable to the use of the Mobile Application 25
7.5 Rights and obligations of the user of the Mobile Application 25

7.6 Service Provider's liability 26
7.7 Copyrights 26
8 Logfile retention 27
9 Protection of personal data 28
9.1 Provisions related to data processing 28
9.1.1 Content of the data processing relationship 28
9.1.2 Data Controller's rights and obligations 29
9.1.3 Data Processor's rights and obligations 29
9.1.4 Data security 30
9.1.5 Use of additional data processor 30
9.1.6 Exercising the data subject's rights 31
9.1.7 Personal data breach 31
9.1.8 Register of data processing activities 31
9.1.9 Audits and inspections 32
9.1.10 Technical and organisational measures 32
10 Suggested verification procedure for Certificate status 32
11 Other conditions and important information 33
11.1 Communication and complaint management 33
11.2 Obligation of confidentiality 34
11.3 Procedure to be applied in the event of disputes 36
11.4 Other conditions 36

1 Introduction

1.1 Overview

These General Terms and Conditions (hereinafter: GTC) contain the general terms and conditions applicable to the use of the certificate, timestamp and signature services of the NETLOCK Informatics and Network Security Services Limited Liability Company (hereinafter: Service Provider) and of the optional services that may be ordered in connection with those as well as to the NETLOCK Mobile Application (hereinafter: **Mobile Application**) operated by the Service Provider.

The use of the Mobile Application shall be conditional upon the acceptance of the GTC.

1.2 Service provider

The entity referred to herein as the Service Provider shall be NETLOCK Kft.

Data of the Service Provider:

Name:	NETLOCK Informatics and Network Security Services Limited Liability Company
Short name:	NETLOCK Kft.
Seat:	H-1143 Budapest Hungária krt. 17-19. Hungary
Postal address:	H-1439 Budapest, Pf. 663, Hungary
Company registration number:	01-09-563961
Tax number:	12201521-2-42
Customer service phone:	(1) 437-6655
Website:	netlock.hu
Customer service e-mail:	info@netlock.hu
Send requests, documents to:	igenylesek@netlock.hu

For information on the Service Provider, its registration by the supervisory authority, compliance assessment, voluntary accreditation and other qualifications see Section 1.1.2 of the Service Practice Statement.

The Service Provider performs (and has others perform) compliance inspections and checks in the interest of ensuring that the processes, staff, devices, and environment related to its Services always meet relevant legislative and professional requirements.

Before commencing the provision of its services, the Service Provider had an external, independent conformity assessment body evaluate those on the basis of applicable standards and legislation, adhering to the following:

- evaluation takes place on the basis of the pieces of legislation and standards laid out in this Chapter;
- the evaluation takes into account all of the unique features of the Service Provider's trust services to be audited;
- the evaluation covers all service activities related to its subject.

1.3 Definitions

Fee package	Services of specific volume and quality included in the Service Provider's Price List (e.g., X pieces of timestamps or X MB storage space).
Parties	NETLOCK Kft. – as the Service Provider – and the Applicant and Subscriber for the Services together.
Periodic Service	The Service Provider's trust services and non-trust certification services, for which service agreements may be concluded for a specific, pre-defined period.
Optional service	Supplementary services – usually subject to a fee – available in addition to certain Periodic Services
Other services	All services rendered by the Service Provider not qualifying as periodic or optional services.
"NETLOCK" cloud service	The name of the latest-generation cloud-based remote key management, signature, and certificate service of Service Provider. Within the framework of the "NETLOCK" cloud service the signature and seal certificates specified in Subsection 1.2.1 Certificate types of *Service Practice Statement for Qualified Certificate Services* may be applied for subject to online, video identification (whose type designation includes the designation (VideoRA). The private keys of certificates requested within the framework of the "NETLOCK" cloud service will be generated in QSCD HSM managed by the Service Provider in such a way that those will be under the sole control of the End Users. The private keys can be used by the End Users for the generation of qualified signatures or seals within the framework of the Service Provider's remote key management and signature service, relying on the "NETLOCK" mobile and web application. The "NETLOCK" cloud service is not the same as the Service Provider's "NETLOCK Sign" service, which is also cloud-based.
NETLOCK SIGN	An electronic signature/seal service, accessible through web interface, where the End User can activate his signature creation data remotely and is able to execute the electronic signature operation online. Within the framework of the NETLOCK SIGN service, the End User may also use the Service Provider's general time stamping service. The service can be used via a public signature portal by ordering the cloud-based NETLOCK SIGN Business signature service and/or integrated with corporate IT systems (through REST API web calls) under the NETLOCK SIGN Enterprise brand name. The NETLOCK SIGN ENTERPRISE service is a public cloud with central key storage, or it may also be used as a hybrid cloud service partly installed with the Customer.
Service	Services defined in Service Policy as service.
Service Policy	Service Policy for Qualified Certificate Services, Service Policy for Qualified Archiving Services, Service Policy for Qualified Timestamp Services, Service Policy for Non-qualified Certificate Services and Service Policy for Non-eIDAS Certificate Services.

Service Practice Statement	Service Practice Statement for Qualified Certificate Services, Service Practice Statement for Service Practice Statement for Qualified Timestamp Services, Service Practice Statement for Non-qualified Certificate Services and Service Practice Statement for Non-eIDAS Certificate Services.
Subscriber	The Service Provider's contractual partner, who undertakes the payment of the service fees. His rights and obligations are presented separately in the GTC. In the case of certificate services, if an organization is also specified as the certificate Subject, or only a natural person is specified in it, it is usually the same. In the case of signature services, it is the same as the Signatory Partner or the End User.
Customer	The party concluding the agreement with the Service Provider. In the case of Certificate Services, the Applicant for the certificate and the Subscriber (where applicable, these actors are the same). In the case of timestamp services, the Subscriber to the service. In the case of NETLOCK SIGN serviceand the "NETLOCK" cloud service, the Signatory Partner and the End User. When the GTC refers to the Customer, this shall mean the Subscriber, the Applicant and the End User at all times.
Applicant	In the case of certificate services, the natural person acting in the certificate issuance, certificate management and status change procedure, approving the Service Agreement on behalf of the Customer, who may be: ● the natural person designated as the Subject of the certificate (in the case of the Pseudonym the applicant for the pseudonym); or ● the representative or proxy of the organisation specified as the Subject; or ● the owner of the domain name, trademark or product name designated as the Subject, or – in the case of the organisation – the representative or proxy of it, or the person controlling the domain name. This is the same as the Subscriber if a natural person has been designated as the Subject of the certificate (without an organisation).
End User	In the case of Certificate Services, the natural person who controls the private key pair of the public key included in the certificate (uses it exclusively or is responsible for the use of it). In the case of timestamp services, the person who contacts the service provider in order to use the timestamp service. In the case of NETLOCK SIGN service and the "NETLOCK" cloud service, the person who – within the signature services – by activating his private key, executes an electronic signing/stamping operation or carries out the verification of electronic signature/seal or the person responsible for such operation.
Signatory Partner	The Service Provider's partner, who provides its own customers with the signature service, as part of which it may participate in the identification of Applicants (in respect to whom it has limited information and administration rights) and who uses the signature service for providing the service integrated with its own service, and who – as Subscriber – undertakes to pay the fee in respect to the end users.

Consumer	A natural person acting outside the scope of his profession, independent trade or business activity.
NETLOCK Mobile Application	A mobile application supporting the End User's usage of the "NETLOCK" cloud service, provided by the Service Provider, and installable on smart phones from the official app stores. The application supports, among others, the application, through video identification, for end user certificates available within the "NETLOCK" cloud service (see Section 1.2.1 Certificate types of the Service Practice Statement for Qualified Certificate Service) and its life cycle management (see Section 4. Life cycle requirements of the Service Practice Statement for Qualified Certificate Service); the remote management of end user private keys belonging to the certificates (remote key management service), and the qualified signature or qualified sealing of documents (remote signature service).
Mobile Application User	The natural person or organisation, who downloads the NETLOCK Mobile Application from any webshop or from the Service Provider's website and installs it.

The definition of additional terms used in GTC is included in Sections 1.6 of the Service Policy and the Service Practice Statement.

2 Purpose, scope and management of GTC

2.1 Purpose of GTC

The purpose of the GTC is to determine the general legal and commercial conditions of service agreement – and thereby of the legal relationship – entered into between the Service Provider and the Customer. The Service Agreement concluded with the Customer determines the services used within the framework of the contractual relationship and whether the Service Provider renders it as a qualified or non-qualified service.

2.2 Scope of GTC

2.2.1 Material Scope

The subject matter of these GTC includes the Service Provider's Certificate, Timestamp and Signature services, and the optional services connected with those.

The Service Provider continuously provides public information on its services through its website, which shall not qualify as an offer.

2.2.2 Personal scope

The Service Provider renders the services to the Customers who conclude a Service Agreement with it. In respect to the Services the personal scope of the GTC covers the Customers and the Service Provider.

Certain Services of the Service Provider are also available publicly. The parties using such services shall fall outside the scope of GTC.

2.2.3 Territorial scope

All services rendered by the Service Provider are available all over the world. The Service Provider carries out its operation based on the prevailing Hungarian laws.

2.2.4 Temporal scope

These GTC are effective from the date specified on the coversheet as *Effective from* and shall be in force until repealed or a new version is published (see Section 2.4).

2.3 Revision of GTC

The Service Provider is entitled to modify these General Terms and Conditions unilaterally at, in accordance with the provisions of Section 2.4.

Customers who do not accept the modification of the GTC are entitled to terminate the Service Agreement in writing with immediate effect within 30 days from the publication or notification, at the latest.

2.4 Disclosure, notification and acceptance

The Service Provider publishes its effective General Terms and Conditions on its website specified in Section 1.2. Upon the modification of the GTC, the Service Provider shall publish the new version of GTC 30 days prior to its effective date on its website specified in Section 1.2. If the modification of the GTC is necessitated by legislative changes or an administrative decision, the changes may enter into force with immediate effect.

The Service Provider shall notify Customers and Applicants of the modification of the GTC by publishing the new version on the website. In the case of significant changes, the Service Provider may also notify Customers directly by e-mail.

Any issues or comments related to these GTC should be addressed to the Service Provider's customer service (see Section 1.2).

2.5 Document versions

OID	Description of change	Entry into force	Prepared by:
- (GTC v1.1)	First public version		NetLock Kft.
1.3.6.1.4.1.3555.0.1.011026	Introduction of the requirements specified in the Electronic Signature Act for registration as an advanced authentication provider	26 October 2001	NetLock Kft.
1.3.6.1.4.1.3555.0.1.20030331	Introduction of the requirements specified in the Electronic Signature Act for registration as a qualified authentication provider	31 March 2003	NetLock Kft. Practice Statement Approval Unit (PSAU)
1.3.6.1.4.1.3555.0.1.20060411	Updating the document with the requirements of the Administrative Proceeding Act for the authentication service accepted in the public administration	11 April 2006	Dr László Szentirmai

1.3.6.1.4.1.3555.0.1.20060728	Harmonisation of definitions necessary after the administrative review in 2006	28 July 2006	Dr László Szentirmai
1.3.6.1.4.1.3555.0.1.20060828	Clarification based on official findings	28 August 2006	NetLock PSAU
1.3.6.1.4.1.3555.0.1.20061025	Clarification based on official findings	25 October 2006	NetLock PSAU
1.3.6.1.4.1.3555.0.1.20070926	Clarification based on official findings	26 September 2007	NetLock PSAU
1.3.6.1.4.1.3555.0.1.20071114	Simplification and clarification based on official findings	14 November 2007	NetLock PSAU
1.3.6.1.4.1.3555.0.1.20100723	Modifications related to the launch of qualified electronic archiving and other clarifications	23 July 2010	NetLock PSAU
1.3.6.1.4.1.3555.0.1.20110215	Clarification based on the findings of the National Media and Infocommunications Authority	15 March 2011	NetLock PSAU
1.3.6.1.4.1.3555.0.1.20131215	Clarification due to the change of NETLOCK's registered office	15 December 2013	NetLock PSAU
1.3.6.1.4.1.3555.0.1.20140709	Modification of the section related to the Service Provider's rights Modification of the Service Provider's data (postal address, fax number)	9 July 2014	NetLock PSAU
1.3.6.1.4.1.3555.0.1.20151130	Modifications: • change in opening hours for customers, • definitions of new terms in connection with the introduction of new product (NETLOCK SIGN), description of the special rules applicable to the service, • clarification of references to legal provisions	1 January 2016	NETLOCK PSAU
1.3.6.1.4.1.3555.0.1.20160106	Updating the document with the findings of the National Media and Infocommunications Authority	1 February 2016	NETLOCK PSAU
1.3.6.1.4.1.3555.0.1.20160531	Updating the document with the eIDAS and Hungarian legislative requirements	31 May 2016	Dr Anett Barabás
1.3.6.1.4.1.3555.0.1.20160630	Clarification of the updates related to the eIDAS and Hungarian legislative requirements	30 June 2016	Dr Anett Barabás
1.3.6.1.4.1.3555.0.1.20160902	Clarification based on the findings of the National Media and Infocommunications Authority	5 September 2016	Dr Anett Barabás
1.3.6.1.4.1.3555.0.1.20160909	Additional clarification based on the recommendation of the National Media and Infocommunications Authority	9 September 2016	Dr Anett Barabás
1.3.6.1.4.1.3555.0.1.20170301	Application of legislative changes Revised and modified content based on the new Service Policies and Service Practice Statements published simultaneously with this version of GTC. The structure of the document has been changed.	28 April 2017	Dr Zsófia Fehér Zoltán Szabó
1.3.6.1.4.1.3555.0.1.20170515	Version clarified and supplemented based on the findings from the compliance assessment procedure conducted by MATRIX Auditing, Evaluating and Certification Ltd.	19 June 2017	Zoltán Szabó
1.3.6.1.4.1.3555.0.1.20181127	Updating the document with the modifications necessary due to the change in the method of concluding the standard service agreements when permitted by these GTC.	26 December 2018	Dr Zsófia Fehér Zoltán Szabó
1.3.6.1.4.1.3555.0.1.20201216	Supplementation of the GTC with the provisions related to data processing, the conditions of using the NETLOCK Mobile Application, the new method of concluding the Service Agreement, additional clarifications, correction of the title of service practice statements and policies.	18 December 2020	Dr Dóra Káli
1.3.6.1.4.1.3555.0.1.20210827	Supplementation of the GTC with the conditions of using the personal signature certificates issued within the framework of	27 September 2021	Zoltán Kővári-Szabó

	the "NETLOCK" cloud service and online SSL certificates; specifying the data processing deadlines.		
1.3.6.1.4.1.3555.1.1.1.0.211216	Added sections 8 and 10	16 December 2021	Zoltán Kővári-Szabó
1.3.6.1.4.1.355.1.1.1.0.230315	In Section 1.2 of the GTC, the fax number has been deleted, the Section has also been supplemented with the addition of compliance tests; clarifications in the Definitions section in Section 1.3; in Sections 2.1, 2.2.2 and 2.4, the terminology has been clarified; in Section 3.3, the availability of Services has been added; in Section 4.3, the termination of the Service Agreement has been completed; in Section 5, the wording has been clarified; in Sections 9, 11.2 and 11.3, the references have been updated.	13 March 2023	NL Compliance
1.3.6.1.4.1.3555.1.1.1.0.230930	In Section 1.3 of the GTC, the "NETLOCK" cloud service, Service Policy, Service Practice Statement, Subscriber, Customer and End User concepts has been clarified. Section 3 was supplemented with provisions regarding the ECC transition as section 3.4. Section 3 was supplemented with provisions regarding the fulfilment of certificate requests based on the Bit4ID card. In Section 4 the penultimate paragraph regarding the indivicual services has been clarified with referring to the Price List. In Section 4.3. clarifications were made. In Section 4.7 clarifications were made regarding the application for the website authentication online SSL certificates and their method. In Section 5.1. regarding the application for the certificates, the Service Provider's right to refuse to enter a contract was expanded. In Section 5.2 the process of the application for the Optional and other services has been clarified. Section 6.1. has been clarified by referring to other organizations and in the last paragraph, the Service Provider's exclusion of liability has been stated regarding the damages made by the breach of obligations by the Customer. Due to the included additions and paragraphs, the document numbering and the table of contents have been modified. The formatting of the document has been updated.	30 September 2023	NL Legal/NL Compliance
1.3.6.1.4.1.3555.1.1.1.0.231229 Out of force	In the title and Section 1.1 of the GTC the archiving service has been removed. In Section 1.3 the archiving service, has been removed, the definition of other service and end user has been modified. Service Policy for Qualified Archiving Services and Service Practice Statement for Qualified Archiving Services has been removed. In Section 2.2 the archiving service has been removed. In Section 3.3 Service Practice statement for Qualified Archiving Services has been removed. In sections 4.3 and 5.1 archiving service has been removed. In Section 9.1 archiving service has been removed and the definition of purpose of data processing has been modified. In Section 11.1 phone communication has been modified.	31 January 2024	NL Compliance
1.3.6.1.4.1.3555.1.1.1.0.240901	In Section 11.2 implementation of legislative modification	30 August 2024	NL Compliance
1.3.6.1.4.1.3555.1.1.1.0.241115	Added Section 11.4	15 November 2024	NL Compliance
1.3.6.1.4.1.3555.1.1.1.0.241115	1.1,, 1.3, 4.3, 5.1, 9.1,pontok: modification of the archiving service has been removed. 3.1, 5, pontok: clarifications	02 December 2024	NL Compliance
1.3.6.1.4.1.3555.1.1.1.0.250414	1.2. seat modification	14 April 2025	NL Compliance
1.3.6.1.4.1.3555.1.1.1.0.250625	3.4 ECC Transition date update 11.4 Deadline clarification for revoking TLS certificates	25 June 2025	NL Compliance

1.3.6.1.4.1.3555.1.1.1.0.251214	3.5 Bit4id Card deletition 7.1 change of cloud service for private purposes 11.5 new Security Requirements in Contracts with Third Parties		

3 Services

These GTC contain the terms of contract related to the services of the Service Provider. A more detailed description of the individual services is provided by the Service Provider on its website. The detailed procedural and operational rules applicable to the individual services are included in the Service Practice Statement applicable to the respective service, attached hereto as Annex.

The Service Provider is entitled to modify its services and service packages unilaterally complying with the provisions of Section 2.4.

3.1 Service Packages

The Service Provider may also provide the services and certain devices necessary for using those services in the form of service packages. The TSP may make the provision of services conditional upon the use of software support arrangements (such as transaction statistics)
When in a service package the Service Provider also provides the Customer with the use of a computer programme, the use of it shall be subject to the conditions stipulated in the end user licence agreement.
If the Service Provider also provides the Customer with a card reader customer device, it shall do so in such a way that upon the failure of the device during its proper use, it shall replace the device during the term of the agreement free of charge with an identical or a different type of device agreed with the Customer. Any potential fee between the fees applicable to the devices shall be paid by the Customer. If the Customer Device needs to be replaced due to another reason – particularly if it is lost – the Service Provider shall replace it against a fee indicated in the prevailing Price List.
For detailed information on the service packages and the related special conditions see the Service Provider's website (see 1.2).

3.2 Technical conditions of using the services

The use of the services rendered by the Service Provider requires suitable software, an IT device capable of running that software and, for certain services, a cryptographic device.

The Customer must have the appropriate IT equipment to use the services.

In connection with certain services, the Service Provider also provides its Customers with software and cryptographic hardware devices. In these cases, the Service Provider provides technical support for starting to use these devices on its website or over the phone (see Customer Service).

No technical support may be requested in respect to hardware and software tools not provided by the Service Provider.

3.3 Availability of Services

As part of the qualified certificate service provided by the Service Provider, applications for the revocation and suspension of end-user certificates and the availability of revocation records are

provided by the Service Provider in accordance with Section 4.10.2 of the Service Practice Statement for Qualified Certificate Services.

As part of the “non qualified” certificate service provided by the Service Provider, applications for the revocation and suspension of end-user certificates and the availability of revocation records are provided by the Service Provider in accordance with Section 4.10.2 of the Service Practice Statement for Non Qualified Certificate Services.

The availability of the time stamp service provided by the Service Provider is provided by the Service Provider in accordance with Section 4.2 of the Service Practice Statement for Qualified Timestamp Services.

For the non eIDAS Certificate Services provided by the Service Provider, the Service Provider ensures the availability of the service in accordance with Section 4.10.2 of the Service Practice Statement for Non eIDAS Certificate Services.

3.4 ECC Transition

3.4.1. The RSA algorithm used during the provision of its services defined in the Service Policies will be replaced due to compliance with new standards, at the time indicated by Service Provider, but no later than 31.12.2028. Thus, Service Provider will switch to an ECC-based algorithm (hereinafter: “ECC Transition”).

3.4.2. Customer acknowledges that in relation with the ECC Transition, increased cooperation with the Service Provider may become necessary, especially in the case of integrated or complex systems.

3.4.3. Until the time of the ECC Transition, Service Provider performs its certification services defined by this contract by the use of an RSA-based algorithm as follows:

In view of the standards, certificates issued with an RSA-based algorithm shall be revoked by TSP as of the date stated by TSP (which, according to Service Provider’s current information based on the changes of the standards, may be the 31st of December 2028 at the latest.) regardless of their original validity period included in the certificate.

In view of the ECC Transition, TSP can perform the certificate services, defined by this contract, by revoking the certificate based on the RSA algorithm on the day stated by TSP (which, according to Service Provider’s current information based on the changes of the standards, may be the 31st of December 2028 at the latest).

Pursuant to the above, it is recommended that the Partner at all times applies for a certificate based on the RSA algorithm to be issued for 2 (two) years in a way/within a deadline that the certificates can be issued in accordance with the procedure set out in the TSP Policies by December 31, 2026, at the latest.

After December 31, 2023, Service Provider can perform the service obligation of the 2 (two) year certificates as follows:

- either with certificates based on ECC algorithm
- or by issuing certificates based on RSA algorithm in a way that Service Provider revokes the certificate based on RSA algorithm on the day stated by Service Provider (which, according to Service Provider’s current information based on the changes of the standards, may be the 31st of December 2028 at the latest). Customer acknowledges that Service Provider’s

fulfillment of any obligation to withdraw the certificates stemming from the ECC Transition is an objective circumstance beyond any control of the Service Provider.

Service Provider hereby excludes liability for any damages (including any direct, indirect, consequential or other damages, etc.), and the reimbursement of any cost incurred at the Customer, or third parties related to the withdrawal of the affected certificates within the period of the certificates' validity set forth in the contract. The exclusion of liability prescribed in the present provision applies to the requests for a new key storage device (card, HSM, etc.), as well.

Customer is aware that Service Provider made its price offer taking into consideration the above possibilities, i.e. the above were compensated by Service Provider in the price calculation included in the price offer.

Customer acknowledges the above notice of the Service Provider and makes any request taking into account the above possibility.

In addition to the above, Service Provider also draws Customer's attention to the fact that the "RSA"-based time stamps placed on the documents expire in accordance with the above no later than the day stated by the Service Provider (which, according to Service Provider's current information based on the changes of the standards, may be the 31st of December 2028 at the latest) Thus, in accordance with the Service Provider's Policies, over-authentication steps are required.

~~3.5 Fulfillment of certificate requests based on Bit4ID cards~~

~~3.5.1. Service Provider informs Customer that in the case of Bit4ID two-year qualified card certificates, the expiration date of the certification of the card (key storage device) published by the manufacturer of the device is currently: 06.29.2025.~~

~~If the manufacturer does not renew the certification of the cards, Service Provider is obliged by law to withdraw the cards and the corresponding certificates on the date indicated above.~~

~~3.5.2. The revocation of the certificate entails the need to apply for a new certificate and (if Customer still wishes to use card certificate) a new card, in order to retain the ability to sign.~~

~~The eventual expiration of the card's certification within the validity period of the signing certificate is an objective circumstance beyond any control of the Service Provider.~~

~~Service Provider hereby excludes any liability for any damages (including any direct, indirect, consequential or other damages, etc.) and the reimbursement of any cost incurred at the Customer or third parties related to the withdrawal of the affected certificates within the period of of the certificates' validity set forth in the contract. The exclusion of liability prescribed in the present provision applies to the requests for a new key storage device (card), as well.~~

~~Customer acknowledges the above notice of Service Provider and makes any request taking into account the above possibility.~~

~~Service Provider provides information on possible substitute products for card certificates upon a separate request from Customer.~~

4 Service Agreement

For the purposes of using the services the Parties shall conclude a service agreement, in order to define the service(s) to be rendered and used as well as the respective parameters and conditions. The Parties may conclude

- standard service agreements, available with uniform wording and with the standard parameters and conditions in accordance with the Service Provider's Price List and other public communication, and
- individual service agreements, worded by the Service Provider tailored to the Customer's requirements. Such individual service agreements may also contain provisions departing from these GTC. In this case the service agreement shall prevail.

Deviation from the provisions of the Service Policy and the Service Practice Statement applicable to the subject matter of the service agreement is not permitted in either case.

The annexes to the service agreement shall include these GTC, the Service Policy and the Service Practice Statement applicable to the respective service and the Price List.

Should there be any conflict between the service agreement and the annexes thereto, the provisions of the service agreement shall prevail.

Should there be any conflict between the GTC and the Service Practice Statement or the Service Policy, the provisions of the Service Practice Statement or the Service Policy shall prevail.

The individual service agreements are concluded within the framework of individual procedures. The fee of the individual procedures is included in the current Price List.

A single service agreement may apply to the simultaneous use of several services.

4.1 Concluding the Standard Service Agreement

The service agreement is concluded when applying for the services (see Section 5). The service agreement may be concluded in the following ways:

a) The Customer signs the service agreement – prepared by the Service Provider for the respective service based on the application – and, based on the provisions of the Service Practice Statement, returns it to the Service Provider in its original form or as a copy, on paper or electronically. The service agreement must be signed by the Applicant and – if it is different – by the Subscriber – in their own hand or electronically (for the accepted electronic signatures see Section 3.2.3 of the Service Practice Statement).

   The service agreement is created when the copy signed by the Applicant and the Subscriber is signed by the Service Provider, and it enters into force by the commencement of the provision of the services or making them available by the Service Provider and notifying the Customer to this effect. The Parties declare that the service agreement shall also be deemed as signed by the Service Provider when the person authorised to sign for the Service Provider supplies it with his at least non-qualified (advanced) electronic signature or with the Service Provider's at least non-qualified (advanced) electronic seal.

b) In certain cases and in respect to certain service types, specified by the Service Provider, the Service Provider is entitled to define it as the exclusive method of concluding the service agreement and that the Customer accepts the service agreement prepared by the Service Provider based on the data of the application on an electronic device in the Service Provider's system by ticking off the checkbox. When concluding the contract in the manner specified in

this Section 4.1.b), the GTC and the Privacy Policy shall be accepted in such a way that on the electronic device, in the Service Provider's system, the Customer ticks off the checkboxes placed next to the links for downloading the GTC and the Privacy Policy. The electronic device stipulated in this section may be the electronic device supplied by the Service Provider – also including the Service Partner executing certain functions of the Registration and Authentication Unit – or the Customer's own electronic device.

Before finalising the data of the application, the Customer shall verify it on the electronic device in the Service Provider's system or in the system of the Service Partner carrying out certain functions of the Registration and Authentication Unit, and identify the data input errors, if any. The data input error, once identified by the Customer, shall be corrected by the Service Provider of the Service Partner.

The Service Provider shall immediately after receiving the service agreement in its system, or within 48 hours at the latest, commit the agreement to writing – with the content corresponding to the conditions accepted by Applicant – electronically, file it and make it available to the Customer by sending it electronically by e-mail.

c. The service agreement for using the "NETLOCK" cloud service shall be concluded as follows: In order to use the service, the Customer shall – on the electronic device in the Service Provider's system – accept the Service Provider's Service Practice Statement for Qualified Certificate Services and Service Policy for Qualified Certificate Services, the General Terms and Conditions, the Privacy Policy, the Notice on the conditions of video identification and the service agreement, by ticking off the individual checkboxes. The electronic device specified in this subsection shall be Customer's own electronic device. The Service Practice Statements, the service agreement, the Privacy Policy and the GTC shall be sent to the Customer by e-mail within 48 hours from the issuance of the certificate, at the latest.
Prior to finalising the data of the application, the Customer shall verify it on the electronic device in the Service Provider's system, and identify and correct the data input errors, if any. The tool to be used for the correction of the data input error shall be the Service Provider's Application interface.

The technical conditions and process of the video identification necessary for the use of the "NETLOCK" cloud service are stipulated in the Service Provider's Service Practice Statement and Service Policy related to Qualified Certificate Services.

By accepting the application for the service, the Service Provider declares that it has the personal and material conditions necessary for the fulfilment of the services, and the services comply with the prevailing regulations.

Common rules applicable when concluding the contract in the manner specified in Section 4.1.b) and c):

The sending of the service agreement by e-mail qualifies as the confirmation of the order. The service agreement is created by the Service Provider's committing it to writing in accordance with the foregoing and enters into force by the Service Provider's commencing the provision of the service or making it available to the Customer and notifying the Customer

to this effect or – if it is later – on the day of making the service agreement available to the Customer in accordance with the foregoing.

When the Applicant and the Subscriber are different entities, in order to create the service agreement in the manner stipulated in Section 4.1.c) hereof, the Applicant must hold an effective authorisation – stipulate in a private document representing conclusive evidence – for the conclusion of the service agreement. The service agreement created in accordance with Section 4.1.b) c) – despite its having been committed to electronic writing by the Service Provider – shall not qualify as a written agreement. The agreement shall be filed. After making it available to the Applicant by e-mail, the service agreement shall not be accessible in any other way.

The service agreement can be concluded in the Hungarian language.

4.2 Term of the Service Agreement

Depending on the service type, the service agreement may be concluded for a definite or indefinite term.

4.3 Termination of the Service Agreement

Either party may terminate the agreement for an indefinite term by a unilateral written declaration to the other party with 30 days' notice. The Parties shall also treat the exercise of the Customers' right to terminate the contract by ordinary notice, provided for in Section 2.3, as termination by ordinary notice.

Service agreements for a definite term shall not be terminated by ordinary notice; however, Customers' right to terminate the contract by ordinary notice, provided for in Section 2.3 and Section 8.1.4 may also be exercised in respect to service agreements for a definite term.

If the party concluding the agreement with the Service Provider qualifies as a Consumer, they shall be entitled to the termination right specified in Section 20 of Government Decree 45/2014 (II. 26).

The Service Provider may terminate the Service, and the certificate, and timestamp services requested as part of that, by ordinary notice upon the expiry of the related Signatory Partner agreement for the same date, if those have been concluded in connection with the Partner agreement (framework contract).

The service agreement may be terminated by extraordinary notice upon the other Party's material breach (se 4.5) with immediate effect – without prejudice to other claims arising from the breach – in a unilateral reasoned written declaration addressed to the other party, in accordance with the provisions of the Civil Code, which shall take effect on the day of receiving the notice.

The application of international conventions, laws, regulations and other acts relating to economic restrictive measures ("sanctions") is a mandatory and essential part of the Service Provider's operations. The Service Provider is therefore entitled to decide at any time, at its sole discretion, not to establish and maintain a contractual relationship with a natural person or legal entity, respectively other organization that appears is in a national or international restrictions list or is prohibited as a contractual or customer relationship by any international convention, law, regulation, primary or secondary legislation of the institutions of the European Union and is, therefore, subject to sanctions.

Subject to the above provisions, the Service Provider is entitled to terminate contracts for services with immediate effect by unilateral written notice to the other party if the Service Provider becomes aware that the party contracting with it is included in any of the restrictions lists (including, in particular, those listed below) or that the legal relationship between the Service Provider and the party contracting with it is considered as a prohibited contractual or customer relationship by any international convention, laws, regulation or primary or secondary legislation of the institutions of the European Union, or if the party contracting with the Service Provider is subject to sanctions:

i. United Nations Security Council restrictive list
ii. European Union sanctions list
iii. The Sanction List maintained by the US Office of Foreign Assets Control (OFAC), which includes Specially Designated Nationals (SDNs) and Blocked Persons, as well.

The termination of the agreement may only be initiated in writing in all cases, which in the case of electronic form means authentication by electronic signature/seal of at least advanced.

The termination of the Agreement at the same time shall be also regarded as a request to withdraw the certificate issued in connection with the agreement.

If the service agreement is based on an individual business agreement, the terms of termination are defined by the provisions of the individual business agreement.

For the fee refund policy of the Service Provider see Section 9.1.5 of the Service Practice Statement.

The Service Provider is entitled to refuse, limit or terminate the performance of its obligations under the contract for the signature service or the requested certificate, time stamp services and the provision of the service to be provided by it and, in addition, at its option, to terminate the contract with immediate effect, by applying the legal consequences of breach by the Customer, if the Customer:

- impedes or compromises the security of the service to be provided by the Service Provider;
- uses the service to be provided by the Service Provider in violation of the provisions set forth in the contracts (including standard and custom service agreements), laws, standards, the present General Terms and Conditions, or the Service Provider's current Service Practice Statement, Service Policy or the NETLOCK SIGN Regulation for Availability;
- uses the service in such a way as to affect the service, its capacity or its quality in any way, including in the event that the Service Provider would not be able to fulfil its obligations towards other contractual partners as a consequence of the conduct set out in this Clause;
- operates other than as stipulated herein, modifies, transforms, adapts, uses or connects without authorisation any device to any device or software provided to him by the Service Provider, which is necessary for the use of the Service;
- uses the service in a way that significantly exceeds the calculated limits or in a suddenly increased manner that has not been approved in advance, which may cause an overload of the system.

4.4 Ceasing of the Service Agreement

Unless the Parties agree otherwise, the service agreement shall cease:

- upon the expiry of the definite period;
- by the ordinary or extraordinary notice of the Customer or the Service Provider (in accordance with the provisions hereof);
- upon the Customer's death or liquidation without legal successor, with immediate effect:
- upon the completion of the Service Provider's contractual service or the Service Provider liquidating (see Section 5.8 of the Service Practice Statement);
- subject to the Parties' mutual written agreement, in accordance with the conditions thereof.

4.5 Cases of material breach

It shall be considered as a material breach of the service agreement when either Party fails to fulfil its obligations set out in the service agreement, in the GTC or in the Service Practice Statement or fulfils them not in accordance with the agreement. Such breach includes, but is not limited to, when

- the data provided by the Customer are untrue;
- the Subscriber fails to discharge its fee payment obligation upon the Service Provider's written notice by the extended deadline specified therein;
- the Customer jeopardises the security or availability of the Services;
- either party breaches the secrecy obligation;
- liquidation or dissolution proceedings are launched against either Party by a non-appealable order, which jeopardises the fulfilment of its obligations;
- the Customer has engaged in prohibited use in accordance with Section 6;
- either Party fails to fulfil its obligation set out in these GTC, the Service Agreement in the Service Practice Statement or fulfils them incorrectly and fails to remedy the breach upon the other Party's written notice by the extended deadline specified therein.

The Service Provider is obliged to provide the contracting party with an extended deadline only in respect to breaches capable of remedy.

In the case of breaches that cannot be remedied or when the extended deadline set for breaches that can be remedied lapses with no result, the Service Provider may terminate the agreement by extraordinary notice as specified in Section 4.3 hereof.

4.6 Amendment of the service agreement

The Parties may amend the service agreement subject to mutual consent.

The Subscriber or its legal successor (when the original Subscriber changes) – with the exception of the certificate service – is entitled to initiate the registration of the transfer. The Service Provider may refuse to register the transfer, if the new subscriber does not the conditions set out in the service agreement, in the GTC or in the relevant Service Practice Statement.

4.7 Website authentication online SSL certificate

If the Customer wishes to request a website authentication online SSL certificate (Domain validated, automatic (DV) SSL-certificate), the ordering process consists of the application at the Service Provider and the provision of domain data, as well as the acceptance of the present GTC.

The Service Provider states that the contractual legal relationship for online SSL is established with the application of the Customer, furthermore the acceptance of the GTC.

The application for a new certificate and the management of existing, already issued certificates is possible as published on Service Provider's operative website.

5 Application and payment for Services

The Services of the Service Provider may be applied for on the Service Provider's website specified in Section 1.2 or through its Mobile Application or – in the case of services stipulated by the Service Provider – in person at the Service Provider's Outsourced Registration Unit. If the Customer has such special requirements that cannot be applied for according to the Service Provider's application interfaces, both the customer service and the commercial department of the Service Provider are ready to assess the needs and prepare the application in an ad hoc procedure, if possible.

For more information related to the application for the various Services see the Service Practice Statement and the Service Provider's customer notice.

For Certificate Services, the relevant procedures are set out in the Service Policies. The procedure for issuing Certificates varies depending on the service used, but in all cases the evidence elements must not be dated more than 30 days prior to the date of issuance and the start of the validity period of the Certificate.

Prior to using the service, the Customer must have and comply with the conditions necessary for the use of the Services, stipulated for the individual services in the Service Practice Statement.

5.1 Application for periodic services

The use of the certificate service, in all cases when applying for a new certificate (initial and re-key application, irrespective of the method thereof), may take place within the framework of a new Service Agreement, except when the Subscriber concluded an individual agreement for the issuance of several certificates, and the Parties waived concluding separate service agreements with the Subscriber for each certificate.

In the case of other periodic services, if there is a valid service agreement between the Parties for a definite or indefinite term for the respective service, within the framework of that the Customer has the option to submit a new application for a Fee packageincluded in the Service Provider's Price List or to initiate the conclusion of a new service agreement. In this case it is up to the Service Provider to decide whether it accepts the application within the framework of the existing or a new agreement.

Certain services may be also applied for together, only in these cases

- The application for signature services at the same time also represents an application for the certificate services, and it must be stated whether it also covers timestamp services.
- The application for service packages jointly applies to the certificate and timestamp services.

The Service Provider publishes the services that may be applied for jointly on its website specified in Section 1.2.

The Service Provider shall register the incoming applications, and within 15 days it may respond to them in the following way:

- by accepting the application within an existing service,
- accepting the application within a new service,

- requesting that the Customer supplement or clarify the application,
- rejecting the Application, if the Customer fails to comply with the request for supplementation or clarification within 15 days, or he has overdue fees payable to the Service Provider, or if the Customer is unable to comply with the provisions of the GTC or the Service Practice Statement.
- other, within the framework of a decision made by the Service Provider under its own authority, without obligation

No response from the Service Provider within 15 days to the Application received by it shall be deemed a rejection of the Application.

Service Provider excludes its responsibility for cost reimbursement regarding all arising damages (including direct, indirect or consequential damages, etc.) at the Customers or third parties, due to the rejection of the Application. Customer acknowledges that due to the rejection of the Application by the Service Provider, Customer is not entitled to claim compensation under any legal title from the Service Provider

In respect to the Customer's acceptance of the certificate service see Section 4.4.1 of the Service Practice Statement.

5.2 Application for optional and other services

The Parties shall not conclude a separate agreement for the use of an optional service, as these are included in the service agreement for periodic services and they also fall within the scope of these GTC.

An application for optional and other services may be submitted simultaneously with the application for certain periodic services or independently of that, depending on the nature of the service.

5.3 Fees

The Service Provider publishes the fees charged for the individual services in the Price List available on the website specified in Section 1.2. In agreement with the Customer, the Service Provider may also determine individual prices differing from those, and may also apply fees that are available only to certain Customers (e.g., based on a loyalty period or risk assessment).

The Service Provider is entitled to modify the Price List unilaterally at any time. The Service Provider shall notify Customers of the modification by publishing the modified Price List on the website. The modified Price List shall enter into force on the 30th day after its publication. The Customers impacted by the modification, but not accepting it are entitled to terminate the Service Agreement with immediate effect within 30 days from the publication, at the latest. The applications for services shall be governed by the Price List prevailing at the time when the application is received by the Service Provider.

The fees applied by the Service Provider may be:

- Maintenance fees: The fee charged from the date when the requested periodic service is made available for the entire term of the agreement for the carrying out of the service provider's duties irrespective of the actual use.
- Traffic fees: The fee charged based on the volume and quality (e.g., timestamp, storage space) of the actual consumption within a periodic service.
- Fee packages: The fee charged for making available the consumption of a periodic service in a given volume and quality for a given period, and – as the case may be – for the actual

use of it. In the case of service packages, it may apply to several different periodic services jointly.

- Ad hoc fees: The fee charged for an activity carried out on a single occasion based on the Customer's application (see optional services) or for devices provided to the Customer.

More information on Fee packages:

With the exception of the certificate service, periodic services may also be applied for in the form of various Fee packages or – in the case of service packages – the packages containing such Fee packages. After the expiry of the respective period, the services not used from the Fee package applied and paid for will no longer be available and they may not be carried forward to the period following the expiry of the validity of the Fee package.

During the validity period of a Fee package the Customer is entitled to switch to another Fee package, if the change of plan – in respect to the given Fee package – is available in the effective Price List. The change may be implemented by applying for the new Fee package and paying the applicable fee. The Customer shall not claim the refund of the already paid fee for the original Fee package.

If the Customer's Fee package has expired and / or he has not applied for a Fee package, the Service Provider will charge the fee for the services used at the traffic fee specified in the Price List.

For more information on the fees see Section 9.1 of the Service Practice Statement.

5.4 Payment and invoicing

Following the receipt of the application the Service Provider is entitled to issue a pro forma invoice or an invoice for the maintenance fee of the service, the fee of the selected Fee packages and the ad hoc fees, if any. The Service Provider is entitled to invoice the traffic fees at the end of the service period or when the amount of those exceeds HUF 1,000.

The Service Provider issues an electronic invoice, by default, to its Customers, which Customer shall expressly and irrevocably accept by applying for the service. At the Customer's request the Service Provider may also issue paper-based invoices.

The Service Provider shall send the pro forma invoice and the invoices for the service fees to the e-mail / postal address specified by the Applicant for this purpose. The Subscriber shall settle the pro forma invoice or invoice issued by the Service Provider within eight days from the receipt thereof either in person by cash deposit in any branch of the Service Provider's account-keeping banks in Hungary or by bank transfer to the bank account specified by the Service Provider. In the event of late payment, the Service Provider shall be entitled to apply the default interest and collection flat charge specified in the Civil Code.

If the service fee is not credited to the Service Provider's account by the payment deadline and the deadline specified in the Service Provider's reminder also lapses without success, the Service Provider is entitled to reject the application or suspend access to the commenced services with immediate effect. The Service Provider makes the activation of the services conditional upon fee payment.

In certain cases, the Applicant may also opt for online payment by bankcard during the application. If the fee is settled in this way, the Service Provider will issue an invoice subsequently, indicating on it that no financial settlement is required. In such cases late payment is not applicable.

The Service Provider may claim any uncharged fees or fees not collected by mistake within the general term of limitation.

If the Service Agreement is based on an individual business agreement, the terms of termination are defined by the provisions of the individual business agreement.

5.5 Complaints related to invoices

Cancellation of an issued invoice or amending the data of an issued invoice

The Customer shall check the data in the invoice in all cases and if he identifies any discrepancy, he shall report it immediately or not later than within 15 calendar days from the invoice date to igenylesek@netlock.hu or szamlazas@netlock.hu. After the expiry of the aforementioned deadline, the full cost of issuing the invoice with the new data (also including the total fee and cost of self-inspection) shall be borne by the party initiating the amendment of the invoice.

Information related to payment based on a pro forma invoice:

Prior to paying, the Customer shall verify the data in the pro forma invoice and if he finds any discrepancy, he shall report it immediately or within 15 days, at the latest, to igenylesek@netlock.hu or szamlazas@netlock.hu. If the pro forma invoice is duly paid, the Service Provider will issue the zero invoice (not requiring financial settlement) with the data included in the pro forma invoice. If the Customer reports that the data in the pro forma invoice (and on the zero invoice) are incorrect after having settled the pro forma invoice or by more than 15 days after the issuance of the pro forma invoice, the Service Provider shall not issue a new pro forma invoice and invoice.

6 Contracting parties' rights and obligations

6.1 Service Provider's obligations, liability and rights

The Service Provider shall be liable for the damages caused to any natural person or legal entity or other organization by breaching the contract in accordance with the provisions hereof.

In the case of non-qualified services, the wilfulness or negligence of the Service Provider shall be proved by the person claiming damages.

In the case of qualified services, the Service Provider's wilful/negligent conduct shall be presumed until such time as the Service Provider proves the contrary.

The Service Provider shall not be liable for damages exceeding the limitation of liability applicable to the use of services.

The Service Provider shall be liable for the services activity carried out within the scope of its practice statements, as well as for the operation of its Registration and Authentication Unit, even if certain functions are carried out by the Service Partners.

The Service Provider limits its financial liability as follows:

In respect to the individual services and certificate types it defines different liability amounts, which can be enforced by insurance claims (one or several claim events incurred due to the same reason, connected in time). When a given claim event impacts several Customers, or several different contracts and certificates, timestamps or files, the indemnification amounts related to the individual

Customers and contracts (certificates / timestamps / files) shall be determined in such a way that the total indemnification shall not exceed the highest liability amount and the liability amount belonging to the respective service or certificate types is also limited in each case.

The Service Provider provides information on the liability amounts on its website.

The Service Provider shall be liable to the Customer in accordance with Article 13 of eIDAS and – as an underlying rule – the liability for breach of contract as specified in the Civil Code and Section 5 of Decree 24/2016 of the Ministry of Interior.

The Service Provider shall be liable for damages caused by wilful or negligent conduct to third parties (Affected Party) not in a contractual relationship with it in accordance with Article 13 of eIDAS and – as an underlying rule – general liability rules of the Civil Code and Section 5 of Decree 24/2016 of the Ministry of Interior. (For the operation of the revocation registers see Section 4.10 of the Service Practice Statement.)

To cover its liability for damages the Service Provider holds a liability insurance policy.

The Service Provider excludes liability for lost profit, revenue shortfall, cost saving, delays arising in respect to third parties, pecuniary loss and non-pecuniary damages, or consequential damages, with the exception of liability for wilful breaches or breaches damaging life, corporal integrity or health.

The Service Provider is entitled to:

- process the Customer data in accordance with the Service Practice Statement (see Sections 9.3 and 9.4);
- refer to the Customer as a reference unless the Service Agreement or the Customer provides otherwise in writing;
- refuse or restrict the provision of Services upon severe breach by the Customer until the full remedy of the breach or the termination of the agreement.

For the sake of clarity, Service Provider states that it excludes its responsibility regarding all damages and costs incurred by the Customer or third parties as a result of them violating the service contract, Service Practice Statement, or GTC.

Other rights and obligations and liability shall be governed by the Service Practice Statement.

6.2 Customers' obligations, liability and rights

Customers are entitled to use the services specified in their service agreement in accordance with the GTC and the Service Practice Statement, if the related fees are paid by the deadline.

The Applicant shall be responsible for:

- providing and verifying the data necessary for the processing of the applications
- the authenticity, accuracy and validity of the data provided during the registration and application;
- cooperation in the verification of his identity and the data provided during the application, doing his best to ensure that the process is completed as soon as possible;
- the verification of the data in the certificate, once issued, and for notifying the Service Provider of the discrepancies, if any;

- reporting the changes in his data forthwith, applying for the suspension or revocation of the certificate, or terminating the use of the keys;
- reading and accepting, prior to using the service, the content of the service Policy and the Service Practice Statement, the GTC, the Service Application and the service agreement.

End User shall be responsible for:

- the proper use of his Customer device, key and certificate in accordance with the regulations (see Sections 4.5.1 of the Service Policy and the Service Practice Statement);
- secure management of his Customer device, key and activation data,
- forthwith notifying and fully informing the Service Provider of any dispute related to the certificate or the application thereof before taking the matter to court;
- using the service in accordance with the provisions of the law and of these GTC;
- using the certificate for the purposes and in accordance with the limitations specified in the certificate;
- using the private keys belonging to test certificates without any actual commitment and for testing purposes;
- should the private key, Customer device or activation data of the End User be obtained or suspected to have been obtained by unauthorised persons, the End User shall forthwith report this to the Service Provider and initiate the suspension or revocation of the certificate and stop using the certificate.

The Subscriber shall be responsible for:

- reading and accepting the Service Provider's regulations before using the service;
- the authenticity, accuracy and validity of the data provided during the application;
- cooperation in the verification of the data provided during the application, doing his best to ensure that the process is completed as soon as possible;
- initiating the modification of the certificate, the replacement or revocation of his key in accordance with Sections 9.6.3 and 4.9.1 of the Service Policy and Sections 4.7 and 4.8 hereof;
- complying with the fulfilment of the End User's obligation to the extent that he has influence over those
- forthwith notifying and fully informing the Service Provider of any dispute related to the certificate or the application thereof;
- ensuring that no authorised persons have access to the data and devices necessary for using the service;
- complying with the fulfilment of the End User's obligation to the extent that he has influence over those;
- fulfilling his fee payment obligation.

If the Customer caused damage by breaching the service agreement, omitting or failing to comply with his obligations outlined in the GTC or in the Service Practice Statement, he shall be liable in accordance with the liability rules of the Civil Code applicable to breach of contract.

For the obligations and liability of Customers see the Service Practice Statement, particularly Sections 9.6.3, 4.1.2.2 and 4.9.3.1.

7 “NETLOCK” cloud service

7.1 “NETLOCK” cloud service for private purposes

The Service Provider declares that ~~the free~~ use of the “NETLOCK” cloud service with a qualified personal signature certificate~~, as included in the public offers,~~ is provided exclusively for private purposes. Use of the service with a personal signature certificate for business purposes or on behalf of a legal or business organization is ~~subject to a fee~~considered business use. ~~The Customer acknowledges that in case of using the service with a personal signature certificate for business purposes, the Service Provider is entitled to terminate the Customer's free subscription after prior notice. At the same time the Customer is entitled to accept one of the business offers of the Service Provider. If the Customer does not wish to accept any of the Service Provider's business offers, but does not stop using the service for business purposes, the Service Provider is entitled to restrict the service after prior notice again. Furthermore, the Customer acknowledges that if he continues to use the service for business purposes following the repeated notice from the Service Provider, the Service Provider is entitled also to terminate the contract~~.

7.2 NETLOCK Mobile Application

When using the NETLOCK Mobile Application, the provisions of the GTC shall be applied taking into account the deviations specified in this (8) Section.

7.3 Concluding the licence agreement

The licence agreement related to the NETLOCK Mobile Application shall be created between the Parties by accepting these GTC.

7.4 Rules applicable to the use of the Mobile Application

The installation of the Mobile Application is free of charge.

The installation and use of the Application require internet access. The Customer acknowledges that if the download and installation of the Mobile Application is carried out using mobile internet rather than Wi-Fi, the downloading of the Mobile Application – depending on the subscription – may entail additional costs. The Service Provider shall not be liable for the potential faults of the internet connection.

The Service Provider shall not guarantee that the Mobile Application works on any of Customer’s mobiles or computer devices or that it is compatible with any other application installed on those.

7.5 Rights and obligations of the user of the Mobile Application

The user of the Mobile Application commits to and shall be solely liable for

a. providing accurate and true data when using the Mobile Application;
b. reading all documents related to the Mobile Application and complying with the provisions of those;
c. managing the user data and password necessary for logging into the Mobile Application confidentially;

d. using the latest version of the Mobile Application at all times;
e. when transferring his mobile device to a third party – not including the sale of the mobile device – logging out from the Mobile Application;
f. when his mobile device is obtained by a third party for good (e.g., sales), deleting the Mobile Application installed on his mobile device;
g. installing the Mobile Application only on devices that run the original operating system, defined by the manufacturer of the mobile device, free from any custom modification;
h. immediately logging out from the Mobile Application through the web interface should the mobile device be stolen or lost;
i. using the Mobile Application in accordance with the applicable laws and regulations.

The Service Provider shall take no responsibility for losses arising from non-compliance with the above.

By accepting this GTC, the user of the Mobile Application shall undertake to download the Mobile Application only from the official application store and comply with the requirements set forth by the application store. The Service Provider excludes all liability whatsoever for any damages that may arise from downloading the Mobile Application from an inappropriate place.

7.6 Service Provider's liability

The Service Provider excludes all liability for the content of web shops offering the Mobile Application.

The Service Provider excludes all liability for the unlawful use of the application.

By accepting these GTC, the user of the Mobile Application acknowledges that the Service Provider excludes its liability, up to the degree permitted by the law, for the quality of the Mobile Application, its compatibility with the device used by the user of the Mobile Application, any deficiency or inadequate functioning of the Mobile Application, its being free from harmful software, any loss of data, lost profit of revenue shortfall.

7.7 Copyrights

The Mobile Application is protected by Act LXXVI of 1999 on Copyright, and other laws related to intellectual property and international copyright treaties. The Service Provider declares that in respect to the Mobile Application it is entitled to provide the Customer with an open-ended – i.e., for the entire period of the software protection – software licence on its own organisational unit.

The Service Provider declares that no third party has any right in respect to the software product protected by copyright or other copyright works that limits or precludes the acquisition or exercise of the Mobile Application User's rights hereunder.

Based on these GTC the Mobile Application User acquires a non-exclusive and limited right and authorisation to use the Application, and such right shall also cover – if applicable – the new software versions of the mobile application. By accepting these GTC, the Mobile Application User declares that he is aware of the fact that his licence to use is a non-exclusive, limited licence, not transferable to anyone else or any third party and is not for sale. The licence to use is non-exclusive, as the service Provider and the Manufacturer have reserved the licence for the software for themselves as

well, and may also grant licences to third parties. Furthermore, the licence to use is limited in view of the fact that the licence to use provided to the Mobile Application User is required for the video identification necessary for the application for certificates. The Mobile Application User shall not transfer the Mobile Application, under any title, to the ownership, possession or use of others, and shall not use it for selling services to third parties.

The Mobile Application User shall not remove from the Mobile Application or modify the references to brands, copyright, confidentiality or other protection.

The Mobile Application User's right to use shall not provide the Mobile Application User with rights particularly to the following:

- he shall not disconnect the components of the Mobile Application and circumvent any of the technical protective measures integrated into or connected to the Mobile Application;
- he shall not disassemble, decompile, analyse, hack or exploit any of the Mobile Application's components, algorithms, software or aspects, nor retrieve or amend the source code of those;
- he shall not rewrite the Mobile Application to a programming language other than the original one;
- he shall not publish, disclose, copy (except for a backup copy), distribute, alter or revise the Mobile Application, unless the Service Provider expressly authorises it;
- in the absence of the Service Provider's express permission, he shall not rent, lease, sell or export the Mobile Application or transfer it to the possession or use of others under any title;
- he shall not use or utilise the Mobile Application independently in any manner not expressly specified in this agreement.

The technologies, procedures and methods underlying the Mobile Application and the related skills, know-how and software documentation constitute the Service Provider's business secret and are due to the Service Provider, while the Service Provider reserves all rights to those, including the copies or partial copies taken of those, whether legally or illegally.

The Service Provider is entitled to withdraw its licence to use the Mobile Application, if the User breaches its right to use the Mobile Application or uses it beyond the scope of the licence or transfers the use to a third person/party in a manner not permitted in this agreement or breaches the Service Provider's copyright in any other way. In this case the Service Provider will call upon the User in writing to comply with the licence to use the Mobile Application and cease the infringing conduct. On the 5th day from the receipt of the written notice the Service Provider is entitled to withdraw the licence to use the Mobile Application if the User fails to cease the infringing conduct.

In this case the Mobile Application User is obliged to destroy all copies and components of the Mobile Application in his possession.

8 Logfile retention

The IT systems of the Service Provider participating in the provision of its services carry out extensive logging activities in accordance with the requirements specified by law and certain standards and

regulations in order to preserve data related to the provision and use of services and the information used in them.

The log files will be kept for 10 (ten) years from the expiry of the validity of the certificates that can be linked to them, or until the final settlement of the legal dispute arising and reported in connection with them.

See Section 5.4 of the applicable Service Policy for more information on logging procedures.

9 Protection of personal data

In the course of rendering its services, the Service Provider processes the data in part or in full by automated means, in view of which the Service Provider data processing activity falls within the General Data Protection Regulation (GDPR). In the course of rendering its services, depending on the nature of the service, the Service Provider can act both as data controller and data processor. The Service Provider's action in its capacity as the processor shall be governed by the provisions of Chapter 5 of the Privacy Policy. Otherwise, the rules related to data processing by the Service Provider are included in the prevailing Privacy Policy published on the Service Provider's website and in Sections 9.3 and 9.4 of the relevant Service Practice Statement.

9.1 Provisions related to data processing

When using the Service Provider's NETLOCK SIGN and "NETLOCK" cloud service, the Customer becomes data controller, while the Service Provider becomes Customer's Data Processor.

Customer and Service Provider regard the provisions hereof as a legal act under Article 28 (3) of GDPR with the proviso that these GTC also serve as a Data Processing contract between the Customer and the Service Provider.

The scope of this section covers the electronic documents containing the personal data of natural persons, transferred to the Service Provider/uploaded to its system upon the Customer's use of the NETLOCK SIGN or "NETLOCK" cloud service.

9.1.1 Content of the data processing relationship

When using the services listed in Section 9.1, the Customer becomes the Data Controller in respect to the documents uploaded by him, while the Service Provider becomes the Data Processor. During these services, the Service Provider carries out no operation on the documents uploaded by the Customer and on the personal data in those, except for storing the documents.

Subject of data processing: storage of the documents uploaded by the Customer during the Service Provider's service specified in Section 9.1.

Duration of data processing: the Customer is entitled to delete the document uploaded by him at any time when using any of the services. The Service Provider declares that in the case of the "NETLOCK" cloud service, the documents in the storage will be deleted every 30 days.

Data subject's personal data: any personal data included in the uploaded document.

Categories of data subjects: Any natural person whose personal data are included in the document uploaded by the Customer.

Purpose of data processing: In the case of NETLOCK SIGN AND "NETLOCK" cloud services, the purpose of the data processing is to upload the documents to be signed by the Customer electronically for signing and to ensure that they can be downloaded for a specified period of time.

9.1.2 Data Controller's rights and obligations

1. In respect to the documents containing personal data, managed under this Agreement, the Customer has the exclusive right to instruct the Service Provider.
2. The Customer shall acknowledge that if the instruction given by him entails extra costs for the Service Provider, he is obliged to reimburse the Service Provider for such costs.
3. The Customer undertakes to ensure that the instructions given by him comply with the provisions of GDPR and other effective relevant legal provisions, and that the data processing in accordance with the Customer's instructions shall not result in the Data Processor's breach of any Regulation applicable to the respective Service or of the provisions of the data processing contract integrated in these GTC. The Customer shall acknowledge that the Service Provider is not obliged to comply with such instructions.
4. By accepting these GTC, the Customer declares that he uploads only such documents to the Service Provider's system that he possesses lawfully and the legal basis of its processing complies with GDPR. Should the Customer breach this obligation, the Service Provider shall be relieved of its liability and all liability arising from this shall be fully borne by the Customer. The Customer shall ensure that the provisions of this section are complied with throughout the period of data processing.
5. The Customer shall indicate the Service Provider, as the Processor, on all relevant documents, including particularly, but not limited to, the Customer's Privacy Policy. The Service Provider excludes all liability for damages caused by breaching the data subjects' rights resulting from the absence of notification.
6. By accepting these GTC, the Customer shall undertake that if it processes the documents uploaded by him as the data processor rather than as the controller, he shall obtain the authorisation specified in Article 28(2) of GDPR from the processor. Should the Customer breach this provision, the Service Provider shall be relieved of its liability and the Customer shall be liable for all damages resulting from this.

The Customer shall fully indemnify the Service Provider for any damages that the Service Provider may incur as a result of breaching the conditions above.

9.1.3 Data Processor's rights and obligations

1. The Service Provider shall carry out the activities specified in Section 9.1 in accordance with the relevant legislative provisions, the provisions hereof and the Customer's written instructions.
2. Should any of the Customer's instructions conflict with or breach the provisions hereof or the relevant data protection laws, the Service Provider shall immediately notify the Customer to this effect in writing. The Service Provider shall suspend the execution of the instruction until such time as the Customer confirms or modifies his instruction with the proviso that the Service Provider may refuse to execute the Customer's instruction.
3. The Service Provider shall not process the personal data processed within the

framework of the services specified in Section 9.1 for any other purpose, unless the data processing is prescribed by the laws of the EU or of the Member States applicable to the Service Provider. In this case, prior to commencing the data processing, the Service Provider shall inform the Customer of the respective legislative provision unless the law prohibits such information on important grounds of public interest.

4. The Service Provider shall ensure that the persons involved in the carrying out of data processing undertake a confidentiality obligation in a written declaration or they are subject to equivalent obligation.
5. The Service Provider shall ensure that unauthorised persons have no access to the personal data processed within the framework of the services specified in Section 9.1 and that the personal data are stored and positioned in such a way that those cannot be accessed, learnt, changed or destroyed by unauthorised persons.
6. The Service Provider shall provide the Customer with all the information necessary for the fulfilment of the Customer's obligations set forth in GDPR – particularly the carrying out of data protection impact assessments – and that facilitate and foster the audits, including onsite inspections, carried out by the Customer or another inspector commissioned by him.
7. The Service Provider shall – if applicable – ,when the objectives specified in the laws or by the Customer cease and/or after the completion of the activity stipulated in the contract between the Service Provider and Customer, return the personal data processed by it to the Customer or delete all personal data processed within the framework of the services specified by the Service Provider in Section 9.1 that are not necessary for the fulfilment of the Service Provider's other statutory obligations. The Service Provider shall confirm the deletion/destruction upon the Customer's request to this effect (e.g., handover of protocol).
8. The Service Provider shall provide the Customer with all the information necessary for confirming the fulfilment of the obligations set forth in Article 28 of GDPR, and facilitate and foster the audits, including onsite inspections, carried out by the Customer or another inspector commissioned by him.

9.1.4 Data security

Taking into account the state of the art, the costs of implementation and the nature, scope, context and purposes of processing as well as the risk of varying likelihood and severity for the rights and freedoms of natural persons, the Service Provider shall implement appropriate technical and organisational measures to guarantee the level of security appropriate to the risk during the fulfilment of the duties herein.

9.1.5 Use of additional data processor

1. By accepting these GTC, the Customer consents to the Service Provider's use of additional Data Processors.
2. The Service Provider shall conclude with the Data Processor used by it a written agreement that prescribes obligations as strict as those stipulated in these GTC and ensure the fulfilment of and compliance with the provisions of Article 28 of GDPR.
3. When rendering the services stipulated in Section 9.1 the Service Provider uses no additional data processors.
4. Should the Service Provider use additional data processors when rendering the services

stipulated in Section 9.1, it shall inform the Customer accordingly by modifying the Privacy Policy. The Customer may object to the planned modification in writing within 5 (five) working days from the receipt of the notification. The Customer shall state the grounds for his objection. If the Customer's objection is justified, the Service Provider shall make reasonable efforts not to employ the objected additional data processor in connection with the processing of the Customer's data. If the Service Provider is unable to replace the additional data processor it objects to or offer the Customer a different alternative, the Customer may terminate the Service Agreement within 30 days from the notification to this effect in accordance with the provisions of Section 4.3.

5. The Parties state that the Service Provider shall be liable for the activity carried out by the additional Data Processor used by it in the same way as if it had processed the data on its own.
6. The additional data processors used by the Service Provider are included in the Service Provider's Privacy Policy.

9.1.6 Exercising the data subject's rights

1. The Customer, in its capacity as the data controller, shall provide data subjects with the rights set forth in Chapter III of GDPR in respect to the personal data controlled by it.
2. The Customer acknowledges that due to the special nature of the services stipulated in Section 9.1, the Service Provider is unable to delete, block or rectify the data included in the documents.
3. The Service Provider and the Customer agree that the requests received in connection with the exercise of the data subject's rights may be responded to only by the Customer, unless the Customer provides otherwise.
4. The Service Provider undertakes that when the data subject's request is sent to the Service Provider instead of the Customer, it shall forthwith, within five working days at the latest, forward the request to the Customer without investigation on the merits thereof.
5. The Service Provider – if applicable to the services rendered by it – shall assist the Customer in ensuring the exercise of the data subjects' rights as follows:
   a. within 3 (three) working days from the receipt of the enquiry, the Service Provider shall examine whether the data subject's request forwarded by the Customer can be fulfilled in the legal relationship specified in Section 9.1.
   b. If the request sent by the Customer can be fulfilled by the Service Provider, said Service Provider shall fulfil the measures specified by the Customer within 8 (eight) working days from the investigation.
   c. The Customer undertakes not to request the fulfilment of measures that conflict with the GDPR or any other Hungarian data protection law.
   d. The Customer acknowledges that if it requests that the Service Provider carry out a measure that otherwise could be taken by the Customer as well, the Service Provider may refuse to carry out the measure.
6. The Customer shall send the request to dpo@netlock.hu.

9.1.7 Personal data breach

The Service Provider shall report to the Customer any personal data breach impacting the Parties' relationship – i.e., such prejudice to security that could result in the accidental or illegal destruction,

loss, change, unauthorised disclosure of or unauthorised access to personal data forwarded, stored or otherwise processed – without undue delay after obtaining knowledge of such incident.

9.1.8 Register of data processing activities

1. The Service Provider shall keep a register of the data processing activities carried out on behalf of the Customer with the content specified in Article 30(2) of GDPR.
2. Upon the Customer's request, the Service Provider shall provide the Customer with the register in electronic form. The Customer may send such request to the Service Provider to dpo@netlock.hu. The Service Provider shall send the register to the Customer within 15 (fifteen) working days.

9.1.9 Audits and inspections

1. The Parties state that the Customer or an auditor designated by him through a third party is entitled to conduct an inspection or audit, at its own cost, to verify whether the Service Provider, in its capacity as the data processor, is acting in accordance with the relevant data protection laws.
2. The Customer acknowledges that the audit may not entail access to the Service Provider's – in its capacity as qualified trust Service Provider – systems and premises, and significant volume of extra work for the Service Provider's employees.
3. Furthermore, the Customer acknowledges that the Service Provider shall provide no access to its qualified trust or security systems, or the information related to those.
4. The Parties agree that the Customer shall notify the Service Provider of the audit or inspection at least 30 working days in advance in writing, with the proviso that it must also specify its request for onsite inspection. The Parties state that the Service Provider shall permit onsite inspection during working hours, between 8 am and 4 pm, with the proviso that the Customer undertakes to carry out the onsite inspection without hindering the Service Provider's everyday activity.
5. The Customer acknowledges that it shall bear the costs of the data protection audit.

9.1.10 Technical and organisational measures

1. If the Data Processor implements such new data processing activity that also impacts the personal data processed on behalf of the Data Controller, said Data Processor shall notify the Controller of the forthcoming change at least 30 (thirty) days prior to commencing the new data processing activity. When in connection with the new data processing activity it is necessary to carry out a data protection impact assessment, and the Data Processor shall participate in the data protection impact assessment conducted by the Data Controller to the extent that can reasonably be expected of it and provide assistance to facilitate the successful conduct of such assessment.
2. The Data Processor shall implement and use appropriate technical and organisational data protection and security measures to ensure the security of personal data and the related accountability, including protection against unauthorised or illegal data processing (including but not limited to the unauthorised or illegal disclosure of, access to and/or amendment of personal data), and against the accidental loss, destruction of or damage to personal data.

10 Suggested verification procedure for Certificate status

The acceptance and use of the information contained in the Certificate requires due diligence on the Parties involved. It is highly recommended to:

- check the validity period of the end-user certificate;
- check the validity period of the certificate (service provider certificate) of the intermediate Publisher authenticating the end-user certificate;
- check the validity period of the issuer's certificate (service provider certificate) of the top-level root authenticating the intermediate Publisher's certificate;
- check the certificate status of end-user and service provider certificates by retrieving CRL or OCSP-based certificate status information referenced in the certificates.

A certificate is considered valid if the date of the verification time (e.g., the time of signing or stamping) falls within the validity period of the certificate, and the status of the certificate was valid at that time, and the same is true for all certificates in the validity chain.

To determine the past validity of expired certificates, an up-to-date revocation list or OCSP response (such as an embedded electronic signature or stamp at the time of authentication) is required.

The validity of website authentication certificates must be checked at the time the website is authenticated.

Affected parties can obtain information on the current status of each certificate by using revocation data. Only the currently valid certificates can be searched in the public certificate repositories on the Service Provider's website - if the Applicant of the requested certificate has consented to the disclosure of certain data of the certificate. Certificates that are suspended, revoked, or expired are not available in the public certificate store.

For more information on the recommended procedures for checking the certificate status, see section 4.9.6 of the relevant Service Policy, or at https://netlock.hu/info/#!/relyingparties.

11 Other conditions and important information

11.1 Communication and complaint management

For the purposes of communicating with the Customers, the Service Provider operates a customer service office and call centre, the contact details of which have been provided in Section 1.2.

In the course of the administration and procedure related to the use of services and to end user certificates, the Customer Service communicates with the Customer primarily through e-mails sent directly to the Customer. In addition, the Customer Service may also be contacted by phone, fax or in person.

By phone:

A customer service clerk can only be reached on the customer service phone number at the times specified on the website. Outside of those periods a message can be left.

In the Customer Service Office in person:

The Service Provider receives Customers in its customer service office during the customer service hours specified on its website.

Questions, objections or complaints related to the Service Provider's (including the service partners) activity are received by e-mail, by phone or in person in the Service Provider's customer service office.

When any dispute or complaint occurs, prior to taking the matter to court, the Customer shall be obliged, while the Data Subject or any third party are advised to notify the Service Provider immediately and provide it with comprehensive information on all aspects of the case. The Parties shall at all times attempt to settle their disputes amicably, through negotiations.

The Service Provider shall investigate the complaints within 30 calendar days from being notified, and inform the complainant of the result of the investigation by e-mail, unless agreed otherwise by the Parties. If due to the nature of the complaint the investigation is likely to take more than 30 calendar days, the Service Provider shall inform the complainant to this effect separately.

When the complaint is reported in person or by phone, the Service Provider shall record this in a protocol.

After the investigation of the complaint, the Service Provider shall – if applicable – correct the error within the technically justified period and inform the complainant accordingly in writing.

If the complainant Customer does not accept the response, he may initiate consultation with the Service Provider.

Should the consultation between the Customer and the Service Provider yield no result, prior to a potential court procedure, it is recommended that the Customer refer the matter to the Budapest Conciliation Board.

Contact details of the competent organisations on the effective date hereof:

Budapest Conciliation Board

Address: H-1016 Budapest, Krisztina krt. 99., 3rd floor 310

Postal address: 1253 Budapest, Pf.: 10.

e-mail: bekelteto.testulet@bkik.hu

Website: www.bekeltet.hu

Government Office of the Capital City Budapest Consumer Protection Department:

Address: H-1056 Budapest, Váci utca 62–64.

Telephone: +36 1 328 5862

Postal address: H-1364 Budapest, Pf.: 234.

E-mail: budapest@bfkh.gov.hu

11.2 Obligation of confidentiality

The Parties undertake that in the absence of any agreement or contractual provision to the contrary, during the term of the service agreement entered into by and between them:

- in respect to any communication, data, fact and other information provided in any form by the Data Subject or a third party and obtained by them
- and the content of the documents sent to or received by the other party

both Parties are bound by an obligation of secrecy, and they shall treat that as confidential information during and after the term of the Agreement, without any limitation in time, with the exceptions stipulated in the Service Practice Statement.

- The obligation of confidentiality shall not be applicable to the following information:
  a) information that is available to the public or disclosed in the future by no fault of the recipient party (except when it takes place by breaching an obligation resulting from the legal relationship between the Parties), or
  b) information obtained lawfully through a third party that also obtained such information lawfully;
  c) information that was provably known before the legal relationship that was created between the Parties, or
  d) the disclosure of which is prescribed by law, stock exchange requirement, governmental organisation or other authority, provided that the party disclosing the information does its best to ensure that the organisation receiving the information disclosed in this way treats the information confidentially and uses it only for the requested purpose.
  e) the person possessing the information obtained it independently of the other party;
  f) the disclosing party authorised or disclosed the publication in writing.

The Service Provider shall give access to the confidential data it has obtained only to its employees for the work of whom such information is essential (e.g., registration administrators).

The Service Provider may transfer the Customer data to the degree necessary and for the purpose of carrying out the respective tasks to its sub-contractors and agents in the following cases:

- cooperation in the provision of Services (e.g., production of the devices necessary for the use of the Services);
- invoicing;
- enforcement of claims against the Customer.

The Service Provider may disclose confidential data in the following cases:

- Mandatory data supply under Section 97(5)–(6) of Act CIII of 2023 on the Digital State and Certain Rules for the Provision of Digital Services (hereinafter Digital State and Services Act) to the trust service supervisory authority; the Service Provider shall also ensure the confidentiality, authenticity and completeness of the data during the data supply.
- For the purposes of investigating or preventing criminal offences, or for national security reasons – upon the fulfilment of the conditions stipulated in separate law – to the investigation authority and/or the national security services, as stipulated in Section 94(1)–(2) of Digital State and Services Act. The Service Provider shall record the fact of the data transfer; pursuant to the law, and the Service Provider shall not inform the Customer of the data transfer.
- Supply of information in civil or criminal proceedings, in accordance with Section 94 (3) of Digital State and Services Act.

- Upon the termination of the trust service, transfer of the data specified in the Act related to the service to be terminated, to the recipient Service Provider, as specified in Section 92 of Digital State and Services Act.

Apart from the foregoing neither of the contracting parties shall transfer any data, fact, information, plan or document obtained in the course of fulfilling the Agreement to any third party without the other party's prior written consent, except for the cases stipulated in the Service Practice Statement.

Parties shall be liable for the damages caused by breaching this section in accordance with the general rules of civil law.

11.3 Procedure to be applied in the event of disputes

If the dispute cannot be settled through negotiation stipulated in Section 11.1, the Parties may take the matter to court. In this case, the Parties mutually submit themselves to the sole jurisdiction of the Budapest District Court of Districts II and III.

11.4 Other conditions

The Applicant acknowledges that, as a result of the implemented updates, the certificate hierarchy validation for RSA 2048-based SSL/TLS website authentication certificates issued after November 15, 2028, will be guaranteed as trusted certificate only by Windows operating systems.

Applicant acknowledges that for SSL/TLS website authentication certificates, as set out in The Certification Authority Browser Forum's regulatory document *"Baseline Requirements for the Issuance and Management of Publicly-Trusted TLS Server Certificates*", with the exception of short-lived subscriber certificates, the shall revoke a certificate within 24 hours, [...], if the Service Provider is made aware that the certificate was not issued in accordance with the technical requirements of the Baseline Requirements or the Service Provider's policies or certification practice statement.

11.5 Security Requirements in Contracts with Third Parties

The Service Provider declares that the services defined in this General Terms and Conditions (GTC) and in the related contracts are provided exclusively in the manner and under the conditions set forth in the Contract.

The Partner is not entitled to involve any third party in the performance of the Contract without the prior written consent of the Service Provider.

All Partners are required to comply with the applicable laws and regulations, in particular the NIS2 Directive and the related implementing decrees. To this end, each Partner must ensure ISMS (Information Security Management System) compliance, with special attention to the protection, confidentiality, integrity, and availability of data and information.

Each Partner must protect all hardware and software assets used in or contributing to the fulfillment of the contract with the Service Provider against unauthorized access, damage, loss, or alteration. Accordingly, the Partner must apply relevant security procedures, regularly update software, and ensure the protection of assets against physical and digital threats.

Each Partner must ensure the security of data, particularly to prevent data loss or data alteration, in compliance with the GDPR and the Hungarian Information Act (Info tv.). For this purpose, appropriate control and backup procedures must be implemented and applied, and regular testing must be conducted to verify the integrity and recoverability of backups.

Each Partner must treat all confidential information received from the Service Provider strictly confidentially, regardless of whether it was provided in writing or verbally. The copying, disclosure, or publication of such data in any form beyond the scope permitted by the contract is strictly prohibited. This includes the protection of all contractual data, information, and technical documentation.

Each Partner must establish and maintain all operational procedures in compliance with ISMS requirements, with particular emphasis on the management of incidents and security events, compliance with data protection rules, and participation in security audits.