Terms and Conditions
of EuroCert Trust Services

Version 3

Approved by
CEO /-/
Łukasz Konikiewicz .....

Date of approval 04.12.2023
Date of effect 20.12.2023

EuroCert Sp. z o.o. „CENTRUM EUROCERT”
ul. Puławska 474
02-884 Warszawa
https://eurocert.pl

1 The scope of regulation

This document, hereinafter referred to as „Terms and Conditions" has been prepared to support the "Certificate Policy and Certification Practice Statement of EuroCert's Qualified Trust Services", hereinafter referred to as „Certificate Policy".

Within the Certificate Policy, EuroCert provides qualified trust services as defined by the eIDAS Regulation. The current list of Trust Services being the subject of the Terms and Conditions is published on the websites specified in clause 5 and the website of supervisory body (https://www.nccert.pl/) or European Commission's website (https://webgate.ec.europa.eu/tl-browser/#/).

The Trust Services are provided exclusively upon acceptance of these Terms and Conditions and Certificate Policy.

2 Addressee

The Terms and Conditions is for use by EuroCert as a supplemental and simplified document of disclosure and notice. It assists EuroCert to inform a Subscriber of the terms and conditions regarding the use of the Trust Services before entering into a contractual relationship with a Subscriber as well as to inform Relying Parties before they use a Certificate or Time Stamp issued by EuroCert.

The Terms and Conditions responds to these Subscribers and Relying Parties who find the Certificate Policy difficult to understand and assists them in making informed trust decisions.

Furthermore, the aim of the Terms and Conditions is to build consensus on those elements of the Certificate Policy that require emphasis and disclosure.

Consequently, the Terms and Conditions is not intended to replace the Certificate Policy.

A Subscriber is obliged to review and accept this document prior to filing a Certificate Request or receiving Time Stamp and the Relying Party is obliged to do so, before using a Certificate or Time Stamp issued by EuroCert.

The approval of the provisions set out in these Terms and Conditions entails that a Subscriber:

1) has read the Terms and Conditions and Certificate Policy available at https://eurocert.pl/repozytorium;
2) declares that information to be held in a Certificate that they have disclosed in the Certificate Request and during identity verification is true and was provided voluntarily;
3) agrees to the Subscriber's obligations set out in clause 10;
4) is aware that in case of ECSigner remote signature service, the environment in which cryptographic operations take place with the use of private key to create the electronic signature (seal) is managed by a qualified trust services provider, which is EuroCert;
5) agrees for processing by EuroCert their personal data provided in the Certificate Request and during identity verification solely for the purposes of issuing a Certificate (see clause 15) and they hereby acknowledge that: they are entitled to access their personal data and to amend it;
6) agrees to put data in the Certificate according to the Certificate Request and to use this data to verify their electronic signature (seal);
7) is aware that a Certificate and the Subscriber's data contained therein, are, in principle, available to the public;
8) consents to keeping a record by EuroCert of information used in registration and any subsequent revocation, the identity and any specific attributes placed in the Certificate (see clause 9);
9) consents to passing of their personal information above to another trust service provider in case EuroCert terminates its services;
10) has read the data protection statement called "Klauzula Informacyjna RODO" available at https://eurocert.pl/repozytorium/;
11) provides their binding consent to be recorded (audio and visual) when performing identity verification by videoconference, be photographed and have their identification document (both sides) photographed;
12) is aware that it is required to have Internet access and a web cam (video and audio) in order to provide by EuroCert the video verification service; a Subscriber is responsible for ensuring that their device meets required performance specifications in order to complete the identity verification process;
13) agrees to use a qualified electronic signature (seal) creation device;
14) consents to receive e-mails and SMSs about the upcoming expiry date of a Certificate and e-mails about updates of Certificate Policy and Terms and Conditions.

3 Regulations and related documents

3.1 External regulations

EuroCert provides Trust Services in compliance with the following provisions:

1) Regulation (EU) No 910/2014 of the European Parliament and of the Council of 23 July 2014 on electronic identification and trust services for electronic transactions in the internal market, hereinafter the "eIDAS Regulation";
2) The Act on Trust Services and Electronic Identification of 5 September 2016 (Journal of Laws of 2016, item 1579), hereinafter the "Trust Services Act";
3) Regulation (EU) No 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation), hereinafter the "GDPR";
4) The Personal Data Protection Act of 10 May 2018 (Journal of Laws item 1000), hereinafter the "Personal Data Protection Act".

3.2 Internal regulations

EuroCert provides Trust Services compliant with rules set out in "Certificate Policy and Certification Practice Statement of EuroCert's Qualified Trust Services" which is available at https://eurocert.pl/repozytorium.

Certificates issued in compliance with the above document are equivalent to qualified certificates as defined in eIDAS Regulation.

4 Glossary

1) EuroCert – qualified trust services provider EuroCert sp. z o.o., providing qualified trust services as defined by eIDAS Regulation.
2) Certification Authority (CA) – a technical certificate generation service of EuroCert concerned with Certificates issuance, is identified in the Certificate as the issuer and its private key is used to sign Certificates.
3) Registration Authority (RA) – an entity subject to EuroCert providing services on Subscribers registration and verification of their identity.
4) Certificate Policy – policy of trust services provided by EuroCert entitled "Certificate Policy and Certification Practice Statement of EuroCert's Qualified Trust Services", published at https://eurocert.pl/repozytorium, which at the same time constitutes the certification practice statement.
5) ECSigner Service – electronic signature (seal) service, in case of which, private key of Subscriber is stored by EuroCert.
6) Certificate – electronic attestation, by which data used to verify an electronic signature or seal is assigned to a subject creating an electronic signature or seal and which enables identification of a signatory; where in this document reference is made to a Certificate, this indicates a qualified certificate for: electronic signature, electronic seal and website authentication, as set out in the eIDAS Regulation.
7) Time Stamp – data in electronic form which binds other data in electronic form to a particular time establishing evidence that the latter data existed at that time. Where in this document reference is made to a Time Stamp, this indicates a qualified Time Stamp.
8) Certification Request – an electronic request to issue a Certificate in an appropriate format in an IT system responsible for generation of Certificates in EuroCert, addressed by Registration Authority on behalf of Subscriber.

9) TSL (Trust Service Status List) – lists issued by the European Commission and the EU member states, containing information about entities providing trust services, their status (whether "qualified") and data allowing for verifying tokens issued by trust services providers (verification of qualified certificates, time stamps etc.).
10) Subscriber – the subject for whom Certificate or Time Stamp was issued or is going to be issued.
11) Certificate Request – the information to be held in the Certificate.
12) Relying Party – any given subject that decides on approval of Certificate or Time Stamp issued by EuroCert.
13) Trust Services – qualified trust services as defined by the eIDAS Regulation provided by EuroCert within the Certificate Policy.
14) CRL – Certificate revocation list.
15) OCSP service – on-line verification service for Certificates' status (On-line Certificate Status Protocol).

5 Contact details

Mailing address	EuroCert Sp. z o.o. ul. Puławska 472 02-884 Warszawa https://eurocert.pl tel. +48 22 390 59 95 e-mail: biuro@eurocert.pl
Sales department	phone: +48 22 390 59 95 website: https://sklep.eurocert.pl RAs: http://eurocert.pl/PunktyPartnerskie
Revocation of Certificates	uniewaznienia@eurocert.pl +48 22 390 59 95 website: link
Technical support	wsparcie@eurocert.pl +48 22 390 59 95
Complaints	biuro@eurocert.pl +48 22 390 59 95
Data protection officer	iod@eurocert.pl

6 Conditions for concluding and terminating agreement

Contract for the provision of Trust Services is concluded after submission of Certificate Request, acceptance of the Terms and Conditions and the Certificate Policy by Subscriber and confirmation of their identity by EuroCert.

Resignation from Trust Services is possible only in case of revocation of a Certificate, according to terms specified in the Terms and Conditions (see clause 12) and Certificate Policy (see clauses 3.4 and 4.9).

7 Limitations on the usage of trust services

The private key associated with the Certificate for electronic signature or seal generated by the CA can be stored in:

1) cryptographic card – to which a Subscriber is the only user and only they know the PIN and PUK codes, enabling its use in order to create an electronic signature (seal),
2) ECSigner remote component of ECSigner Service – over which only a Subscriber has sole control by possessing an unique identification means, by which the Subscriber is identified and logged in the ECSigner Service, and the one time password which enable them to directly use the private key located in ECSigner component.

In the case of ECSigner Service EuroCert manages the private key on behalf of the Subscriber and ensures that the Subscriber has the sole control over their signing key (private key).

Certificate for electronic signature is used only to verify (validate) qualified electronic signature, which has a legal effect equivalent to the Subscriber's own handwritten signature and as such is recognized in all European Union Member States.

Certificates for electronic seal is used only to verify (validate) qualified electronic seals, which ensures origin authenticity and integrity of the data to which the qualified electronic seal is linked (e.g. to an electronic document).

Qualified electronic seal is not used to express the will of subjects who create the seal.

A Time Stamp is used to certify the date and time and the integrity of the data to which the date and time are bound. A Time Stamp, in terms of the Civil Code (art. 81§2 pkt.3), produces legal consequences of a certified date.

Private keys related to Certificates for electronic signature or seal are processed exclusively in qualified electronic signature (seal) creation devices.

Qualified Certificates for websites authentication are used to confirm reliability of servers and their authenticity. They allow setting up a TSL encrypted connection among servers with such Certificates, and also providing clients with safe logging in. Certificates of that type may be issued only for servers operating in public networks and that have a full, clear domain name defining location of a specific nod in DNS (FQDN - Fully Qualified Domain Name).

It is prohibited for unauthorised individuals to use a Certificate. Private keys related to Certificates shall remain at the sole disposal of a person or subject whose data have been placed in the Certificate. The use of the key is not allowed by any other person or subject.

Any person who creates a qualified electronic signature or advanced electronic signature using the data of another person is subject to a fine, restriction of liberty or imprisonment of up to three years. Anyone who creates a qualified electronic seal or advanced electronic seal without authorization is subject to the same penalty (art. 40 of the Trust Services Act).

8 Registration

Registration of a Subscriber that is verification and acceptance of a Certificate Request is carried out by EuroCert either directly or by relying on an authorized RA in accordance with an agreement with an RA.

EuroCert verifies the identity and if applicable, any specific attributes of the natural or legal person to whom the qualified Certificate is issued:

a) by the physical presence of the natural person or of an authorised representative of the legal person; or
b) remotely, by using a video verification system; or
c) by means of a Certificate of a qualified electronic signature or of a qualified electronic seal issued in compliance with point (a) above.

EuroCert can also verify the identity by a notary.

EuroCert informs the Subscribers about available methods of authentication.

The identity of a person is verified through an official identity document, either ID card or passport.

In the case of video verification system (point b above) a Subscriber applies for a Certificate only by an electronic form. Before initiation of the video session they must read and accept these Terms and Conditions.

The video verification, where the natural person has to be physically present in a video conference call, replaces the personal (physical) presence of the person to be identified. The video conference call is recorded to preserve evidence.

The video verification system for natural persons has been certified for conformity to the requirements of eIDAS Regulation by a conformity assessment body, confirming equivalent assurance in terms of reliability to physical presence, pursuant to Art. 24, par. 1 point d of the eIDAS Regulation.

An operator conducts a video verification on the basis of an identification document provided electronically.

An operator verifies that the Subscriber presents a valid and authentic ID document and that the personal data of the ID document match the data provided in the electronic Certificate Request.

In the second step an additional operator repeats the verification.

The verification is considered successful only if both operators approve the positive verification of the Subscriber.

Dual control ensures that Certificates can be requested by a RA only after the verification and registration of a Subscriber have been successfully completed.

Certification Requests are submitted to EuroCert electronically. Confidentiality of the transmission of Certification Requests is ensured by creating an encrypted channel in the TLS protocol.

EuroCert verifies that the Certification Request comes from a trusted RA.

EuroCert automatically accesses the data from verification process, which have been shared with EuroCert by RA.

Certification request is signed electronically by the Registration Officer who has approved of it.

CA generates the Subscriber's keys and a Certificate in ECSigner component.

After the identity verification has been successfully completed all data collected is submitted to EuroCert. RA transmits to EuroCert all screen shots and other data provided by a Subscriber, and recordings, created as part of the verification process, in 7 days.

All data exchanged electronically with the RAs is protected and is held confidential by encryption. The authenticity and integrity of transmitted data is ensured through an electronic signature.

9 Data retention period

EuroCert retains the following data and documents relating to the provision of Trust Services:

1) Subscriber's registration data, including the one from the ID document (type, numbers, expiry date, issuing authority) and all other documents or data confirming the subscriber's identity;
2) requests of issuance, renewal or re-key of a Certificate;
3) requests of a Certificate revocation, suspension, cancellation of suspension;
4) acceptance of the Terms and Conditions and Certificate Policy by Subscribers, including consent for personal data being processed;
5) written and electronic confirmations of identity of Subscribers from the RA and notary;
6) the audio and visual records of the videoconference, photos/screenshots of the identification document;
7) all issued Certificates;
8) CRL lists;
9) certificates for CAs;
10) Certificate policy;
11) Certification practice statement;
12) Terms and conditions for provision of trust services;
13) Internal regulations;
14) all security events, including changes relating to the security policy, system start-up and shutdown, system crashes and hardware failures, firewall and router activities and system access attempts;
15) all events relating to the life-cycle of CA keys;
16) all events relating to the life-cycle of Certificates;
17) all events relating to the life cycle of keys managed by the CA, including any subscriber keys generated by the CA;
18) other documents or data as long as Certificate Policy requires them to be created and stored,

- in a way that renders their reading and secure storing,
- for 20 years from the date of their creation as set out in the Trust Services Act (art. 17),
- in compliance with the Policy of backup copies and archiving, managing system logs and documentation of EuroCert trust services,
- in particular, for the purpose of providing evidence in legal proceedings and for the purpose of ensuring continuity of the service.

10 Subscriber liability

Subscriber is bound to:

1) review and approve of these Terms and Conditions prior to applying for a Certificate;
2) secure the private key and access codes to that key (e.g. PIN, PUK);
3) provide EuroCert with accurate and complete information;
4) provide documents confirming the authenticity of the information provided;
5) use a pair of keys only within their validity and in accordance with any limitations notified to the Subscriber indicated in clause 7 of the Terms and Conditions and clause 1.4 of the Certificate Policy as well as in a Certificate (keyUsage, extKeyUsage, certificatePolicies);
6) test the correctness of information included in the Certificate, immediately upon its receipt and no later than its first use; in the event of the occurrence of any irregularities, in particular irregular values of fields specifying the Subscriber's identity, the Subscriber is obliged to immediately notify EuroCert about this fact in order to revoke the Certificate and to generate a new Certificate with correct data;
7) not to pass a private key to unauthorized persons, not to disclose access codes to that key, maintain the private key under the Subscriber's sole control (or if the Subscriber is a legal person "control");
8) generate their keys using an algorithm and key length as specified in 6.1.5 of the Certificate Policy if the Subscriber's keys are generated under control of the Subscriber;
9) maintain their private key under their sole control (or if the Subscriber is a legal person "control") if the Subscriber's keys are generated under control of the Subscriber;
10) generate their keys within the qualified electronic signature (seal) creation device if the keys are generated under control of the Subscriber;
11) use the Subscriber's private key(s) for cryptographic functions only within the qualified electronic signature (seal) device;
12) notify EuroCert without any reasonable delay, if any of the following occur up to the end of the validity period indicated in the Certificate:
    a) the Subscriber's private key has been lost, stolen,
    b) the Subscriber's private key has been compromised,
    c) control over the Subscriber's private key has been lost due to compromise of activation data (e.g. PIN code) or other reasons,
    d) inaccuracy or changes to the Certificate content;
13) immediately and permanently discontinue the use of a private key, following compromise of the key;
14) immediately discontinue the use of a private key, when the subscriber's Certificate has been revoked, or the issuing CA has been compromised;
15) not to disclose any data they receive from EuroCert or RA and maintain such data under the Subscriber's sole control and secure such data against access by third parties;
16) verify a Time Stamp by electronic seal of the issuer (CA) of that stamp and verify the Certificate's validity of that issuer by the TSL list.

11 Relying parties' liability

Relying Parties are bound to:

1) review and approve of these Terms and Conditions prior to using a Certificate or Time Stamp issued by EuroCert,
2) verify the validity, suspension or revocation of the Certificate using current revocation status information by CRL or OCSP service, before its use to verify an electronic signature (seal) or website authentication,
3) take account of any limitations on the usage of the Certificate indicated to the Relying Party either in the Terms and Conditions (see point 7) and Certificate Policy (see point 1.4) or in the Certificate (keyUsage, extKeyUsage, certificate policies),
4) verify a Time Stamp by electronic seal of the issuer (CA) of that stamp and verify the certificate's validity of that issuer by the TSL list.

Information on the Certificate's status is available to the public. Verification of Certificates' status is performed based on published CRL lists and OCSP service. Addresses of the CRL and OCSP service are contained in a Certificate in these fields: crlDistributionPoints and authorityInformationAccess, respectively. CRLs and CAs certificates are available at the website https://eurocert.pl/index.php/en-us/documents/certificates-and-crls. To verify the Certificate's status the following steps shall be taken:

1) download an OCSP token for that particular Certificate and verify the Certificate's status saved in that token; and/or
2) download the CRL list issued after the date on which the validity of a Certificate is being verified and then check the status of the Certificate on the CRL list.

An electronic seal of the CRL and OCSP token shall be verified by the Certificate's validity of the CA which created the seal on the basis of the TSL list: https://webgate.ec.europa.eu/tl-browser/#/.

12 Certificate revocation

EuroCert revokes the Certificate based on:

1) revocation requests submitted by the Subscriber;
2) request of authorized entity whose data is contained in the Certificate;
3) information on the threat of the legal or actual interest of the Subscriber or third parties resulting from the use of the Certificate, about which Subscriber shall be immediately notified; Eurocert revokes in this case any non-expired Certificate when:
   a) Certificate is no longer compliant with the Certificate Policy under which it has been issued,
   b) EuroCert is aware of changes which impact the validity of the Certificate (inaccuracy or changes to the Certificate content),
   c) the used cryptography does no longer ensure the binding between the Subscriber and the public key,
   d) Certificate has been compromised or whose issuing CA has been compromised,
   e) cessation of the EuroCert's services and operations, including the handling of the revocation status for unexpired Certificates that have been issued,
   f) EuroCert or any of its designated RAs become aware that a Subscriber's private key has been communicated to an unauthorized person or an organization not affiliated with the Subscriber; in that case Eurocert revokes all Certificates that include the public key corresponding to the communicated private key.

The Subscriber or other authorised person can request the revocation or suspension of the Certificate by submitting a revocation or suspension request at the address specified in clause 5 or

via e-mail or phone call. The identity and authentication of the requesting person is checked against the identity data which has been collected during the identity proofing process.

Revocation requests must include the full name, a phone number, an email address, the revocation code provided during Certificate issuance, the reason for revocation, Subscriber information of the Certificate to be revoked. Only complete revocation requests can be processed.

Confirmation can be required from the Subscriber if a compromise is reported by a third party.

EuroCert revokes or suspends Certificate and publishes its status as "revoked" or „certificate hold" within a period of no longer than 24 hours from the effective receipt of revocation request, no later than 60 minutes after the revocation request has been authenticated.

If the revocation or suspension request cannot be confirmed within 24 hours then the status does not change.

Once a Certificate is definitively revoked (i.e. not suspended) it shall not be reinstated.

In the case of revocation, suspension or revocation of suspension of a Certificate, Subscriber or other authorized person receives a confirmation at their e-mail address.

13 Certificate suspension

A Certificate can be suspended in the event of justified suspicion that there are premises for revoking the Certificate indicated in clause 12 but the registration officer is unable to explain all doubts regarding the revoking of the Certificate within 24 hours from receiving a complete request.

A Certificate's suspension is temporary (usually until the moment of explaining all doubts causing the suspension). Certificate suspension can be cancelled no later than 7 days from the date of suspension (otherwise the Certificate is revoked).

EuroCert cancels the Certificate's suspension in the event of failing to confirm the premises justifying suspending a Certificate, in particular after Subscriber confirms this fact. Otherwise the Certificate is revoked.

Verification of requests for cancellation of suspension proceeds in accordance with clause 8.
Upon suspension cancellation of the Certificate, information about the Certificate is removed from the CRL.

If a Certificate is revoked after its prior suspending, the date of revoking the Certificate is the same as the date of suspending the Certificate. This means that the electronic signature created during the suspension does not have legal effect.

After cancelation of certificate suspension, the legal effect of the electronic signature verified with this Certificate, created during the suspension, takes place at the moment of cancelation of this suspension.

14 Limitation of liability of EuroCert

According to the Art. 21 of the Trust Services Act, EuroCert accepts no liability for damages caused by non-adherence to the rules set out in Certification Policy.

The financial liability of EuroCert is 250 000 EUR with regard to one event, but not exceeding 1 000 000 EUR with regard to all events (equivalent to PLN).

The user is obliged to provide written notice to EuroCert of any damages as contemplated by these Terms and Conditions on liability without delay so that damages may be mitigated as efficiently as possible.

15 Privacy policy

EuroCert collects, processes and uses personal data solely for purposes of providing Trust Services.

The information collected during the identity verification process include:

1) Full name, including surname and given names,
2) date and place of birth,
3) type, validity period, issuing authority and reference number of the nationally recognized identity document,
4) address,
5) nationality
6) phone number,
7) e-mail address,
8) audio and a visual records of the videoconference, photos/screenshots of a Subscriber,
9) photos/screenshots (opto-electronic copy) of the identification document used for identification.

The EuroCert's verification policy (see clause 8) only requires the capture of evidence of identity sufficient to satisfy the requirements of the intended use of the Certificate.

Please refer to the EuroCert data protection statement entitled “Klauzula informacyjna RODO” for details. This statement may be accessed at any time on the EuroCert website: https://eurocert.pl/repozytorium.

Names in the Certificates consist of the full name of the Certificate owner in line with the identity document provided and the following information:

1) reference number on the nationally recognized identity document,
2) citizenship.

EuroCert is the data controller of the Subscribers’ data, with the contact details set out in clause 5.

Subscribers’ data can be passed to a RA solely for the purposes of providing verification services and confirmation of Subscriber’s identity before issuing a Certificate.

16 Disputes settlement, complaints

Subject of dispute resolution, including complaints, may only be discrepancies or conflicts between parties regarding the issue and revocation of a Certificate based on the Terms and Conditions and Certificate Policy.

Disputes, complaints or grievances arising in relation to the use of Time Stamps, Certificates issued by EuroCert, will be settled on the basis of written information through mediation. Complaints should be submitted in writing to address given in clause 5.

Complaints are subjected to written examination within 21 working days of their delivery. If the dispute is not resolved within 45 working days of the conciliation proceedings, the parties have the right to take legal action. The General Court responsible for the defendant will be the competent local court to hear the case.

If other disputes arise as a consequence of the use of a Certificate or other qualified trust service, the Subscriber shall be obliged to inform EuroCert in writing about the case.

17 Audits

Qualified trust services provided by EuroCert are subject to a yearly assessment against the compliance with eIDAS Regulation.

The external body that performs the compliance is CAB TAYLLORCOX PCEB.

Internal audits are performed in line with the internal audit policy by EuroCert. The internal audit is conducted to verify compliance of EuroCert's performance with the procedures and processes set out in EuroCert's documentation.

The TSL list with the information about qualified trust services providers from Poland and information about trust services provided by them is available at: https://www.nccert.pl/.

18 Amendments

1. The Terms and Conditions is effective as of the date indicated on its title page until the effective date of the next version or until it is annulment.

2. EuroCert will have the right to amend the Terms and Conditions unilaterally. EuroCert will be obliged to disclose any such amendment on its website https://eurocert.pl/repository/Terms_Conditions/Qualified/Valid/ at least 14 days before entry into force.

3. Mentioned above changes to the Terms & Conditions will also be communicated to Subscribers via e-mail.

4. In case Subscribers do not accept an amendment, they will have the right to terminate the agreement with immediate effect within 30 days of disclosure or receiving notification thereof, except in the following cases:

    a) When introducing a new service, if it does not affect the conditions relating to already existing service, with regard to that new services can be provided for the Subscriber exclusively if they are ordered,

    b) In the case of expanding services, if it does not represent an extra burden on the Subscriber,

    c) In the case of a change in legislation, a decision made by the authority or a change in the economic and/or technical circumstances, as a result of which EuroCert can only provide the service for the Subscribers on different terms than before, if it does not represent an extra burden on the Subscriber,

    d) In the case that EuroCert's and/or the customer service office's address, telephone number and opening hours change; but EuroCetr is obliged to provide access to this information at its central customer service office, on its website and at its internet customer service address,

    e) In the case of corrections, amendments, deletions for the sake of clarity, which cannot be regarded as substantive modifications to content,

    f) In the case that the conditions of using the service change in a way, which is beneficial only to the Subscriber.

19 Document's specification

General information			
Signature			0-RG-028-03
Protection class			0 public
Status			Approved
Inventory number			
Confidentiality, Integrity, Availability, Archiving			
Confidentiality class			0 – Public
Integrity class			1 – Protected
Availability	Class of Access Rights		1 – Publicly Available, Administered
	Criticality Class of Access Time		2 – Substantial
Archiving requirement			B20 – 20-year archiving period
Amendments			
Date of approval	Valid from	Version	Amendments
08.11.2018	08.11.2018	1	Establishment of this document.
24.02.2021	24.02.2021	2	Change of the title of the document, extension of methods of identity verification by video verification, adding information on server signature.
04.12.2023	20.12.2023	3	Introduction of one helpline number everywhere in chapter 5, amendment of chapter 18.