



**TRUST SERVICE
'REMOTE SIGNING OF E-DOCUMENTS
WITH CLOUD-BASED QES'
OF BORICA AD**

**GENERAL TERMS AND CONDITIONS OF
USE OF THE SERVICE**

Version 1.0

20 April 2019

TRUST SERVICE 'REMOTE SIGNING OF E-DOCUMENTS WITH A CLOUD-BASED QES'

Timeline of document versions				
Version	Author(s)	Date	Status	Comment
1.0	Dimitar Nikolov	20.04.2019	Approved	First publication

TRUST SERVICE 'REMOTE SIGNING OF E-DOCUMENTS WITH A CLOUD-BASED QES'**TABLE OF CONTENTS**

TERMS AND ABBREVIATIONS	4
In Bulgarian:	4
In English:	4
1.1 Subject of the General Terms and Conditions	5
1.2 Information about BORICA AD as a QTSP	5
1.3 Applicability of the General Terms and Conditions	5
2 PARTIES PARTICIPATING IN THE SERVICE	5
3 APPLICATION SCOPE OF THE SERVICE	6
3.1 Legal validity of a Cloud QES	6
3.2 Permitted use	6
3.3 Limited use	6
3.4 Prohibited use	7
4 DESCRIPTION OF THE SERVICE	7
4.1 Cloud QES Platform – (Remote QSCD).....	7
4.2 Functionality	7
4.3 RELYING PARTY's access to the SERVICE	8
4.4 Terms and conditions of use of the SERVICE	8
4.5 SERVICE use termination	9
5 USE OF THE SERVICE (SIGNING)	9
5.1 Relying Party's Application System	9
5.2 Signatory's mobile application	9
5.3 B-Trust Platform for Cloud QES (RQSCD).....	10
5.4 Services for use of a Cloud QES.....	10
5.5 Signing electronic documents through the SERVICE	10
5.6 Receiving signed documents	10
5.7 Automated signing of electronic documents through the SERVICE	10
5.8 User authentication through the SERVICE	10
5.9 Receiving authentication results	11
6 SECURITY OF THE SERVICE	11
6.1 Security of the Cloud QES	11
6.2 Communication security	11
6.3 Security and protection at the RELYING PARTY	11
7 RESPONSIBILITIES OF THE PARTIES	12
7.1 Responsibilities of the Relying party	12
7.2 Responsibilities of BORICA AD	12
7.3 Responsibilities of Users - Signatories	12
8 ACCEPTANCE OF SIGNED E-DOCUMENTS	12
9 STORING OF E-SIGNATURES (SIGNED E-DOCUMENTS)	13
10 AMENDMENTS TO AND PUBLICATION OF THE GENERAL TERMS AND CONDITIONS.....	13
11 FINAL PROVISIONS.....	13

TRUST SERVICE 'REMOTE SIGNING OF E-DOCUMENTS WITH A CLOUD-BASED QES'

TERMS AND ABBREVIATIONS

Within the meaning of these General Terms and Conditions, the following terms and abbreviations are used:

In Bulgarian:

AD	Joint Stock Company
QTSP	Qualified Trust Service Provider
EDTSA	Electronic Document and Trust Services Act
CRC	Communications Regulation Commission
QES	Qualified Electronic Signature
QESeal	Qualified Electronic Seal
SERVICE	Remote signing of e-documents with a Cloud QES

In English:

B-Trust®	Trademark of the operation of BORICA AD as a QTSP
ETSI	European Telecommunications Standards Institute
eIDAS	Regulation (EU) 910/2014
HSM	Hardware Security Module – a Cryptographic module
QSCD	Qualified Signature Creation Device – a secure device for creation of qualified e-signatures
RQSCD	Remote Qualified Signature Creation Device – a secure device for creation of cloud-based QES
SSL/TLS	Secure Sockets Layer/Transport Layer Security – a cryptographic protocol for protected Internet communications

TRUST SERVICE 'REMOTE SIGNING OF E-DOCUMENTS WITH A CLOUD-BASED QES'

1. INTRODUCTION**1.1 Subject of the General Terms and Conditions**

These General Terms and Conditions regulate the general contractual relations between an INTERMEDIARY RELYING PARTY that operates an application system for remote signing of e-documents with a Cloud QES (APPLICATION SYSTEM) and BORICA AD as a Cloud QES Provider, that occur in the course of execution of transactions of remote signing with this e-signature.

By this SERVICE, the customers of the RELYING PARTY's APPLICATION SYSTEM, in their capacity as Cloud QES Signatories, and under their personal control sign remotely (via Internet) electronic documents of arbitrary format in accordance with the EDTSA legal and regulatory provisions in executing remote signing transactions. The document specifies the terms, conditions and manner of use of Cloud QES by an INTERMEDIARY RELYING PARTY compared to those described in the general purpose document of BORICA AD "B-Trust – TERMS, CONDITIONS AND MANNER OF USE OF QUALIFIED ELECTRONIC SIGNATURE AND QUALIFIED ELECTRONIC TIME STAMP".

These General Terms and Conditions shall be an integral part of the Framework Agreement for the performance of the SERVICE signed between the RELYING PARTY and BORICA AD.

1.2 Information about BORICA AD as a QTSP

BORICA AD is a legal person – a trader operating as a QTSP under EDTSA and the regulatory framework. The company develops, operates and manages a public key infrastructure (PKI) under the B-Trust® trademark, according to the legal framework of Regulation (EU) 910/2014 and EDTSA and in accordance with the international specifications and standards ETSI EN 319 411-1/5 and ETSI EN 319 412 with regard to the above Regulation.

As a QTSP registered with the CRC, BORICA AD provides qualified trust services in accordance with Regulation 910/2014, as follows:

- Qualified Electronic Signature (QES) of natural persons;
- Cloud Qualified Electronic Signature (Cloud QES) of natural persons;
- Qualified Electronic Seal (QESeal) of legal entities;
- Advanced Electronic Signature (AES) of natural persons;
- Advanced Electronic Seal (AESeal) of legal entities;
- Qualified Time Stamp;
- Qualified validation of QES/QESeal/AES/AESEal and Cloud QES;
- Qualified long-term storing (Archive) of qualified electronically signed/sealed documents.

1.3 Applicability of the General Terms and Conditions

These General Terms and Conditions shall apply to the contractual legal relations of BORICA AD with each of the RELYING PARTIES. These General Terms and Conditions shall also apply after the termination of the contractual legal relation with the RELYING PARTY until the final settlement of its obligations to BORICA AD.

2 PARTIES PARTICIPATING IN THE SERVICE

The parties involved in the process of operation with the SERVICE shall be:

- INTERMEDIARY RELYING PARTY – a person (natural or legal person), who

TRUST SERVICE 'REMOTE SIGNING OF E-DOCUMENTS WITH A CLOUD-BASED QES'

concludes a Framework Agreement for the SERVICE with BORICA AD and is registered as such. The person receives and validates the electronic documents (files) signed with a Cloud QES based on the terms and conditions of this document before accepting these electronically signed documents.

- SIGNATORY(IES) – a natural person, holder of a valid Cloud QES who acts on its own behalf or on behalf of another natural or legal person they represent, to sign electronic documents (files). The SIGNATORY person shall be registered with the RELYING PARTY for working with its application system, through which they execute transactions with remote signing with a Cloud QES;
- BORICA AD as a QTSP under EDTSA and Regulation EC/9102014 – builds, operates and develops the B-Trust infrastructure for qualified trust services, part of which is the platform for issuance, management and signing with a Cloud QES. The Cloud QES signatories shall be registered in this platform.

3 APPLICATION SCOPE OF THE SERVICE

3.1 Legal Validity of a Cloud QES

A Cloud QES is only a technological variation of the "classic" QES (on a smart card), which meets the strict technical requirements to the cryptographic characteristics, security level and QES functions. Regulation 910/2014 (eIDAS) provides the possibility for a SIGNATORY with an electronic signature to assign the servicing of the QES generation device to a QTSP, if there are appropriate mechanisms and procedures ensuring that the SIGNATORY shall retain sole control over the data related to the remote generation of QES (Cloud QES), and that the use of such a device meets the requirements applicable to the qualified electronic signature. In practice, SIGNATORIES have a "virtual smart card" in the QTSP's cryptographic hardware module (HSM), where the electronic signature keys are generated and stored with the Signatories' guaranteed strict personal control of their keys. Remote QES (Cloud QES) are created in this secure and reliable environment of the QTSP only under the SIGNATORY's control.

Cloud QES certificates, issued by BORICA AD as a QTSP, have the profile of qualified ones, same as for a "classic" QES.

In connection with the above, a Cloud QES issued to SIGNATORIES - natural persons has the same legal force and recognition as the "classic" QES (smart card).

3.2 Permitted Use

In accordance with these General Terms and Conditions, Cloud QES-generated electronic signatures in a RELYING PARTY's APPLICATION SYSTEM shall be used to remotely sign all electronic documents, in accordance with the use restrictions set by the applicable law and the restrictions arising from the published "Policy of Provision of Qualified Certificates of Qualified Electronic Signature, Cloud Qualified Electronic Signature and Qualified Electronic Seal".

3.3 Limited Use

The scope of application of these General Terms and Conditions is limited exclusively to electronic signatures that are generated remotely by the Signatories through the cryptographic

TRUST SERVICE 'REMOTE SIGNING OF E-DOCUMENTS WITH A CLOUD-BASED QES'

hardware module (HSM) on the Cloud QES Platform of the B-Trust infrastructure of BORICA AD.

3.4 Prohibited Use

It is prohibited to generate electronic signatures with Cloud QES, which are accordance with these General Terms and Conditions, for conducting tests with no legal value.

4 DESCRIPTION OF THE SERVICE

4.1 Cloud QES Platform – (Remote QSCD)

The Cloud QES platform is integrated in the B-Trust infrastructure for qualified trust services of BORICA AD as a QTSP, and provides: (1) centralized storage and management of SIGNATORIES' private keys and (2) remote generation of QES in an environment of high security level, strict administrative and operational procedures with physical and logical protection. The SIGNATORY shall keep full and personal control over their private key by a secure (2-factor authentication) mechanism of strong online authentication, which is supported by a cloud QES mobile application. On this basis, by their smart device the Signatories gain 'mobility' for their QES. Signatories are 'free' from the specific technical requirements to signing with a QES – to have a smartcard and a reader, and to install the respective drives required for them, while via the Cloud QES Platform they generate a legally valid Qualified Electronic Signature.

In order to sign with a Cloud QES, a SIGNATORY must have the following:

- a PC with Internet connectivity and a browser;
- a smart device with the *B-Trust Mobile* mobile application, registered on the Cloud QES Platform of BORICA AD as a QTSP;
- a valid Cloud QES qualified certificate.

4.2 Functionality

The SERVICE signs electronic documents (files) of arbitrary format. Pursuant to Commission Implementing Decision (EU) 2015/1506 and depending on the format of the document signed (arbitrary, xml, pdf), the SERVICE supports the following formats and QES levels:

Format/ Levels	BASELINE_B	BASELINE_T	BASELINE_LT	BASELINE_LTA
CAdES	Arbitrary file/document	Arbitrary file/document	Arbitrary file/document	Arbitrary file/document
XAdES	Xml file/document	Xml file/document	Xml file/document	Xml file/document
PAdES	Pdf file/document	Pdf file/document	Pdf file/document	Pdf file/document

For the above formats and levels, the SERVICE shall support the following types of electronic signatures, depending on their availability regarding the files/data signed:

TRUST SERVICE 'REMOTE SIGNING OF E-DOCUMENTS WITH A CLOUD-BASED QES'

Format/Type	CAdES	XAdES	PAdES
Enveloped signature	NA(*)	.xml format	.pdf format
Enveloping signature	.p7m format	.xml format	NA(*)
Detached signature	.p7s format	.xml format	NA(*)

(*) NA – Not applicable (this type is not applicable for the respective signature format)

The signed e-documents/files have the following extensions:

- CAdES-signed files are with extension ".p7m" for "ENVELOPING" type of signature, and extension ".p7s" for a "DETACHED" type of signature;
- XAdES-signed files are with extension "xml" for the three types of signature "ENVELOPING", "ENVELOPED" and "DETACHED";
- PAdES-signed files are with extension „pdf“;

4.3 RELYING PARTY's Access to the SERVICE

Electronic documents signed with a Cloud QES should be delivered (or located) in the INTERMEDIARY RELYING PARTY's domain. Through the APPLICATION SYSTEM, operating with electronic documents signed with a Cloud QES, the RELYING PARTY gains access to the SERVICE.

BORICA AD, as QTSP, provides a program interface (web-services) to each RELYING PARTY, with whom it has a signed Framework Agreement for the use of the SERVICE.

Each RELYING PARTY having a signed Agreement may download the code and documentation for operation with this interface on address: <https://cques-rp.b-trust.bg/signing-api/swagger-ui.html>.

The scope of application of these General Terms and Conditions shall be valid for both approaches for access to the SERVICE:

- The application system delivers to the SERVICE the hash-code of the document(s) for signing and instructions regarding the format/level and the type of execution of a Cloud QES, respectively receives the signed hash produced;
- The application system delivers to the SERVICE an original document(s) for signing and instructions regarding the format/level and the type of execution of a Cloud QES, respectively receives the signed document produced.

4.4 Terms and Condition for Use of the SERVICE

The RELYING PARTY shall use the SERVICE provided it meets the following conditions:

- It shall conclude a Framework Agreement with BORICA AD; these General Terms and Conditions shall be an integral part of the agreement signed between the two parties;
- It shall register itself in the Cloud QES Platform; a valid website authentication qualified certificate (SSL certificate) shall be required for the registration of the application web-system;
- It shall integrate an executable code of the program interface (web services) in the application system;
- It shall execute successfully signing of test electronic documents with a Cloud QES via the test signing platform at address <https://cques-rptest.b-trust.bg/signing-api/swagger-ui.html> ;
- A bilaterally signed Certificate of Successful Testing.

TRUST SERVICE 'REMOTE SIGNING OF E-DOCUMENTS WITH A CLOUD-BASED QES'

4.5 SERVICE Use Termination

The use of the SERVICE may be terminated by termination of the contractual relations unilaterally by the RELYING PARTY with one month's notice in writing, and by BORICA AD with two months' notice.

The termination of the contractual relations shall not release the parties from the performance of their obligations arising before the termination.

The use of the SERVICE may be terminated unilaterally by BORICA AD without notice in the following cases:

- In case of non-fulfillment of any of the obligations under these General Terms and Conditions by the RELYING PARTY;
- In case of non-use of the SERVICE by the RELYING PARTY for a period of more than 1 year;
- Upon initiation of insolvency, liquidation, transformation or winding-up of the legal person - RELYING PARTY of the SERVICE.

5 USE OF THE SERVICE (SIGNING)

Use of the SERVICE by Cloud QES Signatories, who are Customers of the RELYING PARTY' application system, shall occur after successfully meeting the conditions under 4.4 of these General Terms and Conditions. The RELYING PARTY shall notify its Customers, who will sign electronic documents with Cloud QES to fulfill these conditions.

5.1 Relying Party's Application System

The RELYING PARTY's APPLICATION SYSTEM is a server system with registered Customers, who sign electronic documents remotely (from a distance) as Cloud QES Signatories.

The registration of Customers and the authorized access to their documents is outside the scope of these General Terms and Conditions and is regulated by the RELYING PARTY, which has concluded a Framework Agreement for use of the SERVICE.

5.2 SIGNATORY's Mobile Application

The Cloud QES SIGNATORY shall use the mobile application B-Trust Mobile of the QTSP BORICA AD for initiation of remote signing of electronic documents.

RELYING PARTY's Customers, who will use the SERVICE, should download the B-Trust Mobile in a smart device and initialize the mobile application on the Cloud QES Platform of BORICA AD, as the QTSP, which operates as a remote device for qualified QES (Remote QSCD/RQSCD). After successful registration, the QTSP issues a qualified personal Cloud QES certificate and the Signatory Customer may sign remotely.

Information on working with the Cloud QES mobile application is contained in the document "Manual for Installation of the *B-Trust Mobile* Mobile Application and Process of Issuance of Cloud Electronic Signature (OQES)" of BORICA AD.

It is available for both Android and iOS operating systems and can be downloaded from the Google Play Store, iPhone App Store. B-Trust Mobile can also be installed by scanning a QR code on the B-Trust website B-Trust <https://www.b-trust.bg> or in the BORICA e-shop <https://store.borica.bg>.

TRUST SERVICE 'REMOTE SIGNING OF E-DOCUMENTS WITH A CLOUD-BASED QES'

5.3 B-Trust Platform for Cloud QES (RQSCD)

The Cloud QES Platform is an integral part of the common B-Trust infrastructure for qualified trust services of BORICA AD.

This platform, in the role of a remote secure QES device (Remote QSCD / RQSCD), practically performs all cryptographic and management functions, as does the smart card for the "classic" QES, for the Signatory (key pair generation, two-factor authentication, e –signature generation, management).

5.4 Services for Use of a Cloud QES

The RELYING PARTY's application web system uses a software interface (web-services) for accessing and working with the Cloud QES Platform (as an RQSCD) when signing electronic documents. Each RELYING PARTY that signs a SERVICE Agreement shall have access and the right to use this interface in its application system.

5.5 Signing Electronic Documents through the SERVICE

Through the user interface of the RELYING PARTY's application system, the Customer selects one or more electronic documents to sign with a Cloud QES. Irrespective of the mode of operation (according to item 4.3) when signing a single document or multiple electronic document(s) through the program interface (item 5.4), the application system delivers the prepared document(s) for signing with indication of the format, level and type of electronic signature in the Cloud QES Platform.

The Customer receives a notification of the mobile application for the received request and accordingly confirms the signing by entering the PIN code of the certificate.

The user interface of the RELYING PARTY's application system is outside the scope of these General Terms and Conditions.

5.6 Receiving Signed Documents

Within the SERVICE, the e-documents (files) signed with a Cloud QES are delivered back through the program interface in the RELYING PARTY's APPLICATION SYSTEM and are under the control of the Signatory Customer.

5.7 Automated Signing of Electronic Documents through the SERVICE

The RELYING PARTY's Application System can possibly use the SERVICE through an automated mechanism for signing documents without the need of their confirmation by a PIN code by the customer. For this purpose, the RELYING PARTY sends a request for consent to the certificate holder. The Customer confirms and signs the request electronically by entry of the PIN code of the certificate. Based on the consent request signed by the certificate holder, the RELYING PARTY sends documents for automated signing with no need for them to be confirmed individually by the customer via the mobile application.

5.8 User Authentication through the SERVICE

The RELYING PARTY's application system is able to use the SERVICE for authentication of its users by means of a Cloud Qualified Electronic Signature.

TRUST SERVICE 'REMOTE SIGNING OF E-DOCUMENTS WITH A CLOUD-BASED QES'

For this purpose, the RELYING PARTY's application system send to the SERVICE a pre-agreed identifier (the user has to have been registered with this identifier in the SERVICE) and a request at login to the system. The customer receives a notification on the mobile application of the request for login to the relevant RELYING PARTY's application system and confirms the request by signing by means of entering the PIN code of the respective QES certificate.

The user interface of the RELYING PARTY's application system is outside the application scope of these General Terms and Conditions.

5.9 Receiving an Authentication Result

Within the SERVICE, based on the signed login request, data from the Qualified Electronic Signature on the submitted request (identifier and Signatory's full name in Latin letters) are delivered back to the RELYING PARTY's application system via the program interface. In addition to the SERVICE, it can provide additional attributes such as a verified phone number, e-mail address, the Signatory's full name in Cyrillic letters, and other data known to the SERVICE.

6 SECURITY OF THE SERVICE

The security of the SERVICE is conditioned by the two determining factors - Cloud QES security and communication security.

6.1 Security of the Cloud QES

A Cloud QES is a technological variation of the "classic" QES and meets the requirements to a Qualified Electronic Signature under EDTSA and Regulation 910/2014 (Annex I and Annex II), and of the relevant technical specifications under these regulatory documents.

The Cloud QES Platform is an integral part of the common B-Trust infrastructure for qualified trust services, operated by BORICA AD as a QTSP, with registration with the CRC (the Communications Regulation Commission) as the national Regulatory Authority.

Detailed information regarding the overall security of qualified trust services, and the security of QES, Cloud QES, respectively, is provided in the public document "PRACTICE IN PROVIDING QUALIFIED CERTIFICATES AND TRUST SERVICES FOR THEM BY BORICA AD".

6.2 Communication Security

The communication security and protection of the Internet connectivity between the RELYING PARTY's Web-based application system and the Cloud QES Platform (RQSCD) of BORICA AD uses a two-way SSL/TLS protocol for authentication and data exchange protection.

6.3 Security and Protection at the RELYING PARTY

The security and protection of original and signed electronic documents, as well as the authentication/authorization of Customers in the RELYING PARTY's domain, and in the application system in particular, are outside the scope of these General Terms and Conditions.

The RELYING PARTY undertakes to check programmatically the validity of the electronically signed document and, if it is not valid, to carry out the necessary analysis of the problem.

TRUST SERVICE 'REMOTE SIGNING OF E-DOCUMENTS WITH A CLOUD-BASED QES'

7 RESPONSIBILITIES OF THE PARTIES

7.1 Responsibilities of the Relying Party

Pursuant to clause 10.6.4 of the public document "PRACTICE IN PROVIDING QUALIFIED CERTIFICATES AND TRUST SERVICES FOR THEM BY BORICA AD"

Pursuant to clause 2 of the public document "TERMS, CONDITIONS AND MANNER OF USE OF QUALIFIED ELECTRONIC SIGNATURE AND QUALIFIED ELECTRONIC TIME STAMP".

Each RELYING PARTY shall be responsible for the operation, general functionality, and security of the Web-based application system, including the implementation of the application interface(s) for running the SERVICE.

The RELYING PARTY shall be responsible for the inviolability and integrity of the contents of the original electronic documents that are signed through the SERVICE, as well as for the preservation of those signed with a Cloud QES. An exception shall be made when the RELYING PARTY uses the qualified service to store electronically signed/sealed documents of BORICA AD.

The RELYING PARTY shall prepare and publish a separate document "General Terms and Conditions" (Policy) on the operation of the application system.

7.2 Responsibilities of BORICA AD

Pursuant to clause 6 of the public document "B-TRUST® PUBLIC DISCLOSURE STATEMENT OF THE QUALIFIED TRUST SERVICE PROVIDER BORICA AD".

Pursuant to clause 10.6.1 of the public document "PRACTICE IN PROVIDING QUALIFIED CERTIFICATES AND TRUST SERVICES FOR THEM BY BORICA AD"

7.3 Responsibilities of Users - Signatories

Pursuant to clause 4 of the public document "B-TRUST® PUBLIC DISCLOSURE STATEMENT OF THE QUALIFIED TRUST SERVICE PROVIDER BORICA AD".

Pursuant to clause 10.6.3 of the public document "PRACTICE IN PROVIDING QUALIFIED CERTIFICATES AND TRUST SERVICES FOR THEM BY BORICA AD"

8 ACCEPTANCE OF SIGNED E-DOCUMENTS

The RELYING PARTY, addressee of the electronic document(s) signed through the SERVICE, should accept and trust that the signature has the legal value of a handwritten signature with regard to it and is binding for the Signatory, i.e. that it is qualified. The Cloud QES certificate, issued by BORICA AD as a QTSP, is qualified with a profile identical to the profile of the "classical" QES certificate.

In accordance with EDTSA and Regulation 910/2014, as a QTSP BORICA AD operates and provides to Relying parties a trust service of qualified validation of QES, respectively Cloud QES, pursuant to public document "POLICY AND PRACTICE OF THE SERVICE OF QUALIFIED VALIDATION OF QUALIFIED ELECTRONIC SIGNATURES AND SEALS PROVIDED BY BORICA AD".

The use of the trust service of qualified validation of Cloud QES, by which the SERVICE

TRUST SERVICE 'REMOTE SIGNING OF E-DOCUMENTS WITH A CLOUD-BASED QES'

signs electronic documents, is an option of the application scope of these General Terms and Conditions.

9 STORING OF E-SIGNATURES (SIGNED E-DOCUMENTS)

The strength and suitability of the cryptographic mechanisms underlying a Cloud QES are a function of time and give rise to the need to implement appropriate storage mechanisms that maintain the validity of the signed object over long periods of time. In accordance with EDTSA and Regulation 910/2014, as a QTSP BORICA AD operates and provides to the relying parties a trust service of long-term qualified storage of e-signatures and e-seals, pursuant to public document "POLICY AND PRACTICE OF THE SERVICE OF QUALIFIED VALIDATION OF QUALIFIED ELECTRONIC SIGNATURES AND SEALS PROVIDED BY BORICA AD".

Using the trust service of long-term qualified storage of electronic signatures made by a Cloud QES, with which the SERVICE signs electronic documents, is an option of the application scope of these General Terms and Conditions.

10 AMENDMENTS TO AND PUBLICATION OF THESE GENERAL TERMS AND CONDITIONS

Any amendments to these General Terms and Conditions and the Framework Agreement for the provision of the SERVICE shall be provided to the RELYING PARTY by publishing a new version 1 month before their entering into effect.

The RELYING PARTY shall deem itself bound by any amendments, unless it has explicitly notified BORICA AD that it does not accept these amendments by the date of their effectiveness.

In the event the RELYING PARTY does not accept the proposed amendments, it has the right and should immediately, by an explicit written notice to BORICA AD, terminate the Agreement, by the time of effectiveness of the amendments, without being held liable for any costs and indemnities.

In the event the text of these General Terms and Conditions is or becomes illegal, invalid or unenforceable, this will not affect the rest of the General Terms and Conditions.

11 FINAL PROVISION

These General Terms and Conditions shall be an integral part of each application for initial registration for use and the SERVICE Agreement, and shall be considered in their entirety as a single document.