GENERAL TERMS AND CONDITIONS ON TRUST, INFORMATION, CRYPTOGRAPHIC AND OTHER SERVICES

the provision and use of trusted service of issuing and verifying certificates brainit.sk, s.r.o.
effective from 20.07.2023

Table of Contents

Definitions and abbreviations

Unless otherwise stated in the General Terms and Conditions, the above definitions shall have the following meanings:

Certificate:

- a certificate or a qualified certificate for electronic signature within the meaning of the eIDAS Regulation;
- a certificate or a qualified certificate for electronic signature within the meaning of the eIDAS Regulation;
- certificate for authentication of the website in accordance with the eIDAS Regulation;
- any other certificate used for encryption, authentication or other purposes as defined in the Provider's Policy, which has been or is to be issued by the Provider to the Customer.

CRL – Certificate Revocation List - a list of Certificates cancelled before their expiry date.

Trust Services - qualified trust services for the issuance and verification of Certificates provided by the Provider in accordance with the eIDAS Regulation, the Act and the Provider's Policies. Trust Services may also be composed of other associated services in connection with Certificates.

These are mainly:

- Certificate Verification - providing information on the validity or revocation of Certificates - CRL, OCSP response,
- generation of key pairs,
- and more...

Certificate Holder - the person named in the Certificate who is the holder of the private key associated with the public key to which the Certificate is issued.

Regulation eIDAS - Regulation 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 and repealing Directive 1999/93/EC.

OCSP Response - a response to an OCSP request that gives an indication of the validity of the Certificate at the specified time.

Provider Policy / Provider Policies

- the policy of the trust service provider for issuing and verifying qualified certificates, which applies to qualified certificates issued by the Provider under the eIDAS Regulation;
- policy for the provision of trusted service for the issuance and verification of qualified certificates, covering other Certificates not listed in the above clause.

The Provider's policies include all regulations and updates issued by the Provider and are published on the Provider's website.

Provider - the company brainit.sk, s. r. o. with the registered office at Veľký diel 3323, Žilina 010 08, ID No.: 52577465, registered in the Commercial Register of the District Court of Žilina, Section Sro, Insert No. 72902/L.

Acknowledgement - an acknowledgement of receipt of the Certificate by which the Certificate Holder acknowledges, among other things, receipt of the Certificates.

Workplace - the place where Certificates are issued. It is a place operated by the Provider - its registered office.

Relying Party - a natural or legal person who relies on the Provider's Trusted Services to act.

General Terms and Conditions or abbreviated as GTC - this document General Terms and Conditions for the provision and use of the trusted service for the issuance and verification of certificates, always in their effective version.

Qualified device - a device for making an electronic signature/seal that meets the requirements set out in Annex II of the eIDAS Regulation.

Contract - Contract for the provision of trusted service of issuing certificates concluded between the Provider and the Customer, or any other contract between the Provider and the Customer, the subject of which is the provision of Trust Services.

Contract with CA - a contract concluded between the Provider and the Certificate Holder, regulating the rights and obligations of the parties to the use of the Certificate.

Customer means a natural person or legal entity to whom the Provider provides Trust Services on the basis of the agreed Contract and also the person who pays for these services.

Act - Act No. 272/2016 Coll. on trust services for electronic transactions in the internal market and on amendment and supplementation of certain acts.

1. Introduction

1.1 General information

The document General terms and conditions of use of qualified trust services provided by the Provider brainit.sk, s.r.o. (hereinafter referred to as "General terms and conditions") serves to inform clients and third parties about the purpose of using the provided qualified trust services, the main rights and limitations in their use and the main aspects of providing qualified trust services.

The current version of the General Terms and Conditions is published on the Provider's website:

https://nfqes.sk/dokumenty/

An integral part of these General Terms and Conditions is the obligation of the parties to make themselves acquainted with and to comply with:

- the Provider's policy for the provision of qualified trust services,
- CP and CPS for qualified trust services related to the validation of electronic signatures/seals and the issuance of KCs for electronic signatures/seals.

In the event of a difference between the Slovak and English versions of the Certification Policies and Certification Policy Statements or General conditions, the provisions set out in the Slovak version shall apply.

1.2 Information about the provider brainit.sk and its contact details

Brainit.sk is a qualified trust service provider that carries out its activities in accordance with the requirements of Regulation (EU) No 910/2014 and the Slovak Act on Electronic Services and Electronic Trust Services. As such, Brainit.sk is included in the trusted list of trusted service providers.

The General Terms and Conditions (hereinafter referred to as the GTC) regulate the basic rules for the provision and use of the Provider's Trusted Services. And they also regulate the rights and obligations of the Provider on the one hand, and on the other hand, they regulate the rights and obligations in the provision and use of the Trusted Services of the Customer and the Certificate Holder.

These IRs are created in accordance with the Provider's Policies.

The current effective GTC, Provider's Policies and all documents and forms necessary for the provision of Trusted Services are available on the durable medium, on the website of brainit.sk, s. r. o. and also in printed version at individual Workplaces. They are available for inspection and familiarisation for any person interested in Trust Services.

The service of issuing qualified certificates for electronic signature and seal has been subject to conformity assessment in accordance with the eIDAS Regulation and the relevant ETSI standards. It is therefore a service provided at a qualified level within the meaning of the eIDAS Regulation.

Contact details of Brainit.sk:

General Information:	
Company name	*brainit.sk, s. r. o.*
Company Headquarters	*Veľký diel 3323, 010 08 Žilina*
ID	*52577465*
VAT	*2121068763*
VAT NUMBER	*EN 2121068763*
Register	*Commercial Register of the District Court of Žilina, section Sro, insert number 72902/L*
Contact:	
Provider's website	*https://nfqes.com*
Trusted Services website	*https://zone.nfqes.com*
E-mail	*info@brainit.sk*
Mobile	*+421 907 679 106*
Contact for Certificate cancellation request:	
Mobile	*+421 918 022 030*
E-mail	*info@brainit.sk*

1.3 Subscriber Service

Brainit.sk provides qualified and non-qualified trust services through a Certification Authority (CA) and an internal Registration Authority (RA), as well as through a network of external RAs. External RAs perform their activities to provide trust services on behalf of brainit.sk. A complete and up-to-date list of RAs and information on their contact details is available on the provider's website.

1.4 Access and provision of general terms and conditions on a durable medium

This document constitutes the General Terms and Conditions, on the basis of which contracts for the use of trust, cryptographic, information and other services provided by brainit.sk are concluded, and forms an integral part of the contracts for the use of the respective services.

These GTC shall apply in relation to all Subscribers, namely in relation to Users, Provider and all other Subscribers who have concluded a contract with brainit.sk for the services provided by brainit.sk according to the procedure set out in this document. This GTC shall also apply to Relying Parties who rely on electronic identification, or a trusted service provided by brainit.sk

The GTCs are publicly available on the brainit.sk website, on brainit.sk mobile applications and at any brainit.sk headquarters or external RA of brainit.sk.

Each Subscriber and each Relying Party agrees to familiarize itself with these GTCs prior to entering a contract with brainit.sk and using any of the services covered by these GTCs. By accepting these GTC, all Subscribers, Users and Relying Parties also automatically agree to the Privacy Policy (GDPR).

Depending on the manner in which Participants and Related Parties request and/or use brainit.sk's services, the GTC are provided and made available in an appropriate manner in a legible form and on a durable medium as follows:

- When concluding a contract with brainit.sk at the company's registered office or at the registered office of brainit.sk's external RA in paper form.
- When concluding a contract with brainit.sk in electronic form, through a communication channel with brainit.sk other than the mobile application or by personal appearance at the headquarters of brainit.sk or at the headquarters of the external RA of brainit.sk, the GTCs are provided to the Participant by sending an attached and electronically signed file by e-mail to the e-mail address provided by the Participant when concluding the contract. If the Subscriber does not have an email address and if the Policies and Procedures applicable to the specific service(s) that are the subject of the Contract allow for the provision of such services without the Subscriber providing a valid email address, the GTC are sent to the Subscriber via a link in an SMS with an instruction to the Subscriber to immediately download and save them to his/her local device.
- In addition to the above, the GTCs are available in readable form on the brainit.sk website in a format that allows them to be downloaded, saved, and reproduced in electronic form, as well as printed on paper, in the long term. Upon request at brainit.sk's registered office, the GTC may be provided to the Participant in paper form at any time.

2. Binding force of the general conditions and conclusion of the contract

These GTC form an integral part of each Contract and the CA Contract. In the event of a conflict between the General Terms and Conditions and the provisions in the Contracts, the provision under the Contracts shall prevail.

In addition to the GTC, the provision of Trust Services by the Provider and their acquisition by the Customer is also subject to the relevant Provider's Policy, depending on the type of Certificate provided.

The Provider shall inform each potential customer of the trust service with the GTC before entering a contractual relationship with the Provider. The GTC shall also be permanently accessible in electronic form on a durable medium:

- on the website https://zone.nfqes.com
- in the process of applying for a Certificate

The customer interested in the issuance of Certificates, who becomes a Certificate Holder, is forced to actively express his/her consent to the Certificates before their issuance after they have been made available to him/her, i.e. by signing the application for the issuance of the Certificate with a qualified electronic signature using his/her electronic ID card (eID) with a qualified time stamp, which informs that signing the application with a qualified electronic signature means the expression of consent to the Certificates, the interested person is informed immediately in the application form. This qualified signature is subsequently validated, thereby verifying the validity of the signature, the validity and authenticity of the data and the validity of the identification documents. Subsequently, this application for the issue of a Certificate with a qualified electronic signature and a qualified time stamp is kept in the RA's records. By signing and agreeing to these GTCs, the Certificate Holder also automatically agrees to the GDPR Personal Data Processing Policy.

The signing of the application for the issuance of a Certificate by a qualified electronic signature of a person interested in Certificates, who subsequently becomes a Certificate Holder, is a proposal for the conclusion of a contractual agreement on the provision of Trust Services addressed to the Provider, the content of which is formed by these GTCs.

Acceptance of the proposal for conclusion of the contract resulting from the preceding paragraph by the Provider, and consequently the conclusion of the contract between the Provider and the Certificate Holder occurs at the moment of provision of the requested Trusted Service, i.e. at the moment when the requested Certificate is handed over to the Certificate Holder. The content of the contract between the Provider and the Certificate Holder is fully determined by the GTC.

After execution this contract according to the previous paragraph, the Provider shall issue a Confirmation to the Certificate Holder. The Certificate Holder is obliged to sign it with his/her qualified electronic signature.

A contract with a Customer who is not a Certificate Holder at the time shall be in writing and shall not be subject to the procedure set out in the above paragraphs.

In addition to the GTCs, the Provider's Policy is also binding for the provision of Trusted Services by the Provider.

3. Services provided by brainit.sk

These GTCs shall apply in the relationship between the Provider and the Subscribers, as well as in the relationship between the Provider and the Relying Parties when any of the Provider's trusted services are provided.

3.1 Issuing a qualified certificate for electronic signature

A qualified certificate for electronic signature in accordance with Article 28 of Regulation (EU) No 910/2014 shall only be issued to a natural person (Holder) or to a natural person authorized by the Holder or to a person acting on behalf of the Holder by law or by a decision of a competent authority.

Depending on the certificate profile and issuance policy, the certificate can be used for authorship certification in electronic documents, for identification or authentication when accessing web applications, secure communication, and electronic signing of all types of documents (PDF (PaDES), XML (XaDES), TXT (CaDES), etc.). Qualified certificates for electronic signature can also be used for signing document packages (ASiC-E) as well as e-mails (based on S/MIME (Secure/Multipurpose Internet Mail Extensions/Protocol for the secure transmission of e-mails over the Internet or cryptographic system for the protection of messages transmitted via e-mail and data stored on various media). The certificate may also contain details of the legal entity associated with the natural person on whose behalf the signatory is signing. In this case, brainit.sk does not certify that the natural person of the Holder represents the legal entity, but only that there is a legal relationship between the Holder and the legal entity.

The types of profiles of qualified certificates for electronic signature issued by brainit.sk are described below in this chapter.

3.1.1 KC issued to an individual for QES

The issuance of qualified certificate for natural person for qualified electronic signature is a qualified trust service under Regulation (EU) No 910/2014. A Qualified Natural Person Certificate for QES is issued for the purpose of proving the authorship of a natural person in electronic documents signed electronically and to which the Certificate is attached, as well as identifying the Holder with specific additional characteristics as described in the Certificate. All procedures and rules for its issuance and management shall be consistent with the certification policy for the provision of this trust service.

3.1.2 KC issued to a natural person for AES

The issuance of qualified certificate for natural person for advanced electronic signature is a qualified trust service under Regulation (EU) No 910/2014. A qualified certificate for AES shall be issued in compliance with all the principles and procedures for the issuance of qualified certificates as set out in 3.1.1.

3.2 KC issued for electronic seal

A qualified certificate for an electronic seal is issued to any entity (Customer) that is authorized to act on behalf of the legal entity under applicable national legislation and can be used to guarantee the origin and integrity of the legal entity's output data, for example: electronic documents, photographs, architectural designs, software, etc. This brainit.sk trust service is provided in accordance with Article 38 of Regulation (EU) No 910/2014. The types of profiles of qualified certificates for electronic seal issued by brainit.sk are described later in this chapter.

3.2.1 KC issued to a legal entity for a qualified electronic seal

The issuance of qualified certificate for legal person for qualified electronic seal is a qualified trust service under Regulation (EU) No 910/2014. An attribute in the certificate shall contain information that the certificate is qualified and shall indicate whether the private key has been used to create an electronic seal. Brainit.sk issues the certificate and delivers it to the person authorized by the legal entity. By accepting these GTCs when requesting this service, the Holder is deemed to have consented to the use of the Qualified Device to create a Qualified Electronic Signature.

3.2.2 KC issued to legal entity for advanced electronic seal

The issuance of qualified certificate for legal person for advanced electronic seal is a qualified trust service under Regulation (EU) No 910/2014. A qualified certificate for AES-S shall be issued in

compliance with all the principles and procedures for the issuance of qualified certificates as set out in 3.2.1.

3.3 KC issued for website authentication

A qualified certificate for website authentication is issued for the purpose of certification of a website by a specific natural or legal person. It is intended to be used to provide assurance to the visitor that the website is maintained by a genuine and identified entity. The use of SSL technology ensures reliable connectivity under a secure protocol for the exchange of information between the website and its visitors. This qualified trust service is provided by brainit.sk in accordance with Article 45 of Regulation (EU) No 910/2014.

3.4 KC issued for qualified time stamp

Issuance of a Qualified Electronic Time Stamp is a qualified trust service provided by brainit.sk in accordance with Article 42 of Regulation (EU) No 910/2014. Qualified electronic time stamps are issued to natural persons and legal entities. A qualified electronic time stamp shall have the presumption of accuracy of the date and time indicated on it, as well as the integrity of the data submitted before brainit.sk. Such data may be an electronic signature, an electronic seal, a hash of unsigned electronic documents or a hash of other electronic content.

A qualified electronic time stamp can be integrated into the process of creating, sending, or receiving electronic signatures/seals, electronically signed documents and electronic transactions, archiving electronic data, etc. This service uses the technology of binding date and time to data in a way that excludes the possibility of unnoticed changes to the data and provides the possibility to prove later (after the expiry of the validity period of the Qualified Electronic Time Stamp) that an electronic document or other electronic item was signed at a given time.

3.4.1 Specific requirements applicable to relying parties

The main obligation of the Cooperating Party is to check the validity of the signature/seal on the time-stamp token (TST). The Relying Party must check the validity of the time-stamp unit (TSU/time-stamp unit) as well as the validity period of this certificate. If time stamps are checked after the expiry of the TSU certificate, the relying party shall:

- check the time-stamped certificate in the Certificate Revocation List (CRL)
- check the usability of the hashing algorithm used
- verify the security of the electronic signature used by checking the applicable combination of asymmetric and hashing algorithms

When relying on a qualified electronic time stamp, the relying party is obliged to:

- verify that the qualified electronic time stamp has been properly signed and that the private key used to sign the time stamp has not been compromised up to the time of verification,
- consider any limitations on the use of the time stamp set out in these terms and conditions and in the relevant policies and procedures,
- consider all other measures prescribed in these conditions and in the relevant policies and procedures.

3.5 Qualified electronic signature/seal verification service

Qualified validation of a qualified electronic signature/seal is a qualified trust service in accordance with Articles 32, 33 and 40 of Regulation (EU) No 910/2014. This service is used to validate electronic

signatures, electronic seals, registered email services and certificates related to these services issued and provided by brainit.sk. Verification is also performed through qualified certificates for website verification. The qualified validation service is provided by brainit.sk as a qualified trust service provider and by providing it, a special document (the result of the validation process) confirming the validity, or the results of the validation process is generated and handed over to the Client.

In the process of verification of the qualified electronic signature/seal, brainit.sk confirms the validity of the qualified electronic signature/seal provided that:

- The certificate that accompanied the signature/seal at the time of signing was a qualified electronic signature/seal certificate meeting the requirements of Regulation (EU) №910/2014.
- The qualified certificate was valid at the time of signing.

This service may be provided for the verification of qualified certificates for electronic signatures, electronic seals and other qualified certificates issued by qualified trust service providers included in the European Commission's trusted list. These trust services are provided by brainit.sk in accordance with Article 33 and Article 40 of Regulation (EU) No 910/2014. For the verification of electronic signatures and electronic seals from different trust service providers, the same rules and l mentioned earlier in this chapter apply.

3.5.1 Purpose and limitations of use of

The purpose of the service is to provide a qualified trust service for the validation of qualified electronic signatures and seals. The intended use of the service is its integration into the Applicant's processes for validating electronically signed documents or directly by the end user using the NFQES portal.

The service is provided in accordance with the requirements of 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 and repealing Directive 1999/93/EC (eIDAS Regulation). Act No 272/2016 Coll. on trust services for electronic transactions in the internal market and on amending and supplementing certain acts (the Trust Services Act) and the Supervisory Scheme for Qualified Trust Services defined by the Supervisory Authority - NBÚ SR No 05968/2019/ORD-001.

The operation of a qualified trust service shall be governed by the general requirements for the provision of qualified trust services as defined in ETSI EN 319 401 "Electronic Signatures and Infrastructures (ESI), General Policy Requirements for Trust Service Providers".

The Service may only be used for proper and lawful purposes and in accordance with applicable law and the Provider's regulations for purposes within the End User's processes.

The service can be used through predefined interfaces after the service is made available by the Trust Service Provider and exclusively for the defined purpose.

3.6 Qualified electronic mailbox service

A qualified registered electronic mailbox service is a trusted service that enables the electronic transmission of data between third parties and provides evidence of the identity of the sender and recipient of the data transmitted, the time of transmission and receipt of the data, and protects the data transmitted against the risk of loss, theft, corruption, or unauthorized modification. The service provides:

- a high level of confidence in the identification of the sender,

- identification of the sender prior to delivery of the data,
- secure sending and receiving of data by mean of a guaranteed electronic signature or a guaranteed electronic seal of brainit.sk in a way that excludes all possibilities of unobserved data alteration,
- any modification of the data necessary for the purpose of sending or receiving the data is clearly marked for the sender and for the recipient of the data,
- the date and time of transmission and receipt, as well as any change to the data, shall be marked with a qualified electronic time stamp.

When providing this service, brainit.sk signs with an electronic seal and gives the sender proof (electronic delivery) of the facts of sending, receipt, and integrity of the transmitted content.

This brainit.sk trust service is provided in accordance with Article 44 of Regulation (EU) 910/2014. Evidence of sent messages may be stored for 10 years in the Provider's storage. It may be provided to the contracting parties in accordance with the applicable prices and conditions. Types of electronic registered delivery services provided by brainit.sk:

3.6.1 Specific requirements for the provision of a qualified electronic registered delivery service

Successful delivery of electronic content

- Delivery is considered successful if the content sent by the sender has left the sender's information system and is no longer under the sender's control.
- A consignment is deemed to have been delivered if the content sent by the sender has successfully entered the recipient's information system.
- When using the web portal, successful sending is the receipt of an electronic message from the Participant's web browser using the portal on the backend (server) brainit.sk and successful delivery is considered to be the receipt of the sent message in the virtual mailbox accessible in the recipient's account via the web portal.
- When using the qualified REM service, successful sending is considered the time of receipt of the electronic message into the information system on the brainit.sk electronic mail server (backend) and receipt is considered receipt into the electronic mailbox operated by brainit.sk on the brainit.sk electronic mail server.

Brainit.sk ensures that the service protects the transmitted electronic content against loss, theft, breach of integrity or unauthorized modification and meets the requirements of Regulation (EU) No 910/2014.

3.7 Electronic Signature and Seal Storage Service

The service of storing electronic signatures and seals is provided by brainit.sk in accordance with Article 34 and Article 40 of Regulation (EU) No 910/2014. These trust services provide secure and reliable long-term storage of all types of electronic signatures and seals affixed to documents (without storing the documents themselves in the vault) and/or electronically signed/sealed documents (with the vault) of the Participants and provides evidence of the storage process with the possibility of long-term verification of electronic signatures/seals. The data objects, the relevant storage evidence and the additional information required for their verification are accessible via the service interface or by making a specific request for data and/or evidence. They may be provided separately or in an I/O (input/output) package that is securely protected by encryption. In any case, they will only be

transmitted to the Participant or his authorized representative. Brainit.sk stores information about all prepared I/O packages, including the date of the event and the criterion according to which the selected stored objects were included in the package. The request must specify the person requesting the data, the reasons for requesting it and the way he or she wishes to receive it, for example by email or on electronic media. brainit.sk reserves the right to approve or refuse the execution of the request without having to justify its refusal or inform the applicant thereof, except in the cases provided for in the legislative act. To providing data and evidence, brainit.sk may collect fees to ensure the execution of the submitted request. Brainit.sk does not use any external organizations supporting the retention service. After the retention period has expired, the data will be deleted.

4. Price for trust services and payment terms

The current prices for the issuance of Certificates are set out in our price list published on our website https://nfqes.sk (the "Price List"). The price for the provision of the Trusted Service is determined in accordance with the Price List in force during the provision of the Trusted Service, unless otherwise agreed between the parties.

Prices for the issue of Certificates may be agreed individually with the Customer, directly in the contract, in a confirmed order or in another document.

The Customer is obliged to pay the value of the price for the Trusted Services by wire transfer on the basis of an invoice issued by the Provider after the provision of the requested Trusted Service. The due date of this invoice shall be 2 weeks, i.e. 14 days, unless otherwise provided for by generally applicable law or the contract in question. The price for these Trusted Services shall be deemed to be paid on the date on which the amount is credited to the Provider's bank account in full.

It is necessary that the invoice issued by the Provider contains all the elements of a tax document referred to in Section 74(1) of Act No. 222/2004 Coll. on Value Added Tax, as amended. The Customer shall have the right to object to the Provider's substantive or formal deficiencies of the invoice during the term of its due date. The Provider shall evaluate the Customer's objections and, if justified, shall subsequently prepare a new invoice, the due date of which shall commence from the day on which it was delivered to the Customer.

If the Customer fails to pay the full amount for the Trust Services provided by the due date under the GTC or the Contract, the Trust Service Provider shall be entitled to immediate withdrawal from the Contract, which shall also entail the cancellation of any Certificate for which payment has not been received.

5. Issuing certificates

Certificates under the GTCs are issued exclusively to the HSM Device, remotely mediated by the Application, only upon the request of the interested party for the Certificates. If the conditions specified in these GTC and the Provider's Policy are met, the Provider is obliged to issue the Certificate to the Holder and shall deliver it soon. For the issued Certificates, the Provider shall also issue a Confirmation signed by the Certificate Holder. The Acknowledgement identifies the specific Certificate that has been issued to the Certificate Holder. The Trusted Service shall be deemed to be provided now of acceptance of the issued Certificate by the Certificate Holder.

5.1 Restrictions on the use of the services provided by

Subscriber agrees to take all necessary measures to minimize and limit damages resulting from the use of the Services more than the limitations on their use set forth in these GTC. The parties agree and undertake to take all necessary measures when relying on the electronic identification service or trust service provided by brainit.sk to monitor and comply with the limitations on the use of the services as set out in these GTC.

5.1.1 Time limits

Each certificate issued by brainit.sk can only be used until its expiry date. The validity period of the certificates is indicated therein. If the certificate has been revoked, the signer/creator may not use the private key to create an electronic signature/seal.

5.1.2 Intended Purpose

Certificates issued by brainit.sk will be used in accordance with their intended purpose as described in these GTC, in brainit.sk's applicable policies and procedures and in applicable law. Verification of the intended purpose of the certificate will be made based on the information provided in the certificate profile:

- the policy/statement according to which the electronic signature certificate/seal is issued and managed,
- the intended purpose and the limitations of the effect of the certificate with respect to the purposes for which it is used,
- details of the signatory/certificate creator.

6. Restrictions on the use of certificates

Each Certificate that is issued by the Trust Provider, together with the relevant Key Pair, may be used in the usual manner, only for the purpose for which it is intended, in accordance with the terms, conditions and limitations set out in the relevant Provider Policy. The Certificate is intended solely for the execution of an electronic signature or an enhanced electronic signature of the Certificate Holder. As the Device is a qualified device within the meaning of the eIDAS Regulation, it is possible for a qualified electronic signature to be created using the Certificate.

Certificates are valid for a limited period. Upon expiration or cancellation of the Certificate, the Certificate may not be used, even for the purpose specified therein. The use of a Certificate that is invalid or has been revoked, which is also intended for the execution of an electronic signature, will consequently result in the invalidity of this electronic signature.

The verifiability of electronic signatures has limitations, i.e. after the expiration of the validity of the Certificate based on which they were made, it is not guaranteed that it will be possible to verify the validity of the electronic signature in question retrospectively. To ensure the long-term verifiability of this electronic signature even after the expiry of the Certificate based on which it was made, it is necessary to make appropriate use of specialized services designed for this purpose while the Certificate is still valid, for example, the electronic signature storage service and/or the electronic time stamp service.

The use of a Certificate for the creation of an electronic signature does not guarantee that the created electronic signature can be used for its intended purpose. Nor does it mean that they will be in the

required format acceptable to third parties. The format of the electronic signature is determined by the application used to create the electronic signature.

If the Customer or the Certificate Holder uses the Certificate in a manner that violates the rules set out in these GTC or relies on the Certificate in violation of these restrictions and he or a third party suffers damage in connection with this action, the Provider shall not be liable for it under Article 13 (2) of the eIDAS Regulation.

7. Specific conditions for issuing qualified trust services

7.1 Accepting the certificate

Upon receipt of a qualified certificate, the Participant is obliged to verify its contents with respect to the correctness of the data and the existence of a public key corresponding to the private key that he or she holds.

If incorrect information is provided in the certificate, the certificate shall be revoked immediately. If the Participant objects that the issued qualified certificate contains errors or deficiencies within 3 (three) days of its publication in the certificate repository, brainit.sk will remove them free of charge by issuing a new certificate, unless they are due to the provision of incorrect data. If no objections have been raised, the contents of the certificate shall be deemed to have been accepted. The rules set out in this point apply to both the issue of a certificate and the renewal of a certificate.

A Qualified Certificate shall be deemed to be accepted by a Participant if any of the following conditions are met:

- Express approval/confirmation by the Participant,
- The Qualified Certificate is used by the Participant for the first time,
- After the expiration of three (3) days from the date of issuance of the qualified certificate, if the Participant does not object to the content of the certificate within the period.

In the case of certificates of electronic signature or electronic seal, the obligation according to the aforementioned, the possibility of objection, as well as the assumptions under which the certificate is deemed to be accepted, always apply only in relation to the Signatory or the Creator, regardless of whether the issuance of the certificate itself is paid by him or by a third party (another Participant), who has also entered into a contractual relationship with the company brainit.sk according to these GTC.

8. Rights and obligations of the customer and the certificate holder

Both the Customer and the Certificate Holder are obliged to comply with these GTC and the generally binding legal regulations of the Slovak Republic. The Customer is entitled to use the Trusted Services provided by the Provider in accordance with the Contract, these GTC and the Provider's Policies. The Customer has the right to request cancellation of the issued Certificate regardless of the Certificate Holder's consent.

If the Customer is a consumer, he/she has the rights under § 622 and § 623 of the Civil Code in case of defects in the Trust Service.

In particular, the customer has the obligation to:

a) to provide the Provider with all data and documents necessary in accordance with the Provider's Policies for the provision of the requested Trusted Service, the data and documents must be true, up-to-date and complete;
b) in the case of the provision of data necessary for the provision of the Trusted Service, to ensure in advance that such data is sent to the Provider in a manner that guarantees its confidentiality and integrity (e.g. sending an encrypted file electronically and sending the password through a separate channel);
c) use the Certificate and the generated Key Pair only for the purposes intended, in accordance with the law and the restrictions on their use set out in the GTC;
d) exercise care in using and relying on the Certificate in accordance with Section 10 of the GTC;
e) refrain from unauthorized use of the Certificate Holder's private key if the Customer and the Holder are not the same person;
f) in cases where the Customer generates cryptographic keys for which a Certificate is to be issued, the Customer is obliged to create a key pair of the prescribed length, using the algorithm required by the Provider's Policy related to the requested Certificate;
g) allow the private key for which the Certificate is issued to be used for cryptographic functions solely within the Facility and under the exclusive control of the Certificate Holder;
h) to provide the Provider with immediate and prompt assistance, if requested to do so, in verifying the data necessary for the issuance of the Certificate;
i) during the validity of the Certificate, immediately notify the Provider of any changes, errors or obsolescence in the data contained in the Certificate;
j) during the validity of the Certificate, immediately notify the Provider if any misuse, theft, loss, defacement, destruction, compromise or any unauthorized access to the associated private key or access codes (password and token) occurs or if the Customer suspects that the above events may have occurred; and ensure that the Certificate Holder refrains from using a private key and Certificate that has expired, been revoked or compromised (including if the Provider itself has been compromised and the Customer is aware of it).

The Certificate Holder has the right to use the Certificate issued to him by the Provider in accordance with the Agreement and these General Terms and Conditions.

In particular, the Certificate Holder has the obligation to:

a) immediately after obtaining a Certificate, to review the accuracy and currency of the information contained therein and to provide only true and current information and documents in connection with the Trust Services at all times;
b) take reasonable care in using and relying on the Certificate in accordance with Section 10 of these GTC;
c) to use the Certificate and the generated key pair exclusively for the purposes intended, in accordance with generally binding legislation and the restrictions on their use set out in the GTC;
d) protect the access code (password and token) against unauthorized access and also against loss, compromise, destruction or misuse;
e) during the validity of the Certificate, immediately notify the Provider of any changes, incorrectness or outdatedness of the data contained in the Certificate;
f) during the validity of the Certificate, immediately notify the Provider if the related private key, access codes (PIN), recovery codes (PUK) or the device on which the keys are stored are

misused, stolen, lost, destroyed, compromised or any unauthorized access to the Certificate Holder is suspected, that the above events may have occurred and refrain from using a private key and Certificate that has expired, been revoked or compromised (including if the Provider itself has been compromised and the Certificate Holder is aware of it).

Cancellation of the Certificate is requested by the Customer or the Certificate Holder to the Provider using the contact details specified in Article 3 of the GTC.

9. Rights and obligations of the provider

The Provider is entitled not to provide the Trusted Service or to limit the scope of its provision to the Client (e.g. by not specifying all the required attributes in the Certificate) if the prerequisites for the issuance of Certificates as defined in the Provider's Policy or in these GTC are not met.

The Provider is entitled to revoke the Certificate in cases specified in the relevant Provider Policy, especially if:

a) notices that the conditions of the eIDAS Regulation, the Act or the Provider's Policy have not been met for the issuance of the Certificate;
b) notices that the Device on which the Keys are stored, or its software components are or may be compromised;
c) the court orders the Certificate revoked;
d) the Customer has not paid the agreed price of the Trusted Services within a predetermined period of time, even after a notice sent electronically by the Provider;
e) The Customer shall not disclose the contract with the Provider within three months of its conclusion in cases where it is a compulsorily disclosed contract in accordance with Section 5a of Act No. 211/2000 Coll. on Free Access to Information and on Amendments and Additions to Certain Acts (Act on Freedom of Information);
f) termination or expiration of the contract with the Customer or Certificate Holder occurs or if the Certificate Holder fails to sign the Acknowledgement;
g) The Customer or the Certificate Holder breaches the given obligations under these General Terms and Conditions, the Contract or generally applicable law;
h) becomes aware of any changes affecting the validity of the Certificate, in particular in cases where the data provided in the Certificate is incorrect or outdated or becomes aware of the theft, loss or compromise of access codes, etc.;
i) the Customer or Certificate Holder has died (if a natural person) or ceased to exist (if a legal person);
j) cancellation is requested by the Customer or the Certificate Holder;
k) The Certificate is no longer in compliance with the Policy under which it was issued;
l) The cryptography used for a given Certificate no longer provides a link between the Certificate Holder and the public key.

The Provider is entitled to publish the name of the Customer as a reference on its website if the contract does not provide otherwise.

The Provider is obliged to provide Trust Services in accordance with the eIDAS Regulation, the Act, and its own Policies in force at the time of their provision.

10. Information for parties relying on trusted services

The Relying Parties acknowledge that it is their sole and absolute discretion as to whether they choose to trust and rely on the Certificate issued by the Provider and the information contained therein. In the event of a decision to rely on the Provider's Certificate, the relying parties shall be obliged to comply with the obligations described in this Section 10 of the GTC otherwise they shall be solely responsible for the legal consequences caused thereby.

The Relying Party acknowledges that the validity of Certificates, CRLs as well as OCSP Responses issued by the Provider is limited in time:

a) The Certificate is valid for the validity period specified in the body of the Certificate or until it is revoked before the expiry of the validity period;
b) The CRL is valid for the period of validity specified in the CRL body, while in order to obtain the most accurate information about revoked Certificates, it is always necessary to use the most up to date CRL, i.e. the one published by the Provider as the most recent one;
c) The OCSP response is valid at the time indicated in the OCSP response body by "producedAt". The producedAt entry is just the time the OCSP response was signed and has nothing to do with the validity of the certificate.
d) Only CRLs and OCSP responses where the thisUpdate entry contains a time and date after the time and date of the signature that is within the certificate validity interval and is the time at which the certificate is validated can be used to validate signatures or seals.

The Relying Party shall exercise reasonable care in relying on any Certificate issued by the Provider, it shall:

a) evaluate whether the use of the Certificate is in accordance with its intended purpose and whether it is appropriate for that purpose;
b) to check whether the use of the Certificate does not contravene the restrictions on the use of the Certificate set out in the Certificate itself, these General Terms and Conditions or in the Provider's Policies that are related to the given Certificate;
c) when working with the Certificate, including its authentication, use only designated and appropriate hardware or software;
d) verify the validity of the Certificate in question by using an application validating the Qualified Certificate using a trusted list published by the NBÚ and a suitable CRL or OCSP response with a thisUpdate entry containing the time and date after the time of the signature or seal.
e) perform any other verifications that may be required for a particular type of Certificate or its use under the Provider's Policies or standards;
f) verify other certificates in the certification path up to the "trust anchor" in the manner described in a) - e). The trust anchor is stored in a trusted list published by the NSA. Certificates stored in the trusted list constitute the trust anchor.

The Relying Party also acknowledges that the Provider shall archive the information related to the issued Certificates for the purpose of providing evidence for a certain period within the meaning of Article 12 of the GTC.

To rely on a CRL or OCSP response issued by a Provider, it is the relying party's obligation to exercise reasonable care. In particular, the Obliged Party is obliged to verify that the certificate with which the

CRL or OCSP Response has been signed belongs to the Provider by using the trusted list issued by the NBÚ and at the same time to proceed by analogy within the meaning of Article 10 of these GTC.

11. Provider's liability, warranty, and their limitations

The Provider shall be solely liable for damage caused by failure to comply with its obligations under the eIDAS Regulation within the meaning of Article 13 of the eIDAS Regulation.

The Provider is obliged to provide the Trusted Services in accordance with generally binding legislation and the Provider's Policies. The Provider shall be liable for defects in the Trust Service provided in accordance with generally applicable law.

The Provider shall not be liable for indirect losses or damages incurred by the Customer, the Certificate Holder, the Relying Party or any third party in connection with the use of the Trust Services.

The Provider shall not be liable for damages (including lost profits) incurred by the Customer, the Certificate Holder, the Relying Party or any third parties due to:

a) breach of the obligations of the Customer, the Certificate Holder or the Relying Party set out in generally applicable law, these GTC, the relevant Contract or the Provider's Policies, including the obligation to take reasonable care when using and relying on the Certificate;
b) failure of the Customer or the Certificate Holder to provide the necessary cooperation;
c) the technical characteristics, configuration, incompatibility, unsuitability or other defects of the software or hardware used by them;
d) using or relying on a Certificate that has expired or been revoked;
e) The Certificate has been used in violation of its intended purpose or the restrictions set forth in the Certificate, these GTC or the Provider's Policies;
f) delay or non-delivery of requests for verification of the Certificate status to the Provider, for reasons not on the Provider's side (in particular, cases of unavailability or congestion of the Internet network or defects in the equipment or technical equipment used by the verifier);
g) failure to provide any of the Trusted Services or their unavailability during planned maintenance or reorganization announced on the Provider's website;
h) the action of a higher power.

The Provider shall not be liable for damages incurred by the Relying Party due to the fact that it did not follow the procedure set out in Section 10 of these GTC when relying on the Provider's Trusted Services or on the electronic signature or seal made on their basis.

The provider is also not liable:

a) for the unauthorized person having taken possession of the Customer's or Holder's access codes;
b) for damages caused by the use of the Certificate if the Customer or the Certificate Holder does not act in accordance with his/her obligations, especially if an unauthorized person takes access and the Customer or the Certificate Holder does not request the Provider to revoke the Certificate or does not notify the Provider of changes in the data;

The Customer and the Certificate Holder use the Trust Services at their own responsibility and bear all costs for remote communication means or other technical means necessary for the use of the

Provider's Trust Services (e.g. for the software necessary for the execution of an electronic signature or seal based on the Certificate);

12. Privacy and personal data protection

12.1 Processing of personal data

Brainit.sk carries out its activity of providing trust services in accordance with the requirements of Regulation (EU) 2016/679 (GDRP), applicable law and in accordance with its applicable Privacy Policy, which forms an integral part of these GTC and the contract with the Subscriber.

The applicable privacy policy of brainit.sk includes:

- Privacy Policy applicable to trust, information, cryptographic and other services provided by Brainit.sk (all services),
- Other privacy policies that brainit.sk may adopt and apply in connection with the provision of some of its services.

The Privacy Policy applicable to trust, information, cryptographic and other services provided by brainit.sk applies to the activities carried out in the provision of services under this GTC. In addition, in connection with some of its services, brainit.sk may provide and implement specific privacy policies regarding brainit.sk's processing of personal data in the provision of those services. In the event of a conflict between the Privacy Policy applicable to trust, information, cryptography, and other services provided by brainit.sk and this Special Policy, the Special Policy shall prevail, but only with respect to processing activities related to the provision of the relevant services covered by this policy. In case of gaps in the Special Policy, the provisions of the Privacy Policy applicable to trust, information, cryptographic and other services provided by brainit.sk shall apply.

Before entering a contract, the Subscriber shall familiarize himself with the Privacy Policy applicable to the services requested by the Subscriber to find out how, what type of personal data and for what purposes brainit.sk processes, as well as to be informed about his rights and any other important issues related to the protection of personal data in accordance with the GDPR.

The provision of services is inherently related to the receipt, transmission, storage, and processing of the Subscriber's data through the brainit.sk systems, to the relying parties, as well as to the exchange of such data between them and the Provider in accordance with the applicable legislation and the contractual relationships between all the parties. The Subscriber is deemed to be aware of the above and consents to his/her data being disclosed to third parties for the purposes of providing the Services.

The Provider processes the personal data of the data subjects in accordance with the relevant legislation. The Provider may disclose this data to third parties if this is required or permitted by the relevant legislation.

To informing data subjects or persons interested in Trust Services about the processing of personal data carried out by the Provider in the provision of Trust Services, the Information on the processing of personal data is used:

a) always available in electronic form online at https://nfqes.sk
b) which the Certificate Holder is informed about in the process of applying for the Certificate.

The Provider records and archives all essential information and documents related to the issuance or revocation of the Certificate and on the basis of which the Certificate was issued, including the personal data of the Customer, the Certificate Holder, and, where applicable, persons authorized to act on their behalf or authorized by the GTC for 10 years from the date of revocation or expiration of the Certificate in question.

The Certificate Holder acknowledges that if an electronic document is signed based on the Certificate designated for this purpose, the recipient of this electronic document, or any persons who have access or will have access to this electronic document, will gain access to his/her personal data contained in the Certificate.

13. Dispute and complaint resolution

The User is entitled to send the Provider a complaint, suggestion, or complaint about the Trusted Service by email to ca@nfqes.sk. The Provider shall respond to it within 30 days of its receipt, in the case of more complicated complaints or claims, the Provider reserves the right to extend this period.

The courts of the Slovak Republic shall have exclusive jurisdiction to adjudicate any disputes between the Provider and the Customer or the Certificate Holder. If the Customer or the Certificate Holder is a consumer, he/she is entitled to contact an entity for out-of-court dispute resolution, e.g. the Slovak Trade Inspection or another legal entity registered in the list pursuant to Section 5 (2) of Act No. 391/2015 Coll. on Alternative Dispute Resolution for Consumer Disputes, as amended. Before proceeding to judicial or out-of-court dispute resolution, it is the obligation of the parties to try to resolve the dispute by mutual agreement in advance.

14. Applicable law

Legal relations between the Provider and the Customer or the Certificate Holder shall be governed by the laws of the Slovak Republic.

Legal relations not expressly regulated by these GTC, or the Contract shall be governed by the relevant provisions of Act No. 513/1991 Coll. of the Commercial Code, as amended, and other generally binding legal regulations. If the Customer or the Certificate Holder is a consumer, the provisions of Act No. 40/1964 Coll., the Civil Code, as amended, shall apply to legal relations between the Customer and the Provider that are not expressly regulated by these GTC.

15. Duration and termination of contracts

The contract between the Provider and the Customer is concluded for an indefinite period, unless otherwise specified. The contract between the Provider and the Certificate Holder is always concluded for a definite period, until the expiry or cancellation of the Certificate to which the contract relates.

The contract between the Provider and the Customer may be terminated:

a) by mutual agreement of both parties;
b) by notice of either party in the case of a contract concluded for an indefinite period; the period of notice shall be 2 months and shall commence on the first day of the calendar month following the month in which the other party to the contract received the written notice;

c) withdrawal from the contract by either party in the event of a material breach of contractual obligations by the other party.

The following shall be deemed to be a material breach of contractual obligations that gives rise to the right to withdraw from the contract:

a) if the Customer fails to pay the full price for the Trusted Services provided within the agreed period;
b) if the Certificate Holder or the Customer uses the Certificate in a manner that is contrary to the law, these GTC or the Provider's Policies;
c) if the Customer or the Certificate Holder breaches the obligation to request cancellation of the Certificate in the cases specified in these GTC or the Agreement;
d) other reasons within the meaning of generally binding legal regulations of the Slovak Republic.

If the Provider exercises its right to withdraw from the Contract, it shall also have the right to cancel the Certificate to which the breach of duty by the Customer or the Certificate Holder relates.

In the event of termination of the Contract, the Customer's obligation to settle any debts incurred in connection with the use of the Trusted Services shall not be extinguished.

The termination of the contract between the Provider and the Customer or the Certificate Holder does not affect those provisions, the nature of which implies that they are to survive their termination.

15.1 Contract, conclusion, subject matter

brainit.sk will provide, either free of charge or for a fee, the services covered by these GTCs, subject to and in strict compliance with the Subscriber/Subscriber/Contractor's agreement entered under these GTCs as well as under applicable law. The Services are diverse, constantly supplemented and modified to improve and expand them, and on this basis brainit.sk may unilaterally change their number, characteristics, and conditions of their provision at any time, within the limits set by the applicable legislation.

The services of brainit.sk may be requested or provided in different ways depending on their nature and in accordance with these GTC. Requesting a service and entering a contract requires secure identification of the Subscriber in accordance with the level of security required for the service and the Subscriber's agreement to these GTC. Prior to requesting a service, the Subscriber shall familiarize itself with all Policies and procedures applicable to the applicable service. By requesting a service, Subscriber accepts these GTC.

Different brainit.sk services may be requested in different ways, and not every request method provides the ability to request each of the services. Brainit.sk maintains up-to-date information on its website about how to request and use different types of services.

The services of brainit.sk can be requested in any of the following ways:

15.1.1 Personal visit to brainit.sk headquarters

The procedure for requesting a trusted service at the brainit.sk headquarters requires the physical presence of the Participant in cases where the Participant is a natural person, or the presence of a legal representative or attorney duly authorized by a notarized power of attorney if the Participant is a legal person.

For a natural person:

For unambiguous identification and identity verification, the Participant shall provide the following information:

full name (as in the identity document); proof of identity - identity card, international passport, or other proof of identity; national identification number, if any; contact details - mobile phone number, email address and postal address of permanent residence. After successful verification of the Participant's identity, an authorized operator from the internal Registration Authority brainit.sk:

- draft a qualified trust services contract signed on behalf of brainit.sk and keep all submitted documents related to the contract. The contract shall be signed by the Subscriber in paper form together with these GTC, the applicable brainit.sk Privacy Policy and any other documents relevant to the requested service.
- confirms the request for issuance and sends the electronic request for issuance of the certificate to the operating certification authority brainit.sk;
- record the issued certificate on the secure signature creation device and hand it over to the signatory or authorized signatory (if applicable).

The conclusion of a contractual relationship with a natural person shall give rise to:

- based on an application for a certificate that refers to these GTCs,
- by signing a paper or digital contract (by QES).

For a legal entity:

Establishing the identity of the legal entity is carried out by the RA by verifying in the relevant registers based on the provided registration or other unique identification number of the legal entity. Identification of the legal entity and verification of the authorized representative shall be carried out on the spot based on information provided by the Participant through documents sent remotely or by personal meeting. During such identification, all the data that will be provided in the issued certificate as well as the authorization of the legal representative of the person who attended the physical meeting at the brainit.sk headquarters shall be verified.

In the case of legal entities, the following must be submitted:

- a court decision or other document certifying the establishment of the legal entity;
- a document proving your integrity;
- a unique national identifier;
- Other relevant documents.

Once all requested documents have been copied with the consent of the person who submitted the request, the copies remain on file at brainit.sk. For the avoidance of doubt, such consent does not constitute consent under Regulation (EU) No. 679/2016, but contractual consent and is a mandatory condition for the conclusion of a contract. Verification of the data contained in the submitted documents shall be carried out by verifying the "true copy or original" and by a handwritten signature signed by the person representing the Participant in front of the RA employee. The certification of the identity of the RA has two purposes: (1) to verify whether or not the RA exists at the time the application is reviewed, and (2) to verify that the person acting on behalf of the RA has the necessary

representational authority to request the relevant trust services and to validly contract on behalf of the Participant for the provision of such services under these GTC.

Entering a contractual relationship with a legal entity shall give rise to:

- by signing a paper or digital contract (by QES),
- a binding order for the supply of services.

15.1.2 By a personal visit to the external Registration Authority of brainit.sk

The process of requesting a service and concluding a contract begins with the individual Participant or the legal representative or duly authorized representative of the legal entity of the Participant meeting in person at the workplace of the external Registration Authority and submitting a request to the Registration Authority for the relevant service. The request may be submitted to the external registration authority of brainit.sk for any of the services of brainit.sk in respect of which the relevant external registration authority is authorized to act as the registration authority of brainit.sk. Upon submission of the Participant's request to the Registration Authority, the same procedure for requesting the Service as mentioned above in this section will be followed.

16. Final provisions

The Provider is entitled to unilaterally change the GTC or the Price List, for reasons consisting in the business policy of the provision of Trust Services, for reasons of changes in generally binding legislation, changes in standards regulating the provision of Trust Services, for reasons of technical, security or organizational changes in the systems used for the provision of Trust Services on the Provider's side, as well as for reasons of improving the quality, security or availability of Trust Services. In such case, the Provider shall notify the Customer and the Certificate Holders of the changes to these documents at least 30 days before the changes take effect, by sending an informative electronic message to the email address provided in advance and by publishing them on the Provider's website. If the Customer or the Certificate Holder does not agree with the change of the binding document, he/she has the right to terminate the contract with the Provider with immediate effect within 30 days from the date of sending this information by the Provider. The termination can be sent to the Provider's registered office address or to the email address info@nfqes.sk. Unless the Customer or the Certificate Holder rejects the proposed change in writing no later than the effective date of the change in question, the Customer agrees to the change and the change becomes binding on him/her as of the effective date of the change.

For the delivery of legal acts and other legal acts between the Provider on the one hand and the Customer or the Certificate Holder on the other hand, the contact details provided by the parties to each other are used, the email address and the address of residence/residence. It is the obligation of the Party to notify the other Party immediately of any changes to its contact details. Until such time as the other Party is notified of a change in contact details, the contact details provided shall be deemed to be correct.

If any provision or part of these GTC or the Contract is or becomes invalid or ineffective, the validity and effectiveness of any other provision or the remainder of the relevant provision shall not be affected. The parties undertake to replace such invalid or ineffective provision with a provision to which they would have agreed had they been aware of such invalidity or ineffectiveness.

If any provision, part, or portion of these GTC is or becomes invalid, ineffective or unenforceable, the remainder of the relevant provision or the remainder of the provision of the GTC shall not be affected thereby.

These GTC are valid and effective from 20.7.2023.