deepcloud

General Terms and Conditions of DeepCloud Corporation for the use of DeepID (January 2024)

1. General information

1.1 These are the General Terms and Conditions (**GTC**) of DeepCloud Corporation, Abacus Platz 1, 9300 Wittenbach, Switzerland (**DeepCloud**) for the use of the DeepID service and the associated DeepID app (**DeepID**).

1.2 DeepID enables the identification of a natural person (**Identification**), the invitation of additional persons for purposes of their Identification (to enable them to verify an organisation in their capacity as authorised signatories), the **Authorisation** of certain declarations of intent (such as the approval of certain electronic signatures) or actions, as well as the **Self-Identification and Authentication** for certain applications of DeepCloud or third-party providers. For services used by a third-party provider using DeepID, a contract is concluded solely between the user of DeepID (**User**) and the respective third-party provider.

1.3 In these GTC, DeepCloud lays down rights and obligations as well as other relevant aspects related to the use of DeepID.

1.4 The User consents to these GTC during the Identification process in the DeepID app. By consenting, the User declares that they are the authorised owner of the means of self-identification (such as a smartphone, tablet) and that they have sole control over this means of self-identification, and that they aware of, consent to, and will comply with, the rights and obligations set out in the GTC. The User warrants that they are of legal age and have the necessary legal capacity to undertake to comply with these GTC. Minors between the ages of 16 and 18 require the consent of their parents or legal guardians.

2. DeepCloud services

2.1 With DeepID, DeepCloud provides the User with an Identification, verification, authorisation and self-identification service for various use cases.

2.2 DeepCloud provides the DeepID app for this purpose. It can be downloaded from the respective app stores.

3. Identification of the User using the DeepID app

3.1 Before using the functionalities of the DeepID for the first time, the User's identity must be confirmed. To do so, the User shall follow the steps provided for in the DeepID app. The User shall enter their nationality and place of residence and present a valid identity document. They confirm ownership and sole control of their device by entering the four-digit code sent to them by email in the DeepID app. During the process, they define their device PIN, whereby they can also optionally use the access protection of their device (such as device biometrics (fingerprint / facial recognition) or PIN code) for the DeepID login.

3.2 After complete confirmation of the User's identity with the help of a valid identity document and further checks, where applicable, the User can use their DeepID through the app. The DeepID will be stored with all roles and attributes (with ID and access data).

3.3 When collecting and processing the User's data as part of the Identification process, biometric data of the User is also obtained from the photographs and videos created as well as from their identity document. This is the only way to reliably prove the User's identity. The User hereby expressly consents to the processing of their biometric data in order to establish their identity.

3.4 The detailed steps of the Identification process and details of which data is collected and processed in this process are set out in the DeepCloud Privacy Policy in the section "Data processing when using our mobile applications (apps)" under "DeepID service and DeepID Mobile App (Android and iOS)". DeepCloud has the right to adapt and modify the process for establishing identity for legitimate reasons. The User should therefore familiarise themselves with DeepCloud's Privacy Policy at regular intervals in order to keep abreast of any changes.

3.5 If the User wishes to use their confirmed DeepID identity for third party services, there may be certain restrictions or conditions depending on the service in question due to different terms of use. These must be complied with.

3.6 During the Identification process, the User must provide certain data and take photographs and videos of themselves and their identity document. Photographs and videos must be taken by the User themselves.

3.7 The User must check all data entered and provided by them for any read or spelling errors and must repeat any steps (such as the creation of photographs and videos) that have not been successfully completed upon request, otherwise the process cannot be concluded. The User is responsible for presenting complete, accurate and up-to-date personal data. Particularly the details of the User's identity, as indicated in the identity document and in the particulars provided by the User, shall be confirmed and corrected if necessary.

3.8 The User's device must be registered as their means of self-identification for the use of DeepID in accordance with the prescribed requirements. By doing so, the User confirms that they are the authorised owner of the means of self-identification (such as a smartphone, tablet) and have sole control over it.

3.9 In order to increase the security of the DeepID app, the User must comply with the requested security requirements (such as activation of access protection). For this purpose, the User shall specify a 6-digit PIN and activate the device's access protection (such as face ID, fingerprint) as well as the automatic screen lock in order to unlock the DeepID app. DeepCloud also provides the customer with a recovery code, which must be stored securely. In certain cases, that code is the only way to restore access to DeepID. There is a possibility of generating a new restore code.

3.10 Identifying the User requires compliance with certain requirements, which need to be verified and confirmed (such as identity document, photograph, video). The verification is carried out either fully automatically if the relevant requirements are met, otherwise only during DeepCloud's normal office hours. Users must schedule this accordingly if, for example, they wish to issue electronic signatures via DeepID within a certain prescribed time. To this end, DeepCloud deploys people who are specially trained to carry out the Identification process. Further checks may be necessary in certain cases. The User will be informed of this fact by customer support (e.g., within the DeepID app, by email).

3.11 Once they have confirmed their identity, the User can use the functionalities of DeepID, choose between different settings (such as changing profile details, device security settings, the PIN, updating the identity document) or log out of DeepID.

3.12 After logging out or if the wrong PIN has been entered 3 times, the User must follow the steps provided for by the DeepID app in order to be able to log back into the DeepID app.

3.13 In certain cases, the User must be identified again (**Re-identification**); for example, in the event of changes in the identity document used (such as photograph, name, gender, nationality, expiry of the period of validity of the identity document, loss of the identity document, changes in the NFC code), expiry of the period of validity of the identity determined for purposes of electronic signatures, change in device used as a means of self-identification for DeepID (such as in the case of theft, loss, change), as well as upon expiry of the period of validity of the DeepID identity and for any other circumstance relevant to establishing the identity of the User. To do so, the User will select the function "I already have a DeepID" or "renew a document" and follow the prescribed Identification process.

Copyright © 2024 by DeepCloud Corporation

3.14 DeepCloud is entitled to suspend or (permanently) discontinue an Identification process with the User at any time (e.g. in case of discrepancies in the information provided, infeasibility of the Identification) or to declare a confirmed DeepID identity invalid for legitimate reasons. This shall not entitle the User to any claims (such as damages) or other rights whatsoever.

4. Functionalities of the DeepID app

4.1 The User may view all functionalities in the DeepID app, including "scan QR code", "history", "organisations", "renew document", or "signatures". DeepCloud is entitled to change or discontinue existing functionalities at any time and to add new functionalities.

4.2 DeepID's scope of use consists of the provision of the software required for this purpose within the scope of the rights of use granted herein, including storage of the data. The identity confirmed by DeepID can be used both directly via the DeepID app and for other applications of DeepCloud as well as for the integration of software or applications, including from third-party providers.

4.3 The **functionality "scan QR code"** allows the User to scan a QR code and perform the action contained therein. This may include authorisation (such as the approval of a declaration of intent or action) or the self-identification for a DeepCloud or third-party service (such as login, confirmation of identity or system access).

4.4 The **functionality "Signature history"** lists the actions carried out via DeepID, such as the issue of an electronic signature.

4.5 The **"organisations" functionality** allows the identified User to invite additional persons to also go through the Identification process under DeepID. The purpose of invitations is to identify authorised signatories for an organisation, which makes it possible to verify the organisation. For this purpose, the user must open a DeepCloud account with DeepCloud. They can use it to invite people who then go through the DeepID identification process on their own, whereby the information provided is compared with public sources.

4.6 The **functionality "Renew document"** obliges the User to carry out a Re-identification in the event of relevant changes, of the User's own accord and in a timely manner. The User will be prompted to carry out a Re-identification if their identity document used for Identification or a certificate for their e-signature is no longer valid. This requires the User to repeat the Identification process. The User consents to this reminder in the DeepID app and by email.

4.7 The **functionality "Task"** allows the User to approve advanced and qualified electronic signatures that are provided to the User by a certification or trust service provider.

5. Possible uses of the DeepID identity

5.1 Together with the means of self-identification, the identity confirmed by means of DeepID can be used for authorisations and authentications for different purposes.

5.2 A request for use is made by a DeepService or by a third-party provider outside of the DeepID app (e.g. an invitation to issue an electronic signature) provided that the respective terms and conditions of the third-party provider or of DeepCloud for this service are accepted and complied with.

5.3 If the User does not yet have a valid Identification when making a request, they will be asked to identify themselves. If the User already has a valid Identification but the device used is new or the identity documents have to be renewed (after a maximum of 5 years or after their expiry, whichever comes first), a Re-identification must be carried out or the documents must be renewed.

5.4 The specific action required depends on the service and mode of use chosen. DeepID merely enables the use of the other service. For the third-party services used by the User using the DeepID identity (e.g. as a means of identification when registering for secure access or to issue an electronic signature), a contract is created between the User and the respective third-party provider for this service. The contractual terms of these third-party providers may impose restrictions on the use of DeepID for their services.

5.5 The prerequisite for the use of the third-party service is that the User has successfully identified themselves via the DeepID app, the DeepID identity is accepted by the third-party provider in question and is connected to DeepID, and that the User grants approval for each individual request.

5.6 The DeepID app transfers the data collected during the Identification process to DeepCloud and/or the data processors involved in the Identification process as well as – in case of a request – the required data to an authorised third-party provider to authenticate the User and carry out the requested action. This process may involve the exchange of information with or between systems of a third-party provider or data may be synchronised with them. The parties involved are expressly granted the necessary access; the exchange between the respective systems as well as the processing of the data is expressly permitted. In the process, personal data, documents and transaction data may be transmitted and processed. The User hereby expressly consents to this.

5.7 The authorisation or authentication process for a service is as follows: The User receives a request from the respective service (by email, push notification, SMS, etc.) in order to grant approval within the DeepID app on the User's means of self-identification. There is a certain timeframe within which to do this, which can vary depending on the service. After logging into the DeepID app, the User can grant the requested approval, such as an electronic signature or other action (e.g. access to applications or logins, sharing of data). As soon as the User grants approval, this information will be digitally signed using a cryptographic key stored on the means of self-identification, and the respective service provider will receive confirmation by encrypted transmission that approval was sent from the authorised device (the service provider can check the signed information using the public cryptographic key). It can therefore be safely assumed that approval was granted by the correct person and the requested act can be carried out.

5.8 If the User has not granted approval or has not granted it in time, the service provider will be informed that approval has not been granted and that there is no authorisation or that the authentication has not been successful. DeepID only authorises or authenticates the User for services provided by third-party providers that accept the DeepID identity. If the User does not authorise the requested action or does not authorise it in time, the User is responsible for any resulting consequences.

5.9 The DeepID app supports multi-factor authentication. This legitimises the desired device as an additional factor by means of the Identification process and allows it to be used to confirm the requested action. Two-factor authentication is a security process whereby the User provides two different features to identify themselves or to make an explicit declaration of intent. In the case of DeepID, being in possession of the means of self-identification and, in the case of authorisation or self-identification, the DeepID app constitutes the second component to confirm the action.

5.10 During the Identification process, the device used is identified by way of the AI-based, user-centric authentication suite and can thus be used for authorisations and self-identifications in communications with third-party providers.

6. Possible uses of the DeepID identity for electronic signatures

6.1 The DeepID identity can be used to authorise and authenticate advanced and qualified electronic signatures. Recognised certification or trust service providers (providers) may issue advanced certificates for advanced electronic signatures (AES) and qualified certificates for

Copyright © 2024 by DeepCloud Corporation

qualified electronic signatures (QES) with qualified timestamps (certification or trust services) to an identified person. A User must identify themselves once in order to be able to sign several times, unless a Re-identification is necessary.

6.2 The DeepID app enables the necessary verification of the identity of this person (**Signatory**) for this purpose. These certification or trust services are provided by these providers in accordance with the Swiss Federal Act on Qualified Electronic Signatures (**ZertES**) and the EU Regulation on electronic identification and trust services for electronic transactions in the internal market (**eIDAS Regulation**).

6.3 DeepCloud is a registration body for QES and AES appointed by those providers. It is subject to the applicable DeepCloud Trust Service Practice Statement (TSPS) as amended from time to time. DeepCloud's compliance with the TSPS has been assessed and confirmed by a recognised Conformity Assessment Body (CAB) in Switzerland and the EU. DeepCloud has been certified according to the following conformity assessment scheme (Norm of Accreditation System): ISO 17021-1:2015 (for ZertES) and ISO 17065-1:2013 (for eIDAS VO) for "Remote Identification Certification" according to the requirements of ZertES, VZertES, TAV (SR 943.032.1), EU eIDAS VO, ETSI TS 119 461, ETSI EN 319 401 and ETSI EN 419 241-1.

6.4 As part of a certified Identification process with DeepID, DeepCloud verifies the identity of the Signatory, without the latter having to be present. In doing so, the User must fully comply with the instructions and always provide complete, accurate and up-to-date information. During the Identification process, the User may be asked to provide different documents depending on what the Identification is used for.

6.5 If an Identification was not successful, DeepCloud has the right to rule out a new attempt at Identification for a limited time or permanently. If the Identification meets all the necessary requirements, the DeepID identity will be registered for the creation of AES and QES. This registration will be verified prior to each commissioning by the Signatory.

6.6 In the event that AES or QES are commissioned, special rules apply before they can be approved by the Signatory. The Signatory must have their place of residence in Switzerland, the EU or the EEA and must confirm this when commissioning the creation of QES and AES. If this is not the case, the User may not use these services. The User is fully liable for any consequences of non-compliance with these requirements. In such cases, DeepCloud and the respective third-party providers exclude any warranties and liability with regard to their services.

6.7 The only identity documents that are permitted for purposes of Identification if a QES or an AES is commissioned are those approved by the providers of the certification or trust services for these purposes. These will be indicated during the Identification process. The identity documents must be valid at the time of Identification. The list of acceptable identity documents may change so that Re-identification may be required. Only the identity documents prescribed by the providers of the certification or trust services may be used for Identification and upon commissioning by the Signatory. They also specify which electronic signatures can be created and whether the Signatory must undergo an Identification process for each electronic signature (one-time signature) or whether the Signatory can create multiple electronic signatures during a specified period after the Identification process. This may, where appropriate, result in the need for Re-identification of the Signatory.

6.8 The Signatory will be invited to issue an electronic signature by means of a service (such as DeepSign, the signature service of DeepCloud). Depending on the desired type of signature, either a simple electronic signature (SES) or a QES or AES will be granted in accordance with the applicable legal provisions (ZertES or the eIDAS Regulation). Any form of use other than commissioning the certification or trust services offered by these providers is not permitted (restriction on use).

6.9 DeepCloud registers and stores the information collected about the User during the DeepID Identification process and the data required during the approval process for the certification and/or trust services in accordance with the contractual provisions and applicable regulations.

6.10 The providers are responsible for drawing up the certificates and for the cryptographic key pair for the signature process after the User has granted approval. The Signatory may use this certificate together with their activation data using DeepID. As soon as the Signatory has issued their approval in DeepID following a commission to that end (having accepted the terms of use of the respective provider and having confirmed the required place of residence), the respective provider will prepare the AES or QES for them on the basis of this certificate. For each signature process, a new digital certificate (with a short period of validity) with a new key pair will be created.

6.11 The confirmed Identification via DeepID allows the User to use the respective certification or trust service for the period of validity of the Identification for all signature applications that DeepCloud and the providers have connected to DeepID in order to create a valid QES or AES without the need for a new Identification, as long as this is permitted by the respective signature application and the period of validity of the certificate.

6.12 DeepCloud will verify the identity of the Signatory, authenticate them and allow them to give authorisation.

6.13 The providers are entitled to verify compliance of DeepCloud with its contractual obligations regarding the Identification, authorisation and authentication for AES and QES by way of an audit. As part of the audit, data of the Signatory may also be inspected. The providers may arrange for this to be carried out by their own employees or by third parties and share the results with the relevant conformity assessment bodies and regulatory authorities.

7. Rights of Use, Intellectual Property Rights

7.1 DeepCloud grants the User a personal, non-exclusive, non-transferable, non-assignable, simple, right of use of the software deployed when using DeepID for the duration of the user relationship for personal use on the User's means of self-identification; this right of use is limited in terms of space and time. This means that only the User themselves may use DeepID for their own benefit. The scope of the right of use is set out in these GTC.

7.2 Users are prohibited from making DeepID accessible or available to third parties. Furthermore, the User is not entitled to use the relevant software for any other use than that offered by DeepCloud herein.

7.3 DeepCloud has the right to provide and license interfaces for the purpose of exporting data from DeepID to other systems, where data may be processed further. The User may use such interfaces to services, including third-party services, only within the scope of this user relationship. This also applies if interfaces are used for the purpose of using data via another system. The User shall comply with the usage options and limits specified by DeepCloud in this respect and is not entitled to circumvent them by technical means of evasion.

7.4 The software used by DeepCloud may be subject to export control regulations and other laws. If this is the case, the software must not be exported, re-exported, or transferred to certain countries or individuals or entities who are prohibited from receiving certain export goods (including those who are listed on the relevant sanctions lists for individuals or entities). The User must comply with any local provisions in connection with the use of services with encryption technology as used for DeepID.

7.5 With regard to third-party software used, the licensing provisions of this third party shall apply.

Copyright © 2024 by DeepCloud Corporation

7.6 The User shall immediately inform DeepCloud if third parties assert intellectual property rights (e.g., copyrights or patent rights) against the User that relate to software when using DeepID. The User shall not take any legal action without DeepCloud's authorisation and shall not of their own accord acknowledge any claims of the third party without DeepCloud's consent. DeepCloud will take all necessary defence measures, such as defending against third-party claims, at its own expense, unless they are based on the User's conduct in breach of duty.

7.7 The User acknowledges that their app store is under no obligation to perform maintenance and support services related to the DeepID app. If a third party asserts that DeepID or ownership of the DeepID app violates its intellectual property rights, then DeepCloud, and not the app store, shall be responsible for defending against such claims.

7.8 All intellectual property rights in DeepID (including the software used for this purpose), in content, texts, images, photographs, videos, logos, or other information of DeepCloud, including its websites, belong exclusively to DeepCloud or the relevant rights holders. Written consent of the rights holders must be obtained in advance for any further use of any intellectual property rights. All DeepCloud documentation made accessible in the context of the user relationship is considered its intellectual property.

7.9 DeepCloud has the right to process photos and videos for the identification process or as a selected profile picture without entitling the User to any claim to remuneration.

8. Terms of use and obligations of the User

8.1 The User has a device that serves as an authorised means of authentication and confirms their identity with the DeepID app. The use of the DeepID app requires that the device used permanently fulfils the necessary device and system requirements.

8.2 The User is responsible for their means of self-identification, which must be available for the sole use of the User. As long as they wish to use DeepID, the User is prohibited from leaving the means of self-identification to third parties.

8.3 The software of the means of self-identification must be kept up to date. In particular, the updates provided by the manufacturer (updates, upgrades, service packs, hotfixes, etc.) as well as the current version of the DeepID app provided by DeepCloud from time to time must be installed.

8.4 The User undertakes to use all reasonable and up-to-date means of protecting their means of self-identification against attacks and malware ("viruses", "worms", "Trojan horses", and similar), particularly by using state-of-the-art software from official sources.

8.5 The means of self-identification must be used in accordance with the manufacturer's contractual terms and conditions and appropriately, in particular by refraining from any actions that encourage or cause risks by modifying or replacing the device software installed by the device manufacturer (e.g., by means of "jailbreaking/rooting" or other software that violates the terms and conditions of use prescribed by the manufacturer). The User undertakes to install software (particularly other apps) on their means of self-identification from trustworthy sources only.

8.6 The operating system on the means of self-identification must correspond to the official version provided by the manufacturer and be compatible with the DeepID app, otherwise the DeepID app will not be supported. DeepID requires an active connection to the network of a mobile service provider. The supported versions of the respective operating system are displayed in the corresponding app stores.

8.7 The User is obliged at all times during the Identification process and when using their confirmed identity to provide complete, accurate and up-to-date information and to promptly update any changes. DeepCloud reserves the right to request proof of the accuracy of the information provided by the User and to carry out verifications itself. The duty to inform relates in particular to the following circumstances: name, nationality, gender, place of residence, contact details such as email address, telephone, change of identity document and means of self-identification in case of loss, theft, change, or any other factual or legal situation that could influence the Identification of the User and the user relationship with DeepCloud.

8.8 The possible uses of the identity confirmed via the DeepID app and the respective prerequisites for its use are set out in the respective contract that the User enters into with DeepCloud or a third-party provider.

8.9 DeepID can only be used for a service that accepts its identity as confirmed via DeepID. In addition, the User must accept the respective contractual terms of these services, which apply separately. The User must strictly comply with any additional prerequisites.

8.10 The User undertakes to use certain services only if they meet the prerequisites. Thus, the User is only permitted to commission a provider to create an AES or QES if they have used the required identity documents for purposes of Identification and live at the required place of residence. Should the User provide confirmations in that regard even though they are not true, DeepCloud and the respective third-party providers exclude any warranties and liability for the services provided, such as issuing a QES or AES, and reserve the right to take appropriate legal action against the User. In such a case, the User shall indemnify both DeepCloud and the corresponding third-party provider against all third-party claims arising from the incorrect information provided by the User.

8.11 As regards the use of DeepID, knowledge of the DeepID PIN, of the restore code and/or the device's access protection, on the one hand, and possession of the means of self-identification, on the other, constitute personal security elements, whose protection is the responsibility of the User.

8.12 To ensure protection against misuse of DeepID and the confirmed identity, no trivial or common combinations (e.g. 123456) or other number combinations that can be determined with little effort – such as telephone number, date of birth, car registration number – may be chosen when the DeepID or device PIN is selected.

8.13 The User is responsible for protecting their access data, in particular for choosing a secure PIN, securing their recovery code, as well as for protecting against access by third parties to the authentication means and the DeepID app installed on it. Security-relevant information must be kept secret and must not be disclosed to any other person (including the respective third-party provider). Any records of access data must be stored safely and separately from the means of self-identification or encrypted and protected against third-party access.

8.14 If the User knows or has reasonable grounds to suspect that a third party has knowledge of their access data, they must change it immediately in the device settings and, if necessary, promptly inform DeepCloud of the incident.

8.15 If the means of self-identification was stolen or lost, or if the User knows or suspects that another person has gained knowledge of the access data (compromise), they have the following obligations: the User must arrange for the DeepID to be frozen by notifying support, they must immediately refrain from using their confirmed identity and services that require the User's authorisation and authentication, such as the creation of AES and QES, they must immediately invalidate the certificate for the creation of signatures, and they must modify their access data if necessary (e.g. in the case of DeepCloud in the DeepID app, in the DeepCloud account or at the respective third-party provider).

Copyright © 2024 by DeepCloud Corporation

8.16 As soon as there are changes made to a device used for self-identification (e.g. the device itself, the email address) or to the relevant data for the User's Identification (such as name, nationality, other attributes), the User shall immediately notify DeepCloud either by using "I already have a DeepID", "renew document" or by adjusting the data in their profile. If this is unsuccessful, the User shall immediately contact DeepCloud support. DeepCloud will then take the relevant steps and inform the providers of certification or trust services so that the User's confirmed identity and the certificate can be declared invalid. The User will take the necessary steps with their other service providers concerned.

8.17 The User undertakes to check the information provided about their identity on a continuous basis following its confirmation and to promptly report any discrepancies as well as any suspicions of misuse of the DeepID identity to DeepCloud.

8.18 Users are strictly prohibited from using DeepID for illegal purposes; they must not use fake or third-party identity documents for the Identification process. In such cases, DeepCloud reserves the right to prohibit the use of DeepID and to take legal action against the User.

8.19 If the User breaches their duties, they shall assume all risks that are increased or caused by the breaches of duty.

8.20 If the User does not consent to the data processing carried out by DeepID, the User shall refrain from using DeepID.

8.21 Whether third-party providers or DeepCloud charge a fee when providing services using DeepID depends on the contract between the User and DeepCloud or the respective service provider. In addition, data transfer costs may be incurred by the User's mobile service provider, for which the User is responsible.

9. Support

9.1 Support is only provided during DeepCloud's usual support hours (as in the form of forums or FAQs, by email). DeepCloud support can be reached at support @deepid.swiss

9.2 If there are any anomalies or security incidents in the relevant Identification, authorisation or authentication processes, the User must contact DeepCloud without delay.

9.3 DeepCloud does not warrant that Identifications, authorisations, or authentications (such as the commissioning of an electronic signature) can be performed in a timely manner at any time.

9.4 Support is also available to answer any questions about the technical requirements, the functionalities of DeepID, or in the event of faults in its use.

9.5 DeepCloud retains the right to charge for its services within the framework of support according to its hourly rates current at any time. Details on support and the specific support hours can be found on DeepCloud's websites.

10. Operating life of the confirmed identity

10.1 Taking into account the requirements of these GTC as well as the GTC of DeepCloud for a DeepCloud account, the User may use their confirmed identity using the means of self-identification chosen during Identification for a maximum period of five years for certification or trust services; this period is reduced accordingly if the identity document presented by the User expires earlier, the certificate of the providers of the certification or trust services expires, or any other circumstance requiring Re-identification occurs.

10.2 For authentications other than for certification or trust services, there may also be time limits, including due to the terms of use of third party providers. In all other cases, it is at the discretion of DeepCloud to define the operating life for a confirmed Identification, including any necessary Re-identification of the User.

11. Data Protection and Confidentiality

11.1 DeepCloud will comply with the provisions of applicable data protection law in its data processing. Within its area of responsibility, it shall organise its operations in such a way that it meets the special requirements of data protection. It takes technical and organisational measures that comply with the requirements of data protection law to ensure that the User's data is adequately protected against misuse and loss.

11.2 DeepCloud will treat as confidential all not commonly known information it learns about the User and their business relationships. It will only make this information accessible to third parties insofar and to the extent permitted by the user relationship or by law, if the User has expressly permitted it, or this is necessary due to an official or judicial order or a statutory obligation. It shall also ensure compliance with the duty of confidentiality of all employees and third parties involved in connection with this user relationship.

11.3 In addition to the data collected in accordance with the applicable regulations and required for the provision of a certification or trust service, DeepCloud collects, stores, and processes all data and information that it requires to provide its services to the User. The handling of such data is governed not only by the applicable laws but also by the certification guidelines for the certification and trust services.

11.4 DeepCloud will involve third parties for its services in connection with the Identification of the User. These third parties perform commissioned data processing on behalf of DeepCloud. DeepCloud has entered into the necessary data protection agreements with these third parties.

11.5 The handling of personal data by DeepCloud is described in its Privacy Policy on its website. The currently published version shall apply.

11.6 Based on the data provided by the User during the Identification process and collected by DeepCloud, the respective provider of a certification or trust service issues, upon request and with the express consent of the User, a qualified or advanced certificate containing the necessary information about the User.

11.7 DeepCloud will store the data described above as well as the means by which the identity was verified in accordance with contractual and statutory retention obligations, also to enable the User to use a certification or trust service. In the case of QES under ZertES, the retention period is 11 years and in the case of the eIDAS Regulation, 30 years, in the case of AES – both under ZertES and under the eIDAS Regulation – the retention period is 7 years. Due to the maximum period of validity of an Identification of 5 years – taking into account an additional safety period of one year – this results in retention periods for QES of up to 17 years under ZertES and up to 36 years under the eIDAS Regulation, and for AES of up to 13 years – both under ZertES and under the eIDAS Regulation.

11.8 These retention periods ensure that the correctness of an electronically-signed document continues to be verifiable in the years following its creation. All relevant information on the data issued and received will be recorded and stored in such a way that it is available to provide relevant evidence, in particular in court proceedings, and to ensure the continuity of the certification or trust service.

11.9 DeepCloud will delete the necessary data after the expiry of at least 17 years in the case of ZertES and after the expiry of at least 36 years in the case of the eIDAS Regulation after completion of the Identification process. In the case of an Identification following a request for an AES, DeepCloud will delete this data after the expiry of at least 13 years after the completion of the Identification process – both under ZertES and under the eIDAS Regulation. The data may only be deleted after expiry of existing retention obligations.

11.10 For purposes of notifying the User that the operating life of the confirmed identity and a possible signature permit is about to expire, DeepCloud will save the time when this will occur and will notify the User of this circumstance in writing or in another manner (e.g. within

Copyright © 2024 by DeepCloud Corporation

its DeepID app, an existing DeepCloud account or by email) to enable the User to perform a Re-identification in a timely manner. The User hereby expressly agrees to this.

11.11 If data may be required to defend any third-party providers or DeepCloud against any claims for damages, this will be kept for the duration of any statute of limitations.

11.12 The User has the option of releasing data, documents and information to third parties for various purposes within the scope of an authentication using DeepID, with or without the use of third-party services, such as the transmission of data to a potential employer, an insurance company, or a bank. The User may also use their confirmed identity to authenticate themselves as an organisation's authorised representative. The User should refer to the data protection provisions of these third-party providers for details on how they process the User's data and how the User may influence such processing. DeepCloud is not responsible for this data processing.

12. Involvement of third parties

12.1 DeepCloud may at any time engage third parties for the proper performance of its obligations, which the User hereby approves. These third parties are carefully selected and commissioned by DeepCloud. They are bound by instructions and are regularly monitored. In particular, hosting providers and service providers offering server solutions in Switzerland will be brought in, whose registered office is in Switzerland or the EU.

13. Warranty

13.1 DeepCloud will provide the services to the User under these GTC faithfully and carefully.

13.2 DeepCloud does not warrant, either generally or at any specific point in time, the uninterrupted or fault-free operation of DeepID (including the DeepID app) and the use of its functionalities. Any warranties on the part of DeepID (including the app used, software, hosting, etc.) are excluded to the extent permitted by law. DeepID is made available "as is".

13.3 DeepCloud endeavours to provide DeepID without any interruptions. However, it is not possible to guarantee uninterrupted availability. DeepCloud may temporarily restrict or interrupt the availability of DeepID at any time, particularly if this is necessary in view of capacity limits, the security or integrity of the servers, or in order to carry out technical maintenance or repair measures, or if this serves the proper or improved provision of the services. In doing so, it endeavours to take the User's interests into account and will notify the User, to the extent possible, of any interruptions with reasonable notice.

13.4 Services provided free of charge are provided without any claims to performance or warranty. DeepCloud may discontinue, modify or require payment for services offered free of charge at any time and without prior notice. This does not give rise to any claims by or rights of the User.

13.5 No guarantees or warranties have been given that DeepID will meet the individual needs of the User regardless of whether these have been communicated to DeepCloud. Statements on the DeepCloud website or other promotional statements by DeepCloud do not constitute representations or warranties.

13.6 By carrying out the Identification process as part of a certification or trust service, DeepCloud – in the role of registration body – must meet the requirements imposed on such services by law and technical standards. DeepCloud employs appropriate state-of-the-art security measures to this end. DeepCloud is responsible for assessing and specifying the requirements arising from applicable laws and regulations.

13.7 The User acknowledges that, despite all efforts on the part of DeepCloud, the use of state-of-the-art technology and security standards, and checks carried out by an independent body regarding compliance with technical standards and legal provisions, no guarantee or warranty is given as to the absolute security and absence of any faults of the Identification process and of the certification and/or trust services.

13.8 DeepCloud offers no guarantee or warranty that an Identification, verification, authorisation, or authentication can be carried out and concluded at any time, and hereby excludes any liability for possible loss or damage suffered as a result of delayed, omitted, or unsuccessful Identification, verification, authorisation, or authentication to the extent permitted by law.

14. Liability and force majeure

14.1 DeepCloud's liability is limited to damage caused wilfully or through gross negligence, as well as injury to life and limb. Any further liability is expressly excluded, in particular for slight negligence, consequential damage, financial loss, immaterial and indirect damage (such as the total or partial loss of documents or data, additional expenses, loss of profit, damage due to disruptions to availability, claims by third parties, etc.) and for auxiliary persons (including third parties brought in). The same exclusion applies to any no-fault liability.

14.2 DeepCloud does not assume any liability for the continuous availability of the DeepID app, its support, the processes offered and possible uses, as well as the individual functionalities of the DeepID app.

14.3 DeepCloud will not be liable to the User for the proper functioning of third-party systems, particularly not for the hardware and software used by the User or for any third-party service where the User uses their confirmed identity for purposes of authentication.

14.4 DeepCloud shall not be liable if provision of its service is temporarily interrupted, impaired in whole in or in part, or impossible for reasons of *force majeure*. *Force majeure* events shall be deemed to include, in particular, especially intense natural disasters (avalanches, floods, landslides, etc.), armed conflicts, riots, unforeseeable administrative restrictions, as well as pandemics and epidemics. If DeepCloud is unable to meet its obligations, their performance or the deadline for performance will be postponed accordingly in line with the event that has occurred. DeepCloud will not be liable for any loss or damage suffered by the User by the postponement of the performance.

14.5 Any claims shall be asserted by the Owner within six months after performance of the services.

14.6 The above disclaimers and limitations of liability shall apply to contractual as well as non-contractual claims of the Owner.

14.7 DeepCloud shall not be liable for any loss or damage resulting from the non-contractual or unlawful use of DeepID by the User.

14.8 Existing mandatory liability rules based on product liability laws, consumer protection laws, ZertES, or the eIDAS Regulation as well as their implementing legislation are excluded from these limitations and exclusions of liability. In such cases, any limitations and exclusions of liability provided for in those provisions shall also apply to DeepCloud.

14.9 DeepCloud has set out its liability to the User with respect to the use of DeepSign in its General Terms and Conditions for use of the DeepCloud account and the DeepServices.

14.10 In particular, the User will be liable and indemnify and hold DeepCloud harmless from and against any (damage) claims in connection with the use of DeepID that are based on the fact that the User violates applicable laws and regulations, public policy, these GTC or contractual provisions of DeepCloud or third-party providers such as certification and/or trust service providers.

Copyright © 2024 by DeepCloud Corporation

15. Changes to these GTC

15.1 DeepCloud reserves the right to change and supplement the DeepID app and these GTC at any time. In particular – in the event of amendments to the ZertES, the eIDAS Regulation and their respective implementing legislation, as well as in the event of orders issued by the competent approval, confirmation and regulatory authority or an independent entity verifying the signatures – certification or trust service providers may be forced to adapt existing certification guidelines and, consequently, DeepCloud may have to adapt these GTC in its role as registration body. Before the changes to DeepCloud begin to apply, the User will be informed of any changes or will be notified of the latest provisions when using a service. This information may be provided in a manner that is appropriate for the User.

15.2 Such changes shall be considered accepted unless the User gives notice of termination of the contractual relationship before the effective date of the new GTCs, in any case when using DeepID after the new provisions come into force, despite the possibility of being aware of the changes.

15.3 The User may also refuse to accept the new terms and conditions by refraining from using DeepID (such as the confirmed identity, authorisations and authentications by DeepID) in accordance with these GTC from the date of application of the amended terms and conditions.

15.4 In the event that individual provisions of these GTC prove to be invalid or null and void, this will not render the remaining provisions invalid or null and void. Instead, they shall be replaced by provisions that most closely reflect their economic purpose. The same applies if there is a gap in the terms of use.

16. Effective Date, Term and Termination

16.1 The user relationship with the User via DeepID takes effect upon acceptance of these GTC within the DeepID app and remains in effect for an indefinite period.

16.2 DeepCloud is entitled to terminate the user relationship at any time without stating reasons. At the time of termination, DeepCloud will freeze access to DeepID and the confirmed DeepID identity, terminate the use of the identity, and discontinue the technical communication to DeepServices or third-party services. This means, in particular, that all pending services as well as any associated status messages and information are no longer transported, executed, or available.

16.3 The User may at any time refrain from using DeepID and delete the DeepID app from their means of self-identification. The User themselves is responsible for planning the termination of the use of DeepID and their DeepID identity. The User must contact DeepCloud in order to block their DeepID identity or delete data.

16.4 Upon termination of the user relationship, the User will no longer have access to their confirmed identity and the use of DeepID.

17. Governing law and place of jurisdiction

17.1 All legal relationships in connection with these GTC are governed by Swiss law to the exclusion of the conflict of law rules and the Vienna Convention on Contracts for the International Sale of Goods, regardless of whether a User uses DeepID in their capacity as a consumer or for a company.

17.2 If the User is a consumer with habitual abode in the EU/EEA, the mandatory consumer protection law of the EU/EEA State applicable to their habitual abode in the EU/EEA will apply in addition. The same applies in the case of a country to which the eIDAS Regulation applies.

17.3 Without prejudice to mandatory jurisdictions, the City of St. Gallen shall have exclusive jurisdiction for all disputes arising from or in connection with these GTC.

18. Final provisions

18.1 The User may not transfer any rights from this user relationship to third parties. DeepCloud is entitled to transfer all rights and obligations from this user relationship to third parties. The User hereby agrees to any assignment or transfer.

18.2 In the event of any dispute, the parties shall endeavour to reach an amicable settlement to the dispute.

18.3 All references to persons in these GTC are to be understood as gender-neutral.

18.4 These GTC are available in different languages. In case of discrepancies or contradictions, the German version shall prevail.

19. Mandatory EU/EEA consumer protection law

19.1 The time limit for objecting to amendments to these GTC for Users to whom mandatory EU/EEA consumer protection law also applies is 4 weeks.

19.2 DeepCloud can terminate the user relationship at any time by giving 30 days' notice to take effect at the end of any month.

19.3 If the User is a consumer in the EU/EEA, DeepCloud is neither willing nor obliged to participate in a dispute settlement procedure before a consumer arbitration body. Consumer information according to Regulation (EU) No. 524/2013: for the purpose of out-of-court settlement of consumer disputes, the European Commission has established an online dispute resolution platform (ODR platform). The ODR platform is available under https://ec.europa.eu/consumers/odr/main/index.cfm?event=main.home2.show&lng=EN.

Copyright © 2024 by DeepCloud Corporation