Conditions générales de DeepCloud SA pour l'utilisation de DeepID (janvier 2024)

1. Généralités

1.1 Le présent document constitue les conditions générales (**CG**) de DeepCloud SA, Abacus-Platz 1, 9300 Wittenbach, Suisse (**DeepCloud**) pour l'utilisation du service DeepID et de l'application DeepID correspondante (**DeepID**).

1.2 DeepID permet d'établir l'identité d'une personne physique (**identification**), d'inviter d'autres personnes à l'identifier (afin qu'elles puissent, en tant que personnes autorisées à signer, vérifier une organisation), l'**autorisation** de certaines manifestations de volonté (comme la validation de certaines signatures électroniques) ou certains actes, ainsi que la **légitimation et l'authentification** des utilisateurs dans certaines applications de DeepCloud ou de prestataires tiers. Pour les prestations utilisées par un prestataire tiers dans le cadre de l'utilisation de DeepID, un contrat est conclu exclusivement entre l'utilisateur de DeepID (**utilisateur**) et le prestataire tiers concerné.

1.3 Par les présentes CG, DeepCloud règle les droits et obligations ainsi que d'autres aspects déterminants liés à l'utilisation de DeepID.

1.4 Le consentement de l'utilisateur aux présentes CG a lieu dans le cadre du processus d'identification au sein de l'application DeepID.L'utilisateur déclare ainsi être le détenteur autorisé du moyen de légitimation (tel qu'un smartphone, une tablette), avoir le contrôle exclusif sur ce moyen de légitimation, connaître les droits et obligations prévus par les CG, les accepter et s'engager à les respecter. Il garantit qu'il est majeur et dispose de la capacité civile nécessaire pour s'engager à respecter les présentes CG. Les mineurs âgés de 16 à 18 ans doivent veiller à obtenir le consentement nécessaire des personnes investies de l'autorité parentale.

2. Prestations de DeepCloud

2.1 Avec DeepID, DeepCloud met à la disposition de l'utilisateur un service d'identification, de vérification, d'autorisation et de légitimation pour différents cas d'application.

2.2 À cet effet, DeepCloud offre l'application DeepID, qui peut être téléchargée depuis les magasins d'application correspondants.

3. Identification de l'utilisateur au moyen de l'application DeepID

3.1 Avant la première utilisation des fonctionnalités de DeepID, l'identité de l'utilisateur doit être confirmée. Pour ce faire, l'utilisateur doit suivre les étapes prévues dans l'application DeepID. Il indique sa nationalité et son domicile et présente une pièce d'identité valable. Il confirme la possession et le contrôle exclusif de son appareil en saisissant dans l'application DeepID le code à quatre chiffres qui lui a été envoyé par e-mail. Au cours du processus, il définit son NIP d'appareil, et peut également utiliser, en option, le contrôle d'accès de son appareil (comme la biométrie d'appareil (empreintes digitales / reconnaissance faciale) ou le code NIP).

3.2 Après confirmation complète de l'identité de l'utilisateur au moyen d'un document d'identité valable et des éventuels contrôles, il peut utiliser sa DeepID via l'application. Son identité est enregistrée en tant que telle avec tous les rôles et attributs y relatifs (avec les données d'identification et d'accès).

3.3 Lors de la saisie et du traitement des données de l'utilisateur dans le cadre du processus d'identification, ses données biométriques sont également extraites et comparées à partir des photos et des vidéos réalisées ainsi que de son document d'identité. Il s'agit du seul moyen de prouver son identité de manière fiable. Par la présente, l'utilisateur consent expressément au traitement de ses données biométriques aux fins de son identification.

3.4 Le déroulement détaillé du processus d'identification et les données collectées et traitées dans ce cadre sont décrits dans la Déclaration sur la protection des données de DeepCloud à la section «traitements de données lors de l'utilisation de nos applications mobiles (applications)» sous «service DeepID et application mobile DeepID (Android et iOS)». DeepCloud a le droit d'adapter et de modifier les processus d'identification en présence de motifs légitimes. Pour cette raison, l'utilisateur devrait consulter à intervalles réguliers la https://www.deepcloud.swiss/fr/politique-des-donnees/ de DeepCloud afin de prendre connaissance d'éventuelles modifications.

3.5 Si l'utilisateur souhaite utiliser son identité DeepID confirmée pour des services de prestataires tiers, certaines restrictions ou conditions peuvent éventuellement s'appliquer selon le service concerné en raison de l'existence de conditions d'utilisation différentes. Celles-ci doivent être respectées.

3.6 Dans le cadre du processus d'identification, l'utilisateur doit indiquer certaines données et créer des photos et des vidéos de lui-même et de son document d'identité. Les photos et les vidéos doivent impérativement être prises par l'utilisateur en personne.

3.7 L'utilisateur est tenu de vérifier toutes les données qu'il a saisies et qui s'affichent sur son écran pour déceler des erreurs de lecture ou de frappe ou, sur demande, de répéter les étapes qui n'ont pas abouti (telles que la création de photos et de vidéos), faute de quoi le processus ne pourra pas être achevé. Il est responsable de la présentation de données complètes, exactes et à jour concernant sa personne. En particulier, les détails relatifs à son identité, tels qu'ils ressortent de sa pièce d'identité et des indications de l'utilisateur, doivent être confirmés et corrigés si nécessaire.

3.8 Il est indispensable que l'appareil de l'utilisateur soit enregistré comme son moyen de légitimation pour l'utilisation de DeepID conformément aux exigences prescrites. L'utilisateur confirme ce faisant qu'il est le détenteur autorisé du moyen de légitimation (tel qu'un smartphone, une tablette) et qu'il en a le contrôle exclusif.

3.9 Afin d'accroître la sécurité de l'application DeepID, l'utilisateur est tenu de respecter les consignes de sécurité requises (comme l'activation du contrôle d'accès). Il fixe à cet effet un NIP à six chiffres, active le contrôle d'accès de l'appareil (p. ex. face ID, empreintes digitales) ainsi que le verrouillage automatique de l'écran pour débloquer l'application DeepID. Il reçoit en outre de DeepCloud un code de récupération qui doit être conservé de manière sûre. Seul celui-ci permet de récupérer l'accès à DeepID dans certains cas. Il est possible de générer un nouveau code de récupération.

3.10 L'identification de l'utilisateur requiert le respect de certaines exigences, qui doivent être vérifiées et confirmées (p. ex. document d'identité, photo, vidéo). La vérification s'effectue soit de manière entièrement automatique si les conditions requises sont remplies, soit uniquement aux heures de bureau habituelles de DeepCloud dans le cas contraire. L'utilisateur doit en tenir compte dans sa planification, par exemple s'il souhaite émettre des signatures électroniques dans un délai donné par le biais de DeepID. Pour ce faire, DeepCloud engage des personnes spécialement formées au processus d'identification. Des clarifications supplémentaires peuvent s'avérer nécessaires. Le cas échéant, l'utilisateur est informé par le biais du service d'assistance (par exemple dans l'application DeepID ou par e-mail).

3.11 Une fois son identité confirmée, l'utilisateur peut utiliser les fonctionnalités de DeepID, choisir entre différentes configurations dans les paramètres (p. ex. modification des données de profil, réglage de la sécurité de l'appareil, modification du NIP, actualisation du document d'identité) ou se déconnecter de DeepID.

3.12 Après la déconnexion ou 3 saisies erronées du NIP, l'utilisateur doit suivre les étapes prévues par l'application DeepID afin de pouvoir se connecter à nouveau à son application DeepID.

3.13 Dans certains cas, une nouvelle identification (**ré-identification**) de l'utilisateur est nécessaire, comme en cas de modification du document d'identité utilisé (photo, nom, sexe, nationalité, expiration de la durée de validité du document d'identité, perte du document d'identité, modifications du code NFC), en cas d'expiration de la durée de validité de l'identité constatée pour les signatures électroniques, de modification de l'appareil servant de moyen de légitimation pour DeepID (comme en cas de vol, de perte, de changement), ainsi qu'à l'expiration de la durée de validité de l'identité DeepID, et lors de toute circonstance pertinente pour l'identification de l'utilisateur. Pour ce faire, l'utilisateur doit choisir la fonction «J'ai déjà une DeepID» ou «Renouveler un document» et suivre le processus d'identification prescrit.

3.14 DeepCloud est en tout temps en droit de suspendre ou de mettre fin (de manière permanente) à un processus d'identification avec l'utilisateur (p. ex. en cas de contradictions dans les indications fournies ou d'impossibilité de procéder à l'identification) ou de déclarer invalide une identité DeepID confirmée pour de justes motifs. Il n'en résulte aucune prétention ni d'autre droit pour l'utilisateur (p. ex. des dommages-intérêts).

4. Fonctionnalités de l'application DeepID

4.1 L'application DeepID affiche toutes les fonctionnalités pour l'utilisateur, à savoir «Scanner un code QR», «Historique», «Organisations», «Renouveler un document» ou «Signatures». DeepCloud est en droit de modifier ou de mettre fin à tout moment aux fonctionnalités existantes et d'ajouter de nouvelles fonctionnalités.

4.2 L'étendue de l'utilisation du DeepID se compose de la mise à disposition du logiciel nécessaire à cet effet dans le cadre des droits d'utilisation qui y sont accordés, y compris l'enregistrement des données. L'identité confirmée par DeepID peut être utilisée aussi bien directement via l'application DeepID que pour d'autres applications de DeepCloud, ainsi que par l'intégration de programmes, de logiciels ou d'applications, y compris de prestataires tiers.

4.3 La **fonctionnalité «Scanner le code QR»** permet à l'utilisateur de scanner un code QR et d'exécuter l'action qu'il contient. Il peut s'agir d'une autorisation (telle que la validation d'une manifestation de volonté ou d'un acte) ou d'une légitimation pour un service DeepCloud ou un service de fournisseur tiers (tel qu'un login, une confirmation d'identité ou un accès au système).

4.4 La **fonctionnalité «Historique des signature»** énumère les actions réalisées au moyen du DeepID, comme l'émission d'une signature électronique.

4.5 La **fonctionnalité «Organisations»** permet à l'utilisateur identifié d'inviter d'autres personnes à passer par le processus d'identification via DeepID. Le but des invitations est d'identifier les personnes autorisées à signer pour une organisation, ce qui permet de vérifier l'organisation. Pour ce faire, l'utilisateur doit ouvrir un compte DeepCloud auprès de DeepCloud. Il peut y inviter des personnes, qui se soumettent ensuite de manière autonome au processus d'identification de DeepID, durant lequel les données fournies sont comparées avec les sources publiques.

4.6 Avec la **fonctionnalité «Renouveler le document»**, l'utilisateur est tenu de procéder de manière autonome et en temps utile à une ré-identification en cas de modifications importantes. Il est ainsi invité à procéder à une ré-identification lorsque le document d'identité utilisé pour l'identification ou un certificat de signature électronique perd sa validité. Pour ce faire, il doit à nouveau se soumettre au processus d'identification. L'utilisateur accepte de recevoir ce rappel dans l'application DeepID ainsi que par e-mail.

4.7 La **fonctionnalité «Tâches»** permet à l'utilisateur de valider les signatures électroniques avancées et qualifiées mises à sa disposition par un fournisseur de services de certification ou de confiance.

5. Possibilités d'utilisation de l'identité DeepID

5.1 L'identité confirmée par le biais de DeepID peut être utilisée pour différents buts, avec le moyen de légitimation, pour des autorisations et des authentifications.

5.2 Une demande d'utilisation est effectuée via un DeepService ou un service de prestataire tiers en dehors de l'application DeepID (comme l'invitation à émettre une signature électronique), étant précisé que les dispositions respectives du prestataire tiers ou de DeepCloud doivent être acceptées et respectées pour ce service.

5.3 Si, lors d'une demande, il n'existe pas encore d'identification valable, l'utilisateur est invité à s'identifier. S'il existe déjà une identification valable, mais que l'appareil utilisé est nouveau ou que les documents d'identité doivent être renouvelés (après 5 ans au plus ou après l'expiration de leur validité, selon ce qui se produit en premier), une ré-identification ou le renouvellement des documents est nécessaire.

5.4 L'action concrètement demandée dépend du service concerné et de l'option d'utilisation choisie. DeepID sert uniquement à rendre l'autre service possible. Pour les prestations que l'utilisateur utilise auprès d'un prestataire tiers en utilisant l'identité DeepID (p. ex. comme moyen d'identification lors de la connexion à un accès sécurisé ou lors de l'émission d'une signature électronique), un contrat est conclu pour ce service entre l'utilisateur et le prestataire tiers concerné. Les dispositions contractuelles de ces prestataires tiers peuvent prévoir des limitations concernant l'utilisation de DeepID pour leurs services.

5.5 L'utilisation du service de prestataires tiers est soumise à la condition que l'utilisateur se soit identifié avec succès au moyen de l'application DeepID, que l'identité DeepID soit acceptée par ce prestataire tiers et soit reliée à DeepID et que l'utilisateur valide la demande concernée.

5.6 L'application DeepID transfère les contenus collectés dans le cadre du processus d'identification à DeepCloud, respectivement aux sous-traitants impliqués dans l'identification, ainsi que, sur demande, les contenus nécessaires à cet effet à un prestataire tiers autorisé pour authentifier l'utilisateur et exécuter l'action demandée. À cette occasion, un échange d'informations peut avoir lieu avec ou entre les systèmes d'un prestataire tiers ou des contenus être synchronisés avec de tels systèmes. Pour ce faire, les parties impliquées sont expressément autorisées à accéder, échanger des données entre les systèmes respectifs et traiter les contenus. Dans ce cadre, des données à caractère personnel, des documents et des données de transactions peuvent être transmis et traités. L'utilisateur y consent expressément par la présente.

5.7 Le déroulement d'un processus d'autorisation ou d'authentification pour un service est le suivant: l'utilisateur reçoit une demande du service concerné (par e-mail, notification push, SMS, etc.) pour émettre la validation dans l'application DeepID sur son moyen de légitimation. Un certain délai est prévu à cet effet, qui peut varier d'un service à l'autre. Après s'être connecté à l'application DeepID, l'utilisateur peut émettre la validation demandée, telle qu'une signature électronique ou une autre action (p. ex. connexion à des applications ou logins, transmission de données). Dès que l'utilisateur donne la validation, cette information est signée numériquement au moyen d'une clé cryptographique enregistrée sur le moyen de légitimation et le prestataire de services concerné reçoit, par transmission cryptée, confirmation que la validation a été envoyée depuis l'appareil autorisé

(le prestataire de services peut vérifier l'information signée à l'aide de la clé cryptographique publique). Ainsi, le prestataire de services peut partir du principe que la validation a été donnée par la bonne personne et que l'action requise peut être accordée.

5.8 Si l'utilisateur n'a pas donné la validation ou ne l'a pas fait en temps utile, le prestataire de services est informé que la validation n'a pas été accordée et que l'autorisation fait défaut ou n'a pas abouti. A cet égard, DeepID permet uniquement l'autorisation ou l'authentification de l'utilisateur pour les services de prestataires tiers qui acceptent l'identité DeepID. Si l'utilisateur n'autorise pas l'action requise ou ne l'autorise pas à temps, il est lui-même responsable des conséquences qui en découlent.

5.9 L'application DeepID supporte l'authentification multifacteur. Ce faisant, l'appareil souhaité est légitimé au moyen de la procédure d'identification en tant que facteur supplémentaire et peut être utilisé pour confirmer l'action demandée. L'authentification à deux facteurs est une procédure de sécurité par laquelle l'utilisateur fournit deux éléments différents pour s'identifier ou émettre une manifestation de volonté explicite. Dans le cas de DeepID, la possession du moyen de légitimation et, dans le cas d'une autorisation ou d'une authentification, l'application DeepID constitue la deuxième composante pour confirmer l'action.

5.10 Dans le cadre du processus d'identification, l'appareil utilisé se légitime grâce à la suite d'authentification centrée sur l'utilisateur et basée sur l'IA, et pourra ainsi être utilisé pour des autorisations et des authentifications pour une communication avec le fournisseur tiers.

6. Possibilités d'utilisation de l'identité DeepID pour les signatures électroniques

6.1 L'identité DeepID peut être utilisée pour l'autorisation et l'authentification de signatures électroniques avancées et qualifiées. Les fournisseurs reconnus de services de certification ou de confiance (**fournisseurs**) peuvent délivrer à une personne identifiée des certificats avancés pour les signatures électroniques avancées (SEA) et des certificats qualifiés pour les signatures électroniques qualifiées (SEQ) avec horodatage qualifié (services de certification ou de confiance). L'utilisateur doit s'identifier une fois pour pouvoir signer plusieurs fois, sous réserve des cas où une ré-identification est nécessaire.

6.2 L'application DeepID permet de vérifier l'identité de cette personne (**signataire**). Ces services de certification ou de confiance sont fournis par ces fournisseurs conformément à la loi fédérale sur la signature électronique (**SCSE**) et au règlement de l'UE sur l'identification électronique et les services de confiance pour les transactions électroniques dans le marché intérieur (**Règlement eIDAS**).

6.3 DeepCloud est l'organisme d'enregistrement des SEQ et des SEA mandaté par ces fournisseurs. Elle est soumise au DeepCloud Trust Service Practice Statement (TSPS) en vigueur. Sa conformité au TSPS a été évaluée et confirmée par un organisme de certification reconnu (Conformity Assessment Body/CAB) en Suisse et dans l'UE. DeepCloud a été certifié selon le schéma d'évaluation de la conformité suivant (Norm of Accreditation System) : ISO 17021-1:2015 (pour SCSE) et ISO 17065-1:2013 (pour règlement eIDAS) pour la "Remote Identification Certification" selon les exigences de la SCSE, de l'OSCSE, des PTA (RS 943.032.1), du règlement eIDAS de l'UE, d'ETSI TS 119 461, de l'ETSI EN 319 401 et de l'ETSI EN 419 241-1.

6.4 Dans le cadre d'un processus d'identification certifié avec DeepID, DeepCloud vérifie l'identité du signataire sans que la présence de celui-ci soit nécessaire. Dans ce contexte, l'utilisateur doit respecter scrupuleusement les prescriptions et fournir en permanence des informations complètes, exactes et à jour. Dans le cadre du processus d'identification, l'utilisateur peut être invité à produire différents documents en fonction du but d'utilisation de l'identification.

6.5 Si une identification ne peut pas être effectuée avec succès, DeepCloud a le droit d'exclure une nouvelle tentative d'identification temporairement ou de manière permanente. Si l'identification remplit toutes les conditions requises, l'identité DeepID est enregistrée pour l'établissement de SEA et de SEQ. Cet enregistrement est réexaminé avant chaque mandat du signataire.

6.6 En particulier, l'émission de SEA ou de SEQ est soumise à certaines spécificités avant leur validation. Ainsi, le signataire doit être domicilié en Suisse, dans l'UE ou dans l'EEE et le confirmer lorsqu'il donne l'ordre d'établir une SEQ ou une SEA. Si tel n'est pas le cas, l'utilisateur ne peut pas utiliser ces services. Il répond intégralement des éventuelles conséquences du non-respect de ces exigences. Dans de tels cas, DeepCloud et les prestataires tiers concernés excluent toute garantie et responsabilité quant à leurs services.

6.7 Seuls les documents d'identité que les fournisseurs de services de certification ou de confiance autorisent à cet effet sont admis pour l'identification dans le cadre de demandes de SEQ et de SEA. Ces documents sont indiqués lors du processus d'identification. Les documents d'identité doivent être valables au moment de l'identification. La liste des documents d'identité autorisés peut être modifiée, de sorte qu'une ré-identification peut s'avérer nécessaire. Seuls les documents d'identité prescrits par les fournisseurs des services de certification ou de confiance peuvent être utilisés pour l'identification et lors d'une demande du signataire. Ils déterminent également si le signataire doit se soumettre à un processus d'identification unique pour chaque signature électronique (signature unique) ou s'il a le droit de créer, après avoir achevé le processus d'identification, plusieurs signatures électroniques pendant une durée déterminée. Il peut en résulter, le cas échéant, la nécessité d'une ré-identification du signataire.

6.8 Le signataire est invité à émettre une signature électronique au moyen d'un service (comme DeepSign, le service de signature de DeepCloud). Selon le choix du type de signature souhaité, une signature électronique simple (SES), une SEQ ou une SEA doivent être délivrées conformément aux dispositions légales applicables (SCSE ou Règlement eIDAS). Un autre mode d'utilisation que le mandat en vue de fournir les services de certification ou de confiance proposés par ces fournisseurs n'est pas autorisé (restriction d'utilisation).

6.9 DeepCloud enregistre et conserve, conformément aux dispositions contractuelles et aux prescriptions en vigueur, les données relatives à la personne de l'utilisateur collectées dans le cadre du processus d'identification DeepID et les contenus nécessaires dans le cadre du processus de validation pour les services de certification ou de confiance.

6.10 Les fournisseurs sont responsables de l'établissement des certificats et de la paire de clés cryptographique pour le processus de signature après l'octroi de la validation par l'utilisateur. Le signataire peut utiliser ce certificat avec ses données d'activation en utilisant DeepID. Dès que le signataire a octroyé sa validation dans le système DeepID après avoir reçu la demande correspondante (en acceptant les conditions d'utilisation du fournisseur concerné et en confirmant le domicile requis), le fournisseur concerné établit pour lui la SEA ou la SEQ sur la base de ce certificat. Pour chaque processus de signature, un nouveau certificat numérique (d'une courte durée de validité) sera établi avec une nouvelle paire de clés.

6.11 Avec l'identification confirmée au moyen de DeepID, l'utilisateur peut utiliser le service de certification ou de confiance correspondant pour la durée de validité de l'identification pour toutes les applications de signature que DeepCloud et les fournisseurs ont relié à DeepID afin de faire établir un SEQ ou un SEA en cours de validité, sans qu'une nouvelle identification ne soit nécessaire tant que l'application de signature respective et la durée de validité du certificat l'autorisent.

6.12 DeepCloud vérifiera l'identité du signataire, l'authentifiera et lui permettra d'effectuer l'autorisation.

6.13 Les fournisseurs sont autorisés à vérifier auprès de DeepCloud le respect de ses obligations contractuelles en matière d'identification, d'autorisation et d'authentification des SEA et SEQ par un audit. À cette occasion, des données du signataire peuvent

également être consultées. Les fournisseurs peuvent faire exécuter l'audit par leurs propres collaborateurs ou par des tiers et partager les résultats avec les organismes d'évaluation de la conformité et les autorités de surveillance compétentes.

7. Droits d'utilisation, droits de propriété intellectuelle

7.1 DeepCloud accorde à l'utilisateur, pour son propre usage, un droit d'utilisation personnel, non exclusif, intransmissible, incessible, simple, limité dans le temps et dans l'espace, sur le logiciel concerné lors de l'utilisation de DeepID pendant la durée des rapports d'utilisation. Cela signifie que seul l'utilisateur peut utiliser DeepID pour lui-même. L'étendue du droit d'utilisation découle des présentes CG.

7.2 Il est interdit à l'utilisateur de rendre DeepID accessible à des tiers ou de la mettre à la disposition de tiers. Enfin, il n'est pas autorisé à utiliser le logiciel à d'autres fins que celles accordées par DeepCloud dans le présent document.

7.3 DeepCloud a le droit d'offrir des interfaces et d'accorder des licences sur celles-ci dans le but d'exporter des données de DeepID vers d'autres systèmes pour y être traitées. L'utilisateur ne peut utiliser de telles interfaces vers des services, y compris de prestataires tiers, que dans le cadre des présents rapports d'utilisation. Il en va de même lorsque des interfaces sont utilisées dans le but d'utiliser des données au moyen d'un autre système. L'utilisateur est tenu de respecter les possibilités d'utilisation et les limites prescrites par DeepCloud et n'est pas autorisé à contourner celles-ci à l'aide de mesures techniques d'évitement.

7.4 Le logiciel utilisé par DeepCloud peut être soumis à des prescriptions en matière de contrôle à l'exportation et à d'autres types de dispositions légales. Le cas échéant, le logiciel ne saurait être exporté, réexporté ou transféré dans certains pays ou à des personnes physiques ou entités frappés par une interdiction de recevoir certains biens d'exportation (y compris ceux qui figurent sur des listes de sanctions applicables à des personnes physiques ou entités). L'utilisateur doit respecter les éventuelles prescriptions locales en relation avec l'utilisation de services de cryptage tels que ceux utilisés pour DeepID.

7.5 Les clauses de licence des logiciels de fournisseurs tiers s'appliqueront.

7.6 L'utilisateur informe immédiatement DeepCloud si des tiers font valoir à son encontre des droits de propriété intellectuelle (par exemple des droits d'auteur ou des droits de brevet) relatifs au logiciel lors de l'utilisation de DeepID. Il n'entreprend aucune action en justice sans l'autorisation de DeepCloud et ne reconnaît pas de son propre chef des prétentions de tiers sans le consentement de DeepCloud. DeepCloud met en œuvre à ses frais tous les moyens de défense nécessaires, tels que la défense face aux prétentions de tiers, dans la mesure où celles-ci ne reposent pas sur un comportement fautif de l'utilisateur.

7.7 L'utilisateur prend acte du fait que son magasin d'applications n'est aucunement tenu de fournir des services d'entretien et d'assistance concernant l'application DeepID. Si un tiers prétend que DeepID ou la possession de l'application DeepID viole ses droits de propriété intellectuelle, c'est DeepCloud et non le magasin d'applications qui est responsable de la défense contre ces prétentions.

7.8 Tous les droits de propriété intellectuelle sur DeepID (y compris le logiciel utilisé à cet effet), sur les contenus, textes, images, photos, vidéos, logos ou autres informations de DeepCloud, y compris ses sites Internet, appartiennent exclusivement à DeepCloud ou aux titulaires de droits concernés. Toute utilisation plus étendue de droits de propriété intellectuelle, quels qu'ils soient, requiert le consentement écrit préalable des titulaires des droits concernés. L'ensemble de la documentation de DeepCloud rendue accessible dans le cadre des rapports d'utilisation est considérée comme propriété intellectuelle de DeepCloud**.**

7.9 DeepCloud est en droit de traiter des photos et des vidéos pour le processus d'identification ou comme photo de profil de l'utilisateur, sans que celui-ci ne puisse en tirer un droit quelconque en matière de rémunération.

8. Conditions d'utilisation et obligations de l'utilisateur

8.1 L'utilisateur dispose d'un appareil servant de moyen de légitimation autorisé et confirme son identité avec l'application DeepID. L'utilisation de l'application DeepID présuppose que l'appareil utilisé remplisse durablement les conditions requises pour l'appareil et le système.

8.2 L'utilisateur est responsable du moyen de légitimation utilisé, qui est à sa disposition exclusive. Tant qu'il souhaite utiliser DeepID, il lui est interdit de confier le moyen de légitimation à des tiers.

8.3 Le logiciel du moyen de légitimation doit être mis à jour. En particulier, les modifications mises à disposition par le fabricant (mises à jour, améliorations, servicepacks, hotfixes, etc.) ainsi que la version actuelle de l'application DeepCloud mise à disposition par DeepCloud doivent être installées.

8.4 L'utilisateur s'engage à utiliser toutes les possibilités raisonnables et actuelles afin de protéger son moyen de légitimation contre les attaques et les logiciels malveillants («virus», «vers», «chevaux de Troie», etc.), notamment en utilisant des logiciels toujours à jour issus de sources officielles.

8.5 Le moyen de légitimation doit être utilisé conformément aux conditions contractuelles du fabricant et de manière appropriée, notamment en s'abstenant de tout acte qui, par la modification ou le remplacement du logiciel installé par le fabricant de l'appareil, favorise ou occasionne des risques (p. ex. par du «jailbreaking ou du rooting» ou d'un autre logiciel qui viole les conditions d'utilisation prescrites par le fabricant). L'utilisateur s'engage à installer exclusivement sur son moyen de légitimation des logiciels (en particulier d'autres applications) qui proviennent de sources fiables.

8.6 Le système d'exploitation du moyen de légitimation doit correspondre à l'état officiel mis à disposition par le fabricant et être compatible avec l'application DeepID, faute de quoi l'application DeepID ne sera pas supportée. DeepID présuppose l'existence d'une connexion active avec le réseau d'un fournisseur de services de téléphonie mobile. Les versions supportées du système d'exploitation concerné sont indiquées dans les magasins d'applications correspondants.

8.7 L'utilisateur est tenu de fournir à tout moment, dans le cadre du processus d'identification et lors de l'utilisation de son identité confirmée, des informations complètes, exactes et à jour et de les mettre immédiatement à jour en cas de changement. DeepCloud se réserve le droit d'exiger des preuves de l'exactitude de ces informations ou d'effectuer elle-même des vérifications. L'obligation d'informer concerne notamment les circonstances suivantes: nom, nationalité, sexe, domicile, coordonnées telles qu'adresse e-mail, téléphone, modification de la pièce d'identité et du moyen de légitimation en cas de perte, vol, changement ainsi que toute autre circonstance de fait ou juridique susceptible d'avoir une influence sur l'identification de l'utilisateur et les rapports d'utilisation avec DeepCloud.

8.8 Les possibilités d'utilisation de l'identité confirmée par l'application DeepID et les conditions d'utilisation de celle-ci sont définies dans le contrat respectif que l'utilisateur conclut avec DeepCloud ou un prestataire tiers.

8.9 DeepID ne peut être utilisée que pour un service qui accepte l'identité confirmée au moyen de DeepID. En outre, l'utilisateur doit accepter les dispositions contractuelles de ces services qui s'appliquent séparément. Les éventuelles conditions supplémentaires doivent être strictement respectées par l'utilisateur.

8.10 L'utilisateur n'est autorisé à utiliser certains services que s'il remplit les conditions requises. Ainsi, il n'est autorisé à confier l'établissement d'une SEA ou d'une SEQ à un fournisseur que s'il a utilisé les documents d'identité nécessaires à cet effet à des fins d'identification et si son domicile remplit les conditions requises. S'il devait fournir des confirmations correspondantes bien que celles-ci ne soient pas exactes, DeepCloud et les prestataires tiers concernés excluent toute garantie et responsabilité pour les services fournis, tels que l'octroi d'une SEQ ou d'une SEA, et se réservent le droit d'entamer des démarches judiciaires contre l'utilisateur. Dans un tel cas, l'utilisateur libérera en outre tant DeepCloud que le prestataire tiers concerné de toute prétention de tiers résultant des indications erronées de l'utilisateur.

8.11 Aux fins de l'utilisation de DeepID, la connaissance du NIP DeepID, du code de récupération et du contrôle d'accès à l'appareil, d'une part, et la possession du moyen de légitimation, d'autre part, constituent des éléments de sécurité personnelle dont la protection relève de la responsabilité de l'utilisateur.

8.12 Afin d'assurer la protection contre l'utilisation abusive de DeepID et de l'identité confirmée, il est interdit de choisir des combinaisons banales ou courantes (p. ex. 123456) ou d'autres combinaisons de chiffres faciles à découvrir, telles que le numéro de téléphone, la date de naissance et le numéro d'immatriculation du véhicule.

8.13 L'utilisateur est responsable de la protection de ses données d'accès, en particulier du choix d'un NIP sécurisé, de la sauvegarde de son code de récupération ainsi que de la protection contre les accès de tiers au moyen de légitimation et à l'application DeepID qui y est installée. Les informations importantes pour la sécurité doivent être tenues secrètes et ne peuvent être communiquées à aucune autre personne (y compris au prestataire tiers concerné). Les éventuels enregistrements de données d'accès doivent être conservés de manière sécurisée et séparément du moyen de légitimation ou cryptés, et être protégés contre les accès de tiers.

8.14 Si l'utilisateur sait ou a des raisons fondées de soupçonner qu'un tiers a connaissance de ses données d'accès, il doit les modifier immédiatement dans les paramètres de l'appareil et, si nécessaire, informer immédiatement DeepCloud de l'incident.

8.15 Si le moyen de légitimation a été volé ou perdu, ou si l'utilisateur sait ou présume qu'une autre personne a eu connaissance des données d'accès (compromission des données), il est tenu de prendre les mesures suivantes: faire bloquer la DeepID en contactant le service d'assistance; renoncer immédiatement à utiliser son identité confirmée et les services qui requièrent son autorisation et son authentification, tels que l'établissement de SEA et de SEQ; faire annuler sans délai le certificat pour la création de signatures; modifier, le cas échéant, ses données d'accès; (p. ex. pour DeepCloud dans l'application DeepID, dans le compte DeepCloud ou auprès du prestataire tiers concerné).

8.16 Dès que des modifications sont apportées à un appareil utilisé pour la légitimation (p. ex. appareil en tant que tel, adresse e-mail) ou aux données pertinentes pour son identification (telles que nom, nationalité, autres attributs), l'utilisateur informe directement DeepCloud, soit en utilisant «J'ai déjà une DeepID» ou «Renouveler un document», soit en adaptant les données dans son profil. S'il n'y parvient pas, il doit s'adresser immédiatement au service d'assistance DeepCloud. DeepCloud prendra alors les mesures nécessaires et informera les fournisseurs de services de certification ou de confiance afin que l'identité confirmée de l'utilisateur et le certificat puissent être invalidés. L'utilisateur prendra les mesures nécessaires auprès de ses autres fournisseurs de services concernés.

8.17 L'utilisateur s'engage à vérifier en permanence ses données d'identité après leur confirmation et à signaler immédiatement à DeepCloud toute divergence ou tout soupçon d'utilisation abusive de l'identité DeepID.

8.18 Il est strictement interdit à l'utilisateur d'utiliser DeepID à des fins illicites. Par conséquent, il a également l'interdiction d'utiliser des documents d'identité falsifiés ou de tiers pour le processus d'identification. Dans de tels cas, DeepCloud se réserve le droit d'interdire l'utilisation de DeepID et d'entamer des démarches judiciaires à l'encontre de l'utilisateur.

8.19 Si l'utilisateur manque à ses obligations, il assume tous les risques qui sont favorisés ou causés par la violation de ses obligations.

8.20 Si l'utilisateur n'est pas d'accord avec les traitements de données effectués dans le cadre de DeepID, il n'est pas autorisé à utiliser DeepID.

8.21 La question de savoir si des prestataires tiers ou DeepCloud exigent des frais lors de la fourniture de leurs services en utilisant DeepID est régie par le contrat conclu entre l'utilisateur et DeepCloud ou le prestataire de services concerné. En outre, le transfert de données par le fournisseur de services de téléphonie mobile de l'utilisateur peut entraîner des frais, dont l'utilisateur est responsable.

9. Assistance

9.1 Le service d'assistance n'est fourni que pendant les heures d'assistance habituelles de DeepCloud (par exemple sous forme de forums ou de FAQ, par e-mail). L'assistance DeepCloud est accessible sous support@deepid.swiss

9.2 Si des anomalies ou des incidents de sécurité surviennent lors des processus d'identification, d'autorisation ou d'authentification respectifs, l'utilisateur doit s'adresser sans délai à DeepCloud.

9.3 DeepCloud ne garantit pas que les identifications, les autorisations ou les authentifications (comme pour le mandat d'une signature électronique) puissent avoir lieu à tout moment et à temps.

9.4 En cas de questions concernant les conditions techniques ou les fonctionnalités de DeepID ou en cas de perturbation de l'utilisation, l'assistance peut être contactée.

9.5 DeepCloud se réserve le droit de facturer les services fournis dans le cadre de l'assistance conformément à ses tarifs horaires en vigueur. Des détails sur l'assistance et les heures d'assistance concrètes figurent sur les sites Internet de DeepCloud.

10. Durée d'utilisation de l'identité confirmée

10.1 Sous réserve du respect des conditions prévues par les présentes CG ainsi que par les CG de DeepCloud pour un compte DeepCloud, l'utilisateur peut utiliser son identité confirmée avec le moyen de légitimation enregistré lors de l'identification, pour des services de certification ou de confiance, pendant une durée maximale de cinq ans, cette durée étant raccourcie en conséquence si la durée de validité du document d'identité présenté par l'utilisateur expire plus tôt, si le certificat des fournisseurs des services de certification ou de confiance expire ou si survient une autre circonstance nécessitant une ré-identification.

10.2 Les authentifications autres que celles destinées aux services de certification ou de confiance peuvent également être limitées dans le temps, notamment en raison des conditions d'utilisation de fournisseurs tiers. Dans tous les autres cas, il appartient à DeepCloud de fixer la durée d'utilisation d'une identification confirmée, y compris une éventuelle ré-identification de l'utilisateur.

Conditions générales de DeepCloud SA pour l'utilisation de DeepID (janvier 2024)

11. Protection des données et confidentialité

11.1 DeepCloud respecte les dispositions du droit applicable en matière de protection des données dans le cadre de ses traitements de données. Dans son domaine de responsabilité, elle aménage son organisation de manière à répondre aux exigences spécifiques de la protection des données. Elle prend des mesures techniques et organisationnelles pour assurer une protection adéquate des données de l'utilisateur contre les abus et les pertes conformément aux exigences du droit de la protection des données.

11.2 DeepCloud traitera de manière confidentielle toutes les informations non notoires dont elle prend connaissance sur l'utilisateur et ses relations commerciales. Elle ne mettra ces informations à la disposition de tiers que dans la mesure permise par les rapports d'utilisation ou par la loi, si l'utilisateur l'a expressément autorisé ou si cela s'avère nécessaire en raison d'une décision administrative ou judiciaire ou d'une obligation légale. Elle garantit également le respect de l'obligation de confidentialité par tous les collaborateurs et tiers impliqués dans les rapports d'utilisation.

11.3 DeepCloud collecte, enregistre et traite, outre les données collectées conformément aux règles applicables et nécessaires à la fourniture d'un service de certification ou de confiance, toutes les données et informations dont elle a besoin pour fournir ses services à l'utilisateur. La gestion de ces données est régie non seulement par les lois applicables, mais aussi par les directives en matière de services de certification ou de confiance.

11.4 DeepCloud fait appel à des tiers pour ses services en lien avec l'identification de l'utilisateur. Il s'agit de sous-traitance de données pour le compte de DeepCloud. DeepCloud a conclu avec ces tiers les accords nécessaires en matière de protection des données.

11.5 Le traitement des données à caractère personnel de DeepCloud est décrit dans sa https://www.deepcloud.swiss/fr/politique-des-donnees/ figurant sur son site Internet. La version en vigueur publiée fait foi.

11.6 Sur la base des données fournies par l'utilisateur lors du processus d'identification et collectées par DeepCloud, le fournisseur respectif d'un service de certification ou de confiance établit, sur demande et suite à une manifestation de volonté correspondante de l'utilisateur, un certificat qualifié ou avancé contenant les informations nécessaires sur l'utilisateur.

11.7 DeepCloud conserve les données décrites ci-dessus ainsi que les moyens sur la base desquels l'identité a été vérifiée conformément aux obligations contractuelles et légales de conservation, également afin que l'utilisateur puisse utiliser un service de certification ou de confiance. Le délai de conservation est de 11 ans pour les SEQ selon la SCSE et de 30 ans selon le Règlement eIDAS, et de 7 ans pour les SEA selon la SCSE et le Règlement eIDAS. En raison de la durée de validité maximale de 5 ans pour une identification, cela conduit, compte tenu d'un délai de sécurité supplémentaire d'un an, à des durées de conservation pour les SEQ pouvant aller jusqu'à 17 ans selon la SCSE et jusqu'à 36 ans selon le Règlement eIDAS, ainsi qu'à des durées de conservation pour les SEA pouvant aller jusqu'à 13 ans selon la SCSE et le Règlement eIDAS.

11.8 Ces délais de conservation garantissent le maintien de la traçabilité de l'exactitude d'un document signé électroniquement dans les années qui suivent son établissement. Toutes les informations pertinentes concernant les données transmises et reçues sont enregistrées et conservées de manière à être disponibles, en particulier dans le cadre d'une procédure judiciaire, afin de fournir des preuves appropriées et d'assurer la continuité du service de certification ou de confiance.

11.9 DeepCloud efface les données nécessaires au plus tôt 17 ans selon la SCSE et au plus tôt 36 ans selon le Règlement eIDAS, à compter de la réalisation du processus d'identification. En cas d'identification effectuée uniquement selon les exigences de la SEA, DeepCloud efface ces données au plus tôt 13 ans à compter de la réalisation du processus d'identification, tant selon la SCSE que selon le Règlement eIDAS. Les données ne peuvent être effacées qu'après l'expiration des obligations de conservation existantes.

11.10 Afin d'informer l'utilisateur de l'expiration de la durée d'utilisation de l'identité confirmée et d'une éventuelle autorisation de signature, DeepCloud enregistre le moment où l'expiration se produira et informe l'utilisateur par écrit ou d'une autre manière (p.ex. au sein de son application DeepID, d'un compte DeepCloud existant ou par e-mail) à ce sujet afin qu'il puisse procéder à temps à une ré-identification. L'utilisateur y consent expressément.

11.11 Si des données sont nécessaires pour défendre des prestataires tiers ou DeepCloud contre d'éventuelles prétentions en dommages-intérêts, ces données sont conservées pendant la durée d'éventuels délais de prescription.

11.12 L'utilisateur a la possibilité de valider à diverses fins la transmission de données, de documents et d'informations à des tiers dans le cadre d'une authentification au moyen de DeepID, avec ou sans l'utilisation de services de prestataires tiers, tels que la transmission de données à un employeur potentiel, une assurance ou une banque. Il peut également utiliser son identité confirmée pour s'authentifier en tant que représentant autorisé d'une organisation. La manière dont les prestataires tiers traitent les données de l'utilisateur et les possibilités d'influence dont celui-ci dispose à cet égard figurent dans les dispositions sur la protection des données de ces prestataires tiers. DeepCloud n'est pas responsable de ces traitements de données.

12. Recours à des tiers

12.1 DeepCloud peut en tout temps faire appel à des tiers pour exécuter ses obligations conformément au contrat, ce que l'utilisateur autorise par les présentes. Ces tiers sont choisis avec soin et mandatés par DeepCloud. Ils sont liés par des instructions et font l'objet de contrôles réguliers. Il est notamment fait appel à des fournisseurs d'hébergement et de services avec des solutions de serveurs en Suisse, dont le siège se trouve en Suisse ou dans l'UE.

13. Garantie

13.1 DeepCloud offre à l'utilisateur une exécution fidèle et diligente des services conformément au présentes CG.

13.2 DeepCloud ne garantit pas, de manière générale ou à un moment donné, une exploitation ininterrompue ou sans perturbations de DeepID (y compris de l'application DeepID) et l'utilisation de ses fonctionnalités. La garantie pour DeepID (y compris l'application, le logiciel, l'hébergement utilisés, etc.) est exclue, dans la mesure autorisée par la loi. DeepID est mis à disposition «en l'état».

13.3 DeepCloud s'efforce de mettre DeepID à disposition sans interruption. Toutefois, DeepCloud n'est pas en mesure de garantir une disponibilité exempte d'interruptions. DeepCloud peut en tout temps limiter ou interrompre temporairement la disponibilité de DeepID, notamment si cela s'avère nécessaire en raison des limites de capacité, de la sécurité ou de l'intégrité des serveurs ou pour l'exécution de mesures techniques d'entretien ou de réparation, ou si cela sert à la bonne exécution ou à l'amélioration des prestations. Elle s'efforce à cet égard de tenir compte des intérêts de l'utilisateur et, dans la mesure du possible, informera celui-ci des interruptions avec un préavis approprié.

13.4 Les services fournis gratuitement sont fournis sans droits à l'exécution ou de garantie. DeepCloud peut à tout moment et sans préavis suspendre ou modifier les services fournis gratuitement ou choisir de les offrir uniquement contre rémunération. Il n'en résulte aucune prétention ou aucun droit de l'utilisateur.

13.5 Il n'existe aucune garantie que DeepID réponde aux besoins individuels de l'utilisateur, que ceux-ci aient été communiqués ou non à DeepCloud. Les informations figurant sur le site Internet de DeepCloud et les autres déclarations publicitaires de DeepCloud ne constituent aucunement des indications concernant la qualité ni des garanties.

13.6 DeepCloud doit - en tant qu'organisme d'enregistrement - remplir les exigences fixées par la loi et les normes techniques pour de tels services au moyen du processus d'identification qui fait partie d'un service de certification ou de confiance. À cet effet, DeepCloud met en place des mesures de sécurité appropriées et conformes à l'état actuel de la technique. DeepCloud est responsable de l'évaluation et de la spécification des exigences découlant des lois et réglementations applicables.

13.7 L'utilisateur prend acte du fait que malgré tous les efforts de DeepCloud, l'utilisation de techniques et de normes de sécurité modernes et le contrôle par un organisme indépendant du respect des normes techniques et des prescriptions légales, il n'est pas possible de garantir une sécurité absolue et l'absence d'erreurs du processus d'identification et des services de certification ou de confiance.

13.8 DeepCloud ne garantit pas qu'une identification, vérification, autorisation ou authentification puisse être effectuée et conclue en tout temps et exclut toute responsabilité pour d'éventuels dommages résultant d'une identification, vérification, autorisation ou authentification tardive, omise ou non achevée avec succès, dans la mesure autorisée par la loi.

14. Responsabilité et force majeure

14.1 DeepCloud ne répond qu'en cas de dol, de négligence grave et de dommages corporels. Pour le surplus, toute autre responsabilité est expressément exclue, en particulier celle pour les dommages consécutifs, les dommages patrimoniaux et indirects (tels que la perte totale ou partielle de documents ou de données, les frais supplémentaires, le gain manqué, les dommages dus à des perturbations de la disponibilité, prétentions de tiers, etc.) ainsi que pour les auxiliaires (y compris les tiers mandatés). Cela vaut également pour une éventuelle responsabilité sans faute.

14.2 DeepCloud n'assume aucune responsabilité pour la disponibilité permanente de l'application DeepID, de son service d'assistance, des processus et des possibilités d'utilisation offerts ainsi que des différentes fonctionnalités de l'application DeepID.

14.3 DeepCloud ne répond pas vis-à-vis de l'utilisateur du fonctionnement normal des systèmes de tiers, en particulier du matériel informatique et des logiciels utilisés par l'utilisateur ou d'un service de prestataires tiers auquel il a recours en utilisant son identité certifiée à des fins d'authentification.

14.4 Elle n'encourt aucune responsabilité lorsque l'exécution de sa prestation est temporairement interrompue, partiellement ou totalement limitée ou impossible en raison d'un cas de force majeure. Sont notamment considérés comme cas de force majeure les catastrophes naturelles d'une certaine ampleur (avalanches, inondations, glissements de terrain, etc.), les guerres, les émeutes, les restrictions administratives imprévisibles ainsi que les pandémies ou épidémies. Si DeepCloud ne peut pas remplir ses obligations, l'exécution de celles-ci ou leur date d'exécution est reportée en conséquence de l'événement survenu. DeepCloud ne répond pas des éventuels dommages causés à l'utilisateur par le report de l'exécution.

14.5 Le détenteur doit faire valoir d'éventuelles prétentions dans un délai de six mois à compter de la fourniture des prestations.

14.6 Les présentes exclusions et limitations de responsabilité s'appliquent aussi bien aux prétentions contractuelles qu'aux prétentions extracontractuelles du détenteur.

14.7 DeepCloud ne répond pas des dommages résultant d'une utilisation contraire au contrat ou illicite de DeepID par l'utilisateur.

14.8 Sont exclues de ces exclusions et limitations de responsabilité les dispositions impératives en matière de responsabilité en vertu de la législation sur la responsabilité du fait des produits, la protection des consommateurs, la SCSE ou le Règlement eIDAS de l'UE et leurs lois d'exécution. Dans ce cas, les limitations et exclusions de responsabilité éventuellement prévues dans ces dispositions sont également applicables à DeepCloud.

14.9 DeepCloud a réglé sa responsabilité vis-à-vis de l'utilisateur en ce qui concerne l'utilisation de DeepSign dans ses conditions générales pour l'utilisation du compte DeepCloud et des DeepServices.

14.10 L'utilisateur répond en particulier et libère DeepCloud de toute prétention (en dommages-intérêts) en relation avec l'utilisation de DeepID résultant d'une violation des lois et prescriptions applicables, des bonnes mœurs, des présentes CG ou des dispositions contractuelles de DeepCloud ou de prestataires tiers tels que des prestataires de services de certification ou de confiance.

15. Modifications des présentes CG

15.1 DeepCloud se réserve le droit de modifier et de compléter en tout temps l'application DeepID ainsi que les présentes CG. En particulier, en cas de modifications de la SCSE, du Règlement eIDAS et de leurs législations d'exécution respectives, ainsi qu'en cas de décisions émanant de l'autorité compétente en matière de reconnaissance, de confirmation et de surveillance ou d'un organisme indépendant chargé de vérifier les signatures, les fournisseurs de services de certification ou de confiance peuvent être contraints d'adapter des directives existantes en matière de certification et, par conséquent, DeepCloud en tant qu'organisme d'enregistrement, d'adapter les présentes CG. L'utilisateur sera informé d'éventuelles modifications avant la date d'application des modifications de DeepCloud ou les dispositions en vigueur lui seront communiquées lors de l'utilisation d'un service. Cette information peut être donnée de manière appropriée à l'utilisateur.

15.2 Les modifications sont réputées acceptées si l'utilisateur ne résilie pas la relation contractuelle avant l'entrée en vigueur des nouvelles CG, mais dans tous les cas lors de l'utilisation de DeepID après l'entrée en vigueur des nouvelles dispositions, malgré la possibilité de prendre connaissance des modifications.

15.3 L'utilisateur peut également refuser d'accepter les nouvelles conditions en renonçant à utiliser DeepID (notamment l'identité confirmée, les autorisations et les authentifications par DeepID) conformément aux présentes CG à partir de la date d'application des nouvelles conditions.

15.4 Si certaines dispositions des présentes CG devaient s'avérer inefficaces ou nulles, cela n'entraînerait pas l'inefficacité ou la nullité des autres dispositions. Dans ce cas, les disposition inefficaces ou nulles seront remplacées par des dispositions se rapprochant le plus possible de leur but économique. Il en va de même en cas de lacune des conditions d'utilisation.

Conditions générales de DeepCloud SA pour l'utilisation de DeepID (janvier 2024)

16. Entrée en vigueur, durée et fin

16.1 Les rapports d'utilisation avec l'utilisateur par le biais de DeepID prennent naissance avec l'acceptation des présentes CG au sein de l'application DeepID et sont valables pour une durée indéterminée.

16.2 DeepCloud est en droit de mettre fin en tout temps aux rapports d'utilisation sans indication de motifs. Au moment de la résiliation, DeepCloud bloquera l'accès à DeepID et à l'identité DeepID confirmée, mettra fin à leur utilisation et arrêtera la communication technique avec les DeepServices ou les services de prestataires tiers. Cela signifie en particulier que l'ensemble des services en cours ainsi que les informations de statut et données y relatives ne seront plus transmises, exécutées ou mises à disposition.

16.3 L'utilisateur peut en tout temps renoncer à l'utilisation de DeepID et supprimer l'application DeepID de son moyen de légitimation. L'utilisateur est seul responsable de la planification de la fin de l'utilisation de DeepID et de son identité DeepID. En ce qui concerne le blocage de son identité DeepID ou la suppression de données, l'utilisateur s'adresse à DeepCloud.

16.4 A la fin des rapports d'utilisation, l'utilisateur n'a plus la possibilité de disposer de son identité confirmée ni d'utiliser DeepID.

17. Droit applicable et for

17.1 Toutes les relations juridiques en relation avec les présentes CG sont soumises au droit suisse, à l'exclusion du droit international privé et de la Convention de Vienne sur la vente internationale de marchandises, indépendamment du fait qu'un utilisateur utilise DeepID en sa qualité de consommateur ou pour le compte d'une entreprise.

17.2 Si l'utilisateur est un consommateur dont la résidence habituelle se trouve dans l'UE/EEE, les dispositions impératives du droit de protection des consommateurs de l'État UE/EEE dans lequel il réside s'appliquent à titre complémentaire. Il en va de même s'il s'agit d'un pays auquel le Règlement eIDAS s'applique.

17.3 Sous réserve des fors légaux impératifs, le for exclusif pour tout litige découlant des présentes CG ou en relation avec celles-ci est la ville de Saint-Gall.

18. Dispositions finales

18.1 L'utilisateur ne peut transférer à des tiers aucun droit découlant des présents rapports d'utilisation. DeepCloud est en droit de transférer à des tiers tous les droits et obligations découlant des présents rapports d'utilisation. L'utilisateur consent, par les présentes, à une éventuelle cession ou transfert.

18.2 En cas de différend, les parties s'efforcent de le régler à l'amiable.

18.3 Toutes les désignations de personnes figurant dans les présentes CG doivent être interprétées de manière neutre en matière de genre.

18.4 Les présentes CG existent en plusieurs langues. En cas de divergences ou de contradictions, la version allemande fait foi.

19. Droit impératif de l'UE/EEE en matière de protection des consommateurs

19.1 Le délai d'opposition concernant les modifications de ces CG est de 4 semaines pour les utilisateurs auxquels le droit impératif de l'UE/EEE en matière de protection des consommateurs s'applique à titre complémentaire.

19.2 DeepCloud peut résilier les rapports d'utilisation de manière ordinaire à tout moment pour le dernier jour du mois, moyennant un délai de résiliation de 30 jours.

19.3 Si l'utilisateur est un consommateur dans l'UE/EEE, DeepCloud n'est ni disposée, ni tenue de participer à une procédure de règlement des litiges devant un organe de conciliation compétent. Information des consommateurs conformément au Règlement (UE) nº 524/2013: aux fins du règlement extrajudiciaire des litiges de consommation, la Commission européenne a mis en place une plateforme de règlement en ligne des litiges (plateforme RLL). La plateforme RLL est accessible sous https://ec.europa.eu/consumers/odr/main/index.cfm?event=main.home2.show&lng=FR.