

# Conditions Générales d'Utilisation

## ChamberSign France CA3 Qualified eID

### QCP-n



<b>Objet du document :</b>	Ce document décrit les conditions générales d'utilisation des certificats émis par l'Autorité de Certification mise en œuvre par ChamberSign France dans le cadre de ses activités de services de confiance
<b>Version</b>	01
<b>Date de diffusion</b>	06/02/2019
<b>Type de diffusion</b>	Public

## **Avertissement**

Le présent document est une œuvre protégée par les dispositions du Code de la Propriété Intellectuelle du 1<sup>er</sup> juillet 1992, notamment par celles relatives à la propriété littéraire et artistique et aux droits d'auteur, ainsi que par toutes les conventions internationales applicables. Ces droits sont la propriété exclusive de **CHAMBERSIGN FRANCE**. La reproduction, la représentation (y compris la publication et la diffusion), intégrale ou partielle, par quelque moyen que ce soit (notamment, électronique, mécanique, optique, photocopie, enregistrement informatique), non autorisée préalablement par écrit par **CHAMBERSIGN FRANCE** ou ses ayants droit, sont strictement interdites.

A juste titre, aux termes de l'article L.122-4 du Code de la Propriété Intellectuelle, « *toute représentation ou reproduction intégrale ou partielle faite sans le consentement de l'auteur ou de ses ayants droit ou ayant cause est illicite* ».

Par exception, le Code de la Propriété Intellectuelle autorise, aux termes de l'article L.122-5 dudit Code, d'une part, que « *les copies ou reproductions strictement réservées à l'usage privé du copiste et non destinées à une utilisation collective* » ; d'autre part, que les analyses et les courtes citations dans un but d'exemple et d'illustration.

La représentation ou reproduction, par quelque procédé que ce soit, constituerait une contrefaçon sanctionnée notamment par les articles L. 335-2 et suivants du Code de la Propriété Intellectuelle.

Le présent document, propriété de **CHAMBERSIGN FRANCE**, peut être concédé par des accords de licence à toutes entités privées ou publiques qui souhaiteraient l'utiliser dans le cadre de leurs propres services de certification.

Thème	Description						
Point de contact :	Toute question ou remarque concernant les présentes PC peut être adressée par courriel à l'adresse suivante : <a href="mailto:qualite@chambersign.fr">qualite@chambersign.fr</a>						
Type de certificats émis, procédures associées et usages :	<p>Chaque porteur peut choisir librement son support cryptographique.</p> <p>Ce support doit cependant permettre de garantir le contrôle exclusif par le porteur sur sa bi-clé et sur la mise en oeuvre du certificat correspondant.</p> <p>Le porteur s'engage contractuellement auprès de ChamberSign France sur cette conformité. Les clés privées des porteurs ne font l'objet d'aucun séquestre et d'aucune sauvegarde par ChamberSign France.</p> <p>Les supports cryptographiques contenant les clés privées des porteurs doivent assurer la fonction d'authentification ou de signature pour le porteur légitime uniquement et protéger la clé privée contre toute utilisation par des tiers.</p> <p>Les certificats émis peuvent être sous forme logicielle.</p> <p>L'usage est la signature électronique de données par le porteur du certificat (signataire). Une telle signature électronique apporte, outre l'authenticité et l'intégrité des données ainsi signées, la manifestation du consentement du signataire quant au contenu de ces données.</p> <p>Par ailleurs, ChamberSign France peut être amené à émettre des certificats de test. Ces certificats de test sont identifiés comme tels dans leur DN par la mention explicite TEST. Ils ne sont couverts par aucune garantie par ChamberSign France et ils ne doivent en aucun cas être utilisés à d'autres fins qu'à des fins de test. A la fin des phases de tests, ces certificats sont révoqués.</p> <p>Les certificats émis conformément aux présentes Conditions Générales d'Utilisation contiennent l'OID suivant : 1.2.250.1.96.1.8.2.1</p> <p>Les certificats identifient les informations suivantes pour les personnes physiques :</p> <table border="0"> <tr> <td>Champ</td> <td>Description</td> </tr> <tr> <td>DN</td> <td>encodé en UTF8String</td> </tr> <tr> <td>countryName</td> <td>code ISO sur 2 lettres (cf. ISO3166-1) du pays de l'autorité compétente auprès de laquelle l'entité</td> </tr> </table>	Champ	Description	DN	encodé en UTF8String	countryName	code ISO sur 2 lettres (cf. ISO3166-1) du pays de l'autorité compétente auprès de laquelle l'entité
Champ	Description						
DN	encodé en UTF8String						
countryName	code ISO sur 2 lettres (cf. ISO3166-1) du pays de l'autorité compétente auprès de laquelle l'entité						

<p>est officiellement enregistrée (tribunal de commerce, ministère,...)</p> <p>organizationName nom officiel de l'entité (dénomination sociale du siège social)</p> <p>organizationalUnitName identifiant national de la structure parmi :</p> <ul style="list-style-type: none"><li>• Pour les entités basées en France Métropolitaine et les DOM : 0002 &lt;&lt;N° SIRET sur 14 caractères&gt;&gt;</li><li>• Pour les entités basées en Nouvelle-Calédonie : S540 &lt;&lt;N° RIDET sur 9 caractères maximum&gt;&gt;</li><li>• Pour les autres entités basées dans un pays de la communauté européenne : S&lt;&lt;code ISO3166-1 du pays sur 3 chiffres&gt;&gt; &lt;&lt;n° de TVA intracommunautaire sur 14 caractères maximum&gt;&gt;</li></ul> <p>Le champ peut être itéré 3 fois</p> <p>organizationIdentifieur Numéro d'immatriculation officiel du prestataire conformément à [EN_319_412-1] clause 5.1.4. En France, ce numéro d'immatriculation peut également être constitué du préfixe « SI:FR- » suivi du numéro SIREN ou SIRET</p> <p>Identifiant de l'entité avec laquelle le porteur est en lien</p> <ul style="list-style-type: none"><li>• VAT&lt;code pays&gt;-&lt;numéro de TVA intracommunautaire&gt;</li><li>• NTR&lt;code pays&gt;-&lt;numéro de SIREN&gt;</li></ul> <p>locality ville où se trouve l'établissement du porteur</p> <p>surName Nom du porteur</p> <p>givenName Prénom1(,Prénom2,Prénom3,...)</p> <p>Les différents prénoms sont mentionnés dans l'ordre indiqué sur la pièce d'identité présentée lors de l'enregistrement et dont la copie est conservée dans le dossier d'enregistrement.</p> <p>commonName Prénom1(,Prénom2,Prénom3,...) NOM</p> <p>Les différents prénoms sont mentionnés dans l'ordre indiqué sur la pièce d'identité présentée lors de l'enregistrement et dont la copie est conservée dans le dossier d'enregistrement.</p> <p>title le cas échéant, fonction du porteur au sein de sa structure</p> <p>serialNumber numéro séquentiel de 4 chiffres permettant de traiter les cas d'homonymie</p> <p>Par défaut, la valeur de cet attribut est « 0001 ». Si un porteur dont tous les autres attributs du DN sont identiques (countryName, organizationName, organizationIdentifieur, organizationalUnitName et commonName) a déjà été enregistré, la valeur de l'attribut serialNumber pour le nouveau porteur passe à « 0002 » et ainsi de suite.</p> <p>Les fichiers de demande de certificat, contenant la clé publique à certifier, sont scellés à l'aide de la clé privée correspondante.</p> <p>Les informations concernant la structure à laquelle le porteur est rattaché font l'objet de vérification lors de l'enregistrement (existence, validité, ...).</p>
---

L'identité du porteur ou du responsable de certificats est vérifiée au travers de la vérification de documents officiels d'identité effectuée lors d'un face-à-face.

Suite à validation du dossier de demande de certificat par la fonction d'enregistrement de l'IGC, le processus consiste à remettre au porteur ou au responsable de certificats la clé publique certifiée par l'AC : génération de la bi-clé, sous le contrôle et la responsabilité du porteur, dans un support cryptographique (logiciel ou matériel) choisi par le porteur (moyennant le respect des exigences définies au chapitre 6.2 ci-dessous), envoi de la clé publique à la fonction de génération des certificats, téléchargement sur le support du certificat généré.

Le certificat fait l'objet d'une acceptation explicite par le porteur ou le responsable de certificats au moment de sa remise.

Le premier renouvellement, s'il est autorisé par la réglementation au moment de l'expiration du certificat à renouveler, est réalisé en ligne s'il a lieu avant la date d'expiration du certificat correspondant. Le porteur ou le responsable de certificat valide en ligne que les informations liées au certificat à renouveler sont toujours exactes. Le renouvellement suivant est réalisé suivant la procédure d'enregistrement initial.

Le renouvellement suite à révocation est également réalisé suivant la procédure d'enregistrement initial.

La cause principale de la délivrance d'un nouveau certificat et de la bi-clé correspondante est l'arrivée en fin de validité du certificat. La durée de validité des certificats est de 3 ans. Les bi-clés doivent être en effet périodiquement renouvelées afin de minimiser les risques d'attaque cryptographique.

Un renouvellement peut être aussi réalisé de manière anticipée, suite à un événement ou un incident déclaré par le porteur, les plus fréquents étant la perte, le vol ou le dysfonctionnement du support cryptographique.

Une modification des informations contenues dans le certificat entraîne également la délivrance d'un nouveau certificat (avec renouvellement de la bi-clé).

Dans tous ces cas la délivrance d'un nouveau certificat est réalisée de manière identique au processus de délivrance initiale. Seule la phase d'enregistrement peut différer pour un renouvellement. Par exemple seuls quelques documents peuvent ne pas être demandés (acte de nomination du RL notamment).

Toute demande de révocation fait l'objet d'une authentification du demandeur et d'une vérification de son autorité pour une telle demande.

	<p>Il n'y a pas de suspension possible de certificat. Seule la révocation définitive des certificats peut être réalisée. ChamberSign France assure la disponibilité du statut de révocation à tout moment et au-delà de la période de validité du certificat en mettant en œuvre les mesures suivantes :</p> <ul style="list-style-type: none"><li>• Publication sans limite de temps des certificats révoqués dans les LCR publiées ;</li><li>• Conformité de la réponse OCSP, révoqué, en cas de sollicitation après la date de fin de vie du certificat.</li></ul> <p>Les circonstances suivantes peuvent être à l'origine de la révocation d'un certificat :</p> <ul style="list-style-type: none"><li>• la clé privée du certificat est perdue, volée, inutilisable (dysfonctionnement du support), compromise ou suspectée de compromission (demande du porteur lui-même) ;</li><li>• les informations ou les attributs du porteur figurant dans son certificat ne sont plus valides ou plus en cohérence avec l'utilisation prévue du certificat, ceci avant l'expiration normale du certificat ;</li><li>• les algorithmes cryptographiques mis en œuvres sont obsolètes et ne sont plus considérés sûrs ;</li><li>• il a été démontré que le porteur n'a pas respecté les modalités applicables d'utilisation du certificat ;</li><li>• le certificat d'AC est révoqué (ce qui entraîne la révocation des certificats signés par la clé privée correspondante) ;</li><li>• le porteur ne satisfait plus aux conditions professionnelles requises (cessation d'activité, décès).</li></ul> <p>Les causes de révocation ne sont jamais publiées.</p> <p>Les demandes de révocation sont traitées dans les 24h suivant la réception de la demande, 7 jours / 7 (week-ends et jours fériés compris si la révocation est traitée par le porteur, le responsable de certificat ou le représentant légal), hors révocations consécutives à des demandes de modification des données du porteur. La fonction de gestion des révocations est disponible 24 heures sur 24, 7 jours sur 7. La durée maximale d'indisponibilité par interruption (panne ou maintenance) de la fonction de gestion des révocations est de 2h. La durée maximale totale d'indisponibilité par mois de la fonction de gestion des révocations est de 8h.</p>
Limites d'utilisation :	<p>Le Client consent à ce que ChamberSign France conserve les documents relatifs à la preuve du contrôle d'identification des Porteurs pendant les délais prévus dans la Politique de Certification ainsi que les documents relatifs à la conclusion du présent contrat.</p> <p>Les journaux d'évènements sont conservés sur site pendant une durée de trente (30) jours. Après leur génération, ils sont archivés et conservés pendant sept (7) ans.</p> <p>Les dossiers d'enregistrement sont archivés pendant une durée de onze (11) ans à compter de la délivrance du</p>

	<p>Certificat. En cas de demande du Client d'obtenir une copie du dossier d'enregistrement, le Client sera facturé du coût correspondant.</p> <p>Les Certificats et les LCR sont archivés pendant une durée de cinq (5) ans.</p> <p>Si le Client souhaite que les dossiers d'enregistrement, les Certificats ou les LCR soient conservés pour une durée d'archivage supérieure, il devra en faire le nécessaire et en prendre le coût lui-même à sa charge.</p>
Obligations des souscripteurs :	<p>Le Client et son Représentant Légal s'engagent à respecter les stipulations des présentes CGU.</p> <p>Le Client et son Représentant Légal sont responsables de la gestion des Certificats délivrés aux employés, délégataires ou agents du Client dans le cadre du contrat d'abonnement, et s'engage à faire en sorte que tout Porteur de Certificat respecte les obligations prévues par les présentes CGU et qu'aucune fraude ou erreur n'est commise. A ce titre, le Client et son Représentant Légal s'assurent notamment que le Porteur :</p> <ul style="list-style-type: none"><li>- communique les informations utiles à la création du Certificat et les éventuelles modifications pendant toute la durée du Certificat ;</li><li>- respecte la procédure de révocation décrite à l'article 9 Révocation du Certificat ;</li><li>- conserve secrètes et de manière sécurisée, les données confidentielles et le support physique du Certificat.</li></ul> <p>Le Client et son Représentant Légal s'engagent à fournir toutes informations utiles, exactes et à jour pour la création et la gestion des Certificats.</p> <p>Le Client et son Représentant Légal s'engagent à informer le BE de rattachement de toute modification des informations contenues dans le Certificat, par courrier avec les pièces justificatives requises, sans délais. ChamberSign France se réserve le droit de révoquer le Certificat.</p> <p>Le Client et son Représentant Légal sont garants de l'exactitude des informations fournies et de l'exhaustivité des pièces justificatives nécessaires à l'enregistrement des Certificats.</p> <p>Le Client et son Représentant Légal reconnaissent et acceptent que les informations fournies à ce titre soient conservées et utilisées par ChamberSign France pour gérer les Certificats dans les conditions prévues par la loi et en particulier celles relatives à la protection des données personnelles.</p> <p>Le Client et son Représentant Légal reconnaissent être informés des conditions d'installation des Certificats de</p>

	<p>ChamberSign France. En particulier, le Certificat fait l'objet d'un tutoriel disponible sur le site Internet de ChamberSign France.</p> <p>Le Client et son Représentant Légal choisissent le matériel et les logiciels offrant une sécurité en adéquation avec leurs besoins pour l'installation et la protection des Certificats et des supports physiques.</p> <p>Le porteur ou le responsable de certificats est tenu de vérifier la validité du certificat et la conformité de son utilisation.</p>
Obligations de vérification certificats par les parties prenantes :	<p>Les circonstances suivantes peuvent être à l'origine de la révocation d'un certificat :</p> <ul style="list-style-type: none"><li>• la clé privée du certificat est perdue, volée, inutilisable (dysfonctionnement du support), compromise ou suspectée de compromission (demande du porteur lui-même) ;</li><li>• les informations ou les attributs du porteur figurant dans son certificat ne sont plus valides ou plus en cohérence avec l'utilisation prévue du certificat, ceci avant l'expiration normale du certificat ;</li><li>• les algorithmes cryptographiques mis en œuvres sont obsolètes et ne sont plus considérés sûrs ;</li><li>• il a été démontré que le porteur n'a pas respecté les modalités applicables d'utilisation du certificat ;</li><li>• le certificat d'AC est révoqué (ce qui entraîne la révocation des certificats signés par la clé privée correspondante) ;</li><li>• le porteur ne satisfait plus aux conditions professionnelles requises (cessation d'activité, décès).</li></ul> <p>Les causes de révocation ne sont jamais publiées.</p>
Limitations de garanties et limitations de responsabilité :	<p>ChamberSign France est responsable de la conformité de sa Politique de Certification, avec les exigences émises par la PC-Type.</p> <p>ChamberSign France assume toute conséquence dommageable résultant du non-respect de sa Politique de Certification par elle-même ou l'une de ses composantes.</p> <p>ChamberSign France reconnaît engager sa responsabilité en cas de faute ou de négligence prouvées, d'elle-même ou de l'une de ses composantes, quelle qu'en soit la nature et la gravité, qui aurait pour conséquence la lecture, l'altération ou le détournement des données personnelles des Porteurs à des fins frauduleuses, que ces données soient contenues ou en transit dans les applications de gestion des Certificats.</p> <p>ChamberSign France est responsable du maintien du niveau de sécurité de l'infrastructure technique sur laquelle elle s'appuie pour fournir ses services.</p> <p>ChamberSign France ne saurait être tenue responsable du préjudice causé par un usage du Certificat dépassant</p>

les limites de l'usage autorisé.

La responsabilité de ChamberSign France ne saurait être engagée en cas d'informations inexactes dues à de fausses déclarations, à de faux documents ou à l'absence d'information des modifications survenues dans la situation du Client, du Porteur, du Représentant Légal, ou du Mandataire de Certification lors de la création ou en cours de validité du Certificat, que la fausse déclaration, le faux document ou l'omission soit intentionnel ou pas.

ChamberSign France n'assume aucun engagement, ni aucune responsabilité quant aux conséquences des retards de transmission, altération, erreurs ou pertes de tout message électronique, lettre ou document signés ou authentifiés.

ChamberSign France ne saurait en aucun cas être tenue responsable du contenu des fichiers ou transactions signés ou authentifiés en utilisant le Certificat, le Client et le Porteur étant seuls responsables vis-à-vis des tiers du contenu de ces envois.

ChamberSign France ne sera en aucun cas tenue responsable des dommages indirects tels que, par exemple, tout préjudice financier ou commercial, perte de bénéfice ou d'exploitation, trouvant leur origine ou étant la conséquence de l'abonnement ou inhérents à l'utilisation des Certificats émis par ChamberSign France.

ChamberSign France n'assume aucun engagement ni responsabilité quant à l'utilisation par le Porteur d'un Certificat non conforme aux dispositions des présentes CGU, notamment pour ce qui concerne les procédures de contrôle de validité du Certificat lors d'une transaction.

Par ailleurs, ChamberSign France ne saurait être responsable des phénomènes liés à l'usure normale des médias informatiques, et notamment de la détérioration des informations portées sur lesdits médias due à l'influence des champs magnétiques.

ChamberSign France ne saurait être tenue pour responsable des dommages liés notamment à une interruption ou un dysfonctionnement des services et applications de l'Utilisateur de Certificats.

Si le Représentant Légal a fait l'acquisition d'un ou plusieurs supports physiques, ChamberSign France n'est responsable que de leur délivrance physique.

Du fait de l'évolution constante de la technologie et des niveaux de sécurités attachés au référentiel en vigueur,

	<p>en cas de dysfonctionnement du support physique ou de son logiciel pilote associé, le Client devra demander la révocation du Certificat.</p> <p>ChamberSign France ne saurait être responsable de l'usage de la Clé Privée du Porteur, qui en a la responsabilité personnelle. Tout dommage lié à la Compromission de la Clé Privée est à la charge du Client.</p> <p>ChamberSign France ne saurait voir sa responsabilité engagée du fait d'une utilisation illicite du Certificat dès lors que le Client, le Représentant Légal, le Mandataire de Certification ou le Porteur n'aura pas effectué une demande de révocation conformément aux présentes CGU.</p>
Agréments, Politique de Certification applicables :	La politique de certification applicable est publiée à l'adresse suivante : <a href="https://pc.chambersign.fr/ca3/ChamberSign_France_CA3_Qualified_eID.pdf">https://pc.chambersign.fr/ca3/ChamberSign_France_CA3_Qualified_eID.pdf</a>
Politique de protection des données :	Voir annexe 1
Politique d'assurance :	<p>ChamberSign France a souscrit, pour l'ensemble des dommages corporels, matériels et immatériels résultant de son activité une assurance couvrant les conséquences de sa responsabilité civile professionnelle.</p> <p>Aux termes du contrat d'assurance souscrit par ChamberSign France, et dans les limites et conditions de ce contrat, le Porteur pourra bénéficier du remplacement du Certificat perdu ou volé.</p>
Loi applicable et résolution des conflits :	<p>En cas de difficulté de toute nature et avant toute procédure juridictionnelle, les parties s'engagent à mettre en œuvre une procédure de conciliation.</p> <p>Les parties s'engagent à se réunir à l'initiative de la partie la plus diligente dans les huit jours à compter de la réception de la lettre de demande de réunion de conciliation.</p> <p>L'ordre du jour est fixé par la partie qui prend l'initiative de la conciliation.</p> <p>Les décisions, si elles sont arrêtées d'un commun accord, ont valeur contractuelle.</p> <p>Cette clause est juridiquement autonome du présent contrat. Elle continue à s'appliquer malgré l'éventuelle nullité, résolution, résiliation ou anéantissement des présentes relations contractuelles.</p> <p>A défaut, compétence expresse est attribuée aux tribunaux français.</p> <p>Les présentes CGU sont régies par la loi française.</p>

	<p>Il en est ainsi pour les règles de fond et les règles de forme et ce, nonobstant les lieux d'exécution des obligations substantielles ou accessoires.</p>
<p>Publication des informations, conformité :</p>	<p>Les certificats émis sont qualifiés eIDAS.</p> <p>Le certificat racine de l'IGC est téléchargeable sur le site Web de ChamberSign. L'utilisateur peut vérifier l'empreinte du certificat racine sur le site sécurisé <a href="https://www.keymanagement.chambersign.fr">https://www.keymanagement.chambersign.fr</a> ou en contactant ChamberSign France par téléphone.</p> <p>Les points de publication des LCR sont les suivants : <a href="http://crl.chambersign.fr/ca3/ChamberSign_France_CA3_Qualified_eID.crl">http://crl.chambersign.fr/ca3/ChamberSign_France_CA3_Qualified_eID.crl</a> <a href="http://crl.chambersign.tm.fr/ca3/ChamberSign_France_CA3_Qualified_eID.crl">http://crl.chambersign.tm.fr/ca3/ChamberSign_France_CA3_Qualified_eID.crl</a></p> <p>Le certificat d'AC est téléchargeable à l'adresse suivante : <a href="https://pc.chambersign.fr/ca3/ChamberSign_France_CA3_Qualified_eID.cer">https://pc.chambersign.fr/ca3/ChamberSign_France_CA3_Qualified_eID.cer</a></p> <p>Les répondeurs OCSP sont accessibles aux adresses suivantes : <a href="http://ocsp_ca3.chambersign.fr/ChamberSign_France_CA3_Qualified_eID">http://ocsp_ca3.chambersign.fr/ChamberSign_France_CA3_Qualified_eID</a> <a href="http://ocsp_ca3.chambersign.tm.fr/ChamberSign_France_CA3_Qualified_eID">http://ocsp_ca3.chambersign.tm.fr/ChamberSign_France_CA3_Qualified_eID</a></p>

## **ANNEXE 1. PROTECTION DES DONNEES A CARACTERE PERSONNEL**

### **1. Données à caractère personnel**

#### **1.1. Traitement de données à caractère personnel**

1. Les données à caractère personnel recueillies par ChamberSign France pour les besoins de la délivrance et de la conservation des Certificats ne seront traitées que pour les fins en vue desquelles elles ont été recueillies.

2. ChamberSign France déclare et garantit que les données à caractère personnel collectées dans le cadre des présentes ainsi que les traitements dont elle est le responsable ou selon le cas, en tant que sous-traitant, sont traitées conformément aux dispositions de la loi n°78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés (modifiée par la loi N° 2018-493 du 20 juin 2018 relative à la protection des données personnelles et l'ordonnance n° 2018-1125 du 12 décembre 2018 relative à l'informatique, aux fichiers et aux libertés et diverses dispositions concernant la protection des données à caractère personnel) ainsi qu'au règlement (UE) 2016/679 du Parlement européen et du Conseil du 27 avril 2016 relatif à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données, et abrogeant la directive 95/46/CE.

3. Le Client, le Représentant Légal, le Mandataire de Certification et le Porteur sont informés que conformément à la réglementation en vigueur, ChamberSign France, en tant que responsable de traitement, ou selon le cas, le sous-traitant, met en œuvre un traitement de données à caractère personnel les concernant ayant pour principales finalités :

- la fourniture des services de certification par ChamberSign France ;
- la gestion de l'accès et du fonctionnement des services de certification fournis par ChamberSign France ;
- l'identification du Porteur ;
- l'authentification du Porteur ;
- la délivrance, la conservation, le renouvellement et la révocation des Certificats et des Bi-clés ;
- l'établissement de statistiques et la mesure de la qualité et de la satisfaction des services de certification fournis par ChamberSign France.

4. Les données collectées sont obligatoires. A défaut, ChamberSign France ne pourra pas fournir les services de certification.

5. ChamberSign France assure la confidentialité et la sécurité des données collectées dans le cadre des présentes. Néanmoins, les données contenues dans le Certificat sont par nature publiques.

6. Les données traitées par ChamberSign France ne font pas l'objet d'un transfert en dehors de l'Union européenne.

7. Les données collectées sont seulement destinées aux services habilités de ChamberSign France. Ces données pourront être transmises à l'opérateur technique de ChamberSign France, qui respecte la même politique de confidentialité que ChamberSign France. Les données sont conservées pendant la durée prévue à l'article 22 Conservation ci-après.



8. Le Représentant Légal, le Mandataire de Certification et le Porteur sont informés par les présentes conditions générales d'utilisation qu'ils disposent d'un droit d'accès, de rectification, d'effacement, de limitation du traitement, d'opposition et du droit de définir des directives relatives au sort de ses données après leur décès, conformément à la loi Informatique et Libertés du 7 janvier 1978 relative à l'informatique, aux fichiers et aux libertés (modifiée) ainsi qu'au règlement UE n° 2016/679 du Parlement Européen du Conseil du 27 avril 2016 relatif à la Protection des Personnes Physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données.

9. Ces mêmes personnes disposent d'un droit d'opposition et de limitation du traitement, du droit à la portabilité des données, ainsi qu'un droit d'opposition à ce que ces données soient utilisées à des fins de prospection commerciale.

10. Afin d'exercer leurs droits, le Représentant Légal, le Mandataire de Certification et le Porteur peuvent écrire au référent RGPD de ChamberSign France par courrier accompagné d'une copie d'une pièce d'identité signée à l'adresse suivante : ChamberSign France – 3, Place de la Bourse – 69002 LYON ou bien :

- Par courrier électronique au Délégué à la Protection des Données à l'adresse suivante : [rgpd@chambersign.fr](mailto:rgpd@chambersign.fr), étant précisé que pour sécuriser l'authentification, l'envoi d'un mail signé électroniquement est privilégié ; l'envoi d'une pièce d'identité scannée (carte d'identité, passeport...) est prohibé afin de garantir la confidentialité des données. En l'absence de signature électronique, ChamberSign France procédera à l'authentification du demandeur par tout moyen approprié, ceci pour éviter toute divulgation des données à caractère personnel.

11. En cas de non-respect par ChamberSign France de la présente clause, ces personnes disposent du droit d'introduire une réclamation auprès de la Commission Nationale de l'Informatique et des Libertés (CNIL).

12. Ces obligations sont également remplies dans la charte de confidentialité, accessible depuis le site internet de ChamberSign, en cliquant sur le lien suivant : <https://www.chambersign.fr/p-charte-de-confidentialite.html>.

## **1.2. Sous-traitance**

13. Dans le cadre de l'exécution des services de certification, ChamberSign France pourra être amenée à traiter des données à caractère personnel pour le compte du Client.

14. Le Client agit dans ce cadre en tant que responsable des traitements et ChamberSign France en tant que son sous-traitant au sens de la réglementation applicable en France dans le domaine de la protection des données à caractère personnel.

15. A ce titre, ChamberSign France s'engage à traiter les données à caractère personnel confiées par le Client dans le respect de la réglementation applicable en France et selon les modalités contractuelles convenues par le Client responsable de traitement et ChamberSign France.