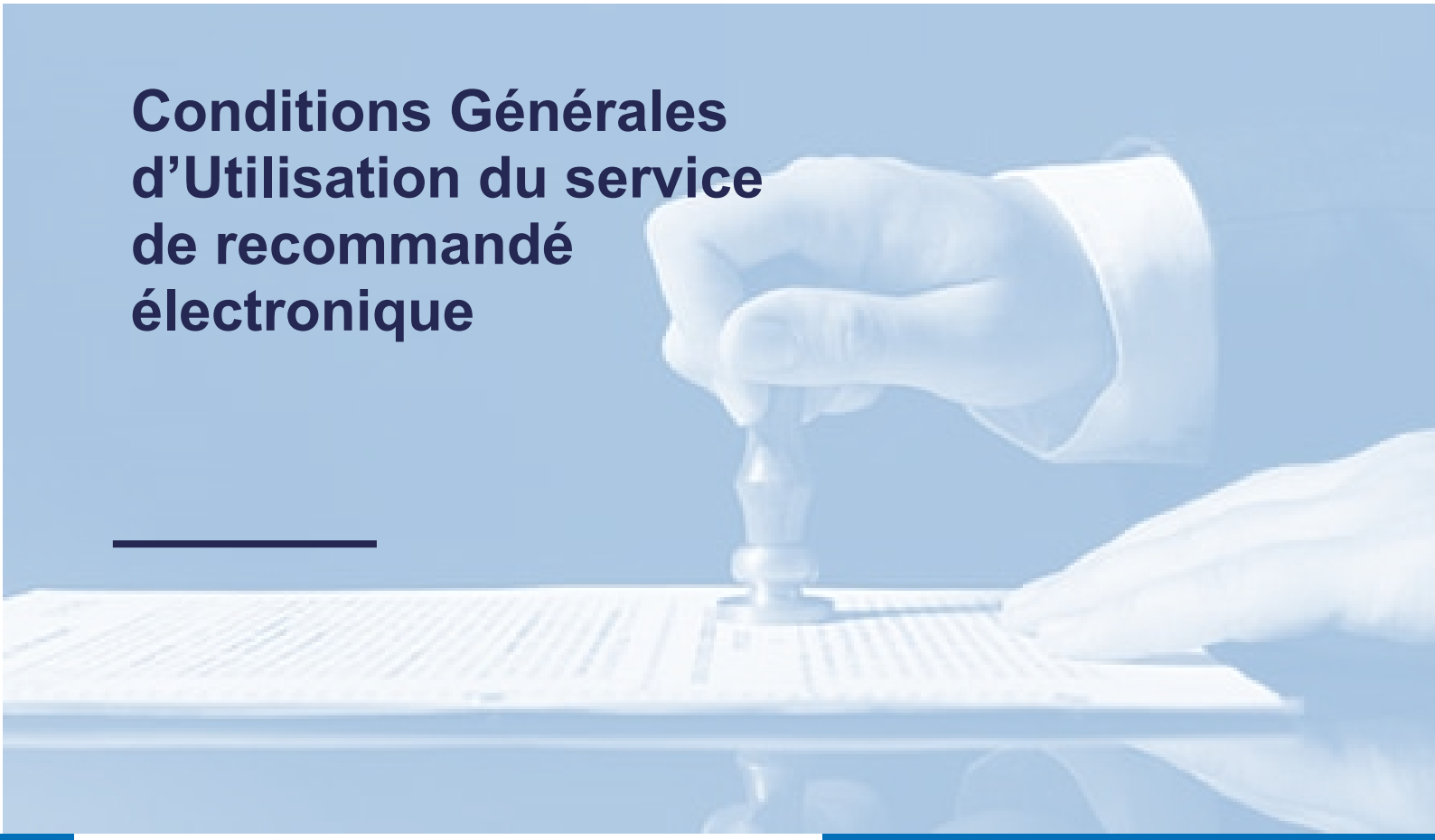
Conditions Générales d'Utilisation du service de recommandé électronique



V 1.2

Niveau de confidentialité : public

Datasure

L’historique du document est dans le tableau suivant :

Numéro de version	Date	Commentaire
1.0	09/07/2024	Version initiale du document
1.1	22/20/2024	Prise en compte du nouveau moyen d’identification
1.2	09/11/2024	Prise en compte des remarques de l’audit LSTI

1 Intégralité du présent accord

Le présent accord ne représente pas l’intégralité de l’accord entre le service de recommandé, les abonnés (expéditeurs et destinataires) et les utilisateurs.
L’intégralité des obligations et engagement du services de recommandé sont décrits dans sa Politique du service/ Déclaration des pratiques du service publique.
Les présentes CGU spécifique complètent la Politique du service spécifique, les CGV et CGU de Datasure.

2 Objet

Le présent document décrit les Conditions Générales d’Utilisation à destination des expéditeurs, destinataires et utilisateurs des preuves souhaitant utiliser le service de recommandé et vérifier les preuves émises par Datasure.

Avant toute utilisation du Service, l’expéditeur, le destinateur ou l’utilisateur reconnaît :

- Avoir pris connaissance des présentes CGU ;
- Disposer de la capacité juridique et des habilitations pour s’engager au titre des présentes CGU
- Accepter sans réserve les présentes CGU.

L’acceptation est matérialisée

- en cliquant sur la case à cocher sur le site lors de la création d'un compte d'Utilisateur ou avant la réception d'un document par le destinataire.

- Le cas échéant, au travers d'une annexe au contrat.

Les CGU sont mises à sa disposition par Datasure sur son site de publication. Elles peuvent être téléchargées au format PDF.

3 Informations de contact

Toute demande relative au service est à adresser au point de contact fourni à l'adresse suivante :

Datasure
Service de recommandé
8 rue Alfred Maurel
34120 PÉZENAS

Datasure peut également être contacté au travers du formulaire de contact disponible sur son site internet : https://www.datasure.net

4 Service de recommandé

Le Service de recommandé permet à un expéditeur de transmettre des documents à un destinataire de façon sécuriser tout en générant des preuves d'envoi, mais également de réception, et éventuellement de refus ou de non-réclamation.

4.1 Accès au service

L'accès au Service nécessite de disposer d'équipements logiciels et matériels adaptés pour accéder au Service ; Ces équipements diffèrent selon le niveau de recommandé cible, le rôle et le moyen de vérification d'identité mis en œuvre.

4.1.1 Accès au service par API (Expéditeur personne moral)

L'utilisation du Service au moyen de l'API nécessite la configuration du système d'information de l'abonné expéditeur selon les prescriptions de la Documentation. Il

nécessite également, lors de la phase d'inscription (vérification initiale de l'identité au moyen d'un dispositif PVID), l'émission d'un certificat de signature par l'AC Datasure. L'identification au service se fait au travers d'une double authentification :

- Authentification sur l'API permettant de limiter son accès aux seuls clients autorisés
- Signature électronique (QCP-n) du document soumis permettant de s'authentifier sur l'interface en vérifiant la signature du document PDF.

4.1.2 Accès au service par le navigateur (destinataire personne physique)

L'offre nécessite d'avoir un navigateur internet récent (Edge, Safari, Chrome ou Firefox par exemple). Certain moyens d'identification à distance peuvent nécessiter des équipements supplémentaires (téléphone portable muni d'une caméra, connexion 4G…) décrit dans les conditions générales de chacun des services.

4.2 Moyen d'identification initiale proposés

Offre LREQ **1.3.6.1.4.1.58753.3.1.1.1**	**Les moyens d'identification proposés sont :** **Procédure d'identification PVID**
Offre recommandé Art. 43 **1.3.6.1.4.1.58753.3.2.1.1**	**Les moyens d'identification proposés sont OTP SMS**

4.3 Source de temps utilisée

Datasure utilise sa propre autorité d'horodatage qualifiée (OID : 1.3.6.1.4.1.58753.1.1.1.1) pour son service de recommandé. Celui-ci est synchronisé à la seconde près au temps UTC.

4.4 Processus de remise

Il est entendu comme constituant une remise du contenu au destinataire le moment où, prenant connaissance de l'avis électronique reçu après son identification, il accepte expressément de recevoir l'envoi électronique et ainsi d'y accéder. La remise est matérialisée à ce moment de l'acceptation, où le destinataire accède à l'envoi électronique en lui-même et peut le télécharger.

Les points suivants détaillent le processus de remise.

4.4.1 Notification du destinataire

Le destinataire est informé par courriel à l'adresse indiquée par l'expéditeur lors du dépôt.

Datasure vérifie que l'envoi du message de notification s'est bien déroulé et qu'aucun message d'erreur n'est retourné à l'expéditeur :

- En cas d'erreur, l'expéditeur est notifié que la notification du destinataire à échoué
- En cas de succès, une preuve de notification est générée.

4.4.2 Processus d'identification du destinataire et Acceptation/rejet du recommandé

L'avis contient un lien permettant à l'utilisateur de réaliser sa procédure de vérification d'identité (PVID dans le cas LREQ ou SMS dans le cas LRE). En cas de succès, il accède à une page permettant d'accepter ou de refuser l'envoi électronique, constituant ainsi en cas d'acceptation la remise du contenu au destinataire.

4.4.3 Délai d'acceptation du recommandé

Le destinataire dispose d'un délai de 15 jours, à compter du lendemain de la première notification, pour accepter ou refuser la LREQ. Il dispose de 21 jours dans le cas de la LRE. Le contenu du recommandé peut ainsi être récupéré, après identification, pendant les délais précités. Par ailleurs dans le cas du LREQ, le destinataire doit formuler son acceptation du recommandé dans le délai d'1h après le succès de son identification, sous peine de voir son identification expirée et devoir se réidentifier.

4.4.4 Transmission du recommandé

Si le destinataire accepte le recommandé, son contenu est présenté dans le navigateur. L'interface lui permet également de télécharger le fichier. Une copie est transmise par e-mail à son adresse avec un lien valide pour la durée prévue au 4.4.3.

Un horodatage qualifié est produit à l'envoi et à l'acceptation du recommandé. En cas de refus ou de non-réclamation, un horodatage qualifié est produit au moment de l'occurrence de l'événement.

5 Limites d’utilisation

Les événements relatifs au cycle de vie d’un recommandé sont conservés pendant une période de 7 ans, conformément aux exigences de l’ANSSI.

Datasure ne vérifie pas l’adéquation du service fourni avec la réglementions applicable à l’abonné. En particulier, Datasure n’est pas habilité à traiter des données de santé ou des données relevant de la diffusion restreinte ou du confidentiel défense.

A ce titre, Datasure décline toute responsabilité en cas d’utilisation non adéquate de son service.

6 Obligation relative au service d’émission de recommandé

6.1 Obligation de l’expéditeur

Le porteur a le devoir de :

- communiquer des informations exactes et à jour lors de la demande de souscription;
- respecter les conditions d’utilisation du certificat d’authentification qui lui a été fournie et respecter les exigences de l’AC ;
- lorsque le destinataire est un particulier, avoir obtenu le consentement pour recevoir des recommandés sous forme électronique.

En souscrivant au service, l’abonnée accepte également :

- que Datasure conserve son dossier d’enregistrement et les traces de sa délivrance de certificat, ainsi que les traces liées au processus de révocation, le cas échéant.
- Qu’en cas d’arrêt d’activité, ces éléments puissent être transmis à un tiers en assurant sa conservation

6.2 Obligation du destinataire utilisant l’interface homme-machine.

Le Destinataire accepte :

- Protéger la confidentialité des notifications reçue et contenant une adresse internet unique de retrait de son recommandé;
- Télécharger le Contenu du recommandé suite à l'acceptation de celui-ci;
- Prendre toutes les mesures appropriées de façon à sécuriser son poste de travail, en particulier contre les codes malveillants et virus;

Le destinataire s'engage à respecter les conditions d'utilisation du moyen de vérification d'identité choisi (vérification d'identité à distance PVID, FranceConnect+, le cas échéant).

7 Obligations relatives à la vérification des preuves générées.

Il est recommandé à l'utilisateur souhaitant utiliser preuves générées par le service de Datasure, d'en vérifier l'origine et l'intégrité. En plus de la validation de la signature électronique, de vérifier le certificat de cachet électronique apposé. Les informations permettant de vérifier ces certificats sont disponibles sur le site de Datasure.

Le Service mis à la disposition de l'utilisateur Datasure permet :

- D'obtenir l'ensemble des certificats de la chaîne de certification jusqu'à l'AC Racine ;
- D'obtenir les listes de certificats révoqués (LCR). Les LCR sont conformes à la norme IETF RFC 5280.

Le service est disponible, en fonctionnement normal, 24h/24 et 7J/7 selon les conditions prévues par la Politique de Certification de l'AC. Datasure met également à disposition un service de répondeur OCSP

Ces vérifications peuvent être réalisées de façon automatique par des outils standard du marché tels qu'Acrobat Reader™ ou les bibliothèques Open-Source SD-DSS (fournies par la Commission européenne) et OpenSSL.

8 Rétention des traces

L'ensemble des traces relatives au service de confiance sont conservées pendant une période de 7 ans à compter du dernier élément du cycle de vie du recommandé (réception, refus ou non-réclamation), conformément aux exigences de l'ANSSI**.**

9 Limites de responsabilité.

La responsabilité de Datasure ne pourra être engagée en cas de non-respect par l'abonné, le destinataureou l'utilisateur des présentes conditions contractuelles.

En particulier, la responsabilité de Datasure ne pourra être engagé en cas d'inadéquation entre le niveau offert par le service, tel que décrit dans les présentes conditions et dans la politique du service, et les besoins de sécurité attendu par le client ou l'utilisateur.

Le service de recommandé de Datasure se limite à la mise à disposition d'un dispositif technique aux abonnés, destinateirs et utilisateurs. La responsabilité de Datasure ne pourra être engagée en cas d'usage du service par l'abonné, un destinataire ou l'utilisateur à des fins illégales ou non-conforme à la réglementation.

De même, Datasure ne pourra être tenu responsable des dommages, directs ou indirect causés par la divulgation des moyens de connexion fournis pour accéder au service.

Datasure ne pourra être tenu responsable d'aucun dommage indirect découlant de l'utilisation du service et en tout état de cause, la responsabilité sera limitée à hauteur du montant versé à Datasure pour l'obtention du certificat de signature électronique et le cas échéant, pour la réalisation d'un processus de signature.

Les informations nécessaires à la mise en œuvre de la procédure de vérification des des signatures et certificats sont disponibles sur le Site de publication de Datasure.

En cas d'évènement affectant la sécurité du Service et qui pourraient entraîner une conséquence sur les certificats, les signatures ou les cachet, une information appropriée sera mise à la disposition des Utilisateurs via le Site de publication de Datasure.

10 Politique applicable

Les politiques applicables pour chacune des offres sont précisées dans le tableau suivant.

LREQ	**1.3.6.1.4.1.58753.3.1.1.1**
Recommandé eIDAS au sens de l'art 43.	**1.3.6.1.4.1.58753.3.2.1.1**

11 Politique de protection des données à caractère personnel

La politique de protection de données à caractère personnel de Datasure est applicable.

12 Politique de remboursement

Il n'est pas prévu de remboursement.

13 Disponibilité

L'engagement de disponibilité du service d'émission de certificat fourni est 99.5% mensuel.

14 Loi applicable

La loi applicable est le droit français.
En cas de litige entre les parties découlant de l'interprétation, l'application et/ou l'exécution du contrat et à défaut d'accord amiable entre les parties ci-avant, la compétence exclusive est attribuée au tribunal de commerce de Béziers.

15 Procédure en cas de litige

En cas de litige, les parties chercheront un accord à l'amiable. A ce titre, Datasure pourra être contacté au point de contact mentionné dans la politique de certification et rappelé dans les présentes ci-dessous.

16 Conformité et audit

Le comité de Direction de Datasure procède à la validation de la conformité du service par rapport à ses engagements inscrits dans la Politique du service.

Un contrôle de conformité est réalisé lors de la mise en service du au travers d'une homologation de sécurité du service. De plus, un audit interne sera réalisé au moins tous les ans.

Dans le cadre d'obtention de la qualification eIDAS du service LREQ et de la certification ETSI 319521 du service de recommandé, l'audit de certification est réalisé par une société externe dûment accréditée et la qualification demandée auprès de l'organe de contrôle national, l'ANSSI.

Pour les certificats qualifiés, ia procédure de qualification de l'organe de contrôle national induit la conformité :

- Aux normes ETSI EN 319401 et ETSI EN 319521 ;
- Aux exigences complémentaires énoncées dans ladite procédure de qualification, en particulier les exigences relatives aux dispositifs cryptographiques.

Pour le service certifié, aux normes ETSI EN 319401 et ETSI EN 319521 ;