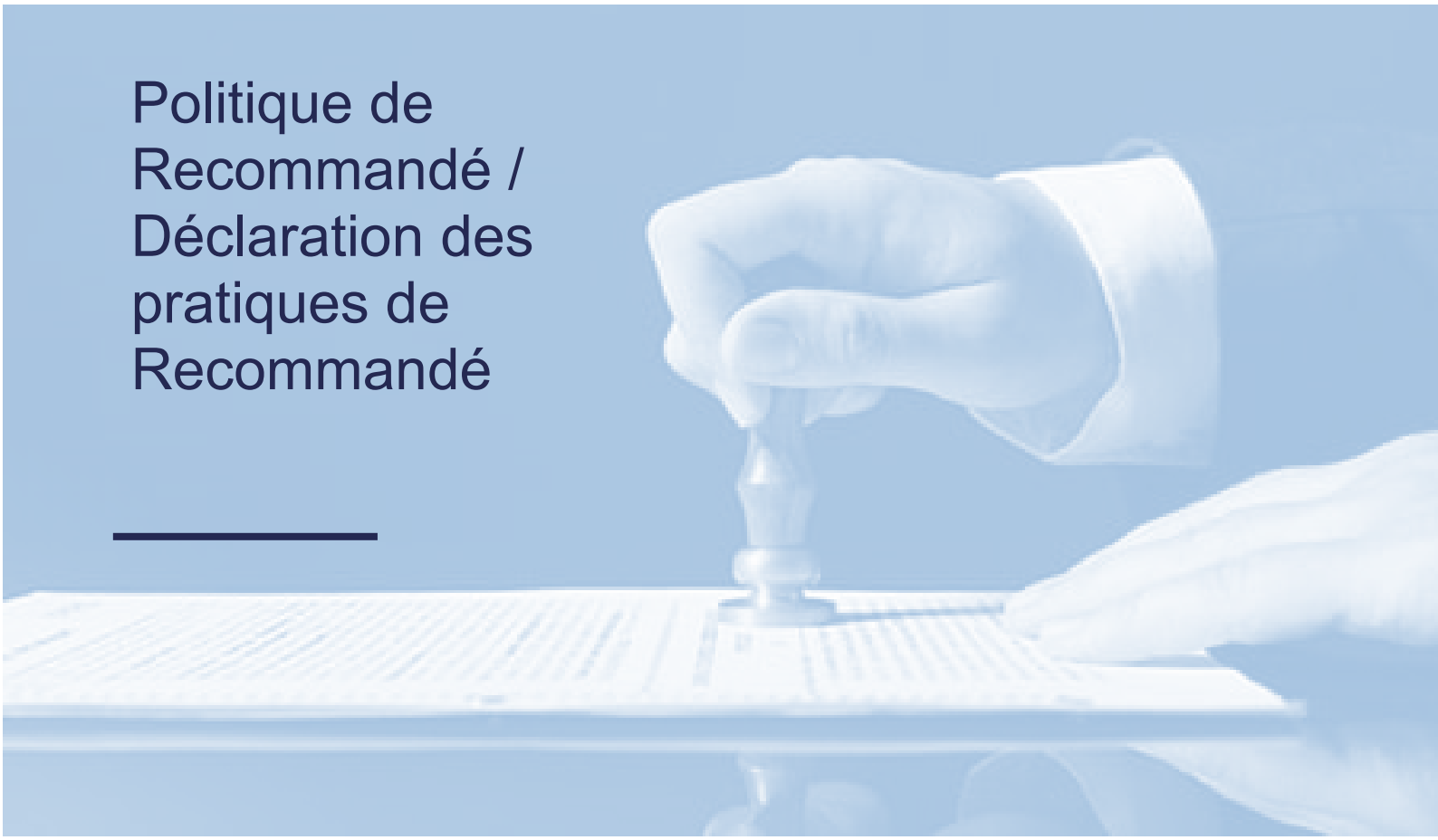
Politique de Recommandé / Déclaration des pratiques de Recommandé



V 1.1

OID : 1.3.6.1.4.1.58753.3.1.1.1

OID : 1.3.6.1.4.1.58753.3.2.1.1

Niveau de confidentialité : Public

Datasure

L'historique du document est dans le tableau suivant :

Numéro de version	Date	Commentaire
1.0	21/10/2024	Version initiale du document
1.1	09/11/2024	Prise en compte des remarques de LSTI

1 Introduction

Datasure est Prestataire de services de confiance qualifié. Dans le cadre de son offre de services, il opère un service de recommandé Datasure, permettant notamment d'envoyé des recommandés « simple » au sens du règlement eIDAS, mais également des lettres recommandés au sens de l'article L.100 du code des postes.
La présente politique vise à être conforme aux référentiels suivants :

- référentiels ETSI EN 319 521,
- référentiels de qualification des services de confiance de l'ANSSI,
- l'article L.100 du Code des postes et communication, ainsi que le Décret n° 2018-347 du 9 mai 2018.

Cette conformité permet de viser la reconnaissance des services par l'ANSSI comme Services qualifiés de recommandé électronique au sens du Règlement eIDAS et comme lettre recommandé électronique (LREQ) au sens du Code des Postes et Communications..

1.1 Identification du document

Cette identifiant est composé de la façon suivante [REQ-QERDS-4.1.2-01]

Racine Datasure	Type de service de confiance	Identifiant du service	Document	Version
1.3.6.1.4.1.58753	3 pour les services de recommandé	1 pour la LREQ	1 pour Politique	1
		2 pour le recommandé certifié.		

L'OID 1.3.6.1.4.1.58753.3.1.1.1 correspond donc à un service de recommandé :

- Qualifié au sens du règlement eIDAS Art. 44
- Conforme aux exigences du code L.100 du code des Postes et Communications.

1.2 Définitions et acronymes

Les définitions suivantes sont utilisées

LRE	Lettre recommandé électronique
LREQ	Lettre recommandé électronique qualifiée
PSCO	Prestataire de service de confiance
PSRE	Prestataire du service de recommandé électronique
OSRE	Opérateur du service de recommandé électronique
AH	Autorité d'horodatage

1.3 Entités intervenant dans le service

1.3.1 Prestataire du service de recommandé électronique (PSRE)

Datasure est le prestataire du service de recommandé électronique. Il est également l'opérateur du service (OSRE). Datasure pourra sous-traiter certaines opérations. La liste des éventuels sous-traitants est documenté dans la partie confidentielle de la déclaration des pratiques du service.

Le service de recommandé s'appuie sur deux autres services de confiance opérés par Datasure [REQ-QERDS-4.1.2-02]

- Un service d'horodatage (voir §1.3.2)
- Un service d'émission de cachet (voir §1.3.3)

1.3.2 Autorité d'horodatage (AH)

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.

1.3.3 Autorité de certificat (AC) et Service de cachet électronique

Datasure utilise les cachets qualifiés émis par son autorité de certification qualifiée (1.3.6.1.4.1.58753.2.1.1.1.1.2.1)
Datasure opère son propre service de cachet mettant en œuvre le certificat (1.3.6.1.4.1.58753.4.1.1.1.1.2.1)

1.3.4 Utilisateurs

Les utilisateurs du service sont les expéditeurs et les destinataires de recommandés électronique.

1.3.4.1 Expéditeurs

Les expéditeurs sont des personnes morales

- ayant contractualisées avec Datasure pour l'accès au service
- ayant réalisé la procédure d'enregistrement décrite dans la présente politique

1.3.4.2 Destinataires

Les destinataires sont des personnes physiques.
Elles doivent avoir réalisé l'une des procédures d'enregistrement décrite dans la présente politique.
Pour les personnes physiques, celle-ci doivent avoir préalablement donner leur consentement à recevoir des recommandés électroniques.

1.4 Gestion de la présente politique

1.4.1 Entité gérant la Politique

Datasure s'est doté d'une entité de gouvernance ayant la responsabilité globale des activités du service et l'autorité pour approuver la présente Politique / Déclaration des pratique du service (PS/DPS) [REQ-6.1-06]. Cette entité de gouvernance est responsable de la validation et de la gestion de la présente la présente Politique / Déclaration des pratiques. L'entité de Gouvernance, en tant que responsable du service, a la charge de mettre en œuvre les exigences de la présente la présente Politique / Déclaration des pratique [REQ-6.1-07]. Datasure s'offre la possibilité de sous-traiter certaines opérations [OVR-5.4.1-01].

En cas de recours à des sous-traitants, Datasure garde l'entière responsabilité de la bonne mise en œuvre des exigences de la présente la présente Politique / Déclaration des pratique [REQ-6.3-05/ REQ-7.1.1-08]. Cela est réalisé au travers de d'accord contractuels définissant les obligations et responsabilités du sous-traitant et au travers de contrôles [REQ-6.3-06/ REQ-7.1.1-07]

Datasure revoit régulièrement la présente la présente Politique / Déclaration des pratique et les politiques et procédures associées. Elle réalise également des contrôles (voir §8) afin de s'assurer de la bonne mise en œuvre des mesures énoncées dans la présente la présente Politique / Déclaration des pratique [REQ-6.1-08].

1.4.2 Point de contact

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

Datasure
Service recommandé électronique
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

1.4.3 Entité déterminant la conformité d'une déclaration des pratiques avec cette Politique

Le service doit être pourvue d'une direction ayant autorité et une responsabilité finale pour déterminer la conformité de la Déclaration des pratiques avec la Politique.

1.4.4 Procédures d'approbation de la conformité de la Déclaration des pratiques du service

Datasure met en place un processus d'approbation de la PS et de la conformité de la DPS avec la PS.
Datasure est responsable de la gestion (mise à jour, révisions) de la PS/DPS. Toute demande de mise à jour de la PS/DPS doit suivre le processus d'approbation mis en place ainsi que la procédure d'amendement (voir §9.12).
Toute nouvelle version de la PS/DPS doit être publiée, conformément aux exigences du paragraphe 2.2 sans délai [REQ-6.1-10].

2 Responsabilité concernant les informations devant être publiées

2.1 Entités chargées de la mise à disposition des informations

Datasure met en œuvre une fonction de publication.
La fonction de publication est accessible en HTTP(s) sur le site de publication suivant :

https://www.datasure.net/services/lre

Le site de publication est accessible publiquement sur internet [DIS-6.1-08, DIS-6.1-09]

2.2 Informations devant être publiées

LDatasure publie les informations suivantes à destination des porteurs et utilisateurs de certificats [REQ-6.1-05A] :

- la présente PS/DPS, exigences des normes ETSI 319521 et ETSI EN 319421;
- les CGUs du service [REQ-6.2-01] ;
- le lien vers les sites de publication de l'AC et de l'AH impliqué dans le service ;

- Les certificats de cachet ayant servi à sceller les preuves générées.

Les détails confidentiels de la déclaration de pratiques ne font pas l'objet d'une publication dans la présente PS/DPS et sont consignée dans une DPS confidentielle.

Les différents documents, y compris la présente PS/DPS et les CGUs sont publiés sous forme électronique, au format PDF scellé par un cachet qualifié Datasure afin d'assurer leur intégrité et leur origine [REQ-6.2-04/REQ-6.2-06].
L'ensemble des documents sont disponibles en langue française [REQ-6.2-05].
Datasure assure une disponibilité du site de publication 24h/24 et 7J/7. En cas de panne technique, ou de toute cas d'indisponibilité qui ne serait pas sous le contrôle de Datasure, Datasure fera tout son possible pour que l'information ne reste pas indisponible plus de 48 heures consécutives.

2.3 Délais et fréquences de publication

Les informations liées au service(nouvelle version de la PS/DPS, etc.) sont publiées dès que nécessaire afin que soit assurée à tout moment la cohérence entre les informations publiées et les engagements, moyens et procédures effectifs du service de recommandé. Les systèmes publiant ces informations sont disponibles 24h sur 24 et 7j/7.

2.4 Contrôle d'accès aux informations publiées

L'ensemble des informations publiées à destination des utilisateurs de certificats est libre d'accès en lecture. L'accès en modification aux systèmes de publication (ajout, suppression, modification des informations publiées) est strictement limité aux fonctions internes habilitées du service de recommandé, au travers d'un contrôle d'accès fort (basé sur une authentification au moins à deux facteurs).

3 Identification et authentification

3.1 Identification de l'expéditeur

Le service d'envoi recommandé électronique qualifié garantit l'identification de l'expéditeur avec un degré de confiance élevé :

- Au moyen d'un dispositif de vérification d'identité à distance certifié par l'ANSSI (PVID) pour la vérification initiale de l'identité
- Au moyen d'un certificat de signature QCP-n remis à l'issue de la vérification initiale de l'identité.

3.1.1 Validation initiale de l'identité

La procédure de vérification initiale de l'identité est strictement identique à la procédure mis en place par Datasure pour l'émission de certificats qualifiés QCP-n (1.3.6.1.4.1.58753.2.1.1.1.1.1.2) [REQ-QERDS-5.2.1.1-01].
Le certificat QCP-n émis est rattaché à l'organisation expéditrice.

L'identité d'un organisme est réalisée au travers de la vérification de l'identité du demandeur identifié comme interlocuteur pour le client personne morale. Le demandeur doit être mandaté par le responsable légal de l'organisation, dans le cas où le responsable légal n'est pas le demandeur.

3.1.1.1 Identité de l'organisation

L'identité de l'organisation doit être justifiée par un document officiel, typiquement un KBIS de moins de 3 mois pour une société

3.1.1.2 Identité du demandeur

La vérification de l'identité du porteur à l'aide d'un dispositif considéré comme équivalent au face-à-face au sens du Règlement eIDAS.
En particulier, la présente version de la PS/DPS autorise comme dispositif équivalent l'utilisation d'un dispositif certifié PVID
Les futurs versions de la présente PS pourront proposer des dispositifs équivalent tel que L'utilisation d'un dispositif FranceConnect+ (MIE de niveau substantiel) ou d'un porte-feuille d'identité eIDAS.

3.1.1.3 Autorité du demandeur sur l'organisation

Si le demandeur est le responsable légal, le demandeur a autorité pour engager l'organisation.
Si le demandeur n'est pas le représentant légal, un mandat signé, et daté de moins de 3 mois, par un représentant légal de l'entité désignant le demandeur doit être produit. Datasure, dans sa procédure d'enregistrement, met à disposition du responsable légal une procédure permettant de signer ce mandat électroniquement.

3.1.2 Moyen d'authentification

3.1.2.1 Remise du moyen d'authentification

Conjointement à la procédure de validation initiale, un certificat de signature QCP-n est délivré au demandeur par l'AC Datasure (OID : 1.3.6.1.4.1.58753.2.1.1.1.1.1.2) ainsi que des identifiants d'authentification sur l'interface. Les identifiants permettent à l'organisation d'accéder à l'interface d'expédition du service. Le certificat de signature permet l'authentification du signataire.

3.1.2.2 Authentification

L'authentification est réalisée par Datasure au moyen du certificat de signature délivré. Tous les documents soumis doivent être signés électroniquement au préalable par l'expéditeur à l'aide de son certificat qualifié. Datasure vérifie la signature avec d'identifier l'expéditeur.

3.1.2.3 Validité des moyens d'identification électronique délivrés par Datasure aux expéditeurs

La validité est limité à la durée de vie maximale du certificat, soit 3 ans.

3.2 Identification du destinataire

3.2.1.1 Cas du recommandé qualifié et LRE

La vérification de l'identité du porteur est réalisée à l'aide d'un dispositif considéré comme équivalent au face-à-face au sens du Règlement eIDAS [REQ-QERDS-5.2.1.1-01]

En particulier, la présente version de la PS/DPS autorise comme dispositif équivalent l'utilisation d'un dispositif certifié PVID.
L'utilisation de dispositifs équivalents au sens du Règlement eIDAS, tel qu'un dispositif FranceConnect+ (MIE de niveau substantiel) ou un portefeuille d'identité, pourra être envisagés dans le futur.
La présente version de la PS/DPS ne propose pas, pour le destinataire personne physique, la distribution d'un moyen d'authentification. Le destinataire devra vérifier son identité de façon systématique [REQ-QERDS-5.2.1.1-02]

3.2.1.1 Cas du recommandé non qualifié

Le vérification de l'identité du porteur se fait par la méthode suivante : vérification par OTP email ou SMS

4 Exigences opérationnelles sur le cycle de vie du recommandé

4.1 Processus d'envoi

La version de cette PS/DPS ne considère que l'envoi de document au format PDF.

4.1.1 Processus et responsabilités pour le dépôt d'un RE

Une Recommandé ne peut être envoyée que par une personne disposant :

- D'un compte (c'est-à-dire ayant souscrit au service)
- D'un certificat d'authentification NCP+ associé à ce compte.

4.1.2 Traitement du dépôt d'un recommandé

Pour déposer un recommandé, l'expéditeur doit s'authentifier fortement à l'aide de son certificat avant otu dépôt sur l'une des interface mise à disposition par Datasure. L'interface lui permet :

- De sélectionner un destinataire
- De soumettre le document (format PDF) sujet du recommandé.

Aucune vérification n'est effectuée sur le contenu du dépôt à l'exception de la vérification du format (PDF).
Une fois le dépôt terminé, le document est scellé par Datasure à l'aide d'un cachet qualifié et horodaté à l'aide d'un horodatage qualifié [REQ-QERDS-5.1.2-01/ REQ-QERDS-5.3.2-01]
Datasure étant son propre fournisseur de cachet et d'horodatage, le service ne réalise pas obligatoirement une vérification du cachet généré et du statut de qualification du prestataire [REQ-QERDS-5.1.2-03]
Les données transmises sont conservées [REQ-QERDS-5.1.2-02]

4.1.3 Acceptation ou rejet du dépôt

Les dépôts sont considérés acceptés lorsque l'expéditeur termine son envoi et le valide.

4.1.4 Remise de la preuve de dépôt

Une preuve de dépôt, reprenant la date du document horodatée, est produite, scellée et horodatée par Datasure. Elle est mise à disposition de l'expéditeur par Datasure. L'interface Datasure lui permet de consulter

cette preuve à tout instant après sa création. Si une erreur survenait lors du processus d'enregistrement du courrier, l'expéditeur serait notifié immédiatement de l'échec de son courrier.

4.2 Processus de remise

4.2.1 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.

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

Le courrier contient un lien permettant à l'utilisateur de réaliser sa procédure de vérification d'identité PVID. En cas de succès, il accède à une page permettant de d'accepter ou de refuser le recommandé.

4.2.3 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 LRE.

4.2.4 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 courriel à son adresse.
Un horodatage qualifié du document est produit à la l'acceptation et remise du document [REQ-QERDS-5.3.2-01]. En cas de refus ou de non-réclamation, un horodatage qualifié est produit au moment de l'occurrence de l'événement [REQ-QERDS-5.3.2-01]

4.2.5 Remise de la preuve de réception

En cas d'acceptation et de présentation du document une preuve de réception est générée et mise à disposition de l'expéditeur. Celui-ci peut récupérer le justificatif via un appel API [REQ-QERDS-4.1.1-11]

4.2.6 Remise de la preuve de refus

En cas de refus, une preuve de refus est générée et mise à disposition de l'expéditeur. L'expéditeur peut récupérer le justificatif à partir du moment du refus via un appel API. [REQ-QERDS-4.1.1-11]

4.2.7 Remise de la preuve de non-réclamation

Si le destinataire n'entreprend aucune action lors du délai d'acceptation (4.2.3) le recommandé est considéré comme non réclamé. Une preuve de non-réclamation est générée et mise à disposition de l'expéditeur. L'expéditeur peut récupérer le document via l'API [REQ-QERDS-4.1.1-11]. Le recommandé ne sera alors plus accessible au destinataire.

4.3 Modification des données

Le document ne fait l'objet d'aucune modification [REQ-ERDS-5.1.1-04].

4.4 Description des preuves

4.4.1 Format des preuves

Toutes les preuves produites par le service sont au format PDF et sont scellées par un cachet électronique du service de recommandé Datasure.
[REQ-QERDS-5.3.2-02]
Datasure fournissant son propre horodatage, la surveillance du statut de qualification du certificat n'est pas nécessaire [REQ-QERDS-5.3.2-03]

4.4.2 Contenu des preuves

4.4.2.1 Preuve d'envoi et de dépôt

La preuve de dépôt et d'envoi contient les éléments suivants :

- Nom et prénom ou raison sociale de l'expéditeur
- Adresse électronique de l'expéditeur
- Nom et prénom ou raison sociale du destinataire
- Adresse électronique du destinataire ou service de notification du destinataire
- Niveau du service et OID correspondant
- Numéro d'identification unique de l'envoi
- Date de l'événement et jeton d'horodatage qualifié
- Une référence non ambigu au document (haché du document transmis)

4.4.2.1 Preuve de réception

La preuve de réception contient en plus des éléments de la preuve de dépot :

- La date et heure de réception
- L'identité de la personne ayant réceptionné le document (fourni par le PVID ou le certificat) ainsi que le moyen utilisé et les éventuelles références.
- Le jeton d'horodatage correspondant à l'événement de réception.

4.4.2.2 Preuve de refus

La preuve de refus contient en plus des éléments de la preuve de dépot :

- La date et heure de refus
- L'identité de la personne ayant refusé le document (fourni par le PVID ou le certificat) ainsi que le moyen utilisé et les éventuelles références.
- Le jeton d'horodatage correspondant à l'événement de refus.

4.4.2.3 Preuve de non réclamation

La preuve de non-réclamation contient en plus des éléments de la preuve de dépôt :

- La date et heure d'expiration du délai
- Le jeton d'horodatage correspondant à l'événement de d'expiration du délai.

5 Mesures de sécurité non techniques

5.1 Mesures de sécurité physique

Datasure met en œuvre des mesure de sécurité physique afin de protéger ces services de confiance [$en particulier les services de recommandé.

5.1.1 Situation géographique et construction des sites

La construction des sites doit respecter les règlements et normes en vigueur

5.1.2 Accès physique

Datasure contrôle les accès physiques aux composants du service de recommandé dont la sécurité est critique pour la fourniture du service afin de minimiser les risques liés à la sécurité physique [REQ-7.6-01]. En particulier, un périmètre clair est définit autour des services sensibles.

L'accès est strictement limité aux seules personnes nominativement autorisées à pénétrer dans les locaux et la traçabilité des accès est assurée (entrée et sortie) [REQ-7.6-02]. Les personnels non-autorisés sont accompagnés en permanence par des personnels autorisés

En dehors des heures ouvrables, la sécurité est renforcée par la mise en œuvre de moyens de détection d'intrusion physique et logique.
Afin d'assurer la disponibilité des systèmes, l'accès aux machines est limité aux seules personnes autorisées à effectuer des opérations nécessitant l'accès physique aux machines [REQ-7.6-03]. Pour cela, les composantes concernées définissent un périmètre de sécurité physique où sont installées ces machines. La mise en oeuvre de ce périmètre permet de respecter la séparation des rôles de confiance telle que prévue dans la présente PS/DPS. Notamment, tout local utilisé en commun avec d'autres fonctions que les fonctions rendues par la composante concernée soit en dehors du périmètre de sécurité.
Les composants critiques pour l'opération sécurisée du service de confiance sont localisés dans un environnement de sécurité muni d'une protection physique contre les intrusions et de mécanismes d'alarme [REQ-7.6-05]
Des mesures sont mises en place pour empêcher que des équipements, des informations, des supports et des logiciels ayant trait aux services soient sortis du site sans autorisation [REQ-7.6-04].

Des contrôles d'accès sont appliqués pour remplir les exigences de sécurité attendues. Les contraintes sur l'environnement d'exploitation, identifiées dans la documentation liée à la certification du module (Profil de Protection, cible de sécurité), sont remplies.

5.1.3 Alimentation électrique et climatisation

Les caractéristiques des équipements d'alimentation électrique et de climatisation permettent de respecter les conditions d'usage des équipements telles que fixées par leurs fournisseurs.
Elles permettent également de respecter les exigences de l'ETSI EN319401 ainsi que les engagements pris par Datasure dans la présente PS, en matière de disponibilité de ses fonctions, notamment les fonctions mise à disposition des preuves.

5.1.4 Exposition aux dégâts des eaux

Datasure s'assure que les moyens de protection contre les dégâts des eaux permettent de respecter les exigences les exigences de l'ETSI EN319401 ainsi que les engagements pris par Datasuredans la présente PS, en matière de disponibilité de ses fonctions, notamment les fonctions de gestion des révocations et d'information sur l'état des certificats.

5.1.5 Prévention et protection incendie

Datasure s'assure que les moyens de prévention et de lutte contre les incendies permettent de respecter les exigences les s exigences de l'ETSI EN319401 ainsi que les engagements pris par Datasure dans la présente PS, en matière de disponibilité de ses fonctions, notamment les fonctions de gestion des révocations et d'information sur l'état des certificats.

5.1.6 Conservation des supports

Datasure assure un niveau de protection des biens approprié. Cela inclut les biens matériels mais également les biens immatériels et informations [REQ-7.3.1-01]
Les différentes informations intervenant dans les activités du service de recommandé sont identifiées et leurs besoins de sécurité définis (en confidentialité, intégrité et disponibilité) en ligne avec les résultats de l'analyse de risque. Datasure maintient un inventaire de ces informations [REQ-7.3.1-02]. Datasure met en place des mesures pour éviter la compromission et le vol de ces informations [. En particulier, tous les supports sont gérés de façon sécurisés en ligne avec les exigences de classification de l'information.
Les supports (papier, disque dur, supports amovible, etc.) correspondant à ces informations sont gérées selon des procédures conformes à ces besoins de sécurité [REQ-7.3.2-01].

En particulier, ils doivent être manipulés de manière sécurisée afin de protéger les supports contre les dommages, le vol et les accès non autorisés.
Des procédures de gestion protègent ces supports contre l'obsolescence et la détérioration pendant la période de temps durant laquelle Datasure engage à conserver les informations qu'ils contiennent [REQ-7.3.2-02].

5.1.7 Mise hors service des supports

En fin de vie, les supports devront être, soit détruits, soit réinitialisés en vue d'une réutilisation, en fonction du niveau de confidentialité des informations correspondantes [REQ-7.3.2-01]
Les procédures et moyens de destruction et de réinitialisation sont conformes à ce niveau de confidentialité visé.
Ces mesures de fin de vie permettent de protéger les données sensibles contre le risque de divulgation lors de la ré-utilisation de leur support [REQ-7.4-10]

5.1.8 Sauvegarde hors site

En complément de sauvegardes sur sites, les composantes du service de recommandé mettent en oeuvre des sauvegardes hors sites de leurs applications et de leurs informations.
Ces sauvegardes sont organisées de façon à assurer une reprise des fonctions du service après incident le plus rapidement possible, ETSI EN 319401 et 319521 ainsi qu'aux engagements de Datasure dans la présent PS en matière de disponibilité, en particulier pour les fonctions mise à disposition des preuves.
Les informations sauvegardées hors site respectent les exigences de de la présente PS Type en matière de protection en confidentialité et en intégrité de ces informations .

Les fonctions de sauvegarde et de restauration sont effectuées par les rôles de confiance appropriés et conformément aux mesures de sécurité procédurales.

5.2 Mesures de sécurité procédurales

Datasure s'assure que ces employés et sous-traitant participent pleinement à la sécurité des opérations [REQ-7.2-01].

5.2.1 Rôles de confiance

Les rôles de sécurité et les responsabilités sont documentés dans des descriptions de poste. Les rôles de confiance, sur lesquels la sécurité du fonctionnement de l'Autorité de certification repose, sont clairement identifiés au travers de fiches de poste mise à disposition des personnels [REQ-7.2-06/ REQ-7.2-07]

Les rôles de confiance incluent les rôles qui impliquent les responsabilités suivantes [REQ-7.2-15] :

- les officiers/responsables chargés de la sécurité : responsabilité complète d'administrer la mise en œuvre des pratiques de sécurité ; Le responsable de sécurité est chargé de la mise en œuvre et du contrôle de la politique de sécurité d'une ou plusieurs composantes de l'IGC. Il gère les contrôles d'accès physiques aux équipements des systèmes de la composante. Il est habilité à prendre connaissance des archives et des journaux d'évènements. Il est responsable des opérations de génération et de révocation des certificats.
- les administrateurs système : autorisés à installer, configurer et maintenir les modules de l'Autorité de certification ; Il est chargé de la mise en route, de la configuration et de la maintenance technique des équipements informatiques de la composante. Il assure l'administration technique des systèmes et des réseaux de la composante
- les opérateurs système : Un opérateur au sein d'une composante de l'IGC réalise, dans le cadre de ses attributions, l'exploitation au quotidien des applications pour les fonctions mises en oeuvre par la composante. L'opérateur système est responsable du fonctionnement les modules de l'Autorité de certification de manière quotidienne. Il est autorisé pour effectuer les opérations de sauvegarde et des secours ;
- L'opérateur de validation de l'identité est en charge de s'assurer que les processus de vérification de l'identité des expéditeurs et destinataires sont conformes aux normes et réglementation.
- les auditeurs de système/contrôleur : autorisés à consulter les archives et les fichiers d'audit des modules de l'autorité de certification. Personne autorisée à accéder et en charge de l'analyse régulière des archives et de l'analyse des journaux d'évènements afin de détecter tout incident, anomalie, tentative de compromission, etc.
- le responsable du cachet de scellement des preuves. Il est responsable du cachet et de son cycle de vie.

Le personnel du service de recommandé doit être formellement nommé aux rôles de confiance par la direction responsable de la sécurité [REQ-7.2-16A]. La personne nommée en rôle de confiance accepte également formellement son rôle et ses responsabilités [REQ-7.2-16B].

Des procédures sont établies et appliquées pour tous les rôles administratifs et les rôles de confiance ayant trait à la fourniture de services de certification [REQ-7.7-08].

Les rôles sont décrits et définis dans la description des postes propre à chaque entité opérant une des composantes du service de recommandé sur les principes de séparation des responsabilités et du moindre privilège. Ces rôles déterminent la sensibilité du poste, en fonction des responsabilités et des niveaux d'accès, des vérifications des antécédents et de la formation et de la sensibilisation des employés [REQ-7.2-10].

De plus, les opérations de sécurité du service de recommandé doivent être séparées des opérations normales [REQ-7.2-11]. Les responsabilités des opérations de sécurité incluent :

- les procédures et responsabilités opérationnelles ;
- la planification et la validation des systèmes sécurisés ;
- la protection contre les logiciels malicieux ;
- l'entretien ;
- la gestion de réseaux ;

- la surveillance active des journaux d'audit, l'analyse des évènements et les suites ;
- la manipulation et la sécurité des supports ;
- l'échange de données et de logiciels.

5.2.2 Nombre de personnes requises par tâche

La DPS confidentielle du service précise quelles sont les opérations nécessitant l'intervention de plusieurs personnes et quelles sont les contraintes que ces personnes doivent respecter.

5.2.3 Identification et authentification pour chaque rôle

Chaque entité opérant une composante du service vérifie l'identité et les autorisations de tous membres de son personnel amené à travailler au sein de la composante avant de lui attribuer un rôle et les droits correspondants, notamment :

- que son nom soit ajouté aux listes de contrôle d'accès aux locaux de l'entité hébergeant la composante concernée par le rôle ;
- que son nom soit ajouté à la liste des personnes autorisées à accéder physiquement à ces systèmes ;
- le cas échéant et en fonction du rôle, qu'un compte soit ouvert à son nom dans ces systèmes ;
- éventuellement, que des clés cryptographiques et/ou un certificat lui soient délivrés pour accomplir le rôle qui lui est dévolu dans le service.

Ces contrôles sont décrits dans la DPS Confidentielle du service et sont conformes à la politique de sécurité de la composante.
Chaque attribution d'un rôle à un membre du personnel du service est notifiée par écrit. Ce rôle est clairement mentionné et décrit dans sa fiche de poste.

5.2.4 Rôles exigeant une séparation des attributions

Des descriptions de fonctions sont définies pour le personnel du service de recommandé (aussi bien provisoire que permanent) du point de vue de la séparation des responsabilités et du principe du privilège minimum, selon la sensibilité de la fonction sur la base des responsabilités et des niveaux d'accès.
Plusieurs rôles peuvent être attribués à une même personne, dans la mesure où le cumul ne compromet pas la sécurité des fonctions mises en oeuvre
En particulier, les rôles pouvant présenter des conflits d'intérêts ainsi que les aires de responsabilité doivent faire l'objet, chaque fois que cela est possible, d'une séparation des rôles pour réduire les opportunités d'atteinte, volontaire ou non, à l'intégrité du SI ou d'une mauvaise utilisation des biens [REQ-7.1.2-01/ REQ-7.2-14].

Concernant les rôles de confiance, les cumuls suivants sont interdits :

- responsable de sécurité et ingénieur système / opérateur / contrôleur ;
- ingénieur système, opérateur et contrôleur.

5.3 Mesures de sécurité vis à vis du personnel

5.3.1 Qualifications, compétences, et habilitations requises

Tous les personnels amenés à travailler au sein de composantes du service sont soumis à une clause de confidentialité vis-à-vis de leur employeur.

Chaque entité opérant une composante du service s'assure que les attributions de ses personnels, amenés à travailler au sein de la composante, correspondent à leurs compétences professionnelles

Datasure emploie un personnel qui possède l'expertise, la formation, l'expérience et les qualifications nécessaires pour les services offerts, tels que l'exige la fonction. En particulier, le personnel a réalisé des formations sur la sécurité informatique et la protection des données à caractère personnel en ligne avec la spécificité d'un service de recommandé et les fonctions occupées au sein de ce service.
Le personnel est en nombre suffisant pour assurer le volume de travail nécessaire pour la fourniture du service [REQ-7.2-02].
L'expertise des employés est acquise au travers de l'expérience, de formations spécifiques ou d'une combinaison des deux [REQ-7.2-03].

Le personnel de gestion employé doit posséder :

- la connaissance de la technologie de cachet et d'horodatage et ;
- pour le personnel avec des responsabilités de sécurité, une bonne connaissance des procédures de sécurité, et ;
- l'expérience avec la sécurité de l'information et l'évaluation des risques.

Le personnel d'encadrement possède également, au travers de son expérience ou d'une formation relative au service de confiance eIDAS, en particulier aux service d'émission de certificat, une familiarité avec les procédures de sécurité applicable à son personnel. Il doit également être familier des procédures de sécurité ainsi que des notions relatives aux responsabilités en matière de sécurité et disposer d'une expérience en sécurité de l'information et en analyse de risque suffisante pour être en mesure d'assurer la fonction d'encadrement [REQ-7.2-12/REQ-7.2-13].

Datasure informe toute personne intervenant dans des rôles de confiance du service :

- de ses responsabilités relatives au service,
- des procédures liées à la sécurité du système et au contrôle du personnel, auxquelles elle doit se conformer.

En particulier, les personnes intervenant dans des rôles de confiance doivent y être formellement affectées par l'encadrement supérieur chargé de la sécurité.

5.3.2 Procédures de vérification des antécédents

Datasure met en œuvre tous les moyens légaux dont elle dispose pour s'assurer de l'honnêteté de ses personnels Datasure ne nomme pas aux rôles de confiance ou de gestion toute personne connue pour avoir une condamnation pour un crime sérieux ou une autre infraction qui affecte son adéquation avec la position. Le personnel n'a pas accès aux fonctions de confiance avant que les contrôles nécessaires ne soient achevés [REQ-7.2-17]
Le contrôle inclut une vérification de l'extrait de casier judiciaire (bulletin n°3).
Datasure peut décider en cas de refus de communiquer cette copie ou en cas de présence de condamnation de justice incompatible avec les attributions de la personne, de lui retirer ces attributions. Ces vérifications sont menées préalablement à l'affectation à un rôle de confiance et revues régulièrement (au minimum tous les 3 ans).

5.3.3 Exigences en matière de formation initiale

Le personnel est préalablement formé aux logiciels, matériels et procédures internes de fonctionnement et de sécurité qu'il met en oeuvre et qu'il doit respecter, correspondant à la composante au sein de laquelle il opère.
Datasure s'assure que les personnels ont la connaissance nécessaire et comprennent les implications des opérations dont ils ont la responsabilité.

5.3.4 Exigences en matière de formation continue et fréquences des formations

Le personnel concerné reçoit une information et une formation adéquates préalablement à toute évolution dans les systèmes, dans les procédures, dans l'organisation ou tout autre domaine pertinent en fonction de la nature de ces évolutions

La formation continue des employés inclut une mise à niveau, a minima annuelle, de la connaissance des nouvelles menaces et pratiques de sécurité [REQ-7.2-04].

5.3.5 Fréquence et séquence de rotations entre différentes attributions

Sans objet

5.3.6 Sanctions en cas d'actions non autorisées

Des sanctions disciplinaires sont prévues en cas de non-respect des consignes énoncées dans la présente PS/DPS, la DPS confidentielle ou dans la PSSI [REQ-7.2-05].

5.3.7 Exigences vis à vis du personnel des prestataires externes

Les exigences vis-à-vis du personnel des prestataires externes sont similaire à celle des employés de Datasure. Ceci est traduit en clauses adéquates dans les contrats avec ces prestataires.

5.3.8 Documentation fournie au personnel

Chaque personnel dispose de la documentation adéquate concernant les procédures opérationnelles et les outils spécifiques qu'il met en oeuvre ainsi que les politiques et pratiques générales de la composante au sein de laquelle il travaille. En particulier, il doit lui être remis la ou les politique(s) de sécurité l'impactant.

5.4 Procédures de constitution des données d'audit

La journalisation d'évènements consiste à les enregistrer de façon manuelle ou automatique. Les fichiers résultants, sous forme papier ou électronique, doivent rendre possible la traçabilité et l'imputabilité des opérations effectuées.

Datasure conserve et garde accessible, pour une période appropriée, y compris en cas de cessation d'activité, toutes les données pertinentes créées et reçues par le service, en particulier à des fins de preuve légales mais également afin d'assurer la continuité du service [REQ-7.10-01].

5.4.1 Type d'événement à enregistrer

Concernant les systèmes liés aux fonctions qui sont mises en oeuvre dans le cadre de l'IGC, chaque entité opérant une composante de l'IGC journalise les évènements tels que décrits ci-dessous, sous forme électronique. La journalisation est automatique, dès le démarrage d'un système et sans interruption jusqu'à l'arrêt de ce système.

- création / modification / suppression de comptes utilisateur (droits d'accès) et des données d'authentification correspondantes (mots de passe, certificats, etc.) ;
- démarrage et arrêt des systèmes informatiques et des applications ;
- évènements liés à la journalisation : démarrage et arrêt de la fonction de journalisation, modification des paramètres de journalisation, actions prises suite à une défaillance de la fonction de journalisation ;
- connexion / déconnexion des utilisateurs ayant des rôles de confiance, et les tentatives non réussies correspondantes.

D'autres évènements sont recueillis, par des moyens électroniques ou manuels. Ce sont ceux concernant la sécurité et qui ne sont pas produits automatiquement par les systèmes informatiques, notamment :

- les accès physiques ;
- les actions de maintenance et de changements de la configuration des systèmes ;
- les changements apportés au personnel ;

- les actions de destruction et de réinitialisation des supports contenant des informations confidentielles (clés, données d'activation, renseignements personnels sur les porteurs,...).

En plus de ces exigences de journalisation communes à l'ensemble des services de confiance, des évènements spécifiques au service de recommandé doivent également être journalisés, notamment :

- données d'identification des expéditeurs et destinataires
- moyen d'identification ou d'authentification mis en œuvre et résultats (résultat du PVID, résultat de l'authentification par certificat,
- dossier d'enregistrement lié à la vérification initiale de l'identité
- traces des différentes opération du service, incluant la vérification de l'identité de l'expéditeur et du destinataire, et les traces des communications
- éléments de preuve démontrant que la vérification de l'identité a été réalisé avant le transfert des données de l'expéditeur,
- preuve de non modification des données durant le transfert
- haché des données soumise, réalisé au travers de l'application du cachet et de l'horodatage de dépôt
- les jetons d'horodatage correspondant aux dates des différents événements (dépôt, réception, refus et non-réclamation

Chaque enregistrement d'un évènement dans un journal doit contenir au minimum les champs suivants :

- type de l'évènement ;
- nom de l'exécutant ou référence du système déclenchant l'évènement ;
- date et heure de l'évènement (l'heure exacte des évènements significatifs de l'AC concernant l'environnement, la gestion de clé et la gestion de certificat doit être enregistrée) ;
- résultat de l'évènement (échec ou réussite).

L'imputabilité d'une action revient à la personne, à l'organisme ou au système l'ayant exécutée. Le nom ou l'identifiant de l'exécutant doit figurer explicitement dans l'un des champs du journal d'évènements.

De plus, en fonction du type de l'évènement, chaque enregistrement devra également contenir les champs suivants :

- destinataire de l'opération ;
- nom du demandeur de l'opération ou référence du système effectuant la demande ;
- nom des personnes présentes (s'il s'agit d'une opération nécessitant plusieurs personnes) ;
- cause de l'évènement ;
- toute information caractérisant l'évènement (par exemple, pour la génération d'un certificat, le numéro de série de ce certificat).

Les opérations de journalisation sont effectuées au cours du processus.
En cas de saisie manuelle, l'écriture se fait, sauf exception, le même jour ouvré que l'évènement.
Les évènements et données spécifiques à journaliser sont documentés par l'AC

5.4.2 Fréquence de traitement des journaux d'événements

Cf. chapitre §5.4.8 ci-dessous

5.4.3 Période de conservation des journaux d'événements

Les journaux d'événements sont conservées pour une durée appropriées afin de permettre la fourniture, le cas échéant, d'éléments de preuve juridique. La durée de conservation est notifiée dans les CGUs.

Les journaux d'évènements sont conservés sur site pendant au moins un (1) mois. Ils sont archivés le plus rapidement possible après leur génération et au plus tard sous un (1) mois (recouvrement possible entre la période de conservation sur site et la période d'archivage).

5.4.4 Protection des journaux d'événements

Datasure assure la confidentialité et l'intégrité des données d'audit concernant les opérations du service [REQ-7.10-02]
Les événements sont générés de façon à ce qu'ils ne puissent pas être altérés ou générés facilement durant leur période de conservation [REQ-7.10-08]

La journalisation est conçue et mise en oeuvre de façon à limiter les risques de contournement, de modification ou de destruction des journaux d'évènements [RGS].

Les journaux d'évènements sont protégés en disponibilité (contre la perte et la destruction partielle ou totale, volontaire ou non).
Le système de datation des évènements doit respecter les exigences du chapitre 6.8.
La définition de la sensibilité des journaux d'évènements dépend de la nature des informations traitées et du métier. Elle peut entraîner un besoin de protection en confidentialité.

5.4.5 Procédure de sauvegarde des journaux d'événements

Chaque entité opérant une composante du service met en place les mesures requises afin d'assurer l'intégrité et la disponibilité des journaux d'évènements pour la composante considérée, conformément aux exigences des PS Type RGS, des normes ETSI EN 319401, ETSI EN 319411-1 et ETSI EN 319411-2.

5.4.6 Système de collecte des journaux d'événements

5.4.7 Notification de l'enregistrement d'un événement au responsable de l'événement

Sans objet

5.4.8 Evaluation des vulnérabilités

Chaque entité opérant une composante du service doit être en mesure de détecter toute tentative de violation de l'intégrité de la composante considérée.

5.5 Archivage des données

5.5.1 Types de données à archiver

Des dispositions en matière d'archivage doivent également être prises par l'AC. Cet archivage doit permettre d'assurer la pérennité des journaux constitués par les différentes composantes du service.
Les journaux concernant les opérations sont archivées de façon complète et confidentielle conformément aux disposition de la politique d'archivage [REQ-7.10-03]

Il doit également permettre la conservation des pièces papier liées aux opérations de certification, ainsi que leur disponibilité en cas de nécessité.
Les données à archiver sont au moins les suivantes :

- les logiciels (exécutables) et les fichiers de configuration des équipements informatiques ;

- les PS ;
- les DPS ;
- les conditions générales d'utilisation ;
- les accords contractuels avec d'autres AC ;
- les certificats, LCR ou réponses OCSP tels qu'émis ou publiés ;
- les récépissés ou notifications (à titre informatif) ;
- les justificatifs d'identité des porteurs et, le cas échéant, de leur entité de rattachement ;
- les journaux d'évènements des différentes entités.

Datasure fournit à chacun de ces clients expéditeurs une interface permettant de récupérer l'ensemble des preuves relative au cycle de vie des documents transmis [REQ-ERDS-4.1.1-11]

5.5.2 Période de conservation des archives

5.5.2.1 Dossier Recommandé

Tout dossier relatif au cycle de vie un recommandé est archivé aussi longtemps que nécessaire, et pendant au moins sept (7) ans après la date de délivrance, de refus ou de non-réclamation pour les besoins de fourniture de la preuve de dans des procédures légales, conformément à la loi applicable [REQ-ERDS-4.1.1-12, REQ-QERDS-4.1.2-04]

La durée de conservation des dossiers d'enregistrement est portée à la connaissance de l'expéditeur et du destinataire au travers de CGUs [REQ-7.10-07]

Au cours de cette durée d'opposabilité des documents, le dossier de demande de certificat sera présenté par Datasure lors de toute sollicitation par les autorités habilitées.

Ce dossier, complété par les mentions consignées par l'AC ou le PVID, permet de retrouver l'identité réelle des personnes physiques ou morale impliquées dans le processus.

5.5.2.2 Journaux d'évènements

Les journaux d'évènements traités au chapitre 5.4 sont archivés pendant sept (7) années après leur génération.

Les moyens mis en oeuvre par par le service pour leur archivage offre le même niveau de sécurité que celui visé lors de leur constitution. En particulier, l'intégrité des enregistrements devra être assurée tout au long de leur cycle de vie

5.5.3 Protection des archives

Pendant tout le temps de leur conservation, les archives, et leurs sauvegardes, sont :

- protégées en intégrité ;
- accessibles aux personnes autorisées ;
- lisibles et exploitables.

Datasure précise dans sa DPS confidentielle les moyens mis en oeuvre pour archiver les pièces en toute sécurité.

5.5.4 Procédure de sauvegarde des archives

Afin d'assurer leur disponibilité, Datasure met en place des procédures de redondances de ces archives. Ces mesures sont décrites en détail dans la DPS confidentielle.

Le niveau de protection des sauvegardes est au moins équivalent au niveau de protection des archives.

5.5.5 Exigences d'horodatage des données

L'heure précise des événements, en particulier relatif à l'environnement du service, de la gestion des clés et de la synchronisation des horloges sont enregistrés [REQ-7.10-05].

Cf. chapitre 5.4.4 pour la datation des journaux d'évènements.
Le chapitre 6.8 précise les exigences en matière de datation / horodatage

5.5.6 Système de collecte des archives

Le système de collecte des archives respecte les exigences de protection des archives

5.5.7 Procédures de récupération et de vérification des archives

Les enregistrements concernant les opérations du services seront rendu disponible en cas de besoin de fournir des éléments de preuve leur bonne mise en œuvre, en particulier en cas de besoin juridique [REQ-7.10-04]

5.6 Reprise suite à compromission et sinistre

5.6.1 Capacités de continuité d'activité suite à un sinistre

Datasure a défini un plan de continuité d'activité et de reprise d'activité en cas de sinistre [REQ-7.11-01]
Les différentes composantes du service disposent des moyens nécessaires permettant d'assurer la continuité de leurs activités en conformité avec les exigences des exigences de l'ETSI 319401, 319521 que de la présente PS/DPS.
En particulier, afin d'assurer la disponibilité du service, les accès réseaux sont redondés afin de permettre la disponibilité du service en cas de panne [REQ-7.8-12].

5.6.2 Procédures de remontée et de traitement des incidents et des compromissions

Chaque entité opérant une composante du service met en oeuvre des procédures et des moyens de remontée et de traitement des incidents, notamment au travers de la sensibilisation et de la formation de ses personnels et au travers de l'analyse des différents journaux d'évènements. Ces procédures et moyens doivent permettre de minimiser les dommages dus à des incidents de sécurité et des dysfonctionnements.

5.6.2.1 Surveillance du système, alerte et incidents

L'activité des différents systèmes mis en œuvre fait l'objet d'une surveillance, en particulier, l'utilisation et les requêtes vers les services sont surveillées [REQ-7.9-01].
Les activités de surveillance prennent en compte la sensitivité des données collectées et analysés [REQ-7.9-02]
La surveillance a pour but la détection de toute activité jugée anormale et indiquant un potentiel incident de sécurité, y compris une intrusion réseau. En cas de détection, une alarme est levée [REQ-7.9-03]
Les éléments suivants font l'objet d'une surveillance [REQ-7.9-04] :

- Le démarrage ou la désactivation des fonctions de génération des traces d'audit,
- La disponibilité et l'utilisation du service, en particulier le réseau.

La surveillance doit inclure la surveillance des traces d'audit ou leur revue régulière afin d'identifier l'existence d'activité malicieuses en mettant en œuvre des mécanismes automatique d'analyse des traces et de génération d'alertes en cas d'événements de sécurité critique [REQ-7.9-09] .

En cas d'incident, Datasure réagit sans délai et de façon coordonnée afin de mettre en œuvre une réponse rapide à l'incident et à limiter l'impact d'une éventuelle faille de sécurité [REQ-7.9-05]
Le suivi des alertes relatives aux potentiels événements de sécurité critiques sont prises en charge par des personnels en rôle de confiance. Ces personnels s'assure que les incidents associés sont biens traités conformément aux procédures. [REQ-7.9-06]
Les mesures de remontées et de réponse aux incidents sont mises en œuvre de façon à limiter les impacts et dysfonctionnements.[REQ-7.9-12]

5.6.2.2 *Incident majeur*

Dans le cas d'un incident majeur, tel que la perte, la suspicion de compromission, la compromission, le vol de la clé privée du certificat de cachet, l'usurpation d'une identité (soupçonnée ou établie) ou la création de preuves ne correspondant pas à un événement réel, l'évènement déclencheur est la constatation de cet incident au niveau de la composante concernée, qui doit en informer immédiatement Datasure. Le cas de l'incident majeur est impérativement traité dès détection et la publication de l'information de révocation du certificat, s'il y a lieu, doit être faite dans la plus grande urgence, voire immédiatement, par tout moyen utile et disponible (presse, site Internet, récépissé …).

En particulier, Datasure a établi une procédure de gestion des incidents majeurs qui inclut une notification de l'ANSSI dans les 24h en cas de d'incident de sécurité ou de perte d'intégrité ayant un impact significatif sur le service fourni. En cas d'incident relatifi aux données à caractère personnel, une notification à la CNIL sera réalisée [REQ-7.9-07]. Si l'incident impacte un porteur de certificat, personne physique ou morale, elle sera également notifiée sans délai [REQ-7.9-08]
En cas de désastre majeur, incluant la compromission d'une clé de signature ou de moyen d'authentification du service, les opérations seront restaurées dans le délai fixé dans le plan de continuité et de reprise d'activité, après avoir, le cas échéant, résolu la cause du désastre par des mesures de correction appropriées [REQ-7.11-01]

Si l'un des algorithmes, ou des paramètres associés, utilisés par le service devient insuffisant pour son utilisation prévue restante, alors Datasure doit informer tous les porteurs et les tiers utilisateurs de certificats avec lesquels Datasure a passé des accords ou a d'autres formes de relations établies. En complément, cette information doit être mise à disposition des autres utilisateurs de certificats ;

5.6.3 Procédures de reprise en cas de corruption des ressources informatiques (matériels, logiciels et / ou données)

Chaque composante de du service dispose d'un plan de continuité d'activité permettant de répondre aux exigences de disponibilité des différentes fonctions de l'IGC découlant, des exigences de l'ETSI 319401 et 319421 ainsi que de la présente PS/DPS.
Ce plan est testé a minima une fois par an.

5.7 Fin de vie du service

Une ou plusieurs composantes du service peuvent être amenées à cesser leur activité ou à la transférer à une autre entité pour des raisons diverses. La présente section présente les dispositions relatives à la fin de vie [REQ-6.1-11 / REQ-QERDS-4.1.2-05].
Datasure dispose d'un plan de fin de vie à jour [REQ-7.12-02].

Datasure prend les dispositions nécessaires pour couvrir les coûts permettant de respecter ces exigences minimales dans le cas où Datasure serait en faillite ou pour d'autres raisons serait incapable de couvrir ces

coûts par elle-même, ceci, autant que possible, en fonction des contraintes de la législation applicable en matière de faillite. [REQ-7.12-03]
Le transfert d'activité est défini comme la fin d'activité d'une composante de du service ne comportant pas d'incidence sur la validité des certificats émis antérieurement au transfert considéré et la reprise de cette activité organisée par le service de recommandé Datasure en collaboration avec la nouvelle entité.
La cessation d'activité est définie comme la fin d'activité d'une composante du service comportant une incidence sur la validité des certificats émis antérieurement à la cessation concernée.

5.7.1 Transfert d'activité ou cessation d'activité affectant une composante du service

Afin d'assurer un niveau de confiance constant pendant et après de tels évènements, Datasures'assure de mettre en place des procédures dont l'objectif est d'assurer un service constant en particulier en matière d'archivage (notamment, archivage des preuves).
Datasure s'engage sur les éléments suivants :

- Dans la mesure où les changements envisagés peuvent avoir des répercussions sur les engagements vis-à-vis des porteurs ou des utilisateurs de certificats, Datasure avise ces derniers aussitôt que nécessaire et, au moins, sous le délai d'un (1) mois.
- Datasure communique à l'ANSSI les principes du plan d'action mettant en oeuvre les moyens techniques et organisationnels destinés à faire face à une cessation d'activité ou à organiser le transfert d'activité. Elle présente notamment les dispositifs mis en place en matière d'archivage (clés et informations relatives aux certificats) afin d'assurer ou faire assurer cette fonction sur toute la durée initialement prévue dans sa PS/DPS. Datasure communique à l'ANSSI, selon les différentes composantes du service concernées, les modalités des changements survenus. Datasure mesurera l'impact et fera l'inventaire des conséquences (juridiques, économiques, fonctionnelles, techniques, communicationnelles, etc.) de cet évènement. Elle présentera un plan d'action destiné à supprimer, ou réduire, le risque pour les applications et la gêne pour les porteurs et les utilisateurs de certificats.
- Datasure tiendra informée l'ANSSI de tout obstacle ou délai supplémentaire rencontré dans le déroulement du processus.

5.7.2 Cessation d'activité affectant le service de recommandé

La cessation d'activité peut être totale ou partielle (par exemple : cessation d'activité pour une famille de recommandé donnée seulement). La cessation partielle d'activité sera mise en œuvre de façon progressive de telle sorte que seules les obligations de conservation des preuves soient à exécuter par Datasure, ou une entité tierce qui reprend les activités, lors de la délivrance du dernier recommandé.
Dans l'hypothèse d'une cessation d'activité totale, Datasure ou, en cas d'impossibilité, toute entité qui lui serait substituée de par l'effet d'une loi, d'un règlement, d'une décision de justice ou bien d'une convention antérieurement conclue avec cette entité, devra assurer la conservation des preuves et des éléments permettant leur vérification conformément aux engagements pris dans la présente PS/DPS.

Datasure doit stipuler dans sa DPS confidentielle les dispositions prises en cas de cessation de service. Elles incluent:

- la notification des entités affectées ;
- le transfert de ses obligations à d'autres parties ;
- la gestion du statut de révocation pour les certificats non-expirés qui ont été délivrés

Lors de l'arrêt du service, Datasure :

- s'interdit de transmettre la clé privée lui ayant permis de sceller les preuves ;
- prend toutes les mesures nécessaires pour la détruire ou la rendre inopérante ;

- révoque son certificat ;

6 Mesures de sécurité techniques

6.1 Mesures de sécurité des systèmes informatiques

Les mesures de sécurité relatives aux systèmes informatiques satisfont aux objectifs de sécurité qui découlent de l'analyse de risque du service. Elles permettent d'assurer la sécurité des données transmises [REQ- ERDS-5.1.1-02 / REQ-ERDS-5.1.1-03]

Datasure a réalisé une analyse de risque afin d'identifier, analyser et évaluer les risques portant sur le service de confiance. En particulier, l'analyse de risque prend en compte les risques techniques mais également les risques métiers [REQ-5-01]. Datasure sélectionne les mesures de traitement du risque appropriés à partir des résultats de l'analyse de risque [REQ-5-02].
Datasure détermine l'ensemble des exigences de sécurité et procédures opérationnelles nécessaires à la mise en place des mesures de sécurité sélectionnées et documentées dans la PSSI et dans la présent PS/DPS [REQ-5-03]. Cette documentation est complétée d'une partie confidentielle de la PS/DPS ainsi que d'un corpus documentaire décrivant les politiques et procédures de Datasure [REQ-5-06]. Ces documents sont approuvés par le management de Datasure, mis à disposition et communiqué aux employés concernés, ainsi qu'aux personnels externes et sous-traitant lorsque cela est approprié [REQ-5-07]
L'analyse de risques est revue et révisée régulièrement, a minima annuellement et lors de chaque changement majeur [REQ-5-04].
L'analyse de risque fait l'objet d'une approbation formelle par l'organisme de gouvernance de Datasure qui accepte le risque résiduel. En particulier, Datasure met en place, conformément aux exigences de l'ANSSI, une procédure d'homologation [REQ-5-05].

6.1.1 Exigences de sécurité technique spécifiques aux systèmes informatiques

6.1.1.1 PSSI

Datasure a défini une politique de sécurité du système d'information (PSSI).

Cette politique présente l'approche mise en oeuvre pour la gestion de la sécurité et reprend, entre autre, les mesures de sécurité identifiées dans l'analyse de risque ainsi que les mesures issues du guide d'hygiène informatique de l'ANSSI, lorsque ces mesures sont applicable. La PSSI fait l'objet d'une approbation formelle par l'autorité de Gouvernance [REQ-6.3-01].

La PSSI est documentée, mis en œuvre et maintenue à jour. Celle-ci inclut, entre autres, les procédures de contrôle et les procédures opérationnelles pour les sites Datasure, les systèmes d'informations et les biens entrant en jeu dans la délivrance du service [REQ-6.3-03].

La PSSI est communiquée à l'ensemble des personnels et sous traitants concernés [REQ-6.3-04].

Toute modification de la PSSI fait l'objet d'une communication aux personnes concernées, éventuellement externe à Datasure [REQ-6.3-02]

La PSSI, ainsi que les différents inventaires des biens, font l'objet de revues régulières, ou sont systématiquement revues en cas de changement majeurs [REQ-6.3-07].

6.1.1.2 Niveau de sécurité des systèmes informatiques

Un niveau minimal d'assurance de la sécurité offerte sur les systèmes informatiques de l'IGC est décrite dans la DPS confidentielle du service de recommandé de Datasure ainsi que dans sa PSSI
Il répond au moins répondre aux objectifs de sécurité suivants :

- identification et authentification forte des utilisateurs pour l'accès au système (authentification à deux facteurs, de nature physique et/ou logique),
- gestion des droits des utilisateurs (permettant de mettre en oeuvre la politique de contrôle d'accès définie Datasure, notamment pour implémenter les principes de moindres privilèges, de contrôles multiples et de séparation des rôles),
- gestion de sessions d'utilisation (déconnexion après un temps d'inactivité, accès aux fichiers contrôlé par rôle et nom d'utilisateur),
- protection contre les virus informatiques et toutes formes de logiciels compromettants ou non-autorisés et mises à jour des logiciels [REQ-7.7-05],
- gestion des comptes des utilisateurs, notamment la modification et la suppression rapide des droits d'accès,
- protection du réseau contre toute intrusion d'une personne non autorisée,
- protection du réseau afin d'assurer la confidentialité et l'intégrité des données qui y transitent,
- fonctions d'audits (non-répudiation et nature des actions effectuées),

La protection en confidentialité et en intégrité des clés privées ou secrètes d'infrastructure et de contrôle font l'objet de mesures particulières découlant de l'analyse de risque.
Des dispositifs de surveillance (avec alarme automatique) et des procédures d'audit des paramétrages du système (en particulier des éléments de routage) sont mis en place.

6.1.1.3 Gestion des accès

L'accès aux différent composants du service est limité aux personnels autorisés [REQ-7.4-01].
Datasure administre les accès des administrateurs, opérateurs et auditeurs sur le principe du moindre privilège [REQ-7.4-04A]. Cette tâche inclut la gestion des utilisateurs et la désactivation/modification des accès sans délai en cas de besoin [REQ-7.4-05]. Les droits sont appliqués conformément à la politique de contrôle d'accès [REQ-7.4-06].

Les composants du service fournissent des mécanismes de contrôle permettant de séparer les différents rôles de confiance identifiés, en particulier en séparant les niveaux administrateurs et opérateurs [REQ-7.4-07].

Le personnel travaillant sur le service est identifié et authentifié avant d'accèder à n'importe quel élément critique de l'infrastructure [REQ-7.4-08]. Les actions des personnels sont tracés (voir 5.4) [REQ-7.4-09]

6.1.1.4 Veille technique et vulnérabilité

Datasure met en place des procédures de veille technique. En particulier, ces mesures permettent de s'assurer que les mises à jour de sécurité sont appliqués dans une délai raisonnable après leur mise à disposition. Les mises à jour de sécurité sont appliquées seulement si elles n'introduisent pas de risques vulnérabilités ou d'instabilités qui surpasseraient les bénéfices de leur application. Lorsqu'une mise à jour de sécurité n'est pas appliquée, elle fait l'objet d'une documentation.[REQ-7.7-09]
Toutes vulnérabilités critiques doit être adressée dans les 48 heures suivant leur découverte [REQ-7.9-10].
Pour chaque vulnérabilité, prenant en compte l'impact potentiel, Datasure :

- Définira et mettra en œuvre un plan de correction ou de contournement de la vulnérabilité, ou
- Documentera de façon factuelle les raisons ne nécessitant pas de corriger la vulnérabilité (par exemple, vulnérabilité sur un interface réseau d'un dispositif hors ligne). [REQ-7.9-11].

6.1.1.5 Scan de vulnérabilité

Des scans de vulnérabilités réguliers sont mis en œuvre sur les IP publiques et privées du service.
Datasure garde les éléments de preuve permettant de démontrer que les scans de vulnérabilités ont été réalisés par du personnel ou une organisation ayant les compétences, les outils, un code d'éthique et l'indépendance nécessaire pour fournir un rapport d'audit fiable [REQ-7.8-13].
Le scan de vulnérabilités est réalisé au moins une fois par trimestre [REQ-7.8-13].

6.1.1.6 Test de pénétration.

Datasure réalise un test de pénétration avant l'ouverture de son service et après chaque modification majeur de celui-ci [REQ-7.8-14].
Ce test est réalisé sur une base annuelle [REQ-7.8-14A].
Datasure garde les éléments de preuve permettant de démontrer que les tests de pénétration ont été réalisés par du personnel ou une organisation ayant les compétences, les outils, un code d'éthique et l'indépendance nécessaire pour fournir un rapport d'audit fiable [REQ-7.8-15].

6.1.2 Niveau de qualification des systèmes informatiques

Voir 6.2.1

6.2 Mesures de sécurité des systèmes durant leur cycle de vie

Les mesures de sécurité relatives aux cycles de vie des systèmes informatiques satisfont aux objectifs de sécurité découlant de l'analyse de risque du service de Recommandé.

6.2.1 Mesures de sécurité liées au développement des systèmes

Une analyse des besoins de sécurité est réalisée en phase amont des développements au travers d'une étapes de spécification des éxigences de sécurité du système à développer [REQ-7.7-02]

6.2.2 Mesures liées à la gestion de la sécurité

Toute évolution significative d'un système d'une composante de du service est signalée à Datasure pour validation par l'autorité de Gouvernance [REQ-6.3-08]. Elle est documentée et apparaît dans les procédures de fonctionnement interne de la composante concernée et être conforme au schéma de maintenance de l'assurance de conformité, dans le cas de produits évalués.

Des procédures de gestion des changements sont mis en place afin d'encadre les livraisons, modifications et mise à jour d'urgence des briques logicielles des différents composants de la plate-forme et de leur configuration [REQ-7.7-03]. Ces procédures incluent la documentation des changements [REQ-7.7-04]

La configuration des différents composants du service font l'objet de vérification régulières, afin d'identifier des changements qui seraient en contradiction avec les règles de la présente PS/DPS ou de la PSSI [REQ-6.3-09] La fréquence des vérifications est précisée dans la DPS confidentielle. Elle est a minima annuelle [REQ-6.3-10].

6.2.3 Niveau d'évaluation sécurité du cycle de vie des systèmes

Non applicable

6.3 Mesures de sécurité réseau

Datasure met en œuvre des mesures de sécurité contre les attaques réseau [REQ-7.8-01]

6.3.1 Segmentation réseau

En particulier, Datasure segmente son Système d'information en zones réseau distinctes en s'appuyant sur l'analyse de risque réalisée. En particulier, les séparations au niveau fonctionnel, logique et physique sont pris en compte [REQ-7.8-02]
Datasure applique des mesures de sécurité similaires à l'ensemble des systèmes d'une même zone réseau [REQ-7.8-03].
Les réseaux dédiés aux opérations et à l'administration font l'objet d'une séparation [REQ-7.8-08] Les systèmes dédiés à l'administration ne peuvent être utilisés pour d'autres usages [REQ-7.8-09]

6.3.2 Filtrage des flux et interconnexions

Les communications et accès entre les différentes zones sont restreintes aux seules nécessaire pour les opérations du service [REQ-7.8-04]. Ces restrictions sont permises par des mesures de contrôles réseaux (tel que la mise en place de pare-feu) permettant de prémunir le service contre les accès non autorisés, y compris les accès des utilisateurs et des abonnés [REQ-7.8-16].
Toutes les communications et services non nécessaires sont explicitement interdits ou désactivés [REQ-7.8-05].
En particulier, les pare-feu sont configurés de manière à ne laisse passer que les flux réseaux strictement nécessaire aux opérations du service [REQ-7.8-17]

En particulier, l'interconnexion vers des réseaux publics est protégée par des passerelles de sécurité configurées pour n'accepter que les protocoles nécessaires au fonctionnement de la composante au sein de l'IGC.
Datasure garantit que les composants du réseau local (routeurs, par exemple) sont maintenus dans un environnement physiquement sécurisé et que leurs configurations sont périodiquement auditées en vue de vérifier leur conformité avec les exigences spécifiées par Datasure [REQ-7.8-06].

6.3.3 Communication entre composants

Les communications entre les différents composants sont sécurisés par des canaux permettant leur isolation. Cette isolation s'appuie sur des mécanismes logiques, cryptographiques ou physiques permettant leur isolation des autres canaux de communications. En particulier, il permettant d'assurer la confidentialité et l'intégrité des échanges [REQ-7.8-11].

6.3.4 Séparation des plates-formes de production et de test.

Les plates-formes de production et les plates-formes hors production (test, pre-production) font l'objet d'une séparation stricte [REQ-7.8-10]

6.4 Horodatage / Système de datation

Les horloges de l'ensemble des systèmes sont synchronisés avec une source de temps UTC a minima toutes les 24h [REQ-7.10-06]

7 Audit de conformité et autre évaluations

Les audits et les évaluations concernent,

- d'une part, ceux réalisés en vue de la délivrance d'une certification de conformité aux normes ETSI 319421 et du processus de qualification eIDAS ainsi que des exigences du Décret LRE;
- d'autre part, les audits dit « interne » afin de s'assurer que l'ensemble du service est conforme aux exigences énoncées dans la présente PS/DPS.

7.1 Fréquences et circonstances des évaluations.

Suite à toute modification significative d'une composante de du service, Datasure procède à une analyse de sécurité et fait évoluer en conséquence, le cas échéant, les mesures techniques et organisationnelles permettant de maintenir ou d'améliorer le niveau de sécurité attendu.
Datasure procède également régulièrement à un contrôle interne de conformité du service , en tout ou partie. La fréquence de ce contrôle est annuelle.
Enfin, Datasure fait évaluer, dans le cadre de la certification et qualification de ses services, son service conformément à la règlement en vigueur par un organisme d'évaluation accrédité.

7.2 Identités / qualifications des évaluateurs

Concernant l'audit interne, Datasure choisit et assigne une équipe d'auditeurs compétents en sécurité des systèmes d'information et dans le domaine d'activité contrôlée.
Dans le cadre de la certification et qualification de ses services, Datasure fait appel à un organisme accrédité.

7.3 Relations entre évaluateurs et entités évaluées

L'équipe d'audit est choisie de façon à assurer une indépendance et une impartialité de l'audit.

7.4 Sujets couverts par les évaluations

L'audit interne couvre l'ensemble des sujets de la présente PS.

7.5 Actions prises suite aux conclusions des évaluations

En cas d'écart ou d'anomalie suite à un audit, qu'il soit un audit interne de conformité ou un audit d'évaluation, un plan de correction sera établi et appliqué

7.6 Communication des résultats

Les résultats des audits internes conformité sont tenus à la disposition de l'organisme d'évaluation.

8 Autres problématiques métiers et légales

8.1 Tarifs

8.1.1 Tarifs pour la fourniture du service

La tarification de la prestation de fourniture de certificat est hors du périmètre de la présente PS/DPS.

8.1.2 Tarifs pour accéder aux preuves

L'accès aux preuves générés est gratuite pour l'expéditeur.

8.1.3 Tarifs pour d'autres services

Non applicable

8.1.4 Politique de remboursement

Non applicable.

8.2 Responsabilité financière

Conformément à ses obligations, Datasure prend les dispositions nécessaires pour couvrir, ses responsabilités liées à ses opérations et/ou activités.

8.2.1 Couverture par les assurances

Datasure s'assure d'avoir les ressources nécessaires pour opérer ses services en toute sécurité et conformité avec la présente PS/DPS et a souscrit une assurance pour couvrir ses activités [REQ-7.1.1-04/ REQ-7.1.1-05].

8.2.2 Autres ressources

Non applicable

8.2.3 Couverture et garantie concernant les entités utilisatrices

Non applicable

8.3 Confidentialité des données professionnelles

8.3.1 Périmètre des informations confidentielles

Les informations considérées comme confidentielles sont au moins les suivantes :

- la partie non-publique de la DPS,
- les clés privées des cachets,
- les données d'activation associées aux clés privées,
- les journaux d'évènements des composantes du service,
- les dossiers de recommandé,
- les documents envoyés par l'expéditeur.

8.3.2 Informations hors du périmètre des informations confidentielles

Sans objet.

8.3.3 Responsabilités en termes de protection des informations confidentielles

Datasure applique des procédures de sécurité pour garantir la confidentialité des informations identifiées au chapitre 9.3.1, en particulier en ce qui concerne l'effacement définitif ou la destruction des supports ayant servi à leur stockage.

De plus, lorsque ces données sont échangées, en particulier les documents, Datasure garantit l'intégrité.
Le service est notamment tenue de respecter la législation et la réglementation en vigueur sur le territoire français. En particulier, elle met à disposition les dossiers contenant les différentes preuves, ainsi que les éléments de vérification des identité des utilisateur, à des tiers dans le cadre de procédures légales.

8.4 Protection des données à caractère personnel

8.4.1 Politique de protection des données à caractère personnel

Datasure respecte la réglementation en vigueur, et en particulier le règlement européen n° 2016/679 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, dit « Règlement Général sur la Protection des Données [RGPD].

8.4.2 Données à caractère personnel

Les données considérées comme personnelles sont les suivantes :

- Le contenu éventuel du document expédié;
- le dossier de vérification de l'identité du porteur.

8.4.3 Données à caractère non personnel

Sans objet

8.4.4 Responsabilité en termes de protection des données à caractère personnel

La législation en vigueur sur le territoire Français est applicable.

8.4.5 Notification et consentement d'utilisation des données à caractère personnel

Conformément à la législation et réglementation en vigueur sur le territoire français, les informations personnelles remises par les porteurs à Datasure ne doivent ni être divulguées ni transférées à un tiers sauf dans les cas suivants : consentement préalable du porteur, décision judiciaire ou autre autorisation légale.

8.4.6 Conditions de divulgation d'informations personnelles aux autorités judiciaires ou administratives

La législation en vigueur sur le territoire Français est applicable.

8.5 Droits de propriété intellectuelle

La législation en vigueur sur le territoire Français est applicable.

8.6 Interprétations contractuelles et garanties

La présente PS/DPS détermine des différentes obligations des composantes de Datasure et des différentes parties prenantes. Les obligations des éventuels différents sous-traitants sont décrits dans la partie confidentielle de la DPS [REQ-6.1-04]

8.6.1 Service de recommandé

Les obligations communes aux composantes de Datasure sont les suivantes :

- protéger et garantir l'intégrité et la confidentialité de leurs clés secrètes et/ou privées,
- respecter et appliquer la partie de la DPS confidentielle leur incombant (cette partie doit être communiquée à la composante correspondante),
- se soumettre aux contrôles de conformité effectués par l'équipe d'audit mandatée par Datasure (cf. chapitre 8) et l'organisme d'évaluation,
- respecter les accords ou contrats qui les lient entre elles ou aux utilisateurs,

documenter leurs procédures internes de fonctionnement,

- mettre en oeuvre les moyens (techniques et humains) nécessaires à la réalisation des prestations auxquelles elles s'engagent dans des conditions garantissant qualité et sécurité.
- Garantir l'intégrité du document tout au long de sa transmission

8.6.2 Expéditeur

Les Expéditeurs garantissent :

- qu'ils ont, lors du dépôt d'une LRE, transmis à AR24, conformément au Décret, les informations suivantes :
  - (i) leurs nom et prénom s'il s'agit de personnes physiques, leur raison sociale s'il s'agit de personnes morales, ainsi que leur adresse électronique et, le cas échéant, leur adresse postale ;
  - (ii) Les nom et prénom ou la raison sociale du Destinataire, ainsi que son adresse électronique ;
  - (iii) Le niveau de garantie choisi par l'Expéditeur contre les risques de perte ou de vol.
- qu'ils ont préalablement obtenu l'accord du Destinataire, lorsque celui-ci est un non professionnel, pour lui adresser une LRE et qu'ils sont en mesure de prouver, par tous moyens, qu'ils ont obtenu le consentement du Destinataire ;
- l'identité du Destinataire, la validité de l'adresse électronique de contact à laquelle la LRE sera adressée et la qualité de consommateur ou de professionnel du Destinataire ; –
- ne pas porter atteinte à leurs obligations contractuelles ou légales et à ne pas introduire lors de leur Dépôts tout virus, vers, bombe logique ou tout contenu pouvant être assimilés à du courrier non désiré.

8.6.3 Cas de moyens d'authentification

En cas de remise d'un moyen d'identification à un Destinataire ou un Expéditeur, celuici doit :

- Protéger celui-ci de toute perte ou divulgation
- Révoquer (4.5.3) sans délai le moyen d'identification en cas de perte, vol, compromission ou de suspicion de compromission des moyens fournis Les moyens d'identification sont strictement personnels et ne doivent pas être communiqués ou transmis à des tiers. L'utilisateur est responsable de l'utilisation qui est faite du moyen d'identification qui lui a été remis.

8.6.4 Tiers en charge de vérifier les preuves

Le service de LRE entièrement électronique produit des preuves de Dépôt, d'Acceptation, de Refus et de Non-Réclamation (4.4) qui sont opposables en justice. Leur authenticité est garantie par l'apposition du cachet Datasure et du jeton d'horodatage qualifié.

Toute personne désirant utiliser ces preuves à des fins de justice peut s'assurer de leur recevabilité en vérifiant la validité du jeton d'horodatage et du cachet conformément aux recommandations de la PC et de la PH.

8.6.5 Autres participants

Sans objet

8.7 Limite de garantie

La présente PS n'expose pas de limites particulière à l'utilisation du service[REQ-QERDS-4.1.2-03]

8.8 Limite de responsabilité

Sous réserve des dispositions d'ordre public applicables, Datasure ne pourra pas être tenue responsable d'une utilisation non autorisée ou non conforme de son service de recommandé ainsi que de tout autre équipement ou logiciel mis à disposition.
Datasure décline en particulier sa responsabilité pour tout dommage résultant :
- d'un emploi du service pour un usage autre que ceux prévus;
- de l'usage de certificats expirés ;
- d'un cas de force majeure
- de l'incapacité d'un utilisateur à procéder à la procédure de vérification d'identité proposée.

Datasure décline également sa responsabilité pour tout dommage résultant des erreurs ou des inexactitudes entachant les informations transmises par l'expéditeur, quand ces erreurs ou inexactitudes résultent directement du caractère erroné des informations communiquées.
Datasure décline également se responsabilité en cas de choix de niveau de recommandé incompatible avec le besoin juridique du client.
En aucun cas, Datasure n'intervient, de quelque façon que ce soit, dans les relations contractuelles qui peuvent se nouer entre le l'expéditeur et le destinataire du recommandé *, notamment quant au contenu des documents soumis.

8.9 Indemnités

Sans objet

8.10 Durée et fin anticipée de validité de la PS/DPS

8.10.1 Durée de validité

La présent PS/DPS reste en application au moins jusqu'à la fin de vie du dernier certificat émis au titre de cette PS/DPS

8.10.2 Fin anticipée de validité

La publication d'une nouvelle version des documents cités au chapitre 1.1 peut entraîner, en fonction des évolutions apportées, la nécessité pour Datasure de faire évoluer sa PS/DPS correspondante. Dans ce cas, cette mise en conformité n'imposera pas le renouvellement anticipé des certificats déjà émis, sauf cas exceptionnel lié à la sécurité. Enfin, la validité de la PS peut arriver à terme prématurément en cas de cessation d'activité du service de recommandé de Datasure.

8.10.3 Effets de la fin de validité et clauses restant applicables

Sans objet

8.11 Notifications individuelles et communications entre les participants

En cas de changement majeur de toute nature intervenant dans la composition de l'IGC, Datasure s'engage à
- A valider en amont ce changement et en identifier les éventuels impacts
- En informer en amont, l'organisme de qualification ainsi que l'organisme d'évaluation

8.12 Amendements à la PS

8.12.1 Procédures d'amendements

Tout amendement de la PS/DPS doit faire l'objet d'une procédure d'approbation et de publication (§1.2.4).

8.12.2 Mécanisme et période d'information sur les amendements

Lorqu'un amendement de la présente PS/DPS affecterait l'acceptation du service par le porteur de certificat, l'abonné ou l'utilisateur, Datasure notifie le changement au préalable 15 jours avant la publication de la nouvelle PS/DPS. Les changements mineurs, tels que les corrections de coquilles ou précisions ne nécessitent pas une notification préalable [REQ-6.1-09A].

8.12.3 Circonstances selon lesquelles l'OID doit être changé

L'OID de la PS/DPS étant inscrit dans les certificats finaux qu'elle émet, toute évolution de cette PS.DPS ayant un impact majeur sur les certificats déjà émis (par exemple, augmentation des exigences en matière d'enregistrement des porteurs, qui ne peuvent donc pas s'appliquer aux certificats déjà émis) se traduit par une évolution de l'OID, afin que les utilisateurs puissent clairement distinguer quels certificats correspondent à quelles exigences [OVR-5.3-01].
En particulier, l'OID de la présente PS/DPS évolue dès lors qu'un changement majeur intervient dans les exigences de la présente PS/DPS.

8.13 Dispositions concernant la résolution de conflits

Datasure en place des politiques et procédures pour le traitement des réclamations et le règlement des litiges émanant des entités pour lesquelles elle fournit des services électroniques de confiance ou d'autres points qui y sont liés [REQ-7.1.1-06]
En particulier, toute réclamation peut être soumis au point de contact indiqué en 1.2.2.

8.14 Juridictions compétentes

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

8.15 Conformité aux législations et réglementations

Datasure se conformes aux lois et règlements en vigueur. En particulier, les pratiques Datasure sont non-discriminatoires [REQ-7.1.1-02]
De façon générale, Datasure essaye, dans la mesure du possible, de mettre en place des procédures permettant de rendre accessible ses services à l'ensemble des demandeurs et utilisateurs, et prendre en compte les personnes en situation de handicap [REQ-7.1.1-03].

8.16 Dispositions diverses

8.16.1 Accord global

Le présent document contient l'intégralité des clauses régissant l'IGC.

8.16.2 Transfert d'activités

Voir 5.8.

8.16.3 Conséquences d’une clause non valide

En cas d'une clause non valide, les autres clauses ne sont pas remises en question.

8.16.4 Application et renonciation

Aucune renonciation à se prévaloir de l'un de ses droits ne saurait intervenir tacitement. Pour être opposable au service de recommandé une renonciation doit avoir été formulée par écrit. Une telle renonciation ne saurait constituer une renonciation pour l'avenir aux dits droits

8.16.5 Force majeure

Datasure ne pourra être tenue pour responsable de tout retard ou manquement dans l’exécution de l’une quelconque de ses obligations au titre de la présente PS/DPS, si ledit retard ou manquement est dû à la survenance d’un cas de force majeure habituellement reconnu par la jurisprudence des cours et tribunaux françai

8.17 Autres dispositions

Sans objet