Postee

Postee Recc

Politique et Pratiques du service

OID : 1.3.6.1.4.1.56045.2.1
Version : v1.0 du 2/07/2023
Classification : Public

Table des matières

1 Introduction

1.1 Présentation générale

Postee édite une plateforme en ligne française pour digitaliser, simplifier et sécuriser les envois électroniques de documents importants.

Postee Reco est un service d'envoi recommandé électronique. Ce service permet d'acheminer de manière sécurisée un courrier électronique depuis un expéditeur, client du service, vers un destinataire désigné par l'expéditeur. Le service assure l'authentification des parties et génère des preuves opposables en justice pour toutes les actions associées aux courriers (envoi, réception, refus, non réclamation).

Le présent document constitue la politique et la déclaration des pratiques du service Postee Reco.

L'objectif de ce document est de définir les engagements pris par Postee, en tant que fournisseur de services de confiance (Trust Service Providers au sens du règlement eIDAS) pour l'envoi des recommandés électroniques et de définir les responsabilités et obligations de chacun des participants.

Le service Postee Reco est qualifié au sens du règlement européen eIDAS (cf. [EIDAS]), et plus précisément conformément à son article 44. La présente politique est ainsi conforme aux exigences du règlement européen, aux normes ETSI applicables ainsi qu'aux exigences de l'organe de contrôle national français.

1.2 Identification du document

Le présent document est identifié par l'OID suivant : 1.3.6.1.4.1.56045.2.1

1.3 Gestion de la politique

1.3.1 Entité gérant la politique

La présente politique et déclaration de pratiques est gérée par les membres du comité de pilotage du service au sein de Postee.

1.3.2 Point de contact

Le point de contact pour toute question à propos de la politique du service est :

- Adresse postale : Postee, 72 rue des Jacobins, 80000 Amiens
- Adresse électronique : hello@postee.io

1.3.3 Procédure d'approbation de la politique

La politique est approuvée par le comité de pilotage Postee après examen et relecture du document par les membres du comité de pilotage, et par les personnes désignées par celui-ci.

Cette relecture a pour objectif d'assurer :

- La conformité de la politique avec les exigences réglementaires et normatives portant sur la fourniture d'un service de recommandé électronique qualifié ;
- La cohérence de la politique avec les autres documents publiés dans le cadre du service, tels par exemple que les conditions générales d'utilisation
- La concordance entre les engagements exprimés dans la politique et les moyens techniques et organisationnels mis en œuvre par Postee et ses partenaires ;
- L'information effective de l'ANSSI pour toute modification importante dans la fourniture du service Postee Reco qualifié (y compris celles entrainant des changements dans la liste de confiance), selon les modalités décrites dans les procédures de qualification. Cela comprend notamment, sans s'y limiter :

- les changements induits par une modification de la politique de service ou des conditions générales d'utilisation associées ;
- les changements de sous-traitants ;
- les modifications des conditions d'hébergement ;
- les changements de matériels cryptographiques ;
- les modifications d'architecture technique ;
- les changements de procédures d'enregistrement et d'identification ;
- les changements dans la gouvernance du service.

Le comité de pilotage s'assure que la date d'entrée en vigueur de la nouvelle politique laisse, dans la mesure du possible, un délai suffisant aux clients pour prendre connaissance des nouvelles dispositions et adapter si besoin leurs pratiques.

1.3.4 Amendements à la politique

Postee contrôle que tout projet de modification de sa politique reste conforme aux exigences réglementaires et normatives applicables.

1.3.4.1 Procédures d'amendement

Des amendements à la présente politique peuvent être prévus au cours de la durée de vie du service, par exemple pour :

- Des corrections induites par les audits du service ;
- Des corrections mineures (erreurs, oublis, précisions supplémentaires…) ;
- Des évolutions ou extensions du service de recommandé électronique ;
- L'acceptation ou la mise en œuvre de nouveaux moyens d'identification électronique ;
- Des changements d'ordre technique (mise en œuvre, partenaires, fournisseurs, etc…).

Toute proposition d'évolution du service fait l'objet d'une analyse d'impact afin de déterminer son éventuelle incidence sur :

- La qualité ou la sécurité du service ;
- Les expéditeurs ou destinataires des envois recommandés ;
- La conformité de l'offre qualifiée aux exigences du règlement eIDAS ;
- La nécessité de mise à jour des autres documents publiés ;
- Les pratiques internes de Postee ou de ses partenaires et fournisseurs.

En cas d'impact majeur, un changement d'OID de politique est prévu, et l'évolution et son analyse d'impact peuvent être soumises à l'ANSSI et à l'organisme de certification pour avis ou commentaire.

L'analyse d'impact est étudiée par le comité de pilotage qui valide ou non le lancement d'une évolution. Le cas échéant, la nouvelle politique sera soumise à l'approbation du comité de pilotage.

1.3.4.2 Mécanisme et période d'information sur les amendements

Une fois l'évolution du service validée par le comité de pilotage, la nouvelle politique est communiqué aux clients (par publication sur le site), au personnel Postee et à toutes les parties prenantes dans la fourniture du service (par envoi par messagerie). Un délai de prévenance suffisant est prévu pour leur permettre de prendre connaissance des nouvelles dispositions et d'adapter si besoin leurs pratiques.

Postee adresse annuellement à l'ANSSI une synthèse de l'ensemble des modifications apportées à la fourniture de son service.

1.3.4.3 Circonstances selon lesquelles l'OID doit être changé

Toute évolution de la présente politique ayant un impact majeur sur le service doit se traduire par une évolution de l'OID, afin que les utilisateurs puissent clairement distinguer quels envois correspondent à quelles exigences.

1.4 Documents associés

1.4.1 Documents métier du service

[CGU]	Conditions Générales d'Utilisation du service Postee Reco https://www.postee.io
[POL_HORO]	Politique du service d'horodatage Certigna http://politique.certigna.fr/PHcertignaTSA.pdf
[POL_CERT]	Politique de Certification Certigna http://politique.certigna.fr/PCunique.pdf

1.4.2 Documents règlementaires et normatifs

[EIDAS]	*Règlement (UE) 2014/910 du Parlement européen et du Conseil du 23 juillet 2014* https://eur-lex.europa.eu/legal-content/FR/TXT/?uri=CELEX:32014R0910
[ANSSI_LRE]	Services d'envoi recommandé électronique qualifiés – Critères d'évaluation conformité au règlement eIDAS, Version 1.0 du 3 janvier 2017 https://www.ssi.gouv.fr/uploads/2016/06/eidas_envoi-recommande-electro qualifie_v1.0_anssi.pdf
[ANSSI_PSCO]	Prestataires de services de confiance qualifiés – Critères d'évaluation de la conform règlement eIDAS, Version 1.2 du 5 juillet 2017 https://www.ssi.gouv.fr/uploads/2016/06/eidas_psc-qualifies_v1.2_anssi.pdf
[EN_319401]	ETSI EN 319 401 V2.3.1 (2021-05) Electronic Signatures and Infrastructures General Policy Requirements for Trust Service Providers. https://www.etsi.org/deliver/etsi_en/319400_319499/319401/02.03.01_60/en_319401v0203
[EN_319521]	ETSI EN 319 521 V1.1.1 (2019-02) Electronic Signatures and Infrastructures (ESI); and security requirements for Electronic Registered Delivery Service Providers. https://www.etsi.org/deliver/etsi_en/319500_319599/319521/01.01.01_60/en_319521v0101
[RGPD]	Règlement (UE) 2016/679 du Parlement européen et du Conseil du 27 avril 2016 https://www.cnil.fr/fr/reglement-europeen-protection-donnees

1.5 Entités intervenant dans le service Postee Reco

1.5.1 Prestataire du service de recommandé électronique (PSRE)

Postee est le prestataire du service d'envoi recommandé électronique Postee Reco.

Postee conserve la responsabilité globale de la conformité du service avec la présente politique, y compris lorsque certaines fonctions sont mises en œuvres par des sous-traitants.

Le service Postee Reco permet d'utiliser certains moyens d'identification électronique qui ne sont pas fournis par Postee et dont Postee n'est pas responsable (moyens d'identification électronique de niveau de garantie substantiel). Postee s'assure que le niveau de sécurité

fourni convient aux exigences portant sur le service Postee Reco et qu'il est bien maintenu dans le temps.

1.5.2 Prestataire d'horodatage électronique qualifié (PSHE)

Postee est partenaire de Certigna, prestataire qualifié du service d'horodatage électronique qualifié.

Dans ce cadre, Certigna doit :

- Délivrer des jetons d'horodatage qualifiés conformément à sa politique d'horodatage [POL_HORO] d'OID 1.2.250.1.177.2.9.1;
- Garantir une précision de 1 seconde pour chaque jeton délivré ;
- Publier les moyens nécessaires à la vérification des jetons d'horodatage ;
- Informer Postee de tout incident de sécurité impactant le service d'horodatage fourni pour Postee Reco.

1.5.3 Prestataire de cachet électronique (PSCE)

Postee est partenaire de Certigna, prestataire qualifié du service de cachet électronique et prestataire de délivrance du certificat qualifié de cachet.

Dans ce cadre, Certigna doit :

- Générer des cachets électroniques sur les preuves, en utilisant le certificat qualifié de cachet du service Postee Reco, selon les algorithmes précisés au §2.6.1 ;
- Assurer la confidentialité, l'intégrité et la disponibilité de la clé de cachet de Postee Reco ;
- Générer un certificat qualifié de cachet émis par l'AC « Certigna Entity CA » conformément à sa politique de certification [POL_CERT] d'OID 1.2.250.1.177.2.6.1.7.1 ;
- Publier les moyens nécessaires à la vérification des cachets produits, et en particulier du certificat de cachet utilisé ;
- Informer Postee de tout incident de sécurité impactant le service de cachet fourni pour Postee Reco.

1.5.4 Prestataires d'identification électronique

Le service Postee Reco permet d'utiliser des moyens d'identification électronique qui ne sont pas fournis par Postee et dont Postee n'est pas responsable :

- Moyens d'identification électronique de niveau de garantie substantiel.

Les prestataires sollicités sont :

- Docaposte, pour la fourniture de l'Identité Numérique La Poste, moyen d'identification életronique certifié par l'ANSSI comme de niveau substantiel.

1.5.5 Prestataire d'hébergement et d'infogérance

L'infrastructure du service Postee Reco est hébergée et infogérée par un partenaire de Postee : Scalair (https://scalair.fr).

Scalair est un hébergeur proposant une offre de services managés pour lequels elle a obtenu la certification ISO 27001. Scalair applique les mesures de sécurité requises pour le service Postee Reco et décrites dans le présent document.

1.5.6 Expéditeurs et destinataires d'envois recommandés

Les expéditeurs et destinataires des envois recommandés Postee Reco sont des personnes physiques ou des personnes morales.

Les expéditeurs et destinataires doivent :

- Accepter les Conditions Générales d'Utilisation du service ;
- Fournir des informations exactes lors de leur enregistrement sur le service Postee Reco ;
- Utiliser l'une des modalités d'identification électronique proposer sur le service pour déposer ou réceptionner des envois recommandés ;
- Dans le cas où ils utilisent un MIE qu'ils ont approvisionnés par ailleurs, assurer la sécurité et le renouvellement de ce MIE ;
- Protéger leurs informations de connexion et leurs secrets d'authentification ;
- Signaler à Postee toute compromission avérée ou suspectée de leur moyen d'authentification ;
- Obtenir le consentement préalable à la réception d'envoi recommandé pour les destinataires personnes physiques ;
- Pour une personne morale, signaler à Postee la perte de l'habilitation d'une personne physique à agir pour son compte ;
- Vérifier les preuves produites par le service dès leur réception.

Les expéditeurs doivent de plus :

- Protéger leurs propres systèmes informatiques afin d'éviter toute intrusion malveillante sur le service Postee Reco ou tout introduction de virus, bombe logique ou malware lors du dépôt d'un envoi recommandé.

Les destinataires doivent de plus :

- Accepter ou refuser l'envoi recommandé dans le délai précisé par cette politique, sous peine de voir l'envoi considéré comme non réclamé et donc devenir indisponible ;
- Télécharger les données de l'envoi recommandé suite à son acceptation, dans le délai requis par le service.

1.5.7 Tiers utilisant les preuves du service

Les tiers exploitant les preuves du service doivent :

- Accepter les Conditions Générales d'Utilisation du service ;
- Vérifier les preuves selon les directives du §2.6.2.

1.6 Abréviations et définitions

1.6.1 Abréviations

AC	Autorité de Certification
ANSSI	Agence nationale de sécurité des systèmes d'information
CET	Central European Time
CGU	Conditions Générales d'Utilisation
CPU	Central Processing Unit
TLS	Transport Layer Security

TSP	Trust Service Provider
UTC	Universal Coordinated Time

1.6.2 Définitions

CGU	Conditions générales d'utilisation
Destinataire	Personne physique ou morale désignée par un Expéditeur comme la personne à laquelle le Service doit transmettre un Courrier Recommandé Électronique
Expéditeur	Personne physique ou morale utilisant le Service pour envoyer un Courrier Recommandé Électronique à un Destinataire
Preuve	Document électronique scellé par un cachet électronique avancé et horodaté par un horodatage électronique qualifié, et qui atteste de la survenance d'un événement relatif au cycle de vie d'un Courrier Recommandé Électronique
Service	Service en ligne Postee Reco fourni par Postee
Utilisateur	Personne physique accédant au Service, agissant en son nom propre ou au nom d'une personne morale qu'elle représente

2 Service Postee Reco

2.1 Identification et authentification des expéditeurs et destinataires

Le service Postee Reco garantit l'identification des expéditeurs et destinataires avec un degré de confiance élevé, avant tout dépôt, acceptation ou refus d'un envoi recommandé.

Les modalités d'identification et d'authentification des expéditeurs et destinataires sont strictement identiques. Ces opérations sont menées dans un environnement contrôlé et sécurisé, que ce soit sur les plateformes de Postee ou chez les prestataires impliqués. Des traces et éléments de preuve de l'identification électronique sont collectées et conservées par le service Postee Reco (cf. §4.10).

2.1.1 Validation initiale de l'identité

La validation initiale d'identité d'un utilisateur est réalisée à distance selon l'une des modalités suivantes :

- Par un moyen d'identification électronique, notifié au niveau européen ou certifié par l'ANSSI, qui satisfait aux exigences du niveau de garantie substantiel ou élevé.

Cette validation initiale d'identité concerne la personne physique qui se connecte au service.

Une personne physique ne peut accéder qu'aux courriers pour lesquels elle accède à la notification de réception. L'habilitation d'une personne physique à agir pour le compte d'une personne morale est soumise à la validaton d'un admninistrateur du compte de cette personne morale sur le service. L'administrateur par défaut est l'utilisateur qui déclare le compte de la personne morale, accède à l'adresse mail de contact de l'entreprise et déclare être un représentant autorisé de cette personne morale. Le responsable légal d'une personne morale doit informer Postee de la fin de l'habilitation d'un utilisateur enregistré sur le service pour son entité.

2.1.2 Authentification

Postérieurement à une première validation initiale d'identité réussie, le service Postee Reco propose de délivrer à l'utilisateur un moyen d'authentification à deux facteurs qui pourra être utilisé pour ses prochaines identifications électroniques sur le service. A défaut, l'utilisateur devra, pour déposer, accepter ou refuser un envoi, réaliser une nouvelle validation d'identité selon l'une des modalités décrites au paragraphe précédent.

Le moyen d'authentification à deux facteurs remis par Postee est constitué par un mot de passe et un code à usage unique de type TOTP que l'utilisateur peut générer après initialisation d'une application TOTP avec un secret généré par Postee. Ce secret est transmis par affichage d'un QR Code à l'utilisateur lors d'une session authentifiée par une validation initiale d'identité. Ce secret doit être renouvelé a minima tous les 3 ans.

L'utilisateur a pour obligation d'informer Postee de toute compromission ou suspicion de compromission de son moyen d'authentification, afin que son accès au service soit bloqué. Le responsable légal d'une personne morale doit informer Postee en cas de compromission avérée ou suspectée du moyen d'authentification de l'un de ses représentants sur le service si son porteur n'est pas ou n'est plus en mesure de le faire directement.

2.2 Dépôt du Postee Reco

2.2.1 Dépôt d'un Postee Reco par l'expéditeur

Le dépôt d'un envoi recommandé est effectué sur le site en ligne de Postee Reco par une personne physique agissant en son nom ou pour le compte d'une personne morale.

La personne physique doit s'authentifier sur le site selon les modalités exposées au §2.1 avant de pouvoir accéder à la fonction d'envoi de Postee Reco. Elle doit explicitement accepter les Conditions Générales d'Utilisation à sa première connexion et à chaque modification de celles-ci.

L'envoi recommandé est défini par :

- L'identification du destinataire :
    - Nom et prénom du destinataire pour le cas d'une personne physique ;
    - Raison sociale et numéro SIREN ou SIRET pour le cas d'une personne morale ;
- L'adresse électronique du destinataire ;
- Les données de l'envoi recommandé :
    - Un message sous forme de texte ;
    - Un ensemble optionnel de pièces jointes (sans contraintes de format).

Lorsque l'expéditeur compose un envoi recommandé à l'attention de plusieurs destinataires, le service le traite comme le dépôt de plusieurs envois recommandés, identiques, avec un envoi recommandé pour chacun des destinataires indiqués.

L'obtention du consentement du destinataire non professionnel à recevoir un courrier recommandé sous forme électronique est à la charge de l'expéditeur, préalablement au dépôt du courrier.

2.2.2 Traitement du dépôt d'un Postee Reco

Le service vérifie que l'identification du destinataire et son adresse électronique sont renseignées, et que le message de l'envoi recommandé n'est pas vide.

Le service attribue un identifiant unique à l'envoi et génère la preuve de dépôt de l'envoi recommandé. Cette preuve de dépôt est mise à disposition de la personne physique ou morale expéditrice sur le site Postee, par un lien de téléchargement.

Le destinataire est informé de l'envoi recommandé par une notification expédiée par messagerie électronique à l'adresse indiquée par l'expéditeur. Cette notification de précise pas l'identité de l'expéditeur.

Postee conserve les données de l'envoi recommandé pour une durée de 10 ans, quelle que soit l'action du destinataire. Au terme de ce délai, les données sont définitivement détruites.

2.3 Acceptation ou refus du Postee Reco par le destinataire

Le destinataire dispose d'un délai de 15 jours à compter du lendemain de l'envoi de la notification de réception pour accepter ou refuser le Postee Reco. Passé ce terme, l'envoi est considéré comme non réclamé (cf. §2.4) et n'est plus accessible à son destinataire.

Le destinataire se connecte sur le site en ligne de Postee Reco en suivant le lien inclus dans la notification de réception ou, s'il a déjà un compte sur le service, en se connectant directement. La personne physique se connectant doit explicitement accepter les Conditions Générales d'Utilisation à sa première connexion et à chaque modification de celles-ci.

La personne physique doit s'authentifier sur le site selon les modalités exposées au §2.1 avant de pouvoir accéder à la fonction d'acceptation d'un Postee Reco. Elle peut alors :

- Accepter l'envoi recommandé : le service génère alors une preuve de réception, informe le destinataire de l'identité de l'expéditeur et lui permet de télécharger cet envoi ;
- Refuser l'envoi recommandé : le service génère alors une preuve de refus et interdit au destinataire toute nouvelle action et tout accès à cet envoi.

La mise à disposition au destinataire du lien de téléchargement de l'envoi recommandé constitue la délivrance du Postee Reco. Le destinataire est responsable du téléchargement effectif des données de l'envoi recommandé pendant leur durée de conservation par Postee.

Les preuves de réception et de refus sont mises à disposition de l'expéditeur qui en est notifié, le destinataire ne pouvant lui accéder qu'à la preuve de réception.

2.4 Non réclamation du Postee Reco

A l'expiration du délai de 15 jours à compter du lendemain de l'envoi de la notification de réception, un Postee Reco non accepté ni refusé est considéré comme non réclamé. Le destinataire n'a plus la possibilité de l'accepter ou de le refuser.

Le service utilise une solution de suivi des messages de notification permettant, dans la plupart des cas, d'identifier la consultation par son destinataire de la notification de réception du Postee Reco. Ainsi, pour un Postee Reco non réclamé, le service génère :

- une preuve de négligence lorsque le service Postee Reco a connaissance du fait que le destinataire a consulté la notification ;
- une preuve de non réclamation dans le cas contraire.

Le service notifie l'expéditeur et met à sa disposition la preuve générée.

2.5 Intégrité et confidentialité des Postee Reco

Le service Postee Reco garantit l'intégrité et la confidentialité des identités des expéditeurs et destinataires et des données des envois recommandés. En particulier, toutes les transmissions d'information entre le service et ses utilisateurs ou ses partenaires sont réalisées via des canaux sécurisés adressant les risques de perte, de vol, de destruction ou de toute altération non autorisée.

Aucune modification des données de l'envoi n'est réalisée par le Service.

Un cachet électronique avancé, réalisé avec un certificat qualifié, est apposé sur l'ensemble des preuves générées par le service (cf. §2.6). Chacun de ces preuves permet de détecter toute perte d'intégrité de l'envoi du fait de la présence de l'identité des expéditeurs et destinataires et de l'empreinte des données parmi les informations de la preuve.

Les données de l'envoi recommandé sont conservées pour une durée de 1 an à compter du dépôt. Le service Postee Reco assure l'intégrité et la confidentialité de ces données par des mesures de sécurité de son système d'information, exposées au chapitre §4.

2.6 Preuves associées aux Postee Reco

2.6.1 Scellement et horodatage des preuves

Le service Postee Reco génère une preuve :

- Lors du dépôt par l'expéditeur d'un envoi recommandé ;
- Lors de l'acceptation ou du refus par un destinataire de l'envoi recommandé ;
- Lors de la fin du délai d'action du destinataire déclenchant la non réclamation de l'envoi recommandé (preuve de négligence ou de non réclamation).

Le cachet électronique est réalisé avec un certificat qualifié de cachet propre au service Postee Reco. Ce certificat est émis conformément à la Politique de Certification [POL_CERT] et en particulier la clé privée de cachet est une clé RSA de 2048 bits. Le cachet est apposé sur la preuve au format PDF selon le format PAdES-T. L'algorithme de signature est de type RSASSA-PSS avec un algorithme de hash SHA-256.

L'horodatage est un horodatage qualifié au titre du règlement eIDAS réalisé selon la politique [POL_HORO].

Le cachet et l'horodatage électronique des preuves est réalisé par un partenaire de Postee (cf. §1.5.2 et 1.5.3). Le service Postee Reco vérifie systématiquement la validité des cachets et des jetons d'horodatage électronique reçus de son partenaire, ainsi que le statut qualifié du service d'horodatage.

Les preuves sont conservées pour une période de 10 ans à compter de leur date de génération.

2.6.2 Vérification des preuves

Les utilisateurs qui téléchargent une preuve doivent en vérifier immédiatement la validité en effectuant les contrôles suivants :

- Contrôle de présence d'un cachet et d'un jeton d'horodatage ;
- Contrôle de l'intégrité de la preuve par validation cryptographique du cachet et du jeton d'horodatage ;
- Vérification du certificat de cachet :
    - Le certificat doit être l'un de ceux publiés dans la liste de confiance eIDAS pour identifier le service Postee Reco ;
    - Le certificat doit être, au moment de la création du cachet, dans sa période de validité et ni révoqué ni suspendu ;
- Vérification du jeton d'horodatage :
    - Le certificat de signature du jeton doit être l'un de ceux publiés dans la liste de confiance eIDAS pour le service d'horodatage partenaire de Postee ;
    - Le certificat doit être, au moment de l'horodatage, dans sa période de validité et ni révoqué ni suspendu ;
    - Le jeton d'horodatage doit être qualifié au moment de sa création ;
- Vérification de l'intégrité des données de l'envoi recommandé par comparaison des empreintes présentes dans la preuve avec celles qui peuvent être recalculées sur les données. Cette comparaison nécessite de disposer des données transmises.

La vérification de la validité d'une preuve peut être réalisée, depuis tout poste disposant d'un accès aux ressources en ligne indiquées au §2.7, pendant toute la durée de vie du certificat de signature du jeton d'horodatage intégré à la preuve.

Le prestataire d'horodatage de Postee (cf. §1.5.2) garantit que la durée de vie restante de ce certificat est a minima de 2 ans après émission d'une preuve. Au-delà de ce délai, la vérification des preuves peut toujours être réalisée jusqu'à 7 ans après génération de la preuve, du fait du recours à un certificat qualifié de cachet et un jeton d'horodatage qualifié. Cette vérification peut cependant nécessiter des ressources potentiellement hors ligne que Postee ou ses partenaires seront en mesure de mettre à disposition sur demande.

2.6.3 Contenu des preuves

Les heures indiquées dans les preuves sont exprimées dans la référence CET.

2.6.3.1 Preuve de dépôt

La preuve de dépôt contient :

Donnée	Précisions
Nom et prénom	Identification de la personne physique qui envoie le courrier
Raison sociale et SIRET de l'expéditeur, le cas échéant	Identification, le cas échéant, de la personne morale qui envoie le courrier
Adresse électronique de l'expéditeur	Adresse électronique de messagerie fournie par l'expéditeur.
Nom et prénom ou entité d'une personne morale	Nom et prénom de la personne physique destinatrice
raison sociale et SIREN /SIRET du destinataire	Identification de la personne physique destinatrice du courrier
Adresse électronique du destinataire	Adresse électronique de messagerie fournie par l'expéditeur.
Numéro d'identification unique de l'envoi recommandé	Ce numéro est généré par le service Postee Reco.
Empreintes cryptographiques de l'envoi recommandé	Empreintes calculées en SHA-256 pour chaque pièce jointe de l'envoi
Date et heure de dépôt	Date et heure de dépôt de l'envoi par l'expéditeur
Cachet électronique avancé	Le cachet électronique avancé est apposé sur la preuve au format PDF.
Jeton d'horodatage qualifié (heure de dépôt)	Le jeton d'horodatage qualifié est apposé sur la preuve scellée par le cachet électronique avancé.
OID de la politique	Identifiant de la politique de service utilisée pour la génération de cette preuve

2.6.3.2 Preuve de réception

La preuve de réception contient :

Donnée	Précisions

Nom et prénom ou raison sociale et SIREN /SIRET de l'expéditeur	Nom et prénom pour une personne physique Raison sociale et SIREN/SIRET pour une personne morale
Adresse électronique de l'expéditeur	Adresse électronique de messagerie fournie par l'expéditeur.
Nom et prénom ou raison sociale et SIREN /SIRET du destinataire	Nom et prénom pour une personne physique Raison sociale et SIREN/SIRET pour une personne morale
Adresse électronique du destinataire	Adresse électronique de messagerie fournie par l'expéditeur.
Numéro d'identification unique de l'envoi recommandé	Ce numéro est généré par le service Postee Reco.
Empreintes cryptographiques de l'envoi recommandé	Empreintes calculées en SHA-256 pour chaque pièce jointe de l'envoi
Date et heure de dépôt	Date et heure de dépôt de l'envoi par l'expéditeur
Date et heure d'acceptation	Date et heure d'acceptation de l'envoi par le destinataire
Nom et prénom de l'utilisateur ayant accepté l'envoi	Nom et prénom issus de la vérification d'identité initiale de l'utilisateur
Cachet électronique avancé	Le cachet électronique avancé est apposé sur la preuve au format PDF.
Jeton d'horodatage qualifié (heure d'acceptation)	Le jeton d'horodatage qualifié est apposé sur la preuve scellée par le cachet électronique avancé.
OID de la politique	Identifiant de la politique de service utilisée pour la génération de cette preuve

2.6.3.3 Preuve de refus

La preuve de refus contient :

Donnée	**Précisions**
Nom et prénom ou raison sociale et SIREN /SIRET de l'expéditeur	Nom et prénom pour une personne physique Raison sociale et SIREN/SIRET pour une personne morale
Adresse électronique de l'expéditeur	Adresse électronique de messagerie fournie par l'expéditeur.
Nom et prénom ou raison sociale et SIREN /SIRET du destinataire	Nom et prénom pour une personne physique Raison sociale et SIREN/SIRET pour une personne morale
Adresse électronique du destinataire	Adresse électronique de messagerie fournie par l'expéditeur.
Numéro d'identification unique de l'envoi recommandé	Ce numéro est généré par le service Postee Reco.
Empreintes cryptographiques de	Empreintes calculées en SHA-256 pour chaque

l'envoi recommandé	pièce jointe de l'envoi
Date et heure de dépôt	Date et heure de dépôt de l'envoi par l'expéditeur
Date et heure de refus	Date et heure de refus de l'envoi par le destinataire
Nom et prénom de l'utilisateur ayant refusé l'envoi	Nom et prénom issus de la vérification d'identité initiale de l'utilisateur
Cachet électronique avancé	Le cachet électronique avancé est apposé sur la preuve au format PDF.
Jeton d'horodatage qualifié (heure d'acceptation)	Le jeton d'horodatage qualifié est apposé sur la preuve scellée par le cachet électronique avancé.
OID de la politique	Identifiant de la politique de service utilisée pour la génération de cette preuve

2.6.3.4 Preuve de négligence

La preuve de négligence contient :

Donnée	Précisions
Nom et prénom ou raison sociale et SIREN /SIRET de l'expéditeur	Nom et prénom pour une personne physique Raison sociale et SIREN/SIRET pour une personne morale
Adresse électronique de l'expéditeur	Adresse électronique de messagerie fournie par l'expéditeur.
Nom et prénom ou raison sociale et SIREN /SIRET du destinataire	Nom et prénom pour une personne physique Raison sociale et SIREN/SIRET pour une personne morale
Adresse électronique du destinataire	Adresse électronique de messagerie fournie par l'expéditeur.
Numéro d'identification unique de l'envoi recommandé	Ce numéro est généré par le service Postee Reco.
Empreintes cryptographiques de l'envoi recommandé	Empreintes calculées en SHA-256 pour chaque pièce jointe de l'envoi
Date et heure de dépôt	Date et heure de dépôt de l'envoi par l'expéditeur
Date et heure de consultation de la notification	Date et heure à laquelle le destinataire a consulté pour la première fois la notification (sans donner suite)
Date et heure de négligence	Date et heure de passage de l'envoi à l'état « non réclamé »
Cachet électronique avancé	Le cachet électronique avancé est apposé sur la preuve au format PDF.
Jeton d'horodatage qualifié (heure de génération de la preuve de non réclamation)	Le jeton d'horodatage qualifié est apposé sur la preuve scellée par le cachet électronique avancé.
OID de la politique	Identifiant de la politique de service utilisée pour

	la génération de cette preuve

2.6.3.5 Preuve de non-réclamation

La preuve de non-réclamation contient :

Donnée	Précisions
Nom et prénom ou raison sociale et SIREN /SIRET de l'expéditeur	Nom et prénom pour une personne physique Raison sociale et SIREN/SIRET pour une personne morale
Adresse électronique de l'expéditeur	Adresse électronique de messagerie fournie par l'expéditeur.
Nom et prénom ou raison sociale et SIREN /SIRET du destinataire	Nom et prénom pour une personne physique Raison sociale et SIREN/SIRET pour une personne morale
Adresse électronique du destinataire	Adresse électronique de messagerie fournie par l'expéditeur.
Numéro d'identification unique de l'envoi recommandé	Ce numéro est généré par le service Postee Reco.
Empreintes cryptographiques de l'envoi recommandé	Empreintes calculées en SHA-256 pour chaque pièce jointe de l'envoi
Date et heure de dépôt	Date et heure de dépôt de l'envoi par l'expéditeur
Date et heure de non réclamation	Date et heure de passage de l'envoi à l'état « non réclamé »
Cachet électronique avancé	Le cachet électronique avancé est apposé sur la preuve au format PDF.
Jeton d'horodatage qualifié (heure de génération de la preuve de non réclamation)	Le jeton d'horodatage qualifié est apposé sur la preuve scellée par le cachet électronique avancé.
OID de la politique	Identifiant de la politique de service utilisée pour la génération de cette preuve

2.7 Informations publiées

Postee assure la publication d'informations à destination des utilisateurs du service (expéditeurs et destinataires) et des tiers ayant à déterminer la validité des preuves produites.

Postee s'engage à publier au minimum les informations suivantes :

- Le présent document, décrivant la politique et les pratiques du service Postee Reco ;
- Les conditions générales d'utilisation du service (§1.4.1) ;
- La liste des certificats de signature des preuves produites par le service ;
- Les points de publication des informations associées aux services des partenaires.

L'ensemble des informations publiées est en accès libre en lecture.

Les informations liées au service (évolutions, nouvelle version de la politique, 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 de Postee. En particulier, toute nouvelle version doit être communiquée aux clients et, le cas échéant, faire l'objet d'un nouvel accord.

Les informations publiées sont au moins disponibles les jours ouvrés. Postee garantit l'intégrité des données publiées.

L'accès en modification aux systèmes de publication des autres informations est strictement limité aux fonctions internes habilitées de Postee, au moins au travers d'un contrôle d'accès de type mots de passe basé sur une politique de gestion stricte des mots de passe.

2.8 Interopérabilité

Le service Postee Reco n'est connecté à aucun autre service d'envoi recommandé.

3 Gestion des risques

3.1 Analyse de risques

Avant le lancement du service qualifié, Postee effectue une évaluation des risques afin d'identifier, d'analyser et d'évaluer les risques, en tenant compte des aspects techniques, métiers et commerciaux. L'analyse de risque identifie, en particulier, les systèmes « critiques » du service.

Les mesures de sécurité seront prises en tenant compte du résultat de cette analyse.

Postee fixe, dans sa PSSI, les exigences de sécurité et les procédures opérationnelles nécessaires pour mettre en œuvre les mesures identifiées.

L'analyse de risques doit être examinée, et révisée si besoin, annuellement. Elle est aussi mise à jour à chaque modification ayant un impact important sur le service, notamment en cas de modification des politiques ou pratiques relatives à sa fourniture.

Les risques résiduels identifiés sont acceptés durant le processus d'homologation du service.

3.2 Homologation

Suite à la finalisation de l'analyse de risque, Postee procèdera à l'homologation du service. Cette homologation est réalisée préalablement à la fourniture du service de confiance qualifié puis révisée au moins tous les deux ans.

3.3 PSSI

Postee dispose d'une politique de sécurité du système d'information (PSSI) du service, qui définit l'organisation de la sécurité de l'information. La PSSO est documentée, implémentée et maintenue par Postee. Elle couvre les mesures de sécurité et les procédures appliquées concernant les infrastructures physiques et techniques et les biens sensibles du service., La PSSI et toutes ses évolutions sont approuvées par la direction de Postee.

La PSSI est communiquée aux employés et aux éventuels sous-traitants, aux prestataires, aux clients du service, aux organismes d'évaluation et à l'ANSSI.

Postee conserve la responsabilité globale de la conformité avec les procédures prévues dans sa PSSI, même lorsque certaines fonctions sont mises en œuvres par des sous-traitants. En particulier, Postee s'assure de la mise en œuvre effective des mesures prévues dans la PSSI.

La PSSI établit un inventaire des actifs du système d'information. Cet inventaire est revu régulièrement et à l'occasion de toute sensible du système d'information.

Tout changement susceptible d'avoir un impact sur le niveau de sécurité fourni doit être approuvé par le comité de pilotage du service.

La configuration du SI est auditée a minima chaque année afin de détecter tout changement pouvant être à l'origine d'une violation des politiques de sécurité.

4 Gouvernance et exploitation du service

4.1 Organisation

4.1.1 Organisation globale

Postee a mis en place une organisation fiable pour la délivrance du service.

Des responsabilités ont été définies au sein de Postee pour piloter les processus définis pour la fourniture et la gestion du service, que ceux-ci soient pris en charge en interne ou par des sous-traitants. Les prestataires de Postee prenant part à la fourniture du service sont soumis à des obligations contractuelles permettant à Postee d'assumer la responsabilité globale de conformité du service à cette politique, en particulier concernant les exigences de sécurité et de qualité de service. Le service repose en particulier sur des partenaires (cf. §1.5) soumis à des obligations au titre du règlement eIDAS, dont Postee s'assume de l'adéquation avec les exigences de son propre service.

Les pratiques mises en œuvre par Postee sont non-discriminatoires. Le service Postee Reco est accessible à toute personne morale ou physique ciblée par le service, à la condition que celles-ci respectent les obligations qui leur sont données par la présente politique et déclaration de pratiques. Des procédures de support et de gestion des différends sont définies afin de répondre aux sollicitations ou difficultés des utilisateurs ou parties prenantes du service.

Postee dispose des moyens matériels, humains et financiers suffisants pour assurer l'exploitation du service conformément à cette politique, y compris pour couvrir les conséquences financières de sa responsabilité résultant de dommages qui pourraient être causés aux utilisateurs.

4.1.2 Séparation des tâches

Les tâches et les domaines de responsabilité conflictuels sont séparés afin de réduire les possibilités d'altération, volontaire ou non, ou d'utilisation abusive des actifs du service.

Plusieurs rôles peuvent ainsi être attribués à une même personne, dans la mesure où le cumul ne compromet pas la sécurité des fonctions mises en œuvre.

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

- Responsable sécurité et administrateur système ou opérateur
- Contrôleur et tout autre rôle
- Administrateur système et opérateur.

4.2 Ressources humaines

4.2.1 Qualifications et compétences requises

Postee s'assure que son personnel et ses sous-traitants sont mobilisés et compétents pour garantir la sécurité et de la fiabilité du service.

Le personnel employé, interne ou sous-traitant, possède l'expertise, l'expérience et les qualifications nécessaires pour accomplir ses fonctions. Le personnel est préalablement formé aux logiciels, matériels et procédures internes de fonctionnement et de sécurité en vigueur. Ceci intègre en particulier les règles de sécurité relatives aux biens sensibles du SI et aux données à caractère personnel. Des sensibilisations régulières sont organisées, au minimum tous les ans, sur les nouvelles menaces et les bonnes pratiques de sécurité. Des sanctions

disciplinaires appropriées sont prévues pour les personnels dérogeant à la politique ou aux pratiques du service.

Le personnel d'encadrement possède l'expertise et l'expérience appropriée à son rôle et est familier des règles de sécurité en vigueur au sein du service.

Les rôles et responsabilités liés à la sécurité sont documentés dans des descriptions de poste accessibles à l'ensemble du personnel concerné. Postee respecte les principes de séparation des rôles et de moindre privilège dans la définition des fonctions et lors de leur affection. L'attribution des rôles prend en compte la sensibilité des responsabilités associées, les compétences et la probité du personnel. Lorsque cela s'avère nécessaire, la description de poste différencie les responsabilités et attendus des rôles générique de Postee par rapport aux spécificités exigées par le service qualifié.

Les personnels ont pris connaissance et compris les implications des opérations dont ils ont la responsabilité.

4.2.2 Procédures de vérification des antécédents

Postee met en œuvre tous les moyens légaux dont il dispose pour s'assurer de l'honnêteté du personnel qu'il emploie. Ces personnels ne doivent notamment pas avoir de condamnation de justice en contradiction avec leurs attributions, ni de conflit d'intérêt susceptible de nuire à l'impartialité des opérations.

À ce titre, Postee peut demander la communication d'une copie du bulletin n° 3 du casier judiciaire et peut décider, en cas de refus de communiquer cette copie ou en cas de présence de condamnation en justice jugée incompatible avec les attributions de la personne, de lui interdire ces attributions.

Ces vérifications sont menées préalablement à l'affectation à un rôle de confiance et revues régulièrement, au minimum tous les 3 ans.

4.2.3 Rôles de confiance

Les rôles de confiance, sur lesquels reposent en premier lieu la sécurité du système d'information, sont explicitement identifiés :

- **Responsable sécurité :** Le responsable de sécurité est chargé de la mise en œuvre de la politique de sécurité de la composante. Il gère notamment les contrôles d'accès physiques aux équipements des systèmes sensibles.
- **Responsable de la vérification d'identité :** Le responsable de la vérification d'identité est chargé de s'assurer que les processus d'identification électronique implémentés par Postee et suivis par les utilisateurs sont effectivement conformes aux processus définis par le présent document de politique et pratiques ;
- **Responsable du cachet :** Le cachet utilisé pour sceller les données, même opéré par un tiers, reste sous la responsabilité de Postee. À ce titre, une ou plusieurs personnes sont responsables du cachet vis-à-vis de Postee, mais aussi de l'Autorité de Certification qui l'a émis.
- **Administrateur et opérateur système :** Personnes chargées de la mise en route, de la configuration et de la maintenance technique des équipements informatiques (configuration, sauvegardes, restaurations…). Elles assurent l'administration technique des systèmes et des réseaux de la composante, ainsi que leur surveillance (détection d'incident).
- **Opérateur métier :** Les opérateurs métier sont les personnes en charge du fonctionnement quotidien du service : support client, gestion éventuelle du MIE, etc.
- **Contrôleur :** Personne autorisée à accéder aux preuves (2.5) et archives du service.

L'attribution d'un rôle de confiance est formalisée entre un responsable de la sécurité du service et le personnel qui accepte explicitement ce rôle.

4.3 Gestion des biens

4.3.1 Généralités

Postee assure la protection des biens (y compris des informations traitées) du service avec un niveau approprié.

Un inventaire des biens est réalisé et tenu à jour dans le cadre de la documentation de l'architecture technique et de l'analyse de risques du service. Les biens sont gérés en adéquation avec leur classification en terme de sensibilité de l'information.

4.3.2 Manipulation des supports

Les supports des biens sensibles sont gérés selon des exigences de sécurité adaptées à leur sensibilité.

Des mesures sont mises en œuvre afin de prévenir l'obsolescence, l'accès non autorisé, le vol ou l'altération des supports du service. Ces mesures sont effectives pour toute la durée de conservation prévue des biens. En fin de vie, et selon des procédures en accord avec le niveau de confidentialité des informations qu'ils contiennent, les supports sont soit détruits, soit réinitialisés en vue d'une réutilisation

4.4 Contrôle d'accès

Postee met en œuvre un contrôle d'accès physique et logique aux systèmes d'information du service.

Des procédures de gestion des habilitations personnelles sont mises en œuvre, prenant en compte les différents rôles identifiés par la présente politique. Ces procédures assurent que l'octroi et le retrait des habilitations s'effectuent en coordination avec la gestion des ressources humaines et respectent le principe de moindre privilège.

Tout utilisateur doit être identifié et authentifié avant de pouvoir accéder aux systèmes critiques du service. Toute action est tracée de sorte à pouvoir être imputable à la personne l'ayant effectuée.

Les habilitations métier et d'administration sont clairement séparés. L'accès aux logiciels d'exploitation (console, utilitaires, scripts, etc.) sur les serveurs est restreint et contrôlé.

Les informations sensibles doivent être protégées contre la divulgation résultant de la réutilisation de ressources (p. ex. fichiers effacés) par des personnels non autorisés.

4.5 Cryptographie

Postee garantit la mise en œuvre des mesures de sécurité appropriées pour la gestion des clés et des matériels cryptographiques sur l'ensemble de leur cycle de vie.

En particulier, concernant la clé privées de cachet des preuves de Postee Reco :

- La génération et l'utilisation d'une clé privée de cachet sont effectuées dans un module cryptographique sécurisé répondant aux exigences du document [ANSSI_PSCO] ;
- Le module cryptographique est placé dans un environnement physique séparé des autres fonctions, dont l'accès est réservé à un personnel restreint disposant d'un rôle de confiance ;
- La clé privée est générée, sauvegardée et restaurée uniquement dans un environnement physiquement sécurisé, par un personnel restreint disposant d'un rôle de confiance. Au moins deux personnes participent à chacune des opérations. Le nombre de personnes autorisées à mener ces opérations est réduit au minimum nécessaire pour garantir la satisfaction des exigences de cette politique (confidentialité et disponibilité en particulier).

- Toute copie de la clé privée de cachet est conservée dans le même type de module cryptographique ou dans des conditions assurant un niveau de sécurité au moins équivalent ;
- Le module cryptographique est protégé contre toute altération, aussi bien durant son transport que son stockage ;
- Le module cryptographique est maintenu en condition opérationnelle et en condition de sécurité, et supervisé afin de garantir son bon fonctionnement ;
- La clé privée de cachet est supprimée d'un module cryptographique à la fin de vie de ce matériel et avant sa mise au rebut.

4.6 Sécurité physique et environnementale

Postee assure un contrôle d'accès physique aux composants dont la sécurité est essentielle à la fourniture du service et minimise les risques liés à la sécurité physique.

Des mesures de sécurité physique et environnementale sont appliquées concernant :

- le contrôle d'accès physique, la protection contre les vol et les accès par effraction ;
- la protection contre les catastrophes naturelles (effondrements, séismes, inondations, …) ;
- la sécurité incendie, la climatisation, les dégâts des eaux ;
- la défaillance des ressources telles que l'électricité, les télécommunications,
- la continuité d'activité et la reprise d'activité après un sinistre.

L'accès aux composantes critiques du service est strictement limité aux seules personnes nominativement autorisées à pénétrer dans les locaux. Tout accès est tracé et surveillé, et les locaux sont sous alarme. Si nécessaire, une personne non-autorisée peut accéder à certaines installations si elle est accompagnée de façon permanente par une personne habilitée. En dehors des heures ouvrables, la sécurité est renforcée par la mise en œuvre de moyens de détection d'intrusion physique et logique.

Des mesures sont mises en œuvre afin de prévenir la perte, le vol, l'altération ou la compromission des actifs matériels ou informationnels nécessaires au bon fonctionnement du service. Toute zone partagée avec d'autres entités est maintenue en dehors du périmètre sensible du système d'information du service.

4.7 Sécurité opérationnelle

Postee utilise des systèmes et produits fiables, protégés contre les altérations, qui assurent la sécurité et la fiabilité des processus qu'ils supportent.

Postee garantit que les objectifs de sécurité sont définis lors des phases de spécification et de conception. Les mesures de sécurité appliquées, définies par l'analyse de risque (cf. §3.1), traitent en particulier les sujets suivants :

- gestion des comptes des utilisateurs, notamment la modification et la suppression rapide des droits d'accès ;
- identification et authentification forte des administrateurs pour l'accès au système (authentification à deux facteurs, de nature physique et/ou logique) ;
- gestion fine des droits des utilisateurs (respectant la politique de contrôle d'accès définie sur le service, notamment pour implémenter les principes de moindre privilège et de séparation des rôles) ;
- gestion de sessions d'utilisation (déconnexion après un temps d'inactivité, accès aux fichiers contrôlé par rôle et identifiant d'utilisateur) ;

- protection contre les virus informatiques et toutes formes de logiciels compromettants ou non- autorisés et mises à jour des logiciels ;
- génération de traces d'audit des opérations réalisées (non-répudiation et nature des actions effectuées) ;
- gestion des erreurs.

Des procédures de gestion des changements sont appliquées pour toute évolution du logiciel, application d'un correctif de sécurité ou modification de configuration qui impacte une composante implémentant la politique de sécurité du service. Toutes les modifications effectuées sont documentées et tracées. Des procédures sont également établies et suivies pour toutes les opérations effectuées par les personnes disposant d'un rôle de confiance et qui impactent la fourniture du service.

Postee a défini et applique des procédures garantissant que :

- les correctifs de sécurité sont appliqués au plus tard 2 mois après leur publication, et au plus tôt en cas de vulnérabilité avérée (cf. §4.9) ;
- les correctifs de sécurité ne sont pas appliqués lorsqu'ils introduisent des vulnérabilités ou des instabilités qui dépassent le bénéfice de leur installation ;
- les justifications de la décision de non application d'un correctif sont documentées.

4.8 Sécurité réseau

Postee garanti que le réseau et les composantes de son système d'information sont protégés contre les attaques.

Le système d'information est segmenté en réseaux ou zones en fonction de l'analyse des risques, compte tenu de la relation fonctionnelle, logique et physique entre les composants et les services. Les mêmes contrôles de sécurité sont appliquées à tous les systèmes partageant la même zone. Tous les systèmes critiques (composantes de cachet, d'horodatage, d'authentification) sont isolés dans une ou plusieurs zones sécurisées.

Les accès et les communications entre les différentes zones sont réduites au strict nécessaire pour le fonctionnement du service. En particulier des pares-feux protègent le réseau interne du service contre toute accès non autorisé, incluant les accès par des clients ou tierces parties du service. Toutes les connexions, interfaces et protocoles non nécessaires sont explicitement interdits ou désactivés, en particulier sur les pares-feux. Postee garantit que les configurations de ces contrôles sont périodiquement auditées en vue de vérifier leur conformité avec les exigences de la présente politique.

L'exploitation des systèmes est réalisée à travers un réseau d'administration dédié et cloisonné. Les systèmes utilisés pour l'administration de la mise en œuvre de la politique de sécurité ne doivent pas être utilisés à d'autres fins. Les systèmes de production du service doivent être séparés des systèmes utilisés pour le développement et les tests.

La communication entre des systèmes de confiance distincts ne doit être établie qu'à travers des canaux sécurisés, logiquement, cryptographiquement ou physiquement distincts des autres canaux de communication. Ces canaux assurent une authentification de bout en bout, l'intégrité et la confidentialité des données transmises. Des protocoles et algorithmes à l'état de l'art sont employés pour assurer le chiffrement des données transmises.

Lorsqu'un niveau élevé de disponibilité du service de confiance est nécessaire, la connexion réseau externe est redondée pour assurer la disponibilité même en cas de panne simple.

Une analyse de vulnérabilité régulière, a minima trimestrielle, sur les adresses IP publiques et privées du service, identifiées par Postee, doit être effectuée par une personne ou une entité ayant les compétences, les outils, la compétence, le code de déontologie et l'indépendance nécessaires. Cette analyse doit donner lieu à un rapport.

Un test d'intrusion sur les systèmes du service doit être réalisé lors de la mise en place, après toute évolution significative de l'infrastructure ou des applications, et a minima de façon annuelle. Le tests d'intrusion doit être effectuée par une personne ou une entité ayant les compétences, les outils, la compétence, le code de déontologie et l'indépendance nécessaires pour délivrer un rapport fiable.

Postee supervise de façon continue le taux de disponibilité du service et la charge constatée sur les systèmes informatiques du service. Des projections des besoins futurs sont également effectuées afin de s'assurer de toujours disposer des ressources nécessaires (puissance CPU, mémoire vive, espaces de stockage…) pour le respects des engagements énoncés par la présente politique du service.

4.9 Gestion des incidents et supervision

Les activités du système concernant l'accès aux systèmes informatiques, l'utilisation des systèmes informatiques et les requêtes métier doivent être surveillées.

Les activités de supervision prennent en compte la sensibilité des données collectées ou analysées. Toute activité d'une composante identifiée comme une potentielle violation de sécurité (incluant une intrusion dans le réseau du service) est détectée et reportée comme une alarme.

Les procédures de déclaration et de traitement des incidents ont pour objectif de minimiser les dommages causés par les incidents de sécurité et les dysfonctionnements. Postee est en capacité de réagir en temps opportun et de manière coordonnée afin de répondre rapidement aux incidents et de limiter l'impact des violations de la sécurité. Des personnels disposant de rôles de confiance sont désignés pour assurer le suivi des alertes sur les événements de sécurité potentiellement critiques et veiller à ce que les incidents pertinents soient signalés conformément aux procédures.

Postee a établi des procédures pour notifier les parties appropriées selon la règlementation applicable de toute atteinte à la sécurité ou toute perte d'intégrité ayant une incidence importante sur le service de confiance fourni ou sur les données à caractère personnel qui y sont conservées. Cette notification est réalisée dans un délai maximal de 24 heures après l'identification de l'incident, et peut concerner selon le cas l'ANSSI ou la CNIL.

Lorsque le manquement à la sécurité ou à la perte d'intégrité est susceptible de nuire à une personne physique ou morale à qui le service de confiance a été fourni, Postee informe sans délai la personne physique ou morale concernée.

La supervision du service inclut la collecte et l'analyse des journaux d'événements des différentes composantes, dans le but de détecter toute activité malicieuse. Des processus automatiques de traitement des journaux d'événements sont mis en œuvre et alertent le personnel de potentiels incidents de sécurité critiques. tentative de violation de son intégrité.

Les procédures d'exploitation du système d'information incluent la veille de sécurité sur ses composantes. Ces procédures assurent que :

- une analyse d'impact est réalisée afin de déterminer les mesures à appliquer pour traiter toute nouvelle vulnérabilité ;
- l'analyse d'impact est effectuée dans les 48 heures suivant la publication de toute nouvelle vulnérabilité critique ;
- toute décision de non traitement d'une vulnérabilité est documentée.

4.10 Gestion des enregistrements de preuve

4.10.1 Collecte, conservation et protection des enregistrement de preuve

Postee collecte, et conserve pour une durée de 7 (sept) ans après leur génération, toutes les informations pertinentes concernant les données délivrées et reçues, notamment afin de

pouvoir fournir des preuves en justice ou pour assurer la continuité de service. La durée de conservation de ces enregistrements perdure, le cas échéant, au-delà de la cessation d'activité du service. Cette durée se conforme aux exigences légales et règlementaires en vigueur, et est précisée dans les conditions générales d'utilisation du service.

Postee garantit le maintien de la confidentialité, de la disponibilité (contre la perte et la destruction partielle ou totale, volontaire ou non) et de l'intégrité des enregistrements courants ou archivés. La sensibilité des enregistrements (selon la nature des informations traitées) est prise en compte par Postee et peut nécessiter une protection spécifique (par exemple un chiffrement des données). Les enregistrements des opérations sur le service sont archivés de façon complète et confidentielle conformément aux engagements des conditions générales d'utilisation.

Les dates et heures précises des événements significatifs concernant l'environnement du service, la gestion des clés cryptographiques et la synchronisation des horloges sont enregistrées. Tous les événements des journaux d'événement sont datés avec l'heure système, en assurant une synchronisation quotidienne de celle-ci, au minimum à la minute près, et par rapport à une source fiable de temps UTC.

Les enregistrements peuvent être extraits et rendus disponibles par Postee à titre de preuve en justice du fonctionnement nominal du service.

La collecte et l'archivage des enregistrement sont conçues et mises en œuvre de façon à limiter les risques de contournement, de modification ou de destruction des enregistrements. Des mécanismes de contrôle d'intégrité doivent permettre de détecter toute modification, volontaire ou accidentelle, de ces journaux.

4.10.2 Périmètre des enregistrement de preuve

Les enregistrements de preuve comprennent a minima :

- Les événements génériques de chaque composante :
    - Démarrage et arrêt des systèmes informatiques et des applications ;
    - Gestion des comptes utilisateur (droits d'accès) et des données d'authentification correspondantes (mots de passe, certificats, etc.)
    - Connexion et déconnexion des utilisateurs sur les composantes du service ;
    - Opérations de maintenance et de configuration des systèmes.
- Les événements spécifiques aux fonctions du service d'envoi recommandé, notamment :
    - Enregistrement sur le service des expéditeurs et destinataires, incluant les données d'identité et coordonnées des utilisateurs ;
    - Validation de l'identité des expéditeurs et destinataires (validation initiale d'identité et authentification successives), incluant la modalité d'identification électronique utilisée et son résultat, et la preuve de succès (le cas échéant) de l'identification ;
    - Événements liés au cycle de vie des envois recommandés : dépôt, acceptation, refus, non réclamation, incluant les empreintes des données des envois ;
    - Événements liés au cycle de vie des clés et des certificats cryptographiques (cachet et horodatage) : génération (cérémonie des clés), sauvegarde et récupération, révocation, renouvellement, destruction, etc.
    - Génération et vérification des preuves produites par le service ;
    - Publication et mise à jour des informations liées au service (politique, conditions générales d'utilisation, etc.) ;
    - Génération et remise à un utilisateur d'un secret TOTP ;

- Réception d'une demande de révocation d'un moyen d'authentification ;
- Validation ou rejet d'une demande de révocation d'un moyen d'authentification.

- Les preuves générées par le service, qui intègrent en particulier :
  - l'identité de l'expéditeur du recommandé électronique ;
  - la référence unique de l'envoi recommandé électronique ;
  - les empreintes des pièces jointes composant l'envoi recommandé électronique ;
  - l'identité du destinataire du recommandé électronique ;
  - les données relatives à la sécurisation de l'envoi, i.e. les cachets électroniques apposés sur les preuves ;
  - les jetons d'horodatage électronique qualifié correspondant aux dates et heures d'envoi, d'acceptation, de refus ou de non réclamation ;

D'autres événements doivent aussi être 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 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 utilisateurs...).

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

- Type de l'événement ;
- Nom de l'exécutant ou référence du système déclenchant l'événement ;
- Date et heure de l'événement ;
- Résultat de l'événement (échec ou réussite).

4.11 Continuité d'activité

Postee a établi un plan de continuité d'activité applicable en cas de sinistre majeur. Ce plan adresse en particulier la perte, la compromission ou la suspicion de compromission de la clé privée de cachet ou d'un autre secret du service.

Les processus adéquats de reprise d'activité doivent être en place. Des infrastructures de secours sont identifiées pour assurer la récupération des informations et composantes essentielles après un sinistre ou une défaillance technique. Les dispositifs de reprise sont régulièrement testés pour s'assurer qu'ils répondent aux exigences du plan de continuité d'activité. Lorsque l'analyse de risque identifie des informations nécessitant un contrôle par au moins deux personnes, alors cette mesure est appliquée aussi par le plan de continuité d'activité.

Postee assure la sauvegarde régulière des informations nécessaires à la reprise du service en cas de sinistre, ce qui inclut les données du service, les logiciels et les configurations. Ces sauvegardes sont conservées, dupliquées et correctement protégées de façon à toujours être disponibles en cas de besoin.

En cas de compromission de la clé privée de cachet du service, le certificat correspondant est immédiatement révoqué. Dès détection du sinistre, Postee informe tous les clients et partenaires de Postee avec lesquels des accords ou relations contractuelles sont passés pour

la fourniture du service. L'information apportée indique que les preuves émises avec la clé compromise peuvent ne plus être valides depuis la date présumée de la compromission. Postee notifie également sans délai l'ANSSI, conformément au processus de gestion des incidents.

Suite à un sinistre majeur, Postee prend les mesures à même d'éviter la reproduction de l'incident lorsque cela est réalisable.

Si l'un des algorithmes, ou des paramètres associés, utilisés par le service devient insuffisant pour son utilisation prévue restante, alors Postee doit :

- informer tous les clients et partenaires de Postee avec lesquels des accords ou relations contractuelles sont passés pour la fourniture du service ;
- sécuriser les preuves existantes avec de nouveaux jetons d'horodatage ;
- le cas échéant, désactiver ou révoquer les moyens d'identification électroniques impactés.

4.12 Cessation d'activité

Postee a établi et maintient un plan de cessation d'activité pour le service Postee Reco. Ce plan a pour objectifs de minimiser les impacts de l'arrêt du service pour les clients, utilisateurs et les tierces parties du service. En particulier, il garantit la poursuite de la fourniture des informations nécessaires à la vérifications des preuves générées par le service.

Avant la cessation d'activité du service, Postee prend les mesures suivantes :

- Postee prévient ses clients et utilisateurs du service, les fournisseurs et partenaires ainsi que l'organisme d'audit de qualification et l'ANSSI. Dans le mesure du possible, cette information est réalisée avec un préavis d'au minimum un mois. Durant cette période, le dépôt de nouveaux envois recommandés n'est plus possible, mais les destinataires peuvent toujours accepter et télécharger des envois.
- Postee informe toutes les tierces parties de la cessation du service par une information postée sur son site institutionnel.
- Postee met fin à l'ensemble des autorisations données à ses partenaires et fournisseurs pour agir en son nom pour la délivrance du service Postee Reco.
- Une fois toutes les preuves relatives aux envois en cours produites (dépôt, réception, refus ou non-réclamation), l'ensemble des enregistrements de preuves et informations de vérification des preuves seront conservées par Postee ou déposées chez un tiers archiveur afin de rester disponibles à des fins légales durant la durée contractuellement prévue. L'ensemble des obligations de Postee concernant ces preuves seront maintenues par Postee ou transférées à ce tiers archiveur.
- Postee informera ses utilisateurs de l'arrêt d'activité et procèdera à la révocation des moyens d'authentification qu'elle a émis, la révocation de son certificat de cachet et à la destruction des clés privées et secrets utilisés par le service du recommandé électronique.
- Postee procèdera à la révocation de son certificat de cachet et à la destruction des clés privées et secrets utilisés par le service (et de toutes leurs copies) de façon à ce que ces données ne puissent plus être reconstituées.
- Postee s'efforcera de passer, dans la mesure du possible, les accords nécessaires au transfert de la fourniture du service pour ses clients existants à un autre fournisseur qualifié de service d'envoi recommandé.

Postee a provisionné les moyens financiers nécessaires à ces opérations pour le cas où Postee ne serait plus en mesure de les financer par elle-même, par exemple en cas de faillite.

4.13 Conformité

Postee s'assure d'opérer le service de manière légale et digne de confiance. Les pratiques de Postee sur le service ne sont pas discriminatoires.

Postee maintient les preuves de sa conformité aux exigences légales applicables, en particulier concernant la protection des données à caractère personnel. Des mesures techniques et organisationnelles appropriées sont prises contre tout traitement illicite des données à caractère personnel et contre la perte, la destruction ou la détérioration accidentelles de données personnelles.

La conception et la mise en œuvre des services, logiciels et procédures de Postee prennent en compte, dans la mesure du possible, l'accessibilité à tous les utilisateurs, y compris ceux en situation de handicap.

5 Autres problématiques métiers et légales

5.1 Responsabilité financière

5.1.1 Couverture par les assurances

Postee atteste avoir souscrit une assurance Responsabilité Civile Professionnelle concernant les prestations décrites dans ce document.

5.1.2 Autres ressources

Postee a garanti les ressources nécessaires au déroulement de son plan de fin de vie, y comrpis en cas de cessation d'activité.

5.1.3 Couverture et garantie concernant les entités utilisatrices

La couverture et les garanties concernant les entités utilisatrices sont exposées dans les Conditions Générales d'Utilisation ([CGU]) du service pour les expéditeurs et les destinataires du service.

5.2 Confidentialité des données professionnelles

5.2.1 Périmètre des informations confidentielles

Les informations considérées comme confidentielles sont au minimum les suivantes :

- Les données d'identité des utilisateurs professionnels et les justificatifs associés ;
- Les courriers envoyés et reçus par les utilisateurs professionnels ;
- Les moyens d'authentification et leurs causes de révocations ;
- Les secrets cryptographiques utilisés par le service (clés secrètes et privées, mots de passe, secrets utilisés pour la génération des cartes à codes ou des OTP, etc.).

5.2.2 Responsabilités en termes de protection des informations confidentielles

Postee respecte la législation et la réglementation en vigueur sur le territoire français et est responsable de la protection des informations confidentielles.

Postee peut cependant devoir mettre à disposition les données dont il dispose à des tiers dans le cadre de procédures légales. Les clients peuvent également accéder à leurs données professionnelles auprès de Postee.

5.3 Protection des données personnelles

5.3.1 Politique de protection des données personnelles

Les utilisateurs du service Postee Reco sont informés que, dans le cadre du service, Postee est amenée à collecter, héberger, et traiter des données à caractère personnel les concernant, aux seules fins d'assurer l'acheminement du courrier auprès du ou des destinataires.

Postee s'engage à conserver confidentielles les données personnelles et les courriers des utilisateurs et à ne pas les divulguer à des tiers (autres que le destinataire légitime de ces données), pendant toute la durée de leur possession par Postee. Pour ce faire, Postee fera ses meilleurs efforts pour :

- Prendre toutes les précautions utiles et mettre en place des contrôles efficaces de protection afin de préserver la sécurité des données personnelles, et notamment empêcher qu'elles ne soient déformées, endommagées, ou que des tiers non autorisés y aient accès ;
- Disposer des moyens organisationnels, techniques et financiers permettant de garantir a mise en oeuvre des mesures de confidentialité et de sécurité ;
- Prendre toute mesure de sécurité pour assurer la conservation et l'intégrité des données.

5.3.2 Informations à caractère personnel

Les informations considérées comme personnelles sont au minimum les suivantes :

- Les données d'identité des utilisateurs particuliers et les justificatifs associés ;
- Les courriers électroniques (expéditeurs et destinataires, données du courrier) ;
- Les informations techniques collectées (adresses IP, navigateurs…) lors de la connexion des utilisateurs du service.

5.3.3 Responsabilité en termes de protection des données personnelles

Postee s'engage à respecter la réglementation légale applicable au traitement de données personnelles et notamment le respect du règlement général de protection des données [RGPD]. Postee agit en qualité de responsable de traitement des données personnelles collectées pour le fonctionnement du service.

5.3.4 Notification et consentement d'utilisation des données personnelles

Les utilisateurs sont information des conditions d'utilisation de leurs données personnelles dans les Conditions Générales d'Utilisation du service, qu'ils doivent lire et accepter avant de bénéficier du service Postee Reco.

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

Postee se conforme strictement aux dispositions légales pour traiter les demandes de divulgation d'informations personnelles aux autorités judiciaires ou administratives.

5.3.6 Autres circonstances de divulgation d'informations personnelles

Postee n'a pas anticipé d'autres circonstances de divulgation d'informations personnelles.

5.4 Droits sur la propriété intellectuelle et industrielle

Postee est propriétaire du service Postee Reco et dispose à ce titre de l'ensemble des droits de propriété intellectuelle sur celui-ci.

Pour l'utilisation du service, l'utilisateur dispose d'une licence d'utilisation, aucun droit de propriété intellectuelle n'est cédé aux clients ou utilisateurs, que ce soit sur les produits ou le service en lui-même. L'utilisation, la reproduction, la modification, totale ou partielle, de ces éléments et/ou des informations qu'ils contiennent est strictement interdite.

5.5 Interprétations contractuelles et garanties

Les interprétations contractuelles et garanties du service sont détaillées dans les Conditions Générales d'Utilisation ([CGU]).

5.6 Dispositions concernant la résolution de conflits

La présente politique est régie par la loi française.

En cas de litige sur l'interprétation ou l'exécution de la présente politique, pour le cas où les parties ne parviendraient pas à trouver un accord amiable dans un délai de 30 jours sauf à ce que ce délai soit reconduit expressément entre les parties, il est attribué compétence expresse et exclusive au tribunal de commerce d'Amiens, lequel sera la seule juridiction compétente pour connaitre de tout différend, nonobstant pluralité de défendeurs ou appel en garantie, même pour les procédures d'urgence ou les procédures conservatoires par voie de référé ou requête ou les oppositions sur injonction de payer.

5.7 Durée et fin anticipée de validité de la politique

La présente politique est applicable pendant toute la durée de fourniture du service Postee Reco par Postee, jusqu'à entrée en vigueur d'une nouvelle version.

Après cessation de fourniture du service par Postee, la présente politique est résiliée de plein droit, excepté la garantie de conservation des preuves (par Postee ou un tiers qu'il aura désigné) sur leur durée de vie nominale prévue.

5.8 Conformité aux législations et réglementations

Postee garantir la conformité de la fourniture du service aux legislations et règlementations en vigueur, et en particulier au règlement RGPD et eIDAS.

Les pratiques de Postee sont non-discriminatoires.

5.9 Force majeure

Sont considérés comme cas de force majeure tous ceux habituellement retenus par les tribunaux français, notamment le cas d'un événement irrésistible, insurmontable et imprévisible.