Stampee

Politique générale de protection des données à caractère personnel de STAMPEE

V 1.1

Niveau de confidentialité : C1 Public

L'historique du document est dans le tableau suivant :

Numéro de version	Commentaire	Date	Auteur
1.0	Version initiale du document	18/04/2025	Florian de Vaulx (Datasure)
1.1	Prise en compte des traceurs strictement nécessaires aux notifications du service LRE	24/07/2026	Florian de Vaulx (Datasure)

1. Objectifs et champ d'application de la Politique

1.1 Objectifs de la Politique

STAMPEE, en tant que Prestataire de Services de Confiance qualifié opérant un service de Lettre Recommandée Électronique (LRE) conformément au règlement eIDAS, s'engage à assurer une protection élevée des données à caractère personnel traitées dans le cadre de ses activités. La présente Politique générale de protection des données à caractère personnel (ci-après la **Politique**) a pour objectif de définir les règles et bonnes pratiques mises en œuvre par STAMPEE afin de garantir la conformité de ses traitements de données personnelles au Règlement Général sur la Protection des Données (RGPD) et aux exigences du règlement eIDAS, ainsi qu'aux lois et réglementations nationales applicables en France.

Cette Politique vise notamment à formaliser les engagements de STAMPEE en matière de respect des principes fondamentaux de protection des données (licéité, finalité, minimisation, sécurité, limitation de conservation, etc.), à décrire les mesures organisationnelles et techniques internes déployées (registre des traitements, analyses d'impact, protection dès la conception, sensibilisation, procédures de gestion des droits et des incidents, encadrement des sous-traitants, contrôles internes…), et à définir la gouvernance mise en place (rôles et responsabilités, notamment le rôle du Délégué à la Protection des Données). STAMPEE entend ainsi assurer une protection effective des droits des personnes concernées et une transparence vis-à-vis de ces dernières.

Enfin, cette Politique contribue à démontrer la responsabilité (accountability) de STAMPEE, en documentant et rendant vérifiables ses actions de conformité. Elle s'inscrit en cohérence avec la Politique de Sécurité des Systèmes d'Information (PSSI) interne de STAMPEE, afin de garantir une approche globale et cohérente de la sécurité et de la confidentialité des informations.

1.2 Champ d'application de la Politique

La présente Politique s'applique à l'ensemble des activités de traitement de **Données à caractère personnel** réalisées par STAMPEE dans le cadre de ses services de LRE qualifiés et de services connexes non qualifiés conformes à la norme ETSI EN 319 521. Sont couverts tous les traitements de données personnelles relatifs aux expéditeurs et destinataires de lettres recommandées électroniques, aux clients de STAMPEE (donneurs d'ordre faisant appel aux services de STAMPEE), aux utilisateurs des services, ainsi qu'aux partenaires et fournisseurs intervenant dans ces services. Elle s'applique également, le cas échéant, aux traitements de données du personnel de STAMPEE et aux données des prospects ou contacts externes dans le contexte des opérations de STAMPEE.

STAMPEE étant une société basée en France, l'ensemble de ses traitements est régi par le cadre juridique français et européen (RGPD, loi Informatique et Libertés modifiée, règlement eIDAS). La Politique s'applique quelle que soit la localisation géographique des personnes concernées par les traitements. Ainsi, même lorsque STAMPEE adresse des clients ou utilisateurs internationaux, les données sont traitées conformément aux exigences de protection des données applicables dans l'Union européenne.

En matière de rôles et responsabilités dans les traitements : STAMPEE agit principalement en qualité de Sous-Traitant (processeur) pour le compte de ses clients (qui sont généralement les Responsables de Traitement des données d'expéditeurs et destinataires utilisant le service de LRE). Toutefois, dans certains cas spécifiques, STAMPEE peut agir en tant que co-Responsable de Traitement aux côtés d'un partenaire. C'est le cas notamment lors des vérifications d'identité des expéditeurs et destinataires réalisées par un prestataire certifié PVID (Prestataire de Vérification d'Identité à Distance) agréé par l'ANSSI : pour ces opérations de vérification d'identité, STAMPEE détermine conjointement avec le prestataire PVID les finalités et moyens du traitement, et partage donc la responsabilité du traitement. La Politique couvre ces deux situations (sous-traitance et co-responsabilité) et décrit les mesures prises par STAMPEE pour chacune d'elles. Enfin, pour les traitements dont STAMPEE détermine seul les finalités (par exemple gestion de ses employés, gestion de son site web, etc.), STAMPEE intervient en tant que Responsable de Traitement à part entière, également soumis aux règles de la présente Politique. STAMPEE agit en outre en qualité de Responsable de Traitement pour le dispositif limité de délivrabilité qu'elle décide d'intégrer aux courriels transactionnels du service LRE. Le prestataire d'envoi de courriels agit alors comme Sous-Traitant, sans finalité propre.

1.3 Révision de la Politique

Cette Politique entre en vigueur à compter de sa date de validation par la Direction générale de STAMPEE. Elle fera l'objet d'une **révision périodique au minimum une**

fois par an, notamment à l'occasion du rapport annuel du DPO (voir section 2.3), et pourra être mise à jour à tout moment en cas d'évolution des activités de STAMPEE, du cadre réglementaire (par exemple modifications du RGPD, nouvelles directives de la CNIL, etc.), ou à la suite d'audits et contrôles internes identifiant des axes d'amélioration.

Toute mise à jour substantielle de la Politique sera approuvée par la Direction générale, en concertation avec le DPO, et communiquée aux collaborateurs de STAMPEE ainsi qu'aux parties prenantes concernées. La version à jour de la Politique pourra être mise à disposition sur l'intranet de l'entreprise et/ou sur le site web de STAMPEE pour information des clients et partenaires, le cas échéant.

2. Organisation et gouvernance de la protection des données

Pour déployer efficacement la Politique et assurer la conformité de STAMPEE au RGPD et au règlement eIDAS, une organisation interne claire est mise en place, avec une définition précise des rôles et responsabilités de chaque acteur clé.

2.1 Acteurs clés et responsabilités

2.1.1 La Direction générale

La Direction générale de STAMPEE porte la responsabilité ultime de la conformité de l'entreprise en matière de protection des données. À ce titre, elle s'engage à promouvoir une **culture de protection des données** au sein de l'organisation et à allouer les moyens et ressources nécessaires à la mise en œuvre de la présente Politique. La Direction générale valide les politiques internes (dont la présente Politique et la PSSI), arbitre les décisions importantes en matière de protection des données (par exemple, validation des analyses d'impact, des plans d'action suite à un incident significatif, etc.), et assure un soutien actif au Délégué à la Protection des Données dans l'exercice de ses missions. Elle reçoit également le rapport annuel du DPO (section 2.3) et veille à la mise en œuvre des recommandations qui en découlent.

2.1.2 Les Directions opérationnelles (métiers)

Les responsables des différentes directions et services de STAMPEE (par exemple : service commercial, service opérations LRE, service support client, etc.) sont chargés d'intégrer les exigences de protection des données dans **leurs processus métiers**. Chaque Direction métier doit veiller, dans son domaine d'activité, à ce que les traitements de données personnelles réalisés respectent les principes et règles définis par la présente Politique. Concrètement, cela implique d'inventorier et tenir à jour les traitements relevant de leur périmètre (en collaboration avec le DPO pour le registre des traitements), de mettre en œuvre les mesures opérationnelles nécessaires (procédures, contrôles) pour garantir la conformité (par exemple, s'assurer que les données collectées auprès des clients sont minimales et à jour, que l'information des personnes est effectuée, etc.), et de remonter au DPO et à la Direction générale toute difficulté ou risque identifié. Les Directions métiers participent activement aux analyses

d'impact (AIPD) lorsque leurs activités sont concernées, et plus généralement coopèrent avec le DPO pour toute action de mise en conformité.

2.1.3 Le Délégué à la Protection des Données (DPO)

STAMPEE a désigné auprès de la CNIL un **Délégué à la Protection des Données** joignable à l'adresse dpo@stampee.fr. Ce rôle est exercé par la personne morale DATASURE, dont le siège est situé au 8 rue Alfred Maurel, 34120 Pézenas (France). En tant que DPO externalisé, DATASURE assure pour le compte de STAMPEE l'ensemble des missions prévues par le RGPD (articles 37 à 39) : conseil et accompagnement de STAMPEE sur la conformité des traitements, information et sensibilisation du personnel à la protection des données, réalisation d'audits et de contrôles du respect de la réglementation et de la présente Politique, conseil lors de la réalisation d'Analyses d'Impact relatives à la Protection des Données (AIPD), réponse aux questions des personnes concernées et traitement des demandes d'exercice de droits, et coopération avec l'autorité de contrôle (CNIL) en étant le point de contact principal de celle-ci.

Le DPO dispose de l'indépendance nécessaire pour accomplir ses tâches et rend compte directement de ses analyses et recommandations à la Direction générale de STAMPEE. Il est consulté en amont de toute décision importante relative à un traitement de données (par exemple, lancement d'un nouveau service de LRE, choix d'un nouveau sous-traitant impliquant des données personnelles, gestion d'un incident de sécurité significatif, etc.). Le DPO tient également à jour le **registre des traitements** (section 4.3) en collaboration avec les Directions métiers, et supervise les démarches de conformité de STAMPEE au quotidien.

2.1.4 La Direction des Systèmes d'Information (IT & Sécurité)

La Direction des Systèmes d'Information et de la Sécurité (DSI) de STAMPEE joue un rôle crucial dans la mise en œuvre des mesures de **sécurité** et de protection de la vie privée dès la conception. Elle est responsable du maintien de l'intégrité, de la disponibilité et de la confidentialité des systèmes d'information traitant des données personnelles. La DSI déploie les mesures techniques adéquates (pare-feux, chiffrement, sauvegardes, contrôles d'accès, etc.) conformément à la PSSI interne, et veille à leur conformité avec les exigences de l'article 32 du RGPD et des standards eIDAS applicables aux Prestataires de Services de Confiance (tels que les normes ETSI applicables à la LRE).

La DSI collabore étroitement avec le DPO, notamment pour intégrer le principe de **Privacy by Design** lors du développement de nouvelles applications ou fonctionnalités (section 4.1), pour réaliser les analyses de risques techniques et contribuer aux AIPD (section 4.2), et pour gérer les incidents de sécurité (section 7). Elle s'assure que les équipes techniques connaissent et appliquent les bonnes pratiques de sécurité des données. En cas d'incident, la DSI applique la procédure de gestion des violations de données en lien avec le DPO. Enfin, elle participe au choix et à l'évaluation des sous-traitants techniques (hébergeurs, prestataires cloud, etc.) sous l'angle de la sécurité des données (section 5).

2.2 Rôle de STAMPEE en tant que sous-traitant ou co-responsable de traitement

Comme mentionné précédemment, STAMPEE intervient principalement en tant que **Sous-Traitant** pour le compte de ses clients lorsqu'elle traite des Données à caractère personnel dans le cadre de la prestation de services de LRE. Dans ce contexte, les clients de STAMPEE déterminent les finalités et les moyens essentiels des traitements (par exemple, l'envoi d'une lettre recommandée électronique à un destinataire donné, avec un contenu déterminé par le client), et STAMPEE agit uniquement sur instruction de ces clients pour exécuter techniquement le service. STAMPEE s'engage alors à respecter strictement les obligations qui lui incombent en vertu de l'article 28 du RGPD et des clauses contractuelles convenues avec chaque client : en particulier, ne traiter les Données personnelles **que pour les finalités** définies par le client, n'agir que sur instruction documentée du client, garantir la confidentialité et la sécurité des données, ne pas faire de sous-traitance ultérieure sans autorisation, assister le client dans le respect de ses propres obligations (par exemple pour les demandes de droits ou la gestion des violations), etc. Ces engagements sont détaillés dans les contrats de service ou accords de sous-traitance conclus avec chaque client (voir section 5. Gestion des tiers).

Par exception, pour certaines opérations précises, STAMPEE partage la détermination des finalités et des moyens avec un partenaire, ce qui en fait un **co-Responsable de Traitement**. C'est le cas dans le processus de **vérification d'identité** des utilisateurs (expéditeurs ou destinataires) lorsque cette vérification est requise pour la fourniture du service de LRE qualifié (par exemple, pour s'assurer de l'identité d'un expéditeur avant l'envoi d'une LRE qualifiée, conformément aux exigences de confiance du règlement eIDAS). STAMPEE s'appuie alors sur un prestataire externe certifié **PVID** par l'ANSSI pour réaliser la vérification d'identité à distance. STAMPEE et le prestataire PVID déterminent ensemble les modalités de cette vérification et poursuivent la même finalité (garantir l'identification fiable de la personne). Ils sont donc considérés comme co-responsables de ce traitement spécifique.

Dans ce cadre de co-responsabilité, STAMPEE veille à ce qu'un **accord de répartition des responsabilités** soit conclu avec le prestataire PVID, conformément à l'article 26 du RGPD. Cet accord définit notamment qui est en charge de fournir l'information aux personnes concernées avant la vérification d'identité, comment sont gérés les droits des personnes sur les données d'identification collectées, qui conserve quelles données et pendant combien de temps, et qui notifiera d'éventuelles violations de données liées à ce processus. STAMPEE assume pleinement ses obligations de Responsable de Traitement pour la part qui lui incombe, par exemple en s'assurant de la conformité du processus global, en vérifiant les garanties de protection des données offertes par le prestataire PVID, et en restant point de contact pour les personnes concernées si nécessaire. En pratique, cela signifie que la personne dont l'identité est vérifiée pourra exercer ses droits tant auprès du prestataire PVID qu'auprès de STAMPEE, et obtiendra une réponse coordonnée.

En résumé, STAMPEE **définit pour chaque traitement son rôle exact** (Responsable, co-Responsable ou Sous-Traitant) et met en œuvre les mesures de conformité adaptées à ce rôle. Ceci fait partie intégrante de sa gouvernance de

protection des données et est documenté dans le registre des traitements et les contrats associés.

2.3 Rapport annuel du DPO

Afin de piloter l'amélioration continue de la conformité, le DPO de STAMPEE établit **un rapport annuel** synthétisant l'état de la protection des données au sein de l'entreprise. Ce rapport, présenté à la Direction générale, comprend notamment :

- Un bilan des actions menées durant l'année écoulée (sensibilisations du personnel effectuées, procédures mises en place ou mises à jour, analyses d'impact réalisées, audits internes, etc.) et des éventuels incidents de données ou réclamations de personnes concernées survenus, avec les mesures correctives apportées.
- Une évaluation du niveau de conformité de STAMPEE vis-à-vis du RGPD, d'eIDAS et des autres exigences (par exemple, conformité des contrats de sous-traitance, efficacité des procédures d'exercice des droits, etc.), s'appuyant sur les contrôles effectués.
- Des indicateurs de suivi (par exemple : nombre de demandes de droits reçues et temps de réponse, nombre d'incidents de sécurité, pourcentage de collaborateurs formés sur l'année, etc.).
- Le plan d'actions recommandé pour l'année à venir afin de **renforcer la protection des données** et traiter d'éventuels points d'amélioration identifiés. Ce plan peut inclure la mise à jour de certaines procédures, des formations supplémentaires, des mesures techniques à implémenter, ou encore des évolutions de la Politique.

La Direction générale examine ce rapport avec attention et valide le plan d'actions. Les recommandations du DPO font l'objet d'un suivi pour s'assurer de leur mise en œuvre effective. Ce rapport annuel du DPO constitue un outil essentiel de **contrôle interne** et de pilotage de la conformité, démontrant l'engagement de STAMPEE dans une démarche proactive de protection des données.

3. Principes fondamentaux en matière de traitement des données personnelles

Conformément à la **Législation applicable** (RGPD, loi française et règlement eIDAS), STAMPEE s'engage à respecter scrupuleusement les principes fondamentaux de protection des données à caractère personnel pour toute opération de traitement. Ces principes directeurs, détaillés ci-après, guident l'ensemble des activités de collecte et d'utilisation des données au sein de STAMPEE.

3.1 Licéité, loyauté et transparence

Tout traitement de **Données à caractère personnel** effectué par STAMPEE doit reposer sur une **base juridique valide** et être réalisé de manière loyale et transparente envers les personnes concernées. STAMPEE s'assure ainsi qu'aucune donnée personnelle n'est collectée ou utilisée sans une justification légale appropriée, et que

les personnes concernées ne font l'objet d'aucune manipulation ou surprise quant à l'utilisation de leurs données.

Les bases légales reconnues par le RGPD et utilisées par STAMPEE, selon le contexte du traitement, peuvent inclure notamment :

- **Le Consentement** de la personne concernée pour une ou plusieurs finalités spécifiques (par exemple, consentement de la personne pour recevoir des informations ou communications de la part de STAMPEE, si ce n'est pas dans le cadre d'un contrat) – voir section 3.2 pour les conditions de validité du consentement.
- **L'exécution d'un contrat** auquel la personne concernée est partie, ou l'exécution de mesures précontractuelles prises à la demande de celle-ci (par exemple, traiter les données d'un client pour lui fournir le service de LRE qu'il a souscrit).
- **Le respect d'une obligation légale** à laquelle STAMPEE est soumis (par exemple, conservation de certaines données pendant une durée légale, obligations découlant du statut de Prestataire de Services de Confiance qualifié, telles que l'identification des utilisateurs conformément à eIDAS).
- **L'intérêt légitime** poursuivi par STAMPEE ou par un tiers, dans le respect des droits et libertés des personnes (par exemple, le traitement de données de contact d'un utilisateur dans le but d'améliorer le service ou de prévenir des fraudes, peut reposer sur l'intérêt légitime dès lors que l'impact sur la vie privée est limité et maîtrisé).
- Plus exceptionnellement : **la sauvegarde des intérêts vitaux** d'une personne concernée ou d'une autre personne physique (hypothèse rare, par exemple communiquer une information médicale en cas d'urgence vitale, bien que STAMPEE ne traite pas de telles données en principe), ou l'exécution d'une **mission d'intérêt public**/relevant de l'exercice de l'autorité publique (ce dernier cas est peu susceptible de s'appliquer aux activités de STAMPEE, qui sont de nature privée).

STAMPEE veille à documenter pour chaque traitement la base juridique retenue, notamment dans le registre des traitements (section 4.3), et s'assure que cette base est valable au regard de la finalité poursuivie.

Lorsqu'un courriel contient un pixel de suivi ou un lien individualisé entraînant une opération de lecture ou d'écriture sur le terminal du destinataire, STAMPEE applique également l'article 82 de la loi Informatique et Libertés. Seuls les dispositifs ayant pour finalité exclusive de permettre ou faciliter la communication électronique et strictement nécessaires à la fourniture du service LRE sont mis en oeuvre sans consentement. Les traitements de données personnelles qui en résultent restent fondés sur l'une des bases de l'article 6 du RGPD, notamment l'exécution du contrat, le respect d'une obligation légale ou l'intérêt légitime, selon la qualité de la personne concernée et la finalité poursuivie.

R1. *Tout Traitement de Données à caractère personnel effectué par STAMPEE repose sur une base légale clairement identifiée, appropriée à la finalité poursuivie, et cette base est documentée dans le registre des traitements.*

Par ailleurs, STAMPEE s'engage à la **transparence** envers les **Personnes concernées**. Cela signifie que les personnes dont les données sont traitées sont informées, au moment de la collecte de leurs données ou dès que possible, des caractéristiques essentielles du traitement les concernant. STAMPEE fournit des informations claires, accessibles et rédigées en des termes compréhensibles, conformément aux articles 12, 13 et 14 du RGPD. Ces informations incluent notamment : l'identité de STAMPEE (et de ses clients le cas échéant), les finalités du traitement, la base légale, les destinataires des données, la durée de conservation prévue, les droits dont disposent les personnes sur leurs données et la manière de les exercer, ainsi que, le cas échéant, les transferts de données hors UE effectués et les garanties associées, et les coordonnées du DPO.

Dans la pratique, cette information est délivrée par différents moyens selon les cas :

- Via la politique de confidentialité mise à disposition sur le site web de STAMPEE pour les utilisateurs et destinataires du service LRE. Cette politique décrit notamment les courriels transactionnels, les dispositifs de délivrabilité strictement nécessaires qu'ils peuvent contenir, les données limitées qui en résultent et les droits des personnes concernées.
- Via les **conditions contractuelles** ou documents d'information fournis par les clients de STAMPEE à leurs propres utilisateurs (STAMPEE contractuellement oblige ses clients à informer les destinataires que leurs données seront traitées par STAMPEE en qualité de sous-traitant pour l'envoi de la LRE).
- Via des **mentions d'information spécifiques** lors de la procédure de vérification d'identité PVID (une notice d'information est présentée à l'utilisateur avant la vérification, expliquant le traitement de ses données d'identité par STAMPEE et le prestataire PVID).
- Plus généralement, pour tout recueil de données directement opéré par STAMPEE (par exemple, formulaire de contact sur le site, inscription à une newsletter), une mention d'information conforme est fournie au moment de la collecte.

R2. *STAMPEE garantit une information transparente des Personnes concernées sur les traitements de leurs Données, en fournissant des informations complètes et intelligibles sur la façon dont leurs Données sont collectées et utilisées, et ce par des supports appropriés (mentions d'information, politiques de confidentialité, etc.).*

3.2 Consentement

Bien que la plupart des traitements effectués par STAMPEE reposent sur des bases légales autres que le consentement, il peut arriver que STAMPEE y recoure pour des traitements facultatifs, de prospection ou portant sur certaines données sensibles. Les dispositifs de délivrabilité décrits à la section 3.9 ne reposent pas sur le consentement : ils sont limités aux opérations strictement nécessaires au fonctionnement des notifications LRE et bénéficient, pour les opérations relevant de l'article 82 de la loi Informatique et Libertés, de l'exemption correspondante.

3.2.1 Les conditions de validité du consentement

Lorsque le consentement est la base légale d'un traitement, STAMPEE s'assure que ce consentement est **libre, éclairé, spécifique et univoque** :

- *Libre* : la personne doit avoir le choix de consentir ou non sans subir de contrainte ni de conséquences négatives en cas de refus. Par exemple, si STAMPEE propose à un utilisateur de recevoir des offres commerciales par email, celui-ci peut refuser sans que cela n'affecte son utilisation du service principal de LRE.
- *Éclairé* : la personne reçoit, préalablement à son choix, une information claire sur l'identité du responsable du traitement, les données concernées, la finalité et les principales implications du traitement, afin de comprendre exactement à quoi elle consent.
- *Spécifique* : le consentement est demandé pour une finalité déterminée. Si plusieurs finalités distinctes sont poursuivies, le consentement est recueilli séparément pour chacune (sauf exception de finalités étroitement liées). STAMPEE évite de demander un consentement global couvrant de multiples usages disparates.
- *Non équivoque* : le consentement se manifeste par un acte positif clair de la part de la personne (par exemple cocher volontairement une case "J'accepte...", cliquer sur "Autoriser", etc.). L'utilisation de cases pré-cochées, le silence ou l'inactivité de la personne ne sont **jamais** considérés comme un consentement valable.

Par ailleurs, lorsque la loi l'exige (notamment en cas de traitement de données sensibles, ce que STAMPEE ne pratique pas, voir 3.8, ou dans certains contextes réglementaires spécifiques), STAMPEE recueille un consentement **explicite** qui suppose une confirmation claire de la part de la personne (par exemple double validation, déclaration écrite ou électronique formelle).

Si le traitement concerne des **mineurs** soumis à obligation de consentement parental (par exemple, moins de 15 ans en France pour certains services de la société de l'information), STAMPEE veille à obtenir le consentement du titulaire de l'autorité parentale, conformément aux exigences légales, bien que ce cas d'usage soit peu courant pour un service de LRE généralement utilisé par des majeurs.

R3. *Lorsque le Consentement est requis, STAMPEE ne procède au traitement qu'après avoir obtenu un consentement valide de la Personne concernée, c'est-à-dire un consentement libre, éclairé, spécifique et exprimé par une action positive claire.*

3.2.2 La gestion du consentement (durée, preuve)

STAMPEE met en place des mécanismes pour **documenter et conserver la preuve** des consentements obtenus. Par exemple, dans ses bases de données ou journaux d'activité, STAMPEE conserve la trace de l'action de l'utilisateur donnant son consentement (date, heure, moyen, contenu de la demande de consentement). Ceci permet d'être en mesure de démontrer, en cas de contrôle ou de contestation, que la personne avait bien consenti au traitement concerné (principe d'accountability).

Le **consentement est conservé** aussi longtemps que nécessaire pour la finalité du traitement concerné. Si la finalité est ponctuelle, la preuve du consentement peut être

conservée au moins jusqu'à ce que l'action soit réalisée plus une période de prescription légale. Si la finalité est continue (par exemple envoi de newsletters récurrentes), la preuve du consentement est conservée pendant toute la durée de l'abonnement de la personne à la newsletter, et éventuellement archivée au-delà pendant le délai de prescription applicable après la fin de l'envoi de newsletters, afin de pouvoir justifier de la conformité passée.

STAMPEE revoit régulièrement les consentements stockés afin de s'assurer qu'ils sont toujours valides au regard du contexte. Si les pratiques ou les finalités évoluent de manière substantielle, un **nouveau consentement** sera requis auprès des personnes concernées préalablement à toute utilisation des données selon les nouvelles modalités.

3.2.3 Le retrait du consentement

Conformément au principe selon lequel le consentement doit pouvoir être **retiré à tout moment**, STAMPEE facilite l'exercice du **droit au retrait du consentement**. Les personnes concernées sont informées, dès le recueil de leur consentement, de leur droit de le retirer ultérieurement si elles le souhaitent, et des moyens simples pour ce faire.

Concrètement, STAMPEE offre des mécanismes de désinscription ou d'opposition clairs. Par exemple, chaque communication électronique envoyée sur la base du consentement (telle qu'une newsletter) comporte un lien de désabonnement en un clic. De même, un utilisateur peut à tout moment contacter STAMPEE (via l'adresse dpo@stampee.fr ou via un formulaire dédié) pour signaler qu'il retire son consentement à un traitement particulier. Aucune justification n'est exigée.

Dès réception d'une demande de retrait de consentement, STAMPEE fera cesser dans les meilleurs délais le traitement concerné (s'il n'a pas d'autre base légale) et prendra les mesures pour que les données correspondantes ne soient plus traitées (suppression ou archivage sécurisé). Le retrait du consentement n'a pas d'effet rétroactif : il n'affecte pas la licéité du traitement effectué avant le retrait. STAMPEE peut néanmoins conserver l'information de ce retrait afin de ne plus solliciter la personne à l'avenir sur la même finalité.

R4. *STAMPEE conserve la preuve des consentements obtenus et permet aux Personnes concernées de retirer facilement et à tout moment leur consentement, sans porter atteinte aux services de base fournis.*

3.3 Limitation des finalités

STAMPEE collecte et traite les Données à caractère personnel **pour des finalités déterminées, explicites et légitimes**, et s'interdit de traiter ces données de manière incompatible avec ces finalités initiales. Autrement dit, toute donnée personnelle recueillie par STAMPEE l'est dans un but précis, clairement défini au moment de la collecte, et ne saurait être ultérieurement utilisée pour un objectif substantiellement différent sans une base légale appropriée (et si nécessaire, le consentement de la personne).

Dans le contexte de ses services, STAMPEE poursuit principalement les finalités suivantes : la fourniture du service de lettre recommandée électronique, incluant la gestion des comptes, l'acheminement des messages, les notifications et relances fonctionnelles, la délivrabilité des courriels, la mise à disposition sécurisée, le suivi de la transmission et la preuve de réception ; la vérification d'identité lorsque requise ; l'amélioration technique et le support ; ainsi que le respect des obligations liées à son statut de Prestataire de Services de Confiance. Des finalités additionnelles peuvent inclure la facturation, la gestion administrative, la prospection commerciale dans le respect du cadre applicable et la gestion des demandes de support.

Chacune de ces finalités est documentée dans le registre des traitements. STAMPEE veille à ne collecter aucune donnée pour des finalités cachées. Si, dans des cas exceptionnels, STAMPEE souhaitait réutiliser des données déjà collectées pour une nouvelle finalité non prévue initialement, elle s'assurerait que la nouvelle finalité est **compatible** avec la finalité d'origine (en tenant compte des critères du RGPD, comme le lien entre les finalités, le contexte de collecte, la nature des données, les conséquences pour les personnes, etc.) ou bien elle recueillerait le consentement spécifique des personnes pour cette réutilisation, ou s'appuierait sur une autre base légale adéquate après les avoir informées.

Par exemple, les données (adresse email, numéro de téléphone) collectées pour notifier un destinataire de la mise à disposition d'une LRE ne seront pas détournées pour lui envoyer ultérieurement des offres commerciales de STAMPEE ou d'un tiers, à moins que cette personne n'y ait consenti séparément. De même, les informations d'identité vérifiées par le processus PVID seront exclusivement utilisées dans le but de sécuriser l'envoi/réception des LRE et pour satisfaire aux exigences de confiance, et non pour d'autres finalités.

R5. *STAMPEE n'utilise les Données personnelles que pour les finalités pour lesquelles elles ont été collectées. Tout changement de finalité ne sera envisagé qu'en conformité avec le RGPD (finalité compatible ou nouveau consentement) et après information préalable des Personnes concernées le cas échéant.*

3.4 Minimisation des données et exactitude

STAMPEE applique le principe de minimisation des données : seules les données strictement nécessaires à chaque finalité sont collectées. Pour le suivi de délivrabilité des courriels LRE, les données sont limitées à l'adresse électronique, à un identifiant technique de message, au statut de transmission et à la date de dernière ouverture au niveau de la journée. L'adresse IP, l'heure précise, le type de terminal, le logiciel de messagerie, la localisation et l'historique détaillé des ouvertures ne sont ni enregistrés ni conservés par ce dispositif.

Par exemple, pour envoyer une lettre recommandée électronique, STAMPEE a besoin de l'adresse électronique du destinataire (ou de son numéro de téléphone si le destinataire choisit d'être avisé par SMS), mais n'a pas besoin de connaître sa date de naissance ou d'autres informations personnelles sans lien avec la remise du message. Ces données supplémentaires ne seront donc pas demandées. De même, dans la procédure de vérification d'identité via PVID, les pièces et informations collectées se limitent à celles nécessaires à l'authentification de la personne

(typiquement, une pièce d'identité officielle et éventuellement une capture vidéo ou photo pour la reconnaissance, selon les exigences PVID), et rien de plus.

Les formulaires (papier ou en ligne) utilisés par STAMPEE sont conçus pour ne requérir que le minimum. Les systèmes d'information de STAMPEE sont configurés de manière à n'afficher ou ne traiter par défaut que les données nécessaires (**privacy by default**, voir section 4.1). En interne, les employés de STAMPEE n'ont accès qu'aux données dont ils ont besoin pour leurs missions (principe du besoin d'en connaître).

R6. *STAMPEE ne collecte et ne traite que les Données personnelles strictement nécessaires à l'objectif visé. Les formulaires et processus de collecte sont conçus dans une optique de minimisation, et toute donnée non indispensable est écartée.*

En complément, STAMPEE veille à maintenir l'**exactitude** et la mise à jour des données personnelles traitées. Il est essentiel que les données soient correctes afin d'éviter des conséquences négatives pour les personnes (par exemple, une erreur dans l'adresse email d'un destinataire pourrait empêcher la bonne réception d'une notification de LRE). STAMPEE prend donc des mesures raisonnables pour que les données inexactes ou obsolètes soient rectifiées ou supprimées.

Concrètement, cela passe par :

- Des contrôles de validité à la saisie des données (par exemple, validation de format sur les adresses email ou numéros de téléphone).
- La possibilité offerte aux personnes concernées (utilisateurs finaux, clients) de corriger ou mettre à jour leurs informations. Par exemple, un expéditeur disposant d'un compte STAMPEE peut accéder à son profil et rectifier ses coordonnées si besoin.
- Des procédures internes de vérification périodique pour certaines données critiques. Par exemple, lors de la vérification PVID, une double vérification est faite (par le prestataire PVID puis par STAMPEE réceptionnant le résultat) pour s'assurer que l'identité correspond bien.
- Si STAMPEE constate qu'une donnée est manifestement incorrecte (par ex. un email qui génère un message d'erreur permanent), elle entreprend de la faire corriger en sollicitant la personne ou le client qui a fourni l'information.

R7. *STAMPEE s'assure de l'exactitude des Données personnelles traitées et procède, le cas échéant, à leur rectification ou mise à jour sans délai. Les Données inexactes ou qui ne sont plus nécessaires sont supprimées ou archivées de manière sécurisée.*

3.5 Limitation de la conservation (durées de conservation)

Le principe de limitation de la conservation stipule que les Données à caractère personnel ne doivent pas être conservées sous une forme identifiable au-delà de la durée nécessaire aux finalités pour lesquelles elles ont été collectées. STAMPEE définit donc, pour chaque catégorie de données et chaque finalité, une **durée de conservation appropriée**, en conformité avec les exigences légales et réglementaires, et s'engage à ne pas conserver les données au-delà de cette durée.

Les règles de conservation sont établies en tenant compte :

- **Des obligations légales ou réglementaires** imposant la conservation pendant une certaine période. Par exemple, en tant que prestataire LRE qualifié, STAMPEE peut être tenue de conserver certaines informations ou preuves liées aux envois recommandés pendant une durée minimale à fins probatoires. De même, des données comptables ou de facturation doivent être conservées 10 ans (obligation fiscale et commerciale).
- **Des recommandations des normes eIDAS/ETSI** applicables. Par exemple, les normes relatives aux services de confiance recommandent souvent de conserver les journaux d'événements et les preuves de transactions pendant au moins 7 à 10 ans, afin de pouvoir apporter la preuve des opérations en cas de litige.
- **Du principe de précaution juridique (intérêt légitime)** pour d'éventuelles actions en justice. STAMPEE peut conserver certaines données pendant le délai de prescription applicable pour se défendre en cas de contentieux (par exemple, conserver la preuve d'envoi et de réception d'une LRE pendant le délai de prescription d'une contestation possible de la notification).
- **Des besoins opérationnels limités**. Si aucune obligation spécifique n'impose une durée longue, STAMPEE fixe une durée de conservation restreinte, correspondant par exemple à la durée de la relation contractuelle plus une courte période.

À titre d'illustration non exhaustive :

- Les données de compte client (identité du client, informations de contact, contrats, historiques de commandes) sont conservées pendant la durée du contrat liant le client à STAMPEE, puis archivées pendant le délai légal de prescription (généralement 5 ans) à compter de la fin du contrat.
- Les données des expéditeurs et destinataires liées à une LRE (comme les coordonnées, les preuves de dépôt et de réception et les journaux d'envoi) sont conservées aussi longtemps que nécessaire pour attester de la bonne exécution du service. Les éléments probatoires sont conservés pendant la durée définie par la politique de conservation et le registre des traitements, en cohérence avec les obligations réglementaires, les normes applicables et les délais de prescription. Au-delà, ces données sont supprimées ou anonymisées.
- Le contenu même des lettres recommandées électroniques (documents envoyés) n'est conservé que le temps de garantir la disponibilité pour le destinataire et l'expéditeur selon les modalités du service. Si STAMPEE propose un service de coffre-fort ou de stockage au-delà de la livraison, ce sera sous des conditions spécifiques et avec l'accord du client, sinon les contenus sont supprimés une fois la distribution confirmée et la période de rétention contractuelle écoulée.
- Les données collectées pour la vérification d'identité (copie de pièce d'identité, enregistrements vidéo) via le prestataire PVID sont conservées uniquement pour le temps nécessaire à valider l'identité et pour se conformer aux exigences d'audit de ce processus, puis supprimées ou archivées de façon sécurisée selon ce qui est prévu contractuellement avec le PVID (typiquement, un délai relativement court, sauf si une loi exige plus).

- Les données de prospection commerciale (par exemple l'adresse électronique d'une personne inscrite à une lettre d'information) sont conservées jusqu'au retrait du consentement ou pendant la durée d'inactivité définie dans le registre des traitements à compter du dernier contact actif, puis supprimées ou placées sur une liste d'opposition lorsque cela est nécessaire pour respecter le choix de la personne.
- Les journaux techniques (logs de connexion, traces d'accès) contenant des données personnelles (adresse IP, identifiants…) sont conservés quelques mois à un an pour la sécurité (détection d'incidents) et la conformité légale (certaines lois peuvent exiger 1 an de conservation des logs de connexion).

Toutes ces durées de conservation sont formalisées dans le registre des traitements et/ou dans une politique interne d'archivage et de purge des données. À l'expiration de la durée définie, STAMPEE procède soit à la **suppression sécurisée** des données concernées, soit à leur **anonymisation irréversible** si les données peuvent être conservées à des fins statistiques ou de pilotage sans identifier les personnes.

R8. *STAMPEE limite la conservation des Données à caractère personnel à la durée nécessaire aux finalités poursuivies. Des durées de conservation sont définies pour chaque type de Données et, une fois ces durées expirées, les Données sont supprimées ou anonymisées de manière sécurisée, sauf obligation légale de conservation plus longue.*

3.6 Intégrité et confidentialité (sécurité des données personnelles)

La sécurité des Données à caractère personnel est une priorité pour STAMPEE, d'autant plus que l'activité de confiance (LRE) nécessite une fiabilité et une confidentialité sans faille. STAMPEE met en œuvre toutes les **mesures techniques et organisationnelles appropriées** afin de garantir l'intégrité et la confidentialité des données, et de protéger celles-ci contre les risques de divulgation non autorisée, d'accès illégal, d'altération, de perte ou de destruction accidentelle. Cet engagement de sécurité s'inscrit à la fois dans le respect de l'article 32 du RGPD et dans le respect des exigences du règlement eIDAS et des normes ETSI en matière de sécurité des services de confiance.

Parmi les mesures déployées par STAMPEE, on peut citer notamment :

- **Contrôle d'accès et confidentialité** : Les accès aux données personnelles sont strictement limités aux employés et sous-traitants qui en ont besoin pour leurs fonctions. Chaque utilisateur du SI dispose d'identifiants individuels et les accès sont protégés par des mots de passe robustes et, lorsque possible, une authentification multi-facteur. Les membres du personnel de STAMPEE sont soumis à une obligation de confidentialité contractuelle. Des profils d'habilitation assurent que chacun ne peut consulter que les données pertinentes pour son rôle.
- **Chiffrement** : STAMPEE utilise des mécanismes de chiffrement pour protéger les données, tant **en transit** (communications chiffrées via TLS/HTTPS pour l'envoi et la récupération des LRE, chiffrement des échanges avec le prestataire

PVID, etc.) qu'**au repos** (données stockées chiffrées sur les serveurs ou bases de données, notamment pour les contenus de lettres ou pièces justificatives, afin qu'elles ne soient pas lisibles en cas d'accès non autorisé aux stockages). Les clés de chiffrement sont gérées de manière sécurisée.

- **Pseudonymisation** (le cas échéant) : Pour certaines analyses internes ou journaux, STAMPEE peut recourir à la pseudonymisation, c'est-à-dire traiter les données personnelles de sorte qu'on ne puisse plus les attribuer à une personne sans information additionnelle (conservée séparément). Ceci limite l'exposition en cas de fuite de ces données pseudonymisées.
- **Sécurité des infrastructures** : Les serveurs et systèmes de STAMPEE, hébergés en France ou dans l'UE, bénéficient de protections physiques et logiques élevées (locaux sécurisés, alimentation électrique redondante, sauvegardes régulières, pare-feux, détection/prévention d'intrusion, anti-virus mis à jour, etc.). Une attention particulière est portée à la **résilience** du service de LRE : plans de reprise d'activité et de continuité sont en place pour faire face à un incident majeur et éviter toute perte de données.
- **Tests et audits** : STAMPEE procède à des tests réguliers, analyses et évaluations de l'efficacité de ses mesures de sécurité (tests d'intrusion, audits de configuration, revues de code orientées sécurité pour ses applications internes…). Des audits externes de sécurité sont également réalisés dans le cadre de la qualification eIDAS (audit de conformité par un organisme certificateur, incluant les aspects de sécurité).
- **Journalisation et traçabilité** : Toutes les actions significatives sur les données (consultation, modification, envoi d'une LRE, accès par un prestataire, etc.) sont journalisées. Ces journaux permettent de détecter des accès non autorisés ou des anomalies et de reconstituer, en cas d'incident, la séquence des événements.
- **Procédure de gestion des incidents** : STAMPEE a formalisé un processus pour gérer tout incident de sécurité ou **Violation de données** (voir section 7), afin de réagir vite et limiter les impacts.
- **Sécurité du développement** : Les projets informatiques de STAMPEE intègrent la sécurité dès la conception. Des revues de code et une validation de la conformité aux exigences de sécurité sont effectuées avant chaque mise en production.
- **Cohérence avec la PSSI** : Toutes ces mesures s'inscrivent dans le cadre de la Politique de Sécurité des Systèmes d'Information (PSSI) interne de STAMPEE, qui détaille les règles de sécurité technique et organisationnelle. La présente Politique de protection des données et la PSSI sont cohérentes et se complètent pour assurer une protection globale des données personnelles.

De plus, STAMPEE veille à la **sensibilisation du personnel** (voir section 10.1) afin que chaque collaborateur connaisse les bons comportements en matière de sécurité (gestion des mots de passe, détection des tentatives de phishing, respect des procédures, etc.). La sécurité est l'affaire de tous au sein de STAMPEE.

R9. *STAMPEE met en œuvre des mesures de sécurité techniques et organisationnelles appropriées pour protéger les Données personnelles contre tout accès ou traitement non autorisé, toute perte, destruction ou altération. Ces mesures incluent notamment le contrôle strict des accès, le chiffrement des données, la*

journalisation des opérations et des audits réguliers de sécurité, en cohérence avec la PSSI interne.

3.7 Transferts de données hors de l'Union européenne

STAMPEE privilégie, dans la mesure du possible, le traitement et le stockage des Données personnelles **sur le territoire de l'Union européenne**, afin de bénéficier pleinement du cadre protecteur du RGPD. L'infrastructure principale de STAMPEE et ses serveurs sont situés en France (ou dans l'UE), et la majorité des sous-traitants de STAMPEE opèrent depuis l'UE. Toutefois, dans certaines situations, des **transferts de données en dehors de l'UE** peuvent avoir lieu, par exemple : l'envoi de messages SMS ou emails de notification de LRE vers des destinataires situés hors UE, l'utilisation ponctuelle de prestataires techniques ou de services cloud dont les serveurs peuvent se trouver hors de l'Espace Économique Européen, ou encore le cas d'assistance technique effectuée depuis un pays tiers.

STAMPEE s'assure que de tels transferts sont effectués **dans le strict respect du cadre juridique applicable aux données personnelles transférées en dehors de l'UE** (chapitre V du RGPD). Concrètement, cela signifie que :

- Si les données sont transférées vers un pays bénéficiant d'une **décision d'adéquation** de la Commission européenne, le transfert est réalisé sur cette base, le pays destinataire étant reconnu comme assurant un niveau de protection adéquat. Par exemple, depuis 2023, les transferts vers les entités certifiées dans le cadre du **Data Privacy Framework** entre l'UE et les États-Unis sont autorisés car ce cadre a été jugé adéquat par la Commission européenne. STAMPEE pourra donc transférer certaines données (non sensibles) à un prestataire situé aux États-Unis **certifié** sous le Data Privacy Framework, en toute conformité.
- Si le pays ne bénéficie pas d'une adéquation, STAMPEE met en place des **garanties appropriées** telles que les Clauses Contractuelles Types (CCT) adoptées par la Commission européenne, complétées au besoin par des mesures additionnelles (chiffrement renforcé, etc.). Ces clauses contractuelles sont signées avec le destinataire des données afin de contractuellement assurer un niveau de protection équivalent à celui de l'UE.
- Dans des cas particuliers, si aucune des garanties précédentes n'est applicable, STAMPEE n'opère un transfert que s'il entre dans l'une des **exceptions légales** prévues par le RGPD (par exemple, consentement explicite de la personne concernée pour le transfert, nécessité du transfert pour l'exécution d'un contrat avec la personne, etc.). Cependant, STAMPEE veille à éviter autant que possible d'utiliser ces exceptions, préférant les solutions structurelles (décision d'adéquation ou garanties adéquates).

En pratique, STAMPEE recense dans le registre des traitements tous les transferts internationaux effectués. Par exemple, si un service d'envoi de SMS basé hors UE est utilisé pour notifier un destinataire, STAMPEE s'assure que ce prestataire a adhéré au Data Privacy Framework ou, à défaut, qu'un contrat intégrant les CCT est en place. De même, si STAMPEE devait utiliser un outil de support client dont l'éditeur est américain, elle vérifierait la certification de cet éditeur au DPF ou mettrait en place les garanties nécessaires.

STAMPEE informe les personnes concernées, via les mentions d'information, de l'existence de ces transferts éventuels et des mécanismes utilisés pour encadrer ceux-ci. Par ailleurs, STAMPEE suit de près l'actualité réglementaire relative aux transferts internationaux (par exemple, évolutions des décisions d'adéquation, jurisprudences type Schrems II sur les transferts vers les USA, etc.) pour adapter ses pratiques en conséquence et garantir en continu un niveau de protection adéquat.

R10. *STAMPEE n'effectue des transferts de Données personnelles hors de l'UE/EEE que dans des conditions assurant un niveau de protection conforme au RGPD : vers des pays reconnus adéquats, ou en mettant en place des garanties appropriées telles que les Clauses Contractuelles Types (et désormais, lorsque applicable, dans le cadre du Data Privacy Framework UE-États-Unis), ou, à titre exceptionnel, sur la base d'une dérogation légale pour une situation particulière.*

3.8 Données personnelles sensibles

Le RGPD accorde une protection particulière aux **catégories particulières de données personnelles** dites "données sensibles" (article 9 : données révélant l'origine raciale ou ethnique, opinions politiques, convictions religieuses ou philosophiques, appartenance syndicale, données génétiques, données biométriques aux fins d'identifier une personne de manière unique, données de santé, données concernant la vie sexuelle ou l'orientation sexuelle) ainsi qu'aux données relatives aux infractions pénales et condamnations (article 10). En principe, de telles données ne peuvent être traitées que dans des cas exceptionnels et sous réserve de garanties renforcées (ex. consentement explicite, nécessité vitale, obligation légale spécifique, etc.).

Dans le cadre de ses activités, **STAMPEE n'a pas vocation à collecter ni traiter de données sensibles** au sens de l'article 9 du RGPD. Les services de LRE fournis par STAMPEE impliquent essentiellement des données d'identification (noms, coordonnées, justificatifs d'identité) et des données de communication (contenu de lettres électroniques, preuves d'envoi/réception), qui en elles-mêmes ne relèvent pas des catégories sensibles. STAMPEE n'exige à aucun moment des informations telles que l'appartenance religieuse, l'état de santé ou les opinions politiques de ses utilisateurs ou des destinataires. De même, STAMPEE n'effectue aucun traitement de données liées à d'éventuelles infractions ou condamnations pénales des personnes concernées.

Il est toutefois possible que, dans certains cas, le **contenu** d'une lettre recommandée électronique (fourni par un client expéditeur) contienne des informations sensibles sur un destinataire (par exemple, une lettre d'un médecin à son patient pourrait contenir des données de santé). Dans une telle situation, STAMPEE agit strictement en tant qu'intermédiaire technique (sous-traitant) transmettant un contenu dont elle n'est pas responsable de la détermination. STAMPEE n'a pas de contrôle éditorial sur les contenus confiés par ses clients expéditeurs ; elle traite ces contenus de manière chiffrée et sécurisée, sans les analyser. Néanmoins, consciente de cette possibilité, STAMPEE applique à ces données la même rigueur de protection (confidentialité, accès restreint, sécurité renforcée) pour empêcher toute divulgation non autorisée. Par ailleurs, STAMPEE invite ses clients, via ses conditions générales, à éviter dans la mesure du possible d'utiliser la LRE pour transmettre des données particulièrement

sensibles, sauf nécessité, et à le faire dans le respect du cadre légal (par exemple, en s'assurant qu'ils ont une base légale pour traiter ces données).

Si, en dépit de sa politique de ne pas traiter de données sensibles, STAMPEE devait exceptionnellement se trouver à traiter de telles données (par exemple, si une copie de pièce d'identité utilisée dans le processus PVID contient des données biométriques comme la photo et que celle-ci est utilisée à des fins d'identification biométrique), STAMPEE s'engage à n'effectuer ce traitement qu'en présence d'une **exception légale valide** (telle que le consentement explicite de la personne pour cette vérification biométrique, ou une obligation légale l'exigeant) et à mettre en place les **garanties spécifiques** appropriées (cryptage renforcé, accès très restreint, suppression dès que possible).

Dans tous les cas, STAMPEE proscrit toute utilisation de données sensibles à des fins de profilage ou de discrimination.

R11. *STAMPEE s'abstient de collecter ou traiter des Données personnelles sensibles (au sens du RGPD) ou des données pénales, sauf nécessité exceptionnelle et légitime encadrée par la loi. En pratique, aucun traitement courant de STAMPEE ne porte sur de telles données.*

3.9 Traceurs strictement nécessaires dans les courriels de notification LRE

Les courriels adressés dans le cadre des services LRE qualifiés et non qualifiés sont des messages transactionnels et fonctionnels : avis de mise à disposition, rappels, relances, alertes de sécurité et messages permettant l'accès au parcours LRE. Ils ne constituent pas des communications publicitaires et ne sont pas utilisés pour promouvoir des produits ou analyser les centres d'intérêt des destinataires.

- **Rôle des acteurs :** STAMPEE détermine la mise en oeuvre du dispositif limité de délivrabilité et agit comme Responsable de Traitement pour cette opération. Le prestataire d'envoi de courriels, actuellement SendEthic, agit comme Sous-Traitant sur instruction documentée de STAMPEE et ne peut réutiliser les données pour ses propres finalités.
- **Finalités :** Le pixel de suivi est utilisé exclusivement pour vérifier la délivrabilité des notifications, connaître la date de dernière ouverture, détecter une difficulté de transmission, adapter ou arrêter les relances et sélectionner, lorsque nécessaire, un autre canal de contact. Les liens individualisés ont pour seule finalité de sécuriser l'accès au parcours LRE réservé au destinataire.
- **Régime de l'article 82 de la loi Informatique et Libertés :** Ces opérations sont mises en oeuvre sans consentement lorsqu'elles ont pour finalité exclusive de permettre ou faciliter la communication électronique et qu'elles sont strictement nécessaires à la fourniture du service LRE. STAMPEE interdit toute extension de finalité qui ferait perdre cette exemption, notamment l'optimisation de campagnes, la personnalisation commerciale, le profilage ou l'analyse comportementale.
- **Bases légales des traitements subséquents :** Les données personnelles issues du dispositif reposent sur l'exécution du contrat pour les clients et utilisateurs contractuellement liés à STAMPEE, sur les intérêts légitimes de

délivrabilité, de sécurité et de continuité du service pour les destinataires qui ne sont pas parties au contrat, et sur le respect des obligations légales lorsque le traitement est nécessaire à l'accomplissement des obligations de STAMPEE en qualité de Prestataire de Services de Confiance.

- **Données limitées :** Le dispositif traite uniquement l'adresse électronique, un identifiant technique du message, le statut technique de transmission et la date de dernière ouverture au niveau de la journée. Toute nouvelle date remplace la précédente. Le dispositif est configuré pour ne pas enregistrer ni conserver l'adresse IP, l'heure précise d'ouverture, le type de terminal, le logiciel de messagerie, la géolocalisation ou un historique détaillé des ouvertures.
- **Absence de profilage :** Les données ne sont pas utilisées pour produire des taux de campagne individuels, évaluer le comportement d'un destinataire, personnaliser des contenus, le cibler sur d'autres canaux, détecter ses préférences ou prendre une décision automatisée à son égard.
- **Conservation :** La dernière date d'ouverture est conservée uniquement pendant le cycle de notification et de relance de la LRE concernée. Elle est ensuite supprimée ou anonymisée et n'est pas intégrée dans l'archive probatoire à long terme comme preuve de réception. Les preuves LRE reposent sur les événements distincts enregistrés sur la plateforme, notamment le dépôt, la mise à disposition, l'acceptation, le refus, la récupération ou la non-réclamation.
- **Transparence et droits :** L'existence de ce dispositif est décrite dans la politique de confidentialité du service LRE. Les droits applicables peuvent être exercés selon les modalités prévues à la section 6, notamment auprès du DPO à l'adresse dpo@stampee.fr. Aucun centre de préférences spécifique n'est requis pour ce dispositif strictement nécessaire ; les demandes individuelles demeurent traitées dans le cadre de la procédure générale d'exercice des droits.

R11 bis. *STAMPEE limite les traceurs intégrés aux courriels LRE aux seules opérations strictement nécessaires à la délivrabilité, à la sécurité et au fonctionnement du service. Ces dispositifs ne sont utilisés ni pour la publicité, ni pour le profilage, ni pour l'analyse comportementale, et les données collectées sont minimisées et conservées pendant le seul cycle de notification.*

4. Documentation et gestion des risques

STAMPEE s'inscrit dans une démarche d'**accountability** (responsabilité démontrable) qui implique de documenter sa conformité et de gérer proactivement les risques relatifs aux traitements de données. Cela se traduit par la tenue de documentations obligatoires (registre des traitements) et la mise en œuvre de processus internes comme la protection des données dès la conception et l'évaluation d'impact sur la vie privée.

4.1 Protection des données dès la conception et par défaut (Privacy by Design/Default)

STAMPEE intègre la protection des données **dès la phase de conception** de tout nouveau projet, produit ou service impliquant des données personnelles, et s'engage

à appliquer la protection des données **par défaut** dans ses systèmes. Ce principe de "Privacy by Design & by Default" garantit que les exigences de protection des données ne sont pas considérées a posteriori, mais bien en amont et de manière continue.

Concrètement, lorsqu'un nouveau projet est initié (par exemple, le déploiement d'une nouvelle fonctionnalité de la plateforme LRE, l'adjonction d'un nouveau service non qualifié, ou l'intégration d'un nouveau prestataire technique), les étapes suivantes sont systématiquement suivies par les chefs de projet, en collaboration avec le DPO et la DSI :

1. **Analyse des principes de base** : Vérifier dès la conception que les principes énoncés en section 3 (licéité, minimisation, finalité, etc.) seront respectés par le projet. Par exemple, s'assurer que seules les données vraiment nécessaires seront collectées dans le cadre de la nouvelle fonctionnalité, ou qu'une information adéquate sera fournie aux utilisateurs.
2. **Mesures de protection envisagées** : Lister les mesures techniques et organisationnelles de sécurité et de confidentialité qui seront mises en œuvre dans le projet pour protéger les données (choix des méthodes de chiffrement, modalités de gestion des consentements si applicables, pseudonymisation éventuelle, restrictions d'accès spécifiques, etc.).
3. **Évaluation préliminaire du risque** : Réaliser une évaluation initiale pour déterminer si le traitement envisagé est susceptible d'engendrer un risque élevé pour les droits et libertés des personnes concernées. Cette évaluation préliminaire permet de décider s'il est nécessaire de conduire une Analyse d'Impact sur la Protection des Données (AIPD) formelle (voir section 4.2). STAMPEE se base pour cela sur les critères définis par le RGPD, les listes de la CNIL (liste des traitements soumis à AIPD obligatoire, et liste des exemptions), ainsi que les lignes directrices du CEPD.
4. **Réalisation de l'AIPD si requise** : Si l'évaluation préliminaire conclut à la probabilité d'un risque élevé (par exemple, le projet implique l'utilisation de nouvelles technologies intrusives, ou porte sur des données personnelles en volume important, etc.), une AIPD complète est menée avant la mise en œuvre du traitement.
5. **Implémentation des mesures de sécurité et de conformité** : Mettre en œuvre effectivement les mesures techniques et organisationnelles adaptées en fonction du niveau de risque identifié. Cela peut inclure le durcissement de certaines sécurités, l'ajout de fonctionnalités de privacy (par ex., option pour l'utilisateur de masquer certaines de ses données, logs spécifiques…), et la formalisation de procédures opérationnelles (par ex., procédure interne pour gérer les demandes de suppression liées à la nouvelle fonctionnalité).
6. **Validation** : Avant le déploiement effectif, valider (avec le DPO et éventuellement via des tests) que le projet respecte bien les exigences de protection des données convenues. Tout défaut identifié doit être corrigé.

En suivant ce processus, STAMPEE s'assure que la **protection des données est intégrée dans le cycle de vie complet** du traitement, de la conception initiale jusqu'à l'exploitation et même la clôture (suppression des données) du traitement. De plus, par défaut, les paramètres des services de STAMPEE sont configurés pour **maximiser la vie privée** : par exemple, les options facultatives de partage de données ou de

publication sont désactivées par défaut, c'est à l'utilisateur de les activer s'il le souhaite (opt-in plutôt qu'opt-out).

Si le projet implique des **tiers (sous-traitants)**, ces considérations de protection des données dès la conception s'étendent au choix du tiers et au contrat (STAMPEE s'assure que le tiers respecte aussi ces principes, cf. section 5).

R12. *Tout nouveau projet ou évolution de service chez STAMPEE intègre le principe de protection des Données dès la conception et par défaut. Une analyse de la conformité et des risques est réalisée en amont, et les solutions retenues intègrent systématiquement des garanties de confidentialité et de minimisation des Données.*

4.2 Analyse d'impact relative à la protection des données (AIPD)

Lorsqu'un traitement existant ou projeté est susceptible d'engendrer un **risque élevé pour les droits et libertés des personnes concernées**, STAMPEE procède à une **Analyse d'Impact relative à la Protection des Données (AIPD)** préalablement à la mise en œuvre du traitement, conformément à l'article 35 du RGPD. L'AIPD est un outil essentiel pour identifier précisément les risques et définir les mesures pour les atténuer.

STAMPEE a défini une procédure interne d'évaluation des risques des traitements, qui prévoit :

- Une **étape de screening** pour tout nouveau traitement (ou modification substantielle de traitement) : à travers un questionnaire ou une grille d'aide à la décision, le chef de projet et le DPO déterminent si le traitement présente des caractéristiques listées par la CNIL ou le CEPD comme justifiant une AIPD (ex : évaluation systématique/profilage, surveillance à grande échelle d'une zone accessible au public, données sensibles à grande échelle, interconnexion de bases de données, etc.).
- Si aucun critère de risque élevé n'est rempli et que le traitement ne figure pas sur la liste des traitements pour lesquels la CNIL a exigé une AIPD, alors une AIPD formelle peut être écartée (en documentant cette décision). Néanmoins, les mesures de base de protection doivent être quand même mises en place (voir 4.1).
- Si un ou plusieurs critères sont remplis, ou en cas de doute sérieux, une **AIPD** est menée.

Une AIPD chez STAMPEE comprend a minima :

- **Description détaillée du traitement** : finalités, base légale, nature des données, catégories de personnes concernées, destinataires, flux de données (y compris transferts internationaux), et contexte/opération envisagée.
- **Évaluation de la nécessité et proportionnalité** : justification de pourquoi ce traitement est nécessaire pour parvenir aux finalités et comment les principes de protection (minimisation, limitation de conservation, etc.) sont respectés dans sa conception.
- **Identification des risques** : pour chaque risque potentiel sur les droits des personnes (atteinte à la vie privée, risque de discrimination, vol d'identité,

atteinte réputationnelle, nuisance financière, etc.), évaluer le **niveau de gravité** et la **probabilité** d'occurrence, en tenant compte des menaces et vulnérabilités envisageables.
- **Mesures envisagées pour traiter les risques** : décrire les mesures de sécurité et d'organisation prises pour éliminer ou réduire les risques identifiés. Par exemple, chiffrement, anonymisation, limitation d'accès, procédure d'information renforcée, etc. Estimer dans quelle mesure ces mesures permettent de ramener le risque à un niveau acceptable.
- **Conclusion sur le risque résiduel** : après mesures, déterminer s'il reste un risque élevé. Si oui, déclencher la procédure de **consultation préalable** de la CNIL (conformément à l'article 36 RGPD, consulter l'autorité de contrôle si malgré tout le risque reste élevé en l'absence de mesures suffisantes).
- **Validation** : la DPO valide l'AIPD, et la Direction générale prend connaissance des risques identifiés et des mesures, et autorise (ou non) la poursuite du traitement avec les conditions proposées.

Tous les documents de l'AIPD sont conservés afin de prouver la démarche effectuée. STAMPEE peut présenter ces analyses en cas de contrôle de la CNIL pour démontrer son sérieux dans l'appréciation des risques.

Exemples de cas où une AIPD pourrait être requise pour STAMPEE : la mise en place d'un système de surveillance généralisée des accès aux LRE (ce qui n'est pas prévu), ou l'utilisation d'une technologie d'intelligence artificielle pour analyser le contenu des messages (hypothèse futuriste), etc. À ce jour, la plupart des traitements de STAMPEE (notification de tiers, gestion de comptes) ne relèvent pas d'un risque élevé systématique, mais STAMPEE reste vigilant notamment sur le traitement PVID (données d'identité + biométrie potentielle) qui a fait l'objet d'une AIPD conjointe avec le prestataire, et sur d'éventuelles évolutions.

R13. *STAMPEE conduit une Analyse d'Impact relative à la Protection des Données (AIPD) pour tout Traitement susceptible d'engendrer un risque élevé pour les droits et libertés des personnes. Cette AIPD est réalisée avant le lancement du traitement, et ses résultats (risques identifiés, mesures d'atténuation) sont validés par le DPO et pris en compte. En cas de risque résiduel élevé, STAMPEE consulte l'autorité de contrôle préalablement à la mise en œuvre.*

4.3 Registre des activités de traitement

STAMPEE tient à jour un **registre des activités de traitement** conformément à l'article 30 du RGPD. Ce registre est un outil central de documentation qui recense et décrit l'ensemble des traitements de données personnelles effectués sous la responsabilité de STAMPEE, que ce soit en qualité de Responsable de Traitement ou pour le compte de ses clients en qualité de Sous-Traitant.

Le registre des traitements de STAMPEE contient, pour chaque activité de traitement identifiée, les informations suivantes :

- **Nom du traitement** et finalité(s) : par exemple "Gestion du service de lettre recommandée électronique – finalité : acheminement des communications et preuve légale".

- **Qualité de STAMPEE** : Responsable (seul ou conjoint) ou Sous-Traitant pour ce traitement, avec indication le cas échéant du client Responsable de Traitement et de ses coordonnées.
- **Base légale** du traitement : exécution contractuelle, obligation légale, etc., selon le cas.
- **Catégories de personnes concernées** : ex. clients expéditeurs, destinataires, utilisateurs de la plateforme, employés STAMPEE, etc.
- **Catégories de données personnelles traitées** : ex. données d'identification (nom, adresse, email, tél…), données de contenu (fichiers des lettres), données techniques (logs IP…).
- **Catégories de destinataires des données** : ex. personnel interne habilité, sous-traitant PVID pour la vérification d'identité, prestataire d'envoi SMS, etc., avec mention des transferts internationaux si applicables.
- **Durées de conservation** : durée de conservation active et durée d'archivage le cas échéant, ou critères pour la déterminer.
- **Mesures de sécurité** principales : par exemple "données chiffrées en stockage, accès restreints, etc." (le RGPD exige d'indiquer les mesures de sécurité d'une manière générale).
- Pour les activités de traitement où STAMPEE est Responsable : mentions complémentaires telles que les finalités, l'intérêt légitime si c'est la base, etc. Pour les activités en sous-traitance : référence au contrat avec le client.

Le DPO de STAMPEE est chargé de la tenue de ce registre, en lien avec chaque service opérationnel. Le registre est mis à jour à chaque fois qu'un nouveau traitement est créé, modifié de manière substantielle ou supprimé. Au moins un examen annuel est réalisé (lors du rapport du DPO, section 2.3) pour vérifier que le registre reflète bien la réalité des opérations.

Outre son caractère obligatoire, ce registre permet à STAMPEE de disposer d'une **vue d'ensemble** de ses traitements et d'assurer la cohérence des mesures de conformité (par exemple, vérifier que chaque traitement a bien une durée de conservation définie et respectée, ou qu'aucun transfert international n'est effectué sans encadrement). En cas de demande de la CNIL, STAMPEE est en mesure de présenter ce registre rapidement, montrant ainsi sa conformité.

R14. *STAMPEE tient et met à jour un registre documenté de l'ensemble de ses activités de Traitement de Données personnelles, conformément à l'article 30 du RGPD. Ce registre, piloté par le DPO, recense notamment les finalités, bases légales, catégories de Données et de personnes concernées, destinataires, durées de conservation et mesures de sécurité pour chaque Traitement.*

5. Gestion des acteurs tiers (clients, partenaires et sous-traitants)

Les traitements de données personnelles effectués par STAMPEE impliquent souvent plusieurs acteurs : STAMPEE elle-même, ses **clients** (expéditeurs utilisant la plateforme), des **destinataires** finaux, mais aussi des **partenaires ou sous-traitants** qui interviennent pour fournir le service (ex. prestataire PVID, hébergeur, opérateur

SMS, etc.). Il est essentiel de bien encadrer ces relations afin de garantir une protection cohérente des données sur l'ensemble de la chaîne de traitement.

5.1 Identification des rôles et responsabilités de chaque partie

Dès qu'un tiers intervient dans un traitement de données aux côtés de STAMPEE, STAMPEE veille à **déterminer précisément le rôle** de chaque intervenant au regard du RGPD :

- Si le tiers détermine les finalités et moyens conjointement avec STAMPEE, il s'agit d'un **co-Responsable de Traitement**. Exemple : le prestataire PVID qui réalise la vérification d'identité partage cet objectif avec STAMPEE, ils sont donc co-responsables (cf. section 2.2).
- Si le tiers traite des données pour le compte et sur instruction de STAMPEE ou de son client, sans en déterminer lui-même la finalité, il agit comme Sous-Traitant. Tel est notamment le cas du prestataire d'envoi des courriels de notification LRE et du dispositif de délivrabilité strictement nécessaire associé. Ce prestataire ne peut utiliser les données à des fins propres, publicitaires, statistiques ou de profilage.
- Si STAMPEE elle-même agit pour le compte d'un client, STAMPEE est sous-traitant du client (responsable) – ce cas est traité via les contrats de service avec le client.
- Parfois, un même tiers peut avoir une double qualité selon les données : par exemple, un partenaire commercial pourrait être Responsable pour les données qu'il collecte lui-même et transmet à STAMPEE, mais une fois que STAMPEE traite ces données pour fournir le service commun, le partenaire pourrait être co-responsable. Ces situations sont clarifiées au cas par cas.

Cette identification est importante car les **obligations légales** en découlent (art. 24 pour responsables, art. 28 pour sous-traitants, art. 26 pour co-responsables). STAMPEE documente ces rôles, notamment dans le registre et dans les contrats.

R15. *Pour chaque collaboration avec un tiers impliquant des Données personnelles, STAMPEE identifie et documente le rôle de chacune des parties (Responsable de Traitement, co-Responsable ou Sous-Traitant) et veille au respect des obligations légales correspondantes.*

5.2 Contrats et accords avec les clients, partenaires et sous-traitants

Conformément aux exigences légales (notamment l'article 28 du RGPD) et pour assurer une protection efficace, STAMPEE encadre par écrit toute relation de traitement avec un tiers :

- Avec ses **clients (Responsables de Traitement)** pour lesquels elle agit en Sous-Traitant : STAMPEE conclut un contrat ou un avenant de **sous-traitance**. Ce contrat stipule notamment que STAMPEE n'agit que sur instructions du

client, décrit la nature et la finalité des traitements confiés, la durée, les types de données et les catégories de personnes concernées, et intègre toutes les clauses requises par le RGPD (devoir de confidentialité, mesures de sécurité, assistance du client pour les droits des personnes et les obligations de sécurité, sort des données en fin de contrat, possibilité d'auditer STAMPEE, etc.). Dans la pratique, ces clauses figurent soit dans les **conditions générales de service** de STAMPEE signées par le client, soit dans un **Data Processing Agreement (DPA)** séparé signé entre STAMPEE et le client.

- Avec ses propres Sous-Traitants (sous-traitance ultérieure) : STAMPEE s'assure de ne faire appel qu'à des sous-traitants présentant des garanties suffisantes. Un contrat de sous-traitance est signé avec chacun, imposant au sous-traitant des obligations équivalentes à celles que STAMPEE a envers ses clients ou envers les personnes concernées. Le contrat détaille le périmètre du traitement confié (finalité, données traitées, durée, etc.) et inclut a minima : obligation de n'agir que sur instruction de STAMPEE, mise en place de mesures de sécurité conformes, obligation de confidentialité des personnels, interdiction de sous-sous-traiter sans autorisation, aide en cas d'exercice de droits ou d'incident, notification des violations de données au plus vite à STAMPEE, sort des données en fin de prestation, etc. Pour les prestataires d'envoi de courriels, le contrat impose en outre la limitation du suivi aux seules finalités de délivrabilité et de sécurité, l'interdiction de toute réutilisation, l'absence d'enregistrement de l'adresse IP, de l'heure précise et des données de terminal, ainsi que la suppression de la date de dernière ouverture à la fin du cycle de notification.
- Avec ses **partenaires co-responsables** : STAMPEE formalise un **accord de co-responsabilité** (par exemple un accord de partenariat) avec le partenaire. Cet accord précise la répartition des responsabilités vis-à-vis des obligations du RGPD pour le traitement commun : qui informe les personnes concernées (et comment), qui gère les demandes d'exercice de droits, qui notifie d'éventuelles violations à la CNIL et/ou aux personnes, quels segments de données chacun conserve et traite, etc. L'accord vise à ce que rien ne soit laissé sans responsable et que les personnes concernées puissent exercer efficacement leurs droits. En général, STAMPEE et le partenaire désignent chacun un point de contact. Dans le cas du prestataire PVID, l'accord précise par exemple que le PVID collecte l'information auprès de la personne et fournit la preuve d'identité à STAMPEE, que STAMPEE et PVID conservent chacun les données nécessaires (le PVID conserve peut-être la vidéo d'identification un certain temps, STAMPEE conserve la confirmation d'identité), et que pour une demande d'accès ou de suppression relative aux données d'identité, la personne peut s'adresser à STAMPEE qui coordonnera avec le PVID pour répondre.
- Avec tout autre tiers destinataire de données (par ex, une autorité publique recevant des données sur réquisition) : STAMPEE vérifie le fondement légal de la communication et journalise celle-ci, afin de pouvoir justifier qu'elle n'est pas abusive.

R16. *Un contrat écrit est conclu avec chaque tiers (client, partenaire ou sous-traitant) impliqué dans le traitement de Données à caractère personnel. Ce contrat ou accord définit clairement les rôles et responsabilités de chacune des parties et comprend les*

clauses de protection des données exigées par la Législation applicable (notamment le RGPD).

5.3 Surveillance et exigences vis-à-vis des sous-traitants

STAMPEE ne se contente pas de contractualiser : elle **surveille activement** la conformité de ses sous-traitants tout au long de la relation. Avant de choisir un prestataire, STAMPEE évalue ses garanties (par ex. existence d'une certification type ISO 27001, localisation des données, mesures de sécurité proposées, politique de confidentialité). Une fois le contrat en place, STAMPEE maintient une communication régulière et peut effectuer des **audits ou contrôles** périodiques chez ses sous-traitants critiques afin de vérifier le respect de leurs obligations.

Le niveau et la fréquence des contrôles sont adaptés en fonction de la sensibilité des données confiées et des risques : par exemple, un hébergeur de données de santé (même si STAMPEE n'en traite pas, c'est pour l'idée) ferait l'objet d'audits plus fréquents ; un sous-traitant fournissant un service non critique pourrait être audité via questionnaire annuel et preuve de certifications. STAMPEE inclut généralement dans ses contrats le droit de réaliser ou faire réaliser des audits de conformité chez le sous-traitant, ou d'exiger des rapports de conformité (ex : rapport d'audit externe, résultats de tests de sécurité, etc.).

En cas de manquement constaté chez un sous-traitant (par exemple, un incident non notifié, ou le non-respect de mesures de sécurité), STAMPEE prend les mesures qui s'imposent : demande de plan correctif, suspension du traitement, voire rupture du contrat si nécessaire pour protéger les données.

R17. *STAMPEE s'assure du respect continu, par ses Sous-Traitants et partenaires, des obligations en matière de protection des données. À cette fin, STAMPEE procède à des évaluations et contrôles réguliers de ses Sous-Traitants (questionnaires de conformité, audits périodiques, examen de certifications) et exige la mise en place d'actions correctives en cas de non-conformité.*

Notons également que STAMPEE impose contractuellement à ses clients (lorsqu'elle est Sous-Traitant) de respecter de leur côté la réglementation, notamment en matière d'information des personnes concernées et de respect des bases légales. Par exemple, le client doit garantir qu'il a le droit d'utiliser les adresses des destinataires qu'il transmet à STAMPEE (soit parce qu'il a leur consentement, soit sur une autre base valable) – ceci est généralement inclus dans les CGU ou contrats avec les clients, où ils assurent tenir eux-mêmes le RGPD. Ainsi, chaque acteur de la chaîne remplit son rôle de conformité, assurant une protection globale.

6. Relations avec les personnes concernées (exercice des droits)

STAMPEE reconnaît et respecte les droits des **Personnes concernées** tels que prévus par la Législation applicable, en particulier le RGPD et la loi française. STAMPEE s'engage à ce que toute personne dont les données sont traitées par ses soins (que ce soit un client, un expéditeur, un destinataire, un utilisateur de la

plateforme, etc.) puisse effectivement exercer les droits dont elle dispose sur ses données.

Les personnes concernées disposent, conformément aux articles 12 à 22 du RGPD, des droits suivants :

1. **Droit à l'information** – le droit d'être informé de manière claire, précise et complète sur l'utilisation de ses Données à caractère personnel (ce droit est exercé en amont via les mentions d'information et la présente Politique).
2. **Droit d'accès** – le droit d'obtenir la confirmation que des Données personnelles la concernant sont traitées, et le cas échéant d'en recevoir une copie ainsi que les informations associées (finalités, catégories de données, destinataires, etc.).
3. **Droit de rectification** – le droit de faire rectifier les Données personnelles inexactes ou incomplètes la concernant.
4. **Droit à l'effacement (droit à l'oubli)** – le droit de faire effacer ses Données dans certaines conditions (par exemple, si les données ne sont plus nécessaires, si la personne retire son consentement et qu'il n'y a pas d'autre base légale, si le traitement est illicite, etc.), sauf si STAMPEE a un motif légitime ou légal de les conserver (par ex. obligation légale, intérêt légitime impérieux, exercice ou défense de droits en justice).
5. **Droit d'opposition** – le droit de s'opposer, pour des raisons tenant à sa situation particulière, à un traitement fondé sur l'intérêt légitime de STAMPEE. En cas d'exercice de ce droit, STAMPEE cessera le traitement, à moins qu'il n'existe des motifs légitimes et impérieux qui prévalent ou que le traitement soit nécessaire pour la constatation, l'exercice ou la défense de droits en justice. Par ailleurs, ce droit d'opposition s'applique sans condition pour la prospection commerciale : une personne peut à tout moment s'opposer à l'utilisation de ses données à des fins de marketing direct (ex: ne plus recevoir de newsletters).
6. **Droit de retirer son consentement** – lorsque le traitement est fondé sur le consentement, le droit de retirer ce consentement à tout moment (voir 3.2.3). Le retrait n'affecte pas la licéité du traitement passé mais met fin à celui-ci pour l'avenir.
7. **Droit à la limitation du traitement** – le droit, dans certains cas, de demander la suspension temporaire d'un traitement, sans exiger l'effacement des données. Par exemple, en cas de contestation sur l'exactitude des données, la personne peut demander de geler l'utilisation des données le temps de la vérification.
8. **Droit à la portabilité des données** – le droit de recevoir les Données personnelles qu'elle a fournies à STAMPEE, dans un format structuré, couramment utilisé et lisible par machine, et de les transmettre à un autre responsable de traitement. Ce droit ne s'applique qu'aux données fournies directement par la personne, traitées de manière automatisée sur base du consentement ou d'un contrat. Dans le contexte de STAMPEE, cela pourrait concerner par exemple les données de compte d'un expéditeur, qu'il pourrait souhaiter récupérer pour les importer chez un autre prestataire.
9. **Droit de ne pas faire l'objet d'une décision automatisée** – le droit de ne pas être soumis à une décision juridique ou significative prise uniquement sur un traitement automatisé (sans intervention humaine) y compris le profilage. STAMPEE ne pratique pas de décision entièrement automatisée produisant des

effets juridiques sur les personnes (comme un refus automatique de service basé sur un profilage). Si cela devait changer, STAMPEE garantirait le droit à une intervention humaine, à exprimer son point de vue et à contester la décision.

10. **Droit de définir des directives post-mortem** – (spécifique au droit français, Art. 85 loi Informatique et Libertés) le droit de définir des consignes sur le sort des Données personnelles après le décès de la personne (conservation, effacement, communication), directives générales ou particulières que STAMPEE, le cas échéant, s'engage à respecter. À défaut de directives, les héritiers peuvent exercer certains droits (accès, suppression) dans le cadre défini par la loi.

Il est possible que des législations locales confèrent des droits additionnels aux personnes concernées (par exemple, le droit à la **déconnexion** en France pour les employés, etc.), mais dans le cadre des activités de STAMPEE ces 10 droits couvrent l'essentiel des situations.

Pour garantir l'exercice effectif de ces droits :

- STAMPEE a mis en place une **procédure interne de gestion des demandes** des personnes concernées. Cette procédure détaille les étapes de réception d'une demande (vérification de l'identité du demandeur pour éviter les usurpations, compréhension de la portée de la demande), de coordination en interne (identifier les données concernées, consulter éventuellement le client responsable si STAMPEE est sous-traitant), de réponse dans les délais impartis, et de traçabilité (enregistrer la demande et la réponse apportée).
- Les demandes peuvent être transmises par différents canaux : par email à l'adresse dédiée (par exemple **dpo@stampee.fr**), par courrier postal à l'attention du DPO, ou via un formulaire de contact sur le site web de STAMPEE. Ces informations de contact sont communiquées dans la politique de confidentialité et dans les mentions légales.
- STAMPEE s'engage à répondre **dans les meilleurs délais** et au plus tard dans le délai d'un mois à compter de la réception de la demande, conformément au RGPD. Ce délai peut être prolongé de deux mois en cas de demande complexe ou de nombre de demandes élevé, mais dans ce cas la personne sera informée du motif de la prolongation dans le délai initial.
- En règle générale, l'exercice des droits est **gratuit**. STAMPEE ne peut réclamer des frais que si les demandes sont manifestement infondées ou excessives (par exemple répétitives), et encore, elle privilégiera d'abord un refus motivé plutôt que de facturer.
- Si STAMPEE n'accède pas à une demande, une justification motivée sera fournie (par exemple, opposition refusée car il existe des motifs impérieux légitimes, ou effacement refusé car les données doivent être conservées pour respecter une obligation légale).
- Toutes les équipes concernées sont formées pour reconnaître une demande de droit et la transmettre sans délai au DPO pour traitement.

Cas particulier de STAMPEE en tant que Sous-Traitant : Lorsque STAMPEE traite des données pour le compte d'un client (Responsable de Traitement), le plus souvent c'est à ce client qu'il appartient de traiter les demandes des personnes concernées.

Par exemple, si un destinataire d'une LRE souhaite exercer son droit d'accès aux données liées à l'envoi, la demande devrait être adressée à l'expéditeur (le client de STAMPEE). Néanmoins, si une telle demande parvient directement à STAMPEE, celle-ci, en sa qualité de sous-traitant, la **transmettra sans délai** au client concerné et l'assistera pour y donner suite (par exemple en extrayant les données demandées de ses systèmes afin que le client puisse répondre). STAMPEE ne répondra directement à la personne **que sur instruction du client** ou dans le cas où cela aurait été convenu contractuellement. Cette règle est prévue dans les contrats de sous-traitance : le client s'engage à traiter les demandes des personnes, et STAMPEE à l'y aider.

Cas de la co-responsabilité (ex: PVID) : STAMPEE et le prestataire PVID conviennent dans leur accord qui gère les demandes relatives à la vérification d'identité. Souvent, la personne pourra s'adresser indifféremment à l'un ou l'autre. STAMPEE dans ce cas coordonnera avec le PVID pour fournir une réponse complète.

En tout état de cause, STAMPEE veille à ce qu'aucune demande ne reste lettre morte, même si elle ne vient pas de l'interlocuteur "préférentiel". La coopération entre STAMPEE et ses clients/partenaires garantit que les personnes ne soient pas ballottées.

Enfin, si une personne estime que ses droits ne sont pas respectés après avoir contacté STAMPEE, nous l'informons de son droit d'introduire une réclamation auprès de l'**Autorité de contrôle** (CNIL en France) – voir section 9.

R18. *STAMPEE met en œuvre une procédure et des moyens dédiés pour permettre aux Personnes concernées d'exercer aisément leurs droits (accès, rectification, effacement, opposition, etc.) et s'engage à donner suite à toute demande légitime dans les délais réglementaires. En qualité de Sous-Traitant, STAMPEE assiste ses clients afin qu'ils puissent eux-mêmes satisfaire aux demandes des personnes concernées.*

7. Gestion des incidents et des violations de données personnelles

Malgré toutes les mesures préventives en place, STAMPEE est consciente qu'un **incident** affectant des Données à caractère personnel (appelé *Violation de données personnelles* dans le RGPD) peut survenir. Une violation de données se définit comme un incident de sécurité entraînant, de manière accidentelle ou illicite, la destruction, la perte, l'altération, la divulgation non autorisée de Données personnelles transmises, stockées ou autrement traitées, ou l'accès non autorisé à de telles Données.

Exemples : une faille de sécurité permettant à un tiers d'accéder à des données de destinataires, l'envoi par erreur de données personnelles à un mauvais destinataire, la perte d'un support de sauvegarde contenant des données non chiffrées, une attaque informatique cryptant des données (ransomware) ou exfiltrant des informations, etc.

STAMPEE a mis en place une **procédure interne de gestion des incidents** afin de réagir rapidement et efficacement en cas de survenance d'une telle violation. Les grands axes de cette procédure sont :

- **Détection et alerte** : STAMPEE encourage ses collaborateurs et ses sous-traitants à signaler immédiatement tout événement suspect ou toute anomalie pouvant constituer une violation de données (par exemple : réception d'un email de phishing ayant compromis un compte, découverte qu'un fichier contenant des données a été accessible publiquement, etc.). Des mécanismes de surveillance technique (systèmes de détection d'intrusion, alertes sur activités anormales) sont également en place pour détecter les incidents.
- **Contenir l'incident** : Dès qu'un incident est confirmé, l'objectif premier est de le circonscrire pour en limiter l'ampleur. Cela peut impliquer de déconnecter un serveur du réseau, de révoquer des accès compromis, de corriger une faille logicielle, etc. La DSI et l'équipe de sécurité sont mobilisées immédiatement.
- **Évaluation initiale** : L'équipe d'intervention (impliquant la DSI, le DPO, et tout autre service concerné) évalue rapidement la nature de l'incident, les types de données touchées, le volume, les personnes potentiellement affectées, et les conséquences potentielles pour elles. Cette évaluation rapide permet de décider des suites à donner, notamment si une notification externe est nécessaire.
- **Notification de la violation aux autorités** : Conformément à l'article 33 du RGPD, si la violation de données est susceptible d'engendrer un risque pour les droits et libertés des personnes, STAMPEE (en tant que Responsable de Traitement) notifiera l'autorité de contrôle compétente (en France, la CNIL) **dans les 72 heures** après en avoir pris connaissance. La notification comprendra les informations requises (nature de la violation, catégories et nombre de personnes et de données concernées, mesures prises ou proposées pour y remédier, etc.). Si toutes les informations ne sont pas disponibles dans les 72h, une notification initiale est faite et des informations complémentaires suivent dès que possible.
    - Si STAMPEE agit en **Sous-Traitant** pour un client, elle **informe sans délai le client** responsable de toute violation de données concernant les données traitées pour son compte, afin que ce client puisse, si nécessaire, procéder aux notifications requises (article 33 RGPD oblige le responsable, pas le sous-traitant, à notifier la CNIL, mais le sous-traitant a l'obligation d'alerter le responsable). Cette communication au client se fait généralement **en urgence dès la découverte** de l'incident, et STAMPEE lui fournit tous les éléments nécessaires. Cet engagement est d'ailleurs stipulé contractuellement avec les clients.
- **Notification aux personnes concernées** : Conformément à l'article 34 du RGPD, si la violation est susceptible d'engendrer un **risque élevé** pour les droits et libertés des personnes (par exemple, divulgation de données sensibles pouvant entraîner un préjudice important), STAMPEE, en tant que Responsable, s'engage à **communiquer** aux personnes concernées, dans les meilleurs délais, des informations sur la violation, les données concernées, les conséquences possibles et les mesures prises pour y remédier, ainsi que des conseils sur les actions à entreprendre (par ex. changer ses mots de passe, être vigilant aux tentatives de fraude). Cette communication est faite de manière claire et en des termes simples. Toutefois, si des mesures techniques efficaces ont déjà été prises et neutralisent le risque (par exemple données chiffrées rendues illisibles), ou si informer individuellement demande des efforts disproportionnés (auquel cas une communication publique équivalente sera

faite), STAMPEE peut ne pas notifier individuellement, selon les conditions de l'article 34.
    - Là encore, si STAMPEE est Sous-Traitant, elle ne communique pas directement aux personnes concernées (ce rôle revient au client responsable), sauf instruction contraire. Elle assiste le client dans cette communication si besoin.
- **Documentation** : STAMPEE documente en interne toute violation de données, qu'elle nécessite ou non une notification. Un registre des incidents est tenu, avec la description des faits, les effets, les actions entreprises et les décisions de notification. Cela permet d'assurer un suivi et de tirer des leçons pour le futur.
- **Analyse a posteriori et correction** : Une fois l'urgence traitée, STAMPEE analyse la cause racine de l'incident et met en place les mesures correctives pour éviter qu'il ne se reproduise. Cela peut impliquer une amélioration des mesures de sécurité, une formation supplémentaire du personnel, le renforcement des contrôles, etc.

STAMPEE n'oublie pas de considérer, outre les obligations du RGPD, ses obligations en tant que Prestataire de Services de Confiance au sens d'eIDAS. Le règlement eIDAS impose en effet aux prestataires qualifiés de notifier sans délai l'autorité de surveillance nationale (en France, l'ANSSI) en cas d'incident de sécurité ayant un impact significatif sur le service de confiance fourni ou sur les données liées à ce service. STAMPEE s'engage donc, le cas échéant, à notifier **ANSSI** pour tout incident de sécurité majeur affectant l'intégrité ou la confidentialité des services de LRE, en plus des notifications CNIL sur la dimension données personnelles. De même, STAMPEE notifiera les entités de confiance concernées (par exemple les clients ou partenaires) si l'incident a des répercussions sur eux.

Par ailleurs, STAMPEE forme et **sensibilise ses employés** à la procédure à suivre en cas d'incident (qui contacter, comment réagir, quoi ne pas faire, etc.), afin qu'aucun temps précieux ne soit perdu en cas de crise. La réactivité est cruciale pour minimiser l'impact d'une violation.

R19. *STAMPEE a établi un protocole de gestion des incidents de sécurité et des violations de Données personnelles. Toute Violation avérée ou suspectée est signalée et traitée sans délai : confinement, évaluation, notification à la CNIL dans les 72h si nécessaire (ou information du client responsable lorsque STAMPEE est Sous-Traitant), communication aux personnes concernées en cas de risque élevé, et mesures correctives. Chaque incident est documenté et suivi d'actions préventives.*

R20. *En tant que Sous-Traitant, STAMPEE notifie immédiatement le Responsable de Traitement client de toute Violation de Données concernant ses données, et lui fournit toute l'assistance nécessaire pour lui permettre de remplir ses obligations de notification (vers l'autorité de contrôle et les personnes concernées).*

8. Coopération avec l'Autorité de contrôle

STAMPEE reconnaît l'importance de la mission des autorités de protection des données (telles que la CNIL en France) et s'engage à coopérer pleinement avec elles. Cette coopération se manifeste de plusieurs façons :

- **Point de contact dédié** : Le Délégué à la Protection des Données (DPO) de STAMPEE (coordonnées en section 2.1.3) sert de point de contact privilégié pour l'autorité de contrôle. Toute communication ou demande de la CNIL sera immédiatement prise en charge par le DPO, qui agira en lien avec les services internes pour y répondre.
- **Consultation préalable** : Si STAMPEE devait se trouver dans une situation où une AIPD révèle un risque résiduel élevé ne pouvant être suffisamment atténué, STAMPEE consulterait la CNIL avant de lancer le traitement (conformément à l'article 36 du RGPD et aux obligations eIDAS le cas échéant). STAMPEE présentera alors le dossier de traitement et suivra les recommandations ou instructions que la CNIL pourrait formuler avant de poursuivre.
- **Réponses aux demandes d'information** : En cas de demande formelle de la part de la CNIL (par exemple, communication du registre des traitements, détails sur les mesures de sécurité, preuves du respect de tel ou tel aspect du RGPD), STAMPEE s'engage à fournir les informations demandées de manière complète et précise, dans les meilleurs délais. STAMPEE conserve une documentation organisée (registre, politiques internes, preuves d'audits, etc.) facilitant ces éventuelles communications.
- **Audits et contrôles** : Si la CNIL décide de réaliser un contrôle (sur pièces ou sur place) de STAMPEE, l'entreprise coopérera activement. Le DPO préparera en amont les documents requis, et pendant un contrôle sur place, les équipes de STAMPEE faciliteront l'accès aux informations, locaux et systèmes requis, dans la limite de ce qui est autorisé. STAMPEE s'attachera à répondre honnêtement et précisément à toutes les questions des inspecteurs. Une procédure interne existe pour gérer ce type de contrôle, définissant les rôles (par ex. qui accueille les inspecteurs, qui fournit tel document, etc.) afin que l'audit se déroule efficacement.
- **Suivi des recommandations** : À la suite d'un contrôle ou d'une mise en demeure de la CNIL, si des points d'amélioration ou de non-conformité sont signalés, STAMPEE prendra les mesures nécessaires pour y remédier dans les délais impartis. Le DPO pilotera la mise en conformité et communiquera l'avancement à la CNIL selon les besoins.
- **Communication proactive** : En dehors même des obligations, STAMPEE peut, si une question de conformité se pose, prendre contact avec la CNIL pour demander conseil ou éclaircissement (via les points de contact que la CNIL offre aux professionnels). Cette approche proactive s'inscrit dans la volonté de bien faire et d'éviter tout manquement.
- **Transparence** : STAMPEE informe la CNIL en cas de changements notables pouvant les intéresser (par exemple, désignation ou changement de DPO, enregistrement d'une activité de traitement de données biométriques si un jour c'était le cas, etc.), conformément aux exigences réglementaires.

STAMPEE suit également les publications et retours d'expérience des autorités de contrôle (lignes directrices du CEPD, recommandations de la CNIL, décisions marquantes) afin d'anticiper les attentes des autorités et d'adapter ses pratiques en conséquence.

R21. *STAMPEE coopère pleinement avec l'Autorité de contrôle compétente (CNIL) : elle répond diligemment à toute demande d'information ou d'audit, consulte l'Autorité en cas de nécessité (par exemple avant un traitement à risque élevé), et met en place une procédure interne pour être prête en cas de contrôle. Le DPO agit en point de contact et pilote ces interactions.*

9. Contrôles internes, formation du personnel et amélioration continue

STAMPEE est engagée dans une démarche de **conformité durable** et d'amélioration continue de la protection des données. Au-delà des mesures et politiques mises en place, l'entreprise s'assure de leur bonne application effective par des contrôles internes réguliers, et investit dans la **formation et sensibilisation** de son personnel.

9.1 Sensibilisation et formation du personnel

Les collaborateurs de STAMPEE jouent un rôle clé dans la protection des données, car même avec les meilleures politiques, ce sont les actions humaines quotidiennes qui garantissent la conformité. STAMPEE met donc un accent particulier sur la **sensibilisation** de l'ensemble de son personnel aux enjeux de protection des données et de sécurité :

- **Formation initiale** : Tout nouvel employé de STAMPEE, lors de son intégration, reçoit une formation de base sur les principes du RGPD, les obligations de confidentialité et les bonnes pratiques à respecter dans l'entreprise. Ceci inclut une présentation de la présente Politique, des règles de sécurité (PSSI), et des cas concrets liés à son poste.
- **Engagement de confidentialité** : Chaque collaborateur signe une clause ou un engagement spécifique de confidentialité l'obligeant à respecter le secret des Données personnelles auxquelles il pourrait avoir accès dans le cadre de ses fonctions. Des sanctions internes (disciplinaires) sont prévues en cas de manquement grave (ex: consultation injustifiée de données, divulgation non autorisée…).
- **Formations continues** : Régulièrement (au moins une fois par an), STAMPEE organise des sessions de formation ou d'information pour mettre à jour les connaissances du personnel. Ces sessions peuvent être adaptées selon les publics : par exemple, une formation spécifique "Privacy by Design" pour les équipes de développement IT, une session "Gestion des demandes de droits" pour l'équipe support client, etc. Le DPO participe souvent à ces formations pour apporter son expertise.
- **Sensibilisation permanente** : Au-delà des formations formelles, STAMPEE diffuse périodiquement des *rappels* et *conseils* via email interne ou affiches sur les points clés (ex : comment reconnaître un email de phishing, l'importance de verrouiller sa session, comment gérer un appel demandant des informations personnelles, etc.). Lorsqu'un incident interne ou externe survient (ex: attaque connue), un retour d'expérience est partagé afin que tous en tirent des enseignements.
- **Culture positive** : STAMPEE encourage une culture où chacun se sent responsable de la protection des données. Les employés savent qu'ils peuvent

et doivent signaler rapidement un problème sans crainte de reproche (le but étant de résoudre, pas de blâmer). Des quizz ou ateliers ludiques peuvent être organisés pour maintenir l'intérêt sur ces sujets souvent perçus comme contraignants.

Grâce à ces efforts, les collaborateurs de STAMPEE comprennent l'importance de la protection des données, connaissent les réflexes à avoir (par exemple, vérifier l'adresse du destinataire avant d'envoyer des informations sensibles, ne pas transférer de données en dehors des canaux autorisés, utiliser les outils sécurisés de l'entreprise plutôt que des solutions non approuvées, etc.) et sont au courant des procédures (comme la gestion des incidents, ou à qui adresser une demande RGPD reçue).

R22. *STAMPEE s'assure que l'ensemble de son personnel est formé et sensibilisé aux règles de protection des Données et de sécurité. Des actions de formation initiales et continues sont déployées, et chaque collaborateur est tenu à une obligation de confidentialité et à l'application stricte des procédures internes relatives aux Données personnelles.*

9.2 Contrôles internes et audits de conformité

Pour vérifier que les principes et procédures décrits dans cette Politique sont bien appliqués, STAMPEE met en place des **contrôles internes réguliers**. Ces contrôles peuvent prendre plusieurs formes :

- **Revues documentaires** : Le DPO effectue périodiquement une revue du registre des traitements, des enregistrements de consentement, des logs de demandes de droits ou d'incidents, afin de s'assurer que tout est complet et à jour.
- **Audits internes** : STAMPEE mandate soit son DPO, soit éventuellement un auditeur interne ou externe, pour conduire des audits ciblés sur certains processus. Par exemple, un audit annuel de conformité RGPD couvrant : le respect des durées de conservation (vérifier que les données plus anciennes que la durée définie sont purgées), le respect du principe de minimisation (vérifier les formulaires de collecte actuels, s'assurer qu'on ne collecte pas de superflu), la conformité des contrats de sous-traitance (échantillon de contrats clients et fournisseurs pour vérifier la présence des clauses RGPD), etc. Des interviews de personnels peuvent être menées pour évaluer leur compréhension des procédures.
- **Tests ponctuels** : Par exemple, simulation d'une demande d'exercice de droit pour voir comment elle est traitée (test interne), ou exercice de simulation d'incident (jeux de rôle) pour tester le temps de réaction.
- **Suivi des plans d'action** : Les éventuelles non-conformités ou points faibles identifiés donnent lieu à des plans d'actions avec responsables et échéances. Le DPO suit l'avancement de ces plans et reporte à la Direction générale.
- **Indicateurs** : STAMPEE peut mettre en place des indicateurs internes (KPI) pour suivre la conformité : nombre de jours moyens pour répondre aux demandes de droits, nombre d'incidents par type, pourcentage de personnels formés, etc. Ces indicateurs, présentés dans le rapport annuel par exemple, permettent de piloter et d'améliorer les processus.

En complément, STAMPEE peut aussi faire réaliser des **audits externes** de conformité si nécessaire (par exemple dans le cadre de la certification de service eIDAS, certains volets RGPD pourraient être audités, ou via des consultants spécialisés pour un regard neuf).

R23. *STAMPEE procède à des contrôles internes et audits réguliers afin de vérifier le respect effectif de la présente Politique et des procédures associées. En cas de non-conformité ou de faiblesse identifiée, des actions correctives sont mises en œuvre sans délai et suivies jusqu'à leur achèvement.*

9.3 Amélioration continue et révision de la Politique

La protection des données n'est pas figée : les risques évoluent, les technologies changent, la réglementation peut être mise à jour (par exemple le règlement eIDAS 2 en discussion, ou de nouvelles lois nationales), et l'organisation de STAMPEE elle-même peut changer. C'est pourquoi STAMPEE inscrit sa démarche dans une logique d'**amélioration continue** :

- Les retours d'expérience (issues d'incidents, d'audits, ou même de suggestions des collaborateurs) sont utilisés pour améliorer les procédures. Par exemple, si un exercice d'incident montre une faiblesse dans la communication interne, la procédure sera ajustée.
- Le DPO assure une **veille juridique et technologique** pour anticiper les évolutions pertinentes. Si de nouvelles obligations apparaissent, STAMPEE adaptera sa Politique et ses pratiques en conséquence. De même, si de nouvelles solutions plus protectrices se présentent (chiffrement homomorphique, nouveaux outils de gestion de consentement, etc.), STAMPEE les évaluera.
- La présente Politique elle-même sera revue (voir section 1.3) régulièrement. STAMPEE s'assure qu'elle reste alignée avec la réalité des traitements et les règles en vigueur. En cas de changement majeur dans les activités de STAMPEE (nouveau service, changement de modèle d'affaires, etc.), une révision de la Politique sera effectuée plutôt que d'attendre l'échéance annuelle.
- STAMPEE maintient un dialogue ouvert avec ses clients et partenaires sur les questions de données personnelles. Leurs préoccupations ou questions peuvent révéler des axes d'amélioration pour STAMPEE. Par exemple, un client international pourrait demander comment STAMPEE se conforme à tel aspect, ce qui pourrait amener STAMPEE à être encore plus transparente ou à affiner une procédure.

En adoptant cette attitude proactive et évolutive, STAMPEE entend maintenir un haut niveau de conformité et de confiance, et éviter tout relâchement qui pourrait conduire à des manquements.

(Fin de la Politique – Les annexes suivantes font partie intégrante de la Politique.)

Annexe 1 – Glossaire des définitions

Les termes clés utilisés dans la présente Politique sont définis ci-dessous pour lever toute ambiguïté. Les termes commençant par une majuscule dans le texte renvoient à ces définitions (sauf lorsqu'il s'agit de noms propres ou de débuts de phrase).

- **Autorité de contrôle** : l'autorité publique indépendante chargée de veiller à l'application de la réglementation sur la protection des données. En France, il s'agit de la Commission Nationale de l'Informatique et des Libertés (**CNIL**). Dans le contexte de STAMPEE, la CNIL est l'autorité chef de file pour les traitements transnationaux dans l'UE, et STAMPEE coopère avec elle ou avec toute autre autorité compétente.
- **Consentement** : toute manifestation de volonté libre, spécifique, éclairée et univoque par laquelle une Personne concernée accepte, par une déclaration ou par un acte positif clair, que des Données à caractère personnel la concernant fassent l'objet d'un Traitement. (Voir section 3.2 pour les conditions précises.)
- **Délégué à la Protection des Données (DPO)** : Personne (physique ou morale) désignée par STAMPEE conformément aux articles 37 à 39 du RGPD, chargée de conseiller et de contrôler l'organisme sur la protection des données personnelles, et de faire le lien avec l'Autorité de contrôle et les Personnes concernées. Chez STAMPEE, le DPO est la société DATASURE (coordonnées en section 2.1.3).
- **Données à caractère personnel** : (ou **Données personnelles** ou simplement **Données** dans le texte) toute information se rapportant à une personne physique identifiée ou identifiable. Est réputée identifiable une personne qui peut être identifiée, directement ou indirectement, notamment par référence à un identifiant (nom, numéro, identifiant en ligne) ou à un ou plusieurs éléments spécifiques propres à son identité physique, physiologique, génétique, psychique, économique, culturelle ou sociale. Par simplification, il s'agit de **toute information concernant une personne physique vivante**. Par exemple : un nom, une photo, une adresse email, un numéro de client, une adresse IP (si elle permet d'identifier), un numéro de téléphone, une empreinte digitale, etc.
- **Personne concernée** : la personne physique à laquelle se rapportent les Données à caractère personnel qui font l'objet d'un traitement. Dans le contexte de STAMPEE, les Personnes concernées peuvent être, par exemple, les clients personnes physiques, les représentants ou employés de clients personnes morales, les expéditeurs de lettres recommandées, les destinataires de ces lettres, les utilisateurs qui se font identifier via le service PVID, ou encore les employés de STAMPEE (pour les traitements RH).
- **Responsable de Traitement** : la personne physique ou morale, l'autorité publique, le service ou tout autre organisme qui, seul ou conjointement, détermine les finalités et les moyens du Traitement. C'est le « décideur » principal. Dans le contexte des services de STAMPEE, le Responsable de Traitement est généralement le client expéditeur (pour les données des destinataires et le contenu de la communication) ou STAMPEE elle-même pour les traitements qu'elle initie (par ex. gestion de comptes utilisateurs ou vérification d'identité conjointe). STAMPEE peut être responsable seul ou co-responsable (voir ci-dessous).
- **Sous-Traitant** : la personne physique ou morale, l'autorité publique, le service ou tout autre organisme qui traite des Données à caractère personnel pour le

compte et sur instruction du Responsable de Traitement. STAMPEE est Sous-Traitant de ses clients pour l'envoi des LRE. De même, les prestataires auxquels STAMPEE fait appel (comme l'hébergeur, l'envoi de notifications) sont ses Sous-Traitants. Un Sous-Traitant n'agit jamais pour son propre compte sur les données, il suit le contrat avec le Responsable.

- **Co-Responsable de Traitement** : situation où deux ou plusieurs entités déterminent conjointement les finalités et les moyens d'un Traitement. Elles partagent donc la responsabilité du traitement. Un accord de répartition doit définir leurs rôles respectifs. Dans cette Politique, le terme **co-Responsable** est utilisé pour désigner STAMPEE lorsqu'elle partage la responsabilité avec un partenaire (exemple : STAMPEE et le prestataire PVID sont co-Responsables du traitement de vérification d'identité).
- **Prestataire de Services de Confiance** : (selon le règlement eIDAS) une entité qui fournit des services électroniques garantissant la sécurité des transactions, tels que les services d'identification électronique, les signatures électroniques, les cachets électroniques, les horodatages, les services d'envoi recommandé électronique, etc. Un **Prestataire de Services de Confiance qualifié** est un prestataire qui a obtenu un statut spécial en remplissant les critères du règlement eIDAS et est supervisé par l'autorité nationale (ANSSI en France). STAMPEE est un Prestataire de Services de Confiance qualifié pour le service de Lettre Recommandée Électronique.
- **Lettre Recommandée Électronique (LRE)** : service électronique permettant d'envoyer des données (typiquement un message ou un document électronique) d'une manière qui fournit des preuves relatives au traitement des données envoyées (envoi, transmission et réception), et qui protège les données contre le risque de perte, de vol, d'altération non détectée. Une LRE qualifiée, selon eIDAS, offre un niveau de garantie élevé équivalent à celui d'un courrier recommandé papier. STAMPEE opère un service de LRE qualifié conforme à eIDAS et un service de LRE non qualifié conforme à la norme ETSI EN 319 521.
- **ETSI EN 319 521** : norme publiée par l'organisme européen de normalisation ETSI intitulée *"Policy and security requirements for Electronic Registered Delivery Service Providers"*. Elle spécifie les exigences de politique et de sécurité pour les fournisseurs de service de livraison électronique recommandée. STAMPEE se conforme à cette norme pour son service non qualifié, assurant ainsi un haut niveau de sécurité et de fiabilité.
- **PVID** : abréviation de **Prestataire de Vérification d'Identité à Distance**. Il s'agit d'un prestataire certifié selon le référentiel de l'ANSSI pour réaliser la vérification d'identité de personnes à distance (par exemple en comparant une photo d'identité et une vidéo selfie, etc.), souvent utilisé pour les besoins de KYC (Know Your Customer) ou de services de confiance (comme la création d'une identité numérique ou la vérification d'un expéditeur pour une LRE). Le prestataire PVID partenaire de STAMPEE est certifié par l'ANSSI, garantissant le respect de critères stricts de sécurité et de protection des données.

- **Pixel de suivi ou traceur de courriel :** image distante, généralement invisible, ou mécanisme équivalent intégré à un courriel et susceptible de déclencher une requête lors de l'affichage du message. Chez STAMPEE, ce mécanisme est limité aux notifications transactionnelles LRE et aux seules données strictement nécessaires à leur délivrabilité, conformément à la section 3.9.

- **RGPD** : Règlement (UE) 2016/679, Règlement Général sur la Protection des Données, texte de référence européen en vigueur depuis le 25 mai 2018, qui encadre la protection des données personnelles au sein de l'UE. En France, il est complété par la loi n°78-17 du 6 janvier 1978 modifiée (dite loi "Informatique et Libertés").
- **eIDAS** : Règlement (UE) n°910/2014 du 23 juillet 2014 sur l'identification électronique et les services de confiance pour les transactions électroniques. Ce règlement établit le cadre juridique pour les services de confiance (dont les LRE) au niveau européen. Il définit notamment les exigences pour qu'un service de confiance soit qualifié. STAMPEE se conforme à eIDAS pour son service LRE qualifié.
- **Data Privacy Framework** : Cadre de protection des données UE-États-Unis adopté par la Commission européenne en 2023, établissant une adéquation partielle pour les transferts de données vers les entreprises américaines certifiées. Il succède au Privacy Shield invalidé. Les entreprises US qui adhèrent aux principes du DPF offrent un niveau de protection considéré comme adéquat pour les données personnelles transférées depuis l'UE. STAMPEE peut s'appuyer sur ce cadre pour certains transferts vers les États-Unis (voir section 3.7).
- **Traitement** : toute opération ou ensemble d'opérations effectuées sur des Données à caractère personnel, quel que soit le procédé utilisé (automatisé ou non). Par exemple : la collecte, l'enregistrement, l'organisation, la conservation, la consultation, l'utilisation, la communication par transmission, la diffusion, ou encore la suppression de données sont des traitements. En pratique, dès que l'on manipule des données personnelles, on effectue un traitement.
- **Transfert de Données (hors UE)** : toute communication, copie ou déplacement de Données à caractère personnel destiné à un destinataire situé dans un pays tiers (en dehors de l'Espace Économique Européen) ou à une organisation internationale. Par exemple, le simple fait qu'un prestataire situé aux USA accède à des données depuis son pays est un transfert international. Ces transferts sont encadrés juridiquement (voir section 3.7).
- **Violation de Données à caractère personnel** : une violation de la sécurité entraînant de manière accidentelle ou illicite la destruction, la perte, l'altération, la divulgation non autorisée de Données personnelles ou l'accès non autorisé à celles-ci (voir section 7 pour la gestion des violations).

Synthèse des engagements de STAMPEE

En conclusion, STAMPEE prend une série d'engagements fermes pour assurer la protection des données personnelles dans l'ensemble de ses activités. La synthèse ci-dessous reprend les règles R1 à R23 ainsi que la règle R11 bis relative aux traceurs strictement nécessaires dans les courriels LRE :

- **R1 – Base légale** : STAMPEE ne réalise que des traitements ayant une base juridique valide et documentée (consentement, contrat, obligation légale, intérêt légitime…).
- **R2 – Transparence** : STAMPEE informe de manière claire et accessible les personnes concernées sur les traitements de leurs données et leurs droits.
- **R3 – Consentement valide** : Si un traitement repose sur le consentement, STAMPEE s'assure que ce consentement est libre, éclairé, spécifique et univoque.
- **R4 – Preuve et retrait du consentement** : STAMPEE conserve la preuve des consentements recueillis et permet aux personnes de retirer aisément leur consentement à tout moment.
- **R5 – Finalités limitées** : STAMPEE n'utilise les données personnelles que pour les finalités explicites pour lesquelles elles ont été collectées, et ne les réutilise pas à d'autres fins incompatibles.
- **R6 – Minimisation** : STAMPEE ne collecte que les données personnelles strictement nécessaires à chaque traitement, évitant toute donnée superflue.
- **R7 – Exactitude** : STAMPEE maintient les données à jour et exactes ; les données inexactes sont corrigées ou supprimées dans les meilleurs délais.
- **R8 – Durée de conservation** : STAMPEE conserve les données personnelles uniquement le temps nécessaire aux finalités poursuivies, puis les supprime ou anonymise, sauf obligation légale de conservation.
- **R9 – Sécurité** : STAMPEE met en place des mesures de sécurité techniques et organisationnelles appropriées (contrôle d'accès, chiffrement, journalisation, etc.) pour garantir la confidentialité, l'intégrité et la disponibilité des données.
- **R10 – Transferts internationaux** : STAMPEE n'effectue de transferts de données hors UE que dans le respect du cadre légal (pays adéquat, clauses contractuelles types, Data Privacy Framework, etc.), assurant un niveau de protection équivalent.
- **R11 – Données sensibles** : STAMPEE s'interdit de traiter des catégories particulières de données sensibles ou des données pénales, sauf exception légale extrêmement encadrée (ce qui n'a pas lieu dans ses traitements courants).
- **R11 bis - Traceurs des courriels LRE :** STAMPEE limite les pixels de suivi aux notifications transactionnelles strictement nécessaires, ne collecte pas de données de terminal ou d'adresse IP à ce titre, exclut toute finalité publicitaire ou de profilage et supprime la dernière date d'ouverture à la fin du cycle de notification.
- **R12 – Privacy by Design** : STAMPEE intègre la protection des données dès la conception de tout nouveau projet ou service, en appliquant par défaut les réglages les plus protecteurs pour la vie privée.

- **R13 – Analyse d'impact (AIPD)** : STAMPEE réalise des analyses d'impact sur la protection des données pour tout traitement à risque élevé, et suit les recommandations issues de ces analyses avant de lancer le traitement.
- **R14 – Registre des traitements** : STAMPEE tient un registre complet de ses activités de traitement, mis à jour régulièrement, reflétant sa conformité et facilitant le pilotage des mesures de protection.
- **R15 – Rôle de chaque partie** : STAMPEE clarifie pour chaque traitement impliquant des tiers qui est Responsable, co-Responsable ou Sous-Traitant, et respecte les obligations associées à son rôle.
- **R16 – Contrats avec les tiers** : STAMPEE conclut un accord écrit avec chaque client, partenaire ou sous-traitant intervenant sur des données, incluant toutes les clauses de protection des données requises par le RGPD.
- **R17 – Contrôle des sous-traitants** : STAMPEE vérifie régulièrement la conformité de ses sous-traitants (audits, rapports, etc.) et exige d'eux un niveau de protection des données constant et élevé.
- **R18 – Droits des personnes** : STAMPEE facilite l'exercice des droits des personnes (accès, rectification, effacement, opposition, etc.) et répond à toute demande dans les délais légaux. En tant que sous-traitant, STAMPEE assiste ses clients pour qu'ils puissent honorer ces demandes.
- **R19 – Gestion des violations** : STAMPEE a une procédure de réponse aux incidents de sécurité ; toute violation de données personnelles est traitée en urgence, documentée, et fait l'objet des notifications nécessaires (CNIL, personnes concernées) en cas de risque.
- **R20 – Notification client** : Si une violation concerne des données traitées pour le compte d'un client, STAMPEE alerte immédiatement ce client pour qu'il puisse prendre les mesures et notifications qui s'imposent.
- **R21 – Coopération avec la CNIL** : STAMPEE coopère activement avec l'autorité de contrôle, répond aux demandes, anticipe les consultations obligatoires et facilite les contrôles, via son DPO notamment.
- **R22 – Personnel formé** : STAMPEE s'assure que tous ses collaborateurs sont formés, sensibilisés et tenus de respecter les règles de protection des données et de sécurité, afin de créer une culture interne forte de conformité.
- **R23 – Contrôles et amélioration continue** : STAMPEE réalise des contrôles internes réguliers sur la mise en œuvre de cette Politique et s'engage dans une amélioration continue de ses pratiques de protection des données (mises à jour de la Politique, nouvelles mesures, etc.).

Par ces engagements, STAMPEE démontre sa volonté de placer la protection des données à caractère personnel au cœur de ses activités de Prestataire de Services de Confiance. Cette Politique générale servira de référence à l'ensemble des collaborateurs, clients et partenaires de STAMPEE pour comprendre les principes et règles appliqués. Elle assure à nos clients et aux utilisateurs de nos services que leurs données seront traitées avec le plus grand soin et dans le respect total de leurs droits et de la réglementation en vigueur. STAMPEE entend ainsi mériter la **confiance** que vous lui accordez.