Charte RGPD

Modalités d'application du Règlement Général sur la Protection des Données (RGPD)

Collaborating as a service
68 rue de Rivoli
75 004 PARIS
FRANCE

SOMMAIRE

1. PREAMBULE

Madame, Monsieur,

Les données personnelles que vous nous confiez, que nous traitons dans le cadre de la livraison de nos services ou que nous enregistrons lors de nos interactions, nous permettent de mieux comprendre et répondre à vos attentes. Elles sont en outre nécessaires à la gestion du contrat pour lequel vous nous accordez votre confiance.

Conscient de l'importance de ces données, SECUSERVE est depuis toujours particulièrement attentive à la manière dont elles sont collectées, utilisées, stockées et protégées.
A compter du 25 mai 2018, une nouvelle réglementation européenne sur les données personnelles entre en vigueur et fera évoluer profondément la loi Informatique et Libertés actuellement applicable en France.
Ce **Règlement Général sur la Protection des Données (RGPD)** sera pour SECUSERVE l'occasion de renforcer ses Conventions de Service et les règles applicables aux procédures de travail de nos équipes en encadrant de manière encore plus stricte l'utilisation et la sécurisation de vos données personnelles.
Le Règlement Général sur la Protection des Données (RGPD) est le cadre juridique du traitement de données à caractère personnel en Europe, à compter du 25 mai 2018. Contrairement à la directive 95/46/CE, qui régissait jusqu'alors ces traitements, le RGPD est d'application directe dans l'Union et ne nécessite pas de transpositions nationales. À ce titre, il va favoriser **l'harmonisation des régimes juridiques** en matière de protection des données à caractère personnel en Europe. Mieux encore, le RGPD dispose d'un principe d'extraterritorialité qui permet, dans certaines circonstances, **d'étendre son périmètre d'application** en dehors des frontières européennes.
Si vous êtes une structure traitant des données à caractère personnel (notamment en tant qu'utilisateur ou administrateur d'un service de messagerie d'entreprise), il y a de fortes chances pour que vous soyez assujettis aux dispositions du RGPD. À cet égard, vous êtes soumis à des obligations auxquelles il faut vous conformer. Il en est de même pour SECUSERVE qui, au regard de sa situation, disposera d'obligations distinctes : en sa **qualité de sous-traitant ou de responsable de traitement**.
Vous trouverez ci-dessous, les principales informations concernant la façon dont nous collectons et traitons vos données personnelles

1.1 DEFINITION

Comprendre les enjeux réels et précis d'un règlement européen n'est pas toujours chose aisée, surtout lorsqu'il comporte 99 articles, 173 considérants et de nombreuses lignes directives servant à préciser son interprétation. C'est pourtant essentiel afin d'éviter tout risque pouvant résulter d'une interprétation trop large ou imprécise des obligations réglementaires incombant à votre structure. La bonne compréhension des quelques termes définis ci-dessous est donc essentielle :

- **données à caractère personnel** : toute information se rapportant à une personne physique identifiée ou identifiable. Est réputée être une personne physique identifiable une personne physique qui peut être identifiée, directement ou indirectement.
- **traitement :** toute opération ou tout ensemble d'opérations effectuées ou non à l'aide de procédés automatisés et appliquées à des données ou des ensembles de données à caractère personnel (collecte, enregistrement, transmission, stockage, conservation, extraction, consultation, utilisation, interconnexion, etc.).

  Exemple : utilisation d'un service de messagerie professionnelle, de contacts ou de calendriers.
- **responsable du traitement** : la personne physique ou morale, l'autorité publique, le service ou un autre organisme qui, seul ou conjointement avec d'autres, détermine les finalités et les moyens du traitement.

  Exemple : société cliente et utilisatrice d'un service de messagerie professionnelle.
- **sous-traitant** : la personne physique ou morale, l'autorité publique, le service ou un autre organisme qui traite des données à caractère personnel pour le compte du responsable du traitement.

  Exemple : SECUSERVE est sous-traitant du responsable de traitement dans le cadre de la livraison des services de messagerie.

2. SECUSERVE EN QUALITE DE SOUS-TRAITANT

C'est certainement en cette qualité que vos attentes envers SECUSERVE sont les plus importantes. SECUSERVE est qualifiée de « sous-traitant » lorsqu'il traite des données à caractère personnel pour le compte d'un responsable de traitement :

- Service e-securemail de relayage de message
- Service Optimails ou SHEX de messagerie hébergée
- Service Sharecan de stockage/partage de fichiers en ligne

Dans la limite de ses contraintes techniques, SECUSERVE ne pourra traiter les données stockées que selon vos instructions, et ce pour votre compte. Selon la loi applicable, la formalisation des instructions pourra être plus ou moins élevée (respect des correspondances privées, par exemple).

2.1 LES ENGAGEMENTS DE SECUSERVE EN QUALITE DE SOUS-TRAITANT

En qualité de sous-traitant, SECUSERVE s'engage notamment à :

- traiter les données à caractère personnel aux seules fins de la bonne exécution des services : SECUSERVE ne traitera jamais vos informations à d'autres fins (marketing, etc.).
- ne pas transférer vos données hors UE ou hors pays reconnus par la Commission européenne comme disposant d'un niveau de protection suffisant : sous réserve que vous ne sélectionniez pas un datacenter dans une zone géographique hors UE.

NOS DATACENTERS PAR DEFAUT pour nos clients français sont exclusivement SITUES EN FRANCE. Vos données de messagerie (messages, contacts, agenda, etc.), sont stockées sur des serveurs en France, mais peuvent se trouver en dehors de l'UE, si vous-même synchronisez ces données sur vos applications de messagerie en dehors de l'UE.

- vous informer de tout recours à des sous-traitants qui pourraient traiter vos données à caractère personnel : à ce jour, aucune prestation impliquant un accès aux contenus stockés par vos soins dans le cadre des services n'est sous-traitée en dehors de SECUSERVE.
- à mettre en œuvre des standards de sécurité élevés afin de fournir un haut niveau de sécurisation à nos services.
- vous notifier dans les meilleurs délais en cas de violation de données.
- vous assister à respecter vos obligations réglementaires en vous fournissant une documentation adéquate de nos services.

2.2 QUI EST PROPRIETAIRE DES DONNEES A CARACTERE PERSONNEL UTILISEES ET STOCKEES PAR LE CLIENT DANS LE CADRE DES SERVICES ?

Les données hébergées par le client dans le cadre des services de SECUSERVE restent la propriété du client. SECUSERVE n'y accède et ne les utilise que lorsque cela est nécessaire dans le cadre de l'exécution des services et dans la limite de ses contraintes techniques. SECUSERVE s'interdit toute revente desdites données, de même que toute utilisation à des fins personnelles (telles des activités de datamining, de profilage ou de marketing direct).

2.3 DANS QUELS CAS SECUSERVE PEUT-IL ETRE AMENE A ACCEDER AUX DONNEES STOCKEES ET UTILISEES PAR LE CLIENT DANS LE CADRE DES SERVICES ?

SECUSERVE accède aux données uniquement dans deux situations :

- Pour les besoins de l'exécution des services et notamment afin d'optimiser l'assistance aux clients lorsque ceux-ci contactent le support SECUSERVE. Dans cette hypothèse, les accès aux données des clients restent encadrés grâce à des habilitations spécifiques et des mesures de contrôle et de sécurité particulières;
- Afin de répondre aux obligations légales dans le cadre des demandes judiciaires et/ou administratives. Ces demandes sont très strictement encadrées.

2.3.1 Accès dans le cadre du support :

Lorsque le client prend contact avec le support SECUSERVE, selon l'objet de l'assistance, deux catégories de données peuvent faire l'objet d'un accès.

- D'une part, afin de traiter au mieux la requête du client, le support prend connaissance des informations fournies par ce dernier lors de la création de son compte SECUSERVE (nom, prénom, numéro de téléphone, adresse e-mail, etc.).
- D'autre part et uniquement à la demande expresse du client, et sous réserve des contraintes techniques propres à chaque service, le support peut avoir accès aux données stockées par celui-ci sur les services de SECUSERVE, afin d'identifier l'origine du problème rencontré et, éventuellement, de le résoudre.

2.3.2 Accès dans le cadre d'une demande des autorités judiciaires/administratives :

Afin d'agir en conformité avec la réglementation en vigueur, SECUSERVE est tenu de répondre aux demandes des autorités judiciaires et/ou administratives. Les demandes d'accès étant soumises à un régime légal strict, SECUSERVE ne les autorise qu'après s'être assuré de la validité et du bien-fondé de la requête. De plus, dès lors que la requête ou la loi ne l'interdit pas, SECUSERVE s'engage à prévenir dans les meilleurs délais le client d'une telle demande. Pour les requêtes qui émaneraient d'un pays tiers, celles-ci ne sont traitées qu'à la condition qu'elles soient fondées sur un accord international, tel qu'un traité d'entraide judiciaire, en vigueur entre le pays tiers demandeur et l'Union ou un État membre.

2.4 LES DONNEES DES CLIENTS EUROPEENS DE SECUSERVE SONT-ELLES TRANSFEREES EN DEHORS DE L'UNION EUROPEENNE ?

Il convient de distinguer deux situations distinctes en la matière. Celles-ci peuvent notamment dépendre des choix réalisés par le client en matière de sélection de l'emplacement des datacenters dans lesquels seront stockées ses données :

- Lorsque **le client choisit un service** dans le cadre duquel sont utilisés un ou plusieurs **centres de données en Union européenne :**
  - Dans ce cas, les données du client ne seront jamais transférées en dehors : de pays membres de l'Union européenne de pays reconnus par la Commission européenne comme disposant d'un niveau de protection suffisant des données à caractère personnel au regard de la protection de la vie privée, des libertés et des droits fondamentaux des personnes.
  - La liste de ces pays peut être retrouvée à tout instant sur le site de la Commission européenne.
  - Suite à l'invalidation du Safe Harbor, et bien que la Commission européenne considère que les organismes américains adhérents au Privacy Shield disposent d'un niveau de protection suffisant, SECUSERVE ne transfère jamais les données des clients, dont la zone géographique sélectionnée est située en UE, à destination des États-Unis d'Amérique.
  - Les transferts de données vers des pays reconnus par la Commission européenne comme disposant d'un niveau de protection suffisant peuvent intervenir dans le cadre d'une intervention du support SECUSERVE. Quand les centres de données SECUSERVE sont situés dans l'Union européenne, les équipes support SECUSERVE pouvant intervenir sont localisées au sein de l'Union européenne ainsi qu'au Canada, étant précisé que le Canada est reconnu par la Commission européenne comme pays présentant un niveau de protection des données à caractère personnel adéquat. SECUSERVE se réserve également le droit de confier des prestations de support pouvant impliquer un accès à distance aux données stockées par le client, dans le

cadre des services, à d'autres entités de SECUSERVE situées dans des pays également reconnus par la Commission européenne comme disposant d'un niveau de protection suffisant (à l'exclusion des USA). Grâce aux garanties offertes par SECUSERVE en matière de transfert de données, le client peut respecter ses obligations réglementaires. L'article 45 du RGPD, déterminant les cas de « transferts fondés sur une décision d'adéquation », stipule en effet qu'un transfert de données à caractère personnel vers un pays tiers ou à une organisation internationale peut avoir lieu lorsque la Commission a constaté par voie de décision que le pays tiers, un territoire ou un ou plusieurs secteurs déterminés dans ce pays tiers, ou l'organisation internationale en question assure un niveau de protection adéquat. Un tel transfert ne nécessite pas d'autorisation spécifique.

Par défaut, les datacenters, les serveurs *relais et les serveurs de messagerie des CLIENTS FRANCAIS de SECUSERVE sont EXCLUSIVEMENT SITUES EN FRANCE, et les données ne sont pas transférées en dehors du territoire français, sauf à l'initiative du client.*

- Lorsque **le client choisit** un service dans le cadre duquel est utilisé un centre de données situé **en dehors de l'Union européenne** :
    - Dans ce cas, il semble évident que des données soient transférées en dehors de l'Union européenne. La localisation ou zone géographique du ou des centres de données, utilisés dans le cadre du service, est communiquée sur le site internet de SECUSERVE. Lorsque plusieurs localisations sont disponibles, le client sélectionne celle de son choix. SECUSERVE s'interdit de modifier, sans l'accord du client et sous réserve de conditions spécifiques propres à certains services, la localisation ou zone géographique convenue à la commande. Afin d'accompagner les structures souhaitant traiter des données à caractère personnel en ayant recours à des centres de données situés hors Union européenne dans un pays n'assurant pas un niveau de protection adéquat des données à caractère personnel, SECUSERVE peut sur demande expresse, discuter de la mise en place de garanties permettant un tel transfert tel que prévu à l'article 46 du RGPD « Transferts moyennant des garanties appropriées ».

2.5 COMMENT LES SERVICES DE SECUSERVE VOUS FACILITE L'APPLICATION DE LA RGPD

Dans le cadre de l'utilisation des services de relayage de messagerie et de messagerie collaborative, vos utilisateurs peuvent manipuler des données personnelles. Tous les contacts, tous les messages, tous les rendez-vous pris dans les calendriers, ne sont pas exclusivement professionnels. De plus, ce sont souvent les utilisateurs eux-mêmes qui sont les mieux placés pour déterminer ce qui a un caractère professionnel et ce qui est d'ordre personnel.
Afin de faciliter cette classification et la confidentialité de ces informations au sein de l'entreprise cliente de SECUSERVE, nous avons intégré un certain nombre de solutions et d'outils dans le cadre de nos services :

- Les utilisateurs peuvent **gérer leurs propres listes blanche (autorisée) et noire (interdite)** dans le cadre du service de filtrage, et ce, via une Console Individuelle de Messagerie (CIM) ;
- Les utilisateurs peuvent définir et gérer une liste d'adresses email déclarées « PERSONNELLE », afin de **catégoriser automatiquement les messages à caractère personnel**. La catégorisation se fait par un TAG [PERSO] ou en déplaçant automatiquement les messages dans un répertoire donné. Ainsi il est très facile au départ d'un collaborateur de lui remettre ces messages personnels ou de les détruire, sans détruire des informations professionnelles. La gestion des listes « PERSO » est opérée par l'utilisateur en toute indépendance.

3. SECUSERVE EN QUALITE DE RESPONSABLE DE TRAITEMENT

SECUSERVE est qualifiée de « responsable de traitement » lorsqu'il détermine les finalités et les moyens de « ses » traitements de données à caractère personnel.

C'est typiquement le cas quand SECUSERVE collecte des données à des fins de **facturation, de gestion des recouvrements, de l'amélioration de la qualité des services et de la performance, de démarchage commercial, de gestion commerciale**, etc. Mais aussi lorsque SECUSERVE traite les données à caractère personnel de **ses propres salariés**.

Dans cette hypothèse, « vos » données, celles que vous stockez sur les services de SECUSERVE, ne sont pas concernées. En revanche, certaines informations vous concernant ou étant relatives à vos salariés (identité et coordonnées de l'interlocuteur SECUSERVE dans le cadre d'une demande d'assistance technique, par exemple) peuvent l'être. C'est pourquoi SECUSERVE tient à vous donner des éléments de compréhension sur les garanties mises en œuvre afin d'assurer la protection de ces données à caractère personnel.

- limiter la collecte de données à celles strictement utiles : c'est dans le cadre de cette démarche que lors de la commande d'un service, vous ne renseignez que des données nécessaires pour que SECUSERVE puisse assurer des services de facturation, de support ou encore respecter ses propres obligations légales en matière de conservation de données(notamment sur le fondement de la loi n° 2004-575 du 21 juin 2004 pour la confiance dans l'économie numérique).
- ne pas utiliser les données collectées à d'autres fins que celles pour lesquelles elles furent collectées.
- conserver les données à caractère personnel durant une période limitée et proportionnée. C'est ainsi qu'à titre d'exemple, les données traitées à des fins de gestion de la relation entre le client et SECUSERVE (nom, prénom, adresse postale, e-mail, etc.) sont conservées par l'entreprise pendant toute la durée du contrat et les trente-six (36) mois suivants. Au terme de ce délai, elles sont supprimées sur tous supports et sauvegardes.
- ne pas transférer ces données à des tiers autres que les sociétés apparentées de SECUSERVE qui interviennent dans le cadre de l'exécution du contrat.
- mettre en œuvre des mesures techniques et organisationnelles appropriées afin de garantir un haut niveau de sécurité.

4. REGISTRE DE TRAITEMENT

L'existence d'un registre de traitement n'est pas une nouveauté. Déjà au temps de la loi informatique et liberté, il fallait tenir un registre pour les traitements exonérés de déclaration auprès de la CNIL. La tenue du registre était à la charge du correspondant informatique et libertés. Ce dernier se basait sur les informations données par le responsable du traitement pour tenir son registre.
Le **RGPD oblige les responsables du traitement et les sous-traitants de tenir un registre des traitements**. Avant, les sous-traitants n'étaient pas soumis à cette obligation. Cette généralisation de l'obligation de tenir un registre des traitements est l'une des applications majeures du « principe d'accountability ».

L'accountability désigne l'obligation pour les entreprises de mettre en œuvre des mécanismes et des procédures internes permettant de démontrer le respect des règles relatives à la protection des données.

Pour rappel, ce dernier impose de prendre les mesures internes nécessaires pour optimiser la protection des données et faciliter l'apport de preuve en cas de contrôle ou en cas de litige devant un tribunal.
SECUSERVE a décidé dans le cadre de sa démarche de qualité et d'exemplarité règlementaire, de s'imposer la tenue d'un tel registre tant en situation de sous-traitant que de responsable de traitement.

4.1 CONTENU D'UN REGISTRE

Le RPGD ne dresse pas une liste exhaustive des informations qui devraient figurer sur un registre. Mais au minimum, ce dernier devrait contenir les informations suivantes :

- Le nom du responsable du traitement ou de son représentant, le cas échéant, le nom du DPO ;
- Les finalités du traitement ;
- Les différentes catégories de données traitées ;
- Les personnes concernées par le traitement ;
- Les destinataires des données ;
- Les délais prévus de destruction des données,
- La description des mesures de sécurité à mettre en place pour protéger les données ;
- Les garanties de sécurité supplémentaires pour les cas de transfert de données à l'international ;

5. CONTACT RGPD

Un DPO (Data Protection Officer) a été nommé et est le contact privilégié des clients de SECUSERVE sur ces aspects.

Tous les interlocuteurs de SECUSERVE (salariés, clients, prospects, fournisseurs, autres…) peuvent solliciter le DPO de SECUSERVE pour prendre connaissance des données personnelles les concernant, en demander une copie, le transfert ou la destruction, lorsque cela est techniquement et juridiquement/légalement possible.
Il est joignable par email : rgpd@secuserve.com