

Notice relative à la protection des données personnelles (Clients professionnels)

Ce document présente le descriptif général des traitements de données à caractère personnel réalisés par POST dans le cadre de l'exécution des contrats passés avec ses clients professionnels, ainsi que les obligations des parties en matière de protection des données personnelles

INTRODUCTION

POST attache une grande importance au respect de la vie privée des personnes physiques et a conscience de l'importance que ses Clients y accordent. POST met dès lors tout en œuvre afin que ses Clients puissent utiliser ses services en toute confiance, notamment en traitant leurs données de manière transparente, dans le strict respect des lois et réglementations applicables en matière de protection des données à caractère personnel, ainsi que de dans le respect de leurs propres instructions.

DÉFINITIONS

"**CGV**" : conditions générales de vente de POST Technologies, accessibles sur www.post.lu/conditions

"**Descriptif Spécifique**" : la présentation des opérations de traitements réalisées par POST dans le contexte de chaque produit et/ou service utilisé par le Client, pour lequel POST est qualifié de sous-traitant et le Client de responsable de traitement au sens du RGPD, consignées dans un contrat, des conditions spécifiques, des documents annexes, un formulaire de souscription ou tout autre document.

"**Loi**" : toutes lois, tous règlements et autres exigences applicables au Grand-Duché de Luxembourg, relatifs à la protection des personnes physiques à l'égard du traitement des données, en ce inclus le Règlement Général sur la Protection des données (Règlement UE 2016/679 – "**RGPD**").

"**POST**" : POST Technologies, la division des télécommunications de POST Luxembourg, établissement public créé par la loi modifiée du 10 août 1992, immatriculé auprès du Registre de Commerce et des Sociétés de Luxembourg sous le numéro J28, ayant son siège au 20 rue de Reims, L-2417 Luxembourg et son établissement opérationnel au 2 rue Emile Bian, L-2999 Luxembourg, Grand-Duché de Luxembourg ;

Les termes utilisés dans la présente notice, doivent être compris au sens des CGV ou du RGPD.

OBJET ET CHAMP D'APPLICATION

Les clauses suivantes s'appliquent uniquement aux traitements de données à caractère personnel réalisés par POST dans le contexte de chaque produit et/ou service souscrit par le Client au titre du Contrat, pour lesquels POST agit en qualité de sous-traitant (au sens donné par le RGPD) et le Client agit en qualité de responsable de traitement (au sens donné par le RGPD). Les clauses suivantes de la présente notice ont pour objet de garantir le respect, à la fois par le Client et par POST, des dispositions de l'article 28, paragraphes 3 et 4, du RGPD et constituent les instructions du Client.

OBLIGATIONS DU CLIENT

Le Client, en sa qualité de responsable de traitement, a la responsabilité première d'assurer la licéité des activités de traitement confiées à POST. En conséquence, le Client est tenu de :

- (i) Établir une base légale appropriée pour chacune des activités de traitement confiées à POST ;
- (ii) Transmettre à POST des instructions claires et suffisamment documentées sur les opérations de traitement à réaliser ;
- (iii) Documenter et conserver un registre des activités de traitement sous sa responsabilité, ainsi que toute autre documentation utile pour lui permettre de démontrer sa conformité aux présentes clauses ;
- (iv) Mettre en place les mesures techniques et organisationnelles pour assurer un niveau suffisant de protection des données personnelles. Ce faisant, le Client devra tenir compte de la nature, l'étendue, le contexte et les objectifs du traitement ainsi que les risques d'atteinte aux droits et libertés des personnes concernées. Ces mesures devront être réexaminées et adaptées lorsque cela sera nécessaire ;
- (v) Respecter les droits des personnes concernées ;
- (vi) Notifier les violations de données personnelles à l'autorité de contrôle compétente et, le cas échéant, aux personnes concernées, conformément aux dispositions de la Loi ;
- (vii) Effectuer lorsque nécessaire une analyse d'impact relative à la protection des données.

OBLIGATIONS DE POST

POST ne traitera les données que sur instruction documentée du Client, à moins que POST soit tenu d'y procéder en vertu du droit applicable. Dans ce cas, POST informera le Client de cette obligation juridique avant le traitement, sauf si la loi l'interdit à POST pour des motifs importants d'intérêt public.

Si POST pense qu'une instruction du Client constitue une violation de la Loi, POST en informe immédiatement le Client.

POST se réserve la possibilité de facturer l'exécution d'instructions documentées complémentaires du Client qui ne sont pas strictement nécessaires pour se conformer à la Loi

3.1. Limitation de finalité

POST traite les données personnelles uniquement pour les finalités spécifiques du traitement, telles que définies dans le Descriptif Spécifique des produits et/ou services souscrits par le Client, sauf instruction complémentaire claire et documentée du Client.

3.2. Durée du traitement des données personnelles

POST traite les données personnelles uniquement pendant les durées précisées dans le Descriptif Spécifique des produits et/ou services souscrits par le Client, sauf instruction complémentaire claire et documentée du Client.

3.3. Sécurité du traitement

POST met en œuvre un ensemble raisonnable de mesures techniques et organisationnelles afin d'assurer la sécurité des données personnelles traitées pour le compte du Client. Les mesures de sécurité mises en œuvre par POST visent à protéger les données personnelles contre toute violation de la sécurité entraînant, de manière accidentelle ou illicite, la destruction, la perte, l'altération, la divulgation non autorisées de données personnelles ou l'accès non autorisé à de telles données. Le document décrivant les mesures de sécurité organisationnelles et techniques de POST relatives à la protection des personnes physiques à l'égard du traitement de données personnelles est consultable sur www.post.lu/conditions.

Le niveau de sécurité mis en œuvre dépend de chaque traitement de données personnelles. Il est adapté à la nature, à la portée, au contexte et aux finalités du traitement, aux types de données traitées ainsi qu'aux risques identifiés pour les personnes concernées. Ce niveau de sécurité tient également compte de l'état des connaissances et des coûts de mise en œuvre. Les mesures de sécurité spécifiques au contexte des traitements réalisés sont précisées dans le Descriptif Spécifique de chaque produit et/ou service souscrit par le Client.

POST s'engage à réévaluer régulièrement l'adéquation des mesures de sécurité au regard des risques.

POST s'engage à notifier le Client au préalable, en cas de modifications significatives des mesures de sécurité ayant une incidence négative sur la sécurité des traitements, afin de laisser à ce dernier la possibilité de s'opposer pour des raisons objectivement justifiables à de telles modifications dans le délai notifié. En cas d'absence d'opposition du Client, POST pourra effectuer les modifications des mesures de sécurité notifiées.

POST veille à ce que tout son Personnel ayant accès aux données personnelles du Client soit soumis à des obligations de confidentialité.

POST n'accorde l'accès aux données personnelles faisant l'objet d'un traitement pour le compte du Client qu'aux seuls membres du personnel agissant sous son autorité en ayant strictement besoin pour la bonne exécution, la gestion ou le suivi du Contrat.

POST a par ailleurs obtenu la certification ISO 27001 pour son Système de Management de la Sécurité de l'Information (SMSI), attestant du haut niveau de maturité des processus de gestion et d'exploitation de ses infrastructures consacrées à la fourniture de services managés (« On Premises » ou dans le « Cloud »), ainsi que tous les processus de support inhérents à la fourniture de ces services à ses Clients. La certification ISO27001 démontre l'expertise de POST sur le sujet, apporte au Client un haut niveau d'assurance sur la sécurité de leurs solutions managées, ainsi que des garanties élevées sur la standardisation des processus de gestion de POST.

3.4. Données sensibles

POST ne traite pas de données sensibles, telles que définies aux articles 9 et 10 du RGPD, sauf instruction complémentaire claire et documentée du Client. Le Client devra dans ce cas de figure préciser à POST quelles limitations spécifiques et/ou garanties supplémentaires doivent être appliquées au traitement de ces catégories de données, POST restant libre de les accepter ou non et, le cas échéant, de les accepter moyennant des frais supplémentaires.

3.5. Documentation et conformité

POST met à disposition du Client, sur demande, toutes les informations nécessaires pour démontrer, dans le cadre du Contrat, le respect des obligations imposées par les présentes clauses à POST en sa qualité de sous-traitant.

A la demande du Client, POST permettra la réalisation d'audits des activités de traitements réalisées dans le cadre du Contrat par POST en tant que sous-traitant et y contribuera, à intervalles raisonnables dans la limite d'un audit tous les deux ans ou en présence d'indices tangibles de non-conformité. Lorsqu'il envisage de formuler une demande d'informations liées à la conformité de POST ou de réaliser un audit, le Client tient compte des certifications pertinentes obtenues par POST au moment de sa demande (comme la certification ISO 27001), afin de déterminer si une demande d'informations ou un audit est réellement nécessaire.

Le Client peut décider de procéder lui-même à l'audit ou de mandater un auditeur indépendant. Dans ce dernier cas, le Client devra préalablement à la demande d'audit :

- Notifier l'auditeur indépendant envisagé à POST, qui pourra dans un délai d'une (1) semaine calendaire s'opposer à cette nomination pour des motifs raisonnables ; et
- Obtenir la signature d'un engagement de confidentialité adéquat par l'auditeur indépendant.

Les audits peuvent également comprendre des inspections dans les locaux de POST, moyennant un préavis raisonnable d'au moins (1) mois, sans préjudice d'un délai plus court imposé par une autorité de contrôle. Dans le cadre d'inspections, le Client s'engage à :

- Respecter la sécurité des locaux de POST, ainsi que toute procédure ou politique interne de POST ;
- Minimiser le risque de perturbation des activités de POST.

Les coûts des audits et inspections sont pris en charge par le Client.

3.6. Recours à des sous-traitants ultérieurs

POST dispose de l'autorisation générale du Client pour confier à des sous-traitants ultérieurs certaines opérations de traitement de données personnelles réalisées par POST pour le compte du Client en exécution du Contrat, sur la base de la liste des sous-traitants qui est précisée dans le Descriptif Spécifique de chaque produit et/ou service souscrit par le Client.

POST informera par écrit le Client de tout projet de modification de cette liste au moins trente (30) jours calendaires à l'avance. Si le Client souhaite s'opposer à ce changement de sous-traitant ultérieur, il devra notifier POST de son opposition dûment justifiée au plus tard trente (30) jours après en avoir été informé. À défaut d'opposition dans le délai indiqué ci-avant, le changement de Sous-Traitant sera réputé accepté par le Client.

Lorsque POST fait appel à des sous-traitants pour mener des opérations de traitement de données spécifiques dans le cadre de l'exécution du Contrat, POST s'assure d'obtenir de la part de ses sous-traitants ultérieurs un engagement contractuel leur imposant en substance les mêmes obligations en matière de protection des données que celles imposées à POST en vertu des présentes clauses.

À la demande du Client, POST fournira une copie des contrats de sous-traitance ultérieure le concernant. Avant d'en diffuser une copie au Client, POST se réserve le droit d'expurger certaines mentions y figurant, afin de protéger le secret des affaires ou certaines informations confidentielles, y compris les données à caractère personnel.

POST demeure pleinement responsable à l'égard du Client de l'exécution des obligations de ses sous-traitants ultérieurs en matière de protection des données personnelles et informera le Client de tout manquement de ses sous-traitants à leurs obligations contractuelles.

3.7. Transferts internationaux

POST ne transfère pas, y compris en accordant l'accès à, des données personnelles que POST traite en tant que sous-traitant à un destinataire en dehors de l'espace économique européen (EEE), à moins qu'il en soit disposé autrement dans le Descriptif Spécifique de chaque produit et/ou service souscrit par le Client.

Le Client en sa qualité de Responsable de traitement convient que lorsque POST recrute un sous-traitant ultérieur conformément à la clause 3.6 pour mener des activités de traitement spécifiques (pour le compte du Client) et que ces activités de traitement impliquent un transfert de données à caractère personnel en dehors de l'espace économique européen (EEE), POST et le sous-traitant ultérieur encadrent ce transfert en utilisant les clauses contractuelles types adoptées par la Commission Européenne.

3.8. Assistance au Client

POST informe sans délai le Client de toute demande reçue directement de la part des personnes concernées par le traitement objet du Contrat. POST ne donne pas suite à ces demandes, à moins que le Client ne lui donne instruction claire et documentée de le faire.

En fonction de la nature des traitements réalisés et des informations mises à sa disposition, POST prête assistance au Client pour respecter son obligation de répondre aux demandes des personnes concernées dans l'exercice de leurs droits. POST se réserve alors la possibilité de facturer cette assistance au Client.

POST aide par ailleurs raisonnablement le Client, en fonction de la nature des traitements réalisés et des informations mises à sa disposition, à garantir le respect de ses autres obligations suivantes :

- Procéder à une analyse d'impact relative à la protection des données, lorsque le traitement est susceptible de présenter un risque élevé pour les droits et libertés des personnes physiques concernées ;
- Consulter l'autorité de contrôle compétente préalablement au traitement lorsqu'une analyse d'impact relative à la protection des données indique que le traitement présenterait un risque élevé si le Client ne prenait pas de mesures pour atténuer ce risque ;
- Informer sans délai le Client si POST apprend que les données personnelles qu'elle traite sont inexactes ou sont devenues obsolètes ;
- Garantir un niveau de sécurité des données personnelles adapté aux risques identifiés.

POST se réserve la possibilité de facturer l'assistance décrite ci-dessus au Client.

Les mesures techniques et organisationnelles appropriées par lesquelles POST est tenu de prêter assistance au Client dans l'application de la présente clause, ainsi que la portée et l'étendue de l'assistance requise, sont précisées dans le document décrivant les mesures de sécurité de POST relatives à la protection des personnes physiques à l'égard du traitement de données personnelles, consultable sur www.post.lu/conditions.

3.9. Notification en cas de violation des données

3.9.1. Notification en rapport avec les données traitées par le Client

En cas de violation de données personnelles en rapport avec les données traitées par le Client dans le cadre du Contrat, POST s'engage à coopérer avec le Client et lui prêter assistance, afin qu'il réponde à ses obligations en matière de (i) notification de la violation à l'autorité de contrôle compétente et (ii) communication de la violation aux personnes concernées.

Pour cela, POST s'engage à prêter une assistance raisonnable dans l'obtention des informations suivantes, devant nécessairement figurer dans la notification du Client :

- Une description de la nature des données concernées par la violation.
- Si possible, les catégories et le nombre approximatif de personnes concernées par la violation, ainsi que les catégories et le nombre approximatif d'enregistrements de données concernés.
- Les conséquences probables de la violation.
- Les mesures prises ou qu'il est proposé par le Client de prendre pour remédier à la violation et/ou en atténuer les éventuelles conséquences négatives.

Lorsqu'il n'est pas possible pour POST de fournir toutes ces informations en même temps au Client, la notification initiale contient les informations disponibles à ce moment-là et, à mesure qu'elles deviennent disponibles, des informations supplémentaires lui seront communiquées dans les meilleurs délais.

3.9.2. Notification en rapport avec les données traitées par POST

En cas de violation de données personnelles en rapport avec les données traitées par POST pour le compte du Client dans le cadre du Contrat, POST s'engage à notifier le Client dans les meilleurs délais après en avoir pris connaissance. Cette notification contient au mois :

- Une description de la nature de la violation constatée.
- Si possible, les catégories et le nombre approximatif de personnes concernées par la violation et d'enregistrements de données à caractère personnel concernés.
- Les coordonnées d'un point de contact chez POST, auprès duquel des informations supplémentaires peuvent être obtenues par le Client au sujet de la violation de données à caractère personnel.

- Les conséquences probables de la violation.
- Les mesures prises ou qu'il est proposé par POST de prendre pour remédier à la violation et/ou en atténuer les éventuelles conséquences négatives.

Lorsqu'il n'est pas possible pour POST de fournir toutes ces informations en même temps au Client, la notification initiale contient les informations disponibles à ce moment-là et, à mesure qu'elles deviennent disponibles, des informations supplémentaires lui seront communiquées dans les meilleurs délais.

3.10. Responsabilité

Conformément à l'article 82 RGPD, POST ne pourra être tenu responsable que du quantum correspondant à sa part de responsabilité dans la réalisation du dommage causé par le traitement et sous réserve que POST n'ait pas respecté les obligations prévues par le RGPD qui incombent spécifiquement aux sous-traitants ou que POST ait agi en-dehors des instructions licites du Client ou contrairement à celles-ci. Faute d'accord entre les Parties sur le quantum de responsabilité des Parties, les Parties soumettent sa détermination à un expert reconnu possédant l'expertise nécessaire (et notamment, de façon non-limitative, dans le domaine de l'IT, de la sécurité, et de la protection des données) aux frais du Client.

3.11. Non-respect des clauses et résiliation

Le Client est en droit de résilier le Contrat dans la mesure où il concerne le traitement de données à caractère personnel conformément aux présentes clauses si :

- (i) POST est en violation grave ou persistante des présentes clauses ou des obligations qui lui incombent en tant que sous-traitant en vertu du RGPD après une mise en demeure non suivie d'effet au-delà d'un (1) mois après sa notification ;
- (ii) POST ne se conforme pas à une décision contraignante d'une juridiction compétente ou de l'autorité de contrôle compétente concernant les obligations qui lui incombent en tant que sous-traitant en vertu des présentes clauses ou du RGPD après une mise en demeure non suivie d'effet au-delà d'un (1) mois après sa notification.

POST est en droit de résilier le Contrat dans la mesure où il concerne le traitement de données à caractère personnel en vertu des présentes clauses lorsque, après avoir informé le Client que ses instructions concernant le traitement de données personnelles constituent une violation de la Loi, le Client insiste pour que les instructions soient suivies.

A la suite de la résiliation du Contrat, POST s'engage, selon le choix du Client :

- (i) à supprimer définitivement toutes les données personnelles traitées pour le compte du Client et certifier auprès du Client que POST a procédé à cette suppression, ou
- (ii) à renvoyer toutes les données personnelles au Client et détruire les copies existantes chez POST, à moins que la Loi n'impose de les conserver plus longtemps.

POST continue de veiller à assurer sa conformité à ses obligations contractuelles en tant que sous-traitant jusqu'à la suppression ou la restitution des données personnelles.