

ANNEXE RELATIVE AU TRAITEMENT DES DONNEES PERSONNELLES (« ADP »)

Aux conditions générales d'adhésion enoprimes (ci-après le "Contrat")

Article 1 – Définition

Les termes définis avec une majuscule tels qu'indiqués dans l'annexe relative à la protection des données personnelles (ci-après désignée l'**Annexe** ou l'**ADP**) ont la signification suivante:

- « **Contrat** » s'entend du contrat intitulé conditions générales d'adhésion enoprimes et ses annexes.
- « **Données Personnelles** » s'entendent des données à caractère personnel telles que définies par l'article 4.1 du RGPD transmises par le Responsable du Traitement au Sous-Traitant en application du Contrat.
- « **Délégué à la protection des données** » ou « **DPD** » s'entend du délégué à la protection des données nommé par le Responsable du Traitement et/ou le Sous-Traitant.
- « **Parties** » désigne à la fois le Responsable du Traitement et le Sous-Traitant.
- « **Personnes Concernées** » s'entendent des personnes physiques dont les Données Personnelles sont traitées par le Sous-Traitant.
- « **Responsable du Traitement** » s'entend de la société Enovos Luxembourg S.A, dont le siège social est établi au 2, domaine du Schlassgoard, L-4327 Esch-sur-Alzette, enregistrée au registre du commerce et des sociétés de Luxembourg, sous le numéro B44683 lequel détermine le but et les moyens du traitement des Données Personnelles.
- « **RGPD** » s'entend du règlement européen 2016/679 du Parlement Européen et du Conseil en date du 27 Avril 2016 portant sur la protection des personnes physiques, en ce qui concerne le traitement de leurs données personnelles et la libre circulation de ces données et abrogeant la Directive 95/46/EC.
- « **Sous-Traitant** » s'entend du Partenaire tel que défini dans le Contrat.
- « **Sous-Traitant Ultérieur** » s'entend de n'importe quel Sous-Traitant engagé par le Sous-Traitant pour effectuer un traitement spécifique des données pour le compte du Responsable du Traitement dans les conditions de l'article 5 de la présente Annexe.

Sauf stipulation contraire dans les présentes, les définitions données par le RGPD, en particulier les termes suivants : « Etat Membre », « violation de Données Personnelles », « Traitement » et « Autorité de Contrôle » sont applicables à la présente Annexe.

Article 2 – Obligation générale de conformité

L'ADP précise les droits et obligations de chacune des Parties dans le cadre du traitement des Données Personnelles.

Le Sous-Traitant accepte et s'engage à se conformer aux lois et réglementations qui régissent le traitement de données personnelles, notamment le RGPD ainsi que toute autre loi nationale applicable ou réglementation régissant le traitement de données personnelles, dans le cadre de l'exécution du Contrat.

Article 3 - Délégués à la protection des données

Le DPD désigné par le Responsable du Traitement peut être contacté aux coordonnées suivantes :

DPD nommé par le Responsable du Traitement
Nom : Brimeyer Michel
Adresse : 2 Domaine du Schlassgoard
L-4327 Esch-sur-Alzette
Téléphone : 2737 6022
Email : dpo@enovos.eu

Article 4 - Description du/des traitement(s) faisant l'objet d'une sous-traitance

Le Sous-Traitant est autorisé à traiter pour le compte du Responsable du Traitement les Données Personnelles nécessaires à la fourniture des service(s)/produit(s) tels que définis par le Contrat, selon la description suivante:

- i. Catégories des Données Personnelles concernées : coordonnées du Client ou personne de contact dans l'entreprise (nom, prénom, adresse, n° de tél, adresse email).
- ii. Objet et nature des opérations réalisées : Gestion de dossiers administratifs dans le cadre de demande de soutien financier - programme enoprimes lié au règlement Grand-Ducal du 7 août 2015 relatif au fonctionnement du mécanisme d'obligations en matière d'efficacité énergétique
- iii. Catégories des Personnes Concernées : Particuliers, professionnels et administrations
- iv. Durée du Traitement : 2 ans après exécution du dernier traitement
- v. Finalité(s) des opérations de Traitement : le traitement sera opéré exclusivement dans le cadre de l'exécution du Contrat auquel il se rattache.

Article 5 - Obligations du Sous-Traitant

Le Sous-Traitant s'engage à respecter les obligations prévues par l'article 28 du RGPD concernant les Données Personnelles et prend notamment les engagements suivants :

- i. Ne pas transférer les Données Personnelles vers un pays situé en dehors de l'Union Européenne, ni à une organisation internationale;
- ii. Stocker les Données Personnelles dans un Etat Membre de l'Union Européenne;
- iii. Traiter les Données Personnelles uniquement pour la/les finalité(s) pour lesquelles elles ont été transmises à l'exception de toute autre finalité ;
- iv. Traiter les Données Personnelles conformément aux instructions documentées du Responsable du Traitement telles que prévues par le Contrat (notamment ne pas vendre, transmettre, donner à bail ou transférer les Données Personnelles à des tiers). Si le Sous-Traitant considère qu'une demande du Responsable du Traitement ou d'un tiers constitue une violation du RGPD ou de toute autre loi ou réglementation applicable en matière de Données Personnelles, il est tenu d'en informer immédiatement le Responsable du Traitement. En outre, si le Sous-Traitant est tenu de transférer des données vers un pays tiers ou une organisation internationale en vertu d'une obligation légale, il devra en informer le Responsable du Traitement avant de procéder au traitement à moins que la loi n'interdise une telle information pour des motifs d'intérêt général ;
- v. Assurer la confidentialité des Données Personnelles traitées dans le cadre du Contrat et prendre toutes les précautions nécessaires au regard de la nature des Données Personnelles et des risques afférant au Traitement ;
- vi. S'assurer que les employés, agents et Sous-Traitant Ultérieurs qui ont accès et/ou sont autorisés ou impliqués dans le Traitement des Données Personnelles se sont engagés à respecter la confidentialité des Données Personnelles dans des

- conditions similaires, ont le niveau de qualification requis et ont reçu une formation appropriée en matière de protection des données;
- vii. Traiter de manière professionnelle et en accord avec les principes propres aux traitements des données personnelles, et plus particulièrement appliquer au sein de son organisation les principes de protection dès la conception et de protection par défaut à l'ensemble de ses outils, produits, applications et services;
 - viii. Fournir à tout moment, au Responsable du Traitement, sur demande de ce dernier et dans un délai raisonnable, toute information nécessaire à l'accomplissement des formalités requises et remettre toute preuve démontrant le respect de ses obligations par rapport à la législation applicable en matière de protection des données personnelles;
 - ix. Ne pas engager de Sous-Traitant(s) Ultérieur(s) pour opérer un traitement spécifique de Données Personnelles sans l'accord préalable et écrit du Responsable du Traitement. L'information fournie au Responsable du Traitement doit inclure une description claire du traitement faisant l'objet d'une sous-traitance, l'identité et les coordonnées du Sous-Traitant Ultérieur. Le Sous-Traitant Ultérieur doit respecter les dispositions de l'ADP et fournir des garanties équivalentes pour assurer la sécurité et la confidentialité des Données Personnelles. Le Sous-Traitant demeure entièrement responsable envers le Responsable du Traitement de l'exécution des obligations du Sous-Traitant Ultérieur en conformité avec le RGPD;
 - x. Dans l'hypothèse où il s'avère que le Sous-Traitant détermine le but et les moyens de traitements opérés sur les Données Personnelles transmises par le Client, il sera considéré comme Responsable du Traitement pour les traitements ainsi opérés et devra à ce titre se conformer aux obligations prévues par le RGPD. Le Responsable du Traitement ne saurait en aucun cas être tenu responsable ou conjointement responsable en cas de manquement à ses obligations par le Sous-Traitant, lorsque ce dernier agit en tant que Responsable du Traitement.

Article 6 - Mesures techniques et organisationnelles requises

Compte tenu de l'état du développement des technologies, des coûts de mise en œuvre de telles mesures et de la nature, de la portée, du contexte et des finalités du traitement ainsi que des risques, dont le degré de probabilité et de gravité varie, pour les droits et libertés des personnes comme le prévoit l'article 32 du RGPD, le Sous-Traitant met en œuvre les mesures techniques et organisationnelles appropriées afin de garantir un niveau de sécurité des Données Personnelles adapté au risque, notamment en fonction des besoins (sans que cette liste soit limitative) :

- (i) La pseudonymisation et le chiffrement des Données Personnelles ;
- (ii) Des moyens permettant de garantir la confidentialité, l'intégrité, la disponibilité et la résilience constante des systèmes et des services de traitement ;
- (iii) Des moyens permettant de rétablir la disponibilité des Données Personnelles et l'accès à celles-ci à bref délai en cas d'incident physique ou technique ;
- (iv) Une procédure visant à tester, à analyser et à évaluer régulièrement l'efficacité des mesures techniques et organisationnelles pour assurer la sécurité du traitement.

Le Sous-Traitant doit évaluer le niveau approprié de sécurité en prenant en compte le risque présenté par le traitement afin d'éviter tout traitement illégal ou non autorisé des Données Personnelles, toute destruction, perte, altération, divulgation, accès non autorisé ou dommage aux Données Personnelles transmises, stockées ou traitées.

Le Sous-Traitant s'engage à s'assurer que chacun des Sous-Traitants Ultérieurs mette en place et maintienne les mesures physiques, techniques et organisationnelles appropriées afin de protéger les Données Personnelles contre les risques susmentionnés.

Article 7 - Droit des Personnes Concernées

Le Responsable du Traitement fournit aux Personnes Concernées les informations nécessaires relatives au traitement de leurs Données Personnelles au moment où les données sont collectées, conformément à la loi applicable.

Le Responsable du Traitement est tenu de gérer les demandes des Personnes Concernées. Les Personnes Concernées s'adresseront au Responsable du Traitement s'ils souhaitent exercer les droits qui leur sont conférés par le RGPD pour des traitements concernant l'ADP (« **Requête des Personnes Concernées** »).

Le Sous-Traitant s'engage à informer le DPD du Responsable du Traitement, par email, dans un délai maximum de quarante-huit (48 heures) de toute requête émanant des Personnes Concernées sans toutefois répondre à de telles requêtes, sauf instruction expresse contraire indiquée par le Responsable du Traitement.

Dans la mesure du possible, le Sous-Traitant s'engage à assister de manière proactive le Responsable du Traitement afin que ce dernier soit en mesure de traiter et répondre aux Requêtes des Personnes Concernées en cas d'exercice par ces derniers de leurs droits, notamment leur droit d'accès, de rectification, droit à l'oubli, droit d'opposition, droit à la limitation des traitements, droit à la portabilité des données et le droit de ne pas être soumis à des décisions individuelles automatisées (incluant le profilage). Le Sous-Traitant devra notamment, conformément aux instructions écrites du Client, corriger, supprimer, bloquer ou modifier le traitement des Données Personnelles et prendre toutes mesures utiles liées aux Requêtes des Personnes Concernées dans l'exercice de leurs droits, conformément à la loi applicable.

Article 8 - Violation des Données Personnelles et Incidents de Sécurité

Les Parties déclarent être parfaitement informées de l'obligation imposée au Client par la réglementation en vigueur d'informer l'Autorité de Contrôle et les Personnes Concernées dans l'hypothèse d'une violation des Données Personnelles. De tels incidents doivent être notifiés au Client, quelle que soit leur origine.

Le Sous-Traitant doit informer le Client à bref délai de tout incident technique, organisationnel ou autre incident (notamment en cas d'incident concernant le(s) Sous-Traitant Ultérieur(s)), ayant engendré ou susceptible d'engendrer une violation des Données Personnelles au sens de l'article 33 du RGPD (« **Incidents de Sécurité** »).

Les Incidents de Sécurité visent notamment les situations suivantes (sans constituer une liste exhaustive) :

- (i) Tout accès non autorisé qu'il soit suspecté ou avéré, toute divulgation, perte, téléchargement, vol, blocage, cryptage, suppression par malveillance ou action non autorisée concernant les Données Personnelles effectuées par des tiers non autorisés ;
- (ii) Tout incident opérationnel avéré ou suspecté ayant un impact sur le traitement des Données Personnelles ;
- (iii) Toute violation avérée ou suspectée de l'ADP ou violation de la loi applicable par le Sous-Traitant, ses salariés ou agents dans la mesure où ce manquement affecte l'intégrité ou la sécurité des Données Personnelles ou affecte de manière substantielle l'exécution des obligations du Sous-Traitant dans le cadre de l'ADP ;
- (iv) Toute requête juridiquement contraignante de divulgation ou la saisie de Données personnelle par la police ou toute autre autorité publique, sauf interdiction du Sous-Traitant de signaler un tel incident au Client en vertu de la loi.

Le Sous-Traitant s'engage à notifier à bref délai les Incidents de Sécurité au Client, par écrit et ce, dans un délai maximum de quarante-huit (48) heures. Cette notification devra être accompagnée de l'ensemble de la documentation utile, pertinente et complète requise par la

loi applicable afin de permettre au Sous-Traitant, si nécessaire, de notifier cette violation à l'Autorité de Contrôle compétente. Des informations complémentaires peuvent être requises au fur et à mesure qu'elles deviennent disponibles.

Le Sous-Traitant s'engage à assister, à première demande, le Responsable du Traitement, et à entreprendre toute action nécessaire pour assurer la conformité au RGPD en cas de violation des Données Personnelles, y compris en ce qui concerne les exigences de notification. Dans l'hypothèse d'une violation des Données Personnelles imputable au Sous-Traitant, ce dernier s'engage à apporter son support sans rémunération supplémentaire.

En cas d'Incident de Sécurité, le Sous-Traitant s'engage, avec l'accord du Responsable du Traitement, à prendre toutes les mesures appropriées pour sécuriser les Données Personnelles non affectées, limiter les conséquences dommageables pour les Personnes Concernées ou potentiellement affectées et mettre en place des mesures préventives pour empêcher tout potentiel Incident de Sécurité à l'avenir.

En cas de violation de la présente ADP, le Sous-Traitant demeure responsable de tout dommage en résultant et de tout dommage résultant du recours à des Sous-Traitants Ultérieurs.

Dans l'hypothèse où, en vertu de la loi applicable, le Sous-Traitant a l'obligation de notifier un Incident de Sécurité à une Autorité de Contrôle, aux Personnes Concernées ou à des tiers (par exemple, si l'Incident de Sécurité engendre une violation de données personnelles au titre de laquelle le Sous-Traitant est responsable en qualité de responsable de traitement), les Parties feront leurs meilleurs efforts pour s'accorder sur une approche commune afin d'éviter que les informations transmises soient contradictoires ou erronées. Cela implique la fourniture réciproque de la documentation nécessaire, en temps utile.

Article 9 - Obligation d'assistance du Sous-Traitant

Le Sous-Traitant s'engage à tenir un registre écrit rassemblant l'ensemble des traitements opérés pour le compte du Client conformément à l'article 30 du RGPD.

Le Sous-Traitant s'engage à assister le Responsable du Traitement sur l'intégralité des domaines pertinents, notamment la conduite d'analyses d'impact relatives à la protection des données (« AIDP ») en application de l'ADP et/ou liées à des requêtes ou des consultations de l'Autorité de Contrôle.

Dans les limites permises par la loi applicable, le Sous-Traitant s'engage à informer immédiatement le Responsable du Traitement de toute requête, demande ou procédure émanant d'une Autorité de Contrôle (Commission Nationale pour la Protection des Données) ou de toute autre autorité publique (tribunaux de justice, police, etc.) concernant les traitements des Données Personnelles effectués directement ou par l'intermédiaire de Sous-Traitants Ultérieurs.

A moins que les lois et réglementations applicables n'en disposent autrement, le Sous-Traitant s'engage à ne pas communiquer d'information concernant le traitement des Données Personnelles à une Autorité de Contrôle ou toute autre autorité publique (y compris les autorités de régulation), sans l'accord exprès du Responsable du Traitement.

Les Parties mettront tout en œuvre pour s'aider mutuellement dans l'hypothèse d'un audit, d'une enquête ou autre procédure lancée par une Autorité de Contrôle ou toute autre administration publique dont la mission est liée au traitement de Données Personnelles.

Article 10 - Restitution et suppression des Données Personnelles

Conformément au principe de limitation de traitement prévu par le GDPR et lorsqu'elles ne sont plus nécessaires à l'exécution du Contrat, le Sous-Traitant s'engage, à la discrétion du Responsable de Traitement, à (i) renvoyer au Responsable du Traitement les Données Personnelles et les résultats du Traitement dans un format structuré, communément utilisé, lisible par machine et interopérable et/ou, ii) s'assurer, sous réserve du consentement préalable du Responsable du Traitement que les Données Personnelles, y compris les copies existantes, sont détruites/effacées de manière sécurisée et efficace, sauf si le Sous-Traitant peut démontrer qu'il existe une obligation légale ou réglementaire l'obligeant à conserver tout ou partie des Données Personnelles pour une période plus longue.

Après réalisation, le Sous-Traitant s'engage à confirmer par écrit de manière suffisamment détaillée au Responsable du Traitement la restitution et/ou la destruction des Données Personnelles.

Article 11 - Pouvoir de contrôle du Responsable du Traitement

Le Sous-Traitant s'engage à fournir dans un délai raisonnable au Responsable du Traitement l'ensemble de la documentation nécessaire démontrant le respect des obligations résultant de l'ADP, autoriser et contribuer à tout audit relatif au traitement des Données Personnelles.

Le Sous-Traitant autorise le Responsable du traitement à procéder à des inspections ou des audits sur les sites où sont traités les données aux fins d'inspecter, contrôler ou examiner le traitement des Données Personnelles, sous réserve d'une notification écrite préalable adressée vingt (20) jours calendaires à l'avance. A la demande du Responsable du Traitement, les audits pourront être effectués par tout moyen électronique (par exemple sous forme de data-room électronique). Le Sous-Traitant s'engage à donner accès à toutes les informations et documents relatifs à la protection des Données Personnelles, notamment au registre de traitement, aux données stockées et aux programmes de traitement des données nécessaires dans le cadre de ces contrôles, inspections et vérifications. Cet audit sera effectué soit par le Responsable du Traitement, soit par ses représentants, consultant ou auditeur dûment mandatés.

Le Sous-Traitant s'engage à coopérer et à contribuer de la manière efficace à ces audits. Si la décision de mener un audit est motivée par un manquement ou une violation de ses obligations de la part du Sous-Traitant ou si le Responsable du Traitement a des motifs légitimes, exposés par écrit, de suspecter une violation de ses obligations par le Sous-Traitant, les coûts générés par l'audit seront supportés par le Sous-Traitant.

Article 12 - Période de rétention des données des employés, agents et Sous-Sous-Traitant des Parties

Chaque Partie s'engage (i) à conserver les Données Personnelles relatives aux employés, agents et Sous-Traitants Ultérieurs respectifs qui auraient pu être transmises lors de la préparation et l'exécution du Contrat jusqu'à l'expiration du délai de prescription légal en vigueur conformément à la loi applicable et (ii) à supprimer ces Données à l'expiration de cette période de conservation.

Article 13. Dispositions diverses

En cas de conflit ou d'incompatibilité entre l'ADP et le Contrat, les dispositions de l'ADP prévaudront sur le Contrat uniquement en ce qui concerne le traitement des données. Les autres dispositions du Contrat resteront pleinement en vigueur.

En cas d'invalidité ou de disposition inapplicable de la présente ADP, la clause litigieuse n'affectera pas la validité de l'ADP dans sa totalité et ne remettra pas en cause les autres dispositions qui demeureront applicables. En cas d'invalidité ou de disposition inapplicable de la présente ADP, la clause litigieuse sera modifiée si cela s'avère nécessaire afin de garantir sa validité et son application tout en préservant, dans la mesure du possible, l'intention des Parties ou, si cela n'est pas possible, (ii) la disposition invalide ou inapplicable sera réputée non-écrite.

Date de dernière mise à jour du document : 25 septembre 2020