



Accord de coopération sur le terrain

CONDITIONS DE PROTECTION DES DONNÉES DU PAM DE L'ACCORD DE COOPERATION SUR LE TERRAIN

Les présentes conditions de protection des données (« **Conditions** ») régissent le traitement des données à caractère personnel dans le cadre de l'Accord. Tous les termes non définis dans les présentes auront la signification indiquée dans le présent Accord.

1. DÉFINITIONS

- 1.1 « **Responsable du traitement** » désigne la personne physique ou morale (y compris une autorité publique, une agence, une ONG ou un autre organisme) qui, seule ou conjointement avec d'autres, détermine les finalités et les moyens du traitement des Données à caractère personnel. Aux fins des présentes Conditions, le PAM agit en tant que Responsable du traitement de toutes les données à caractère personnel traitées dans le cadre du présent Accord.
- 1.2 « **Données à caractère personnel** » désigne toute information liée à une personne physique identifiée ou identifiable (chacune, une « **Personne concernée** »); une personne physique identifiable est une personne qui peut être identifiée directement ou indirectement, notamment par référence à un identifiant tel qu'un nom, un numéro d'identification, des données de localisation, un identifiant en ligne ou à un ou plusieurs éléments propres à l'état physique, physiologique, génétique, l'identité mentale, économique, culturelle ou sociale de cette personne physique. Les Données à caractère personnel couvrent les informations numériques et non numériques qui sont fournies au Sous-traitant ou à ses Sous-traitants ultérieurs par ou au nom du Sous-traitant ou qui sont obtenues par le Sous-traitant ou ses Sous-traitants ultérieurs en lien avec les activités du Sous-traitant en vertu du présent Accord.
- 1.3 « **Traiter** » ou « **traitement** » (ou toute variante de ces termes) désigne toute opération ou ensemble d'opérations effectuées sur des Données à caractère personnel, que ce soit ou non par des moyens automatiques, telles que la visualisation, l'accès, la collecte, l'enregistrement, l'organisation, le stockage, l'adaptation ou modification, la récupération, la consultation, l'alignement, la combinaison, le blocage, la suppression ou la destruction des Données à caractère personnel. Cela inclut également la divulgation par transmission, anonymisation, diffusion ou toute autre forme de mise à disposition de Données à caractère personnel.
- 1.4 « **Règles de confidentialité** » désigne, telles qu'en vigueur de temps à autre, en relation avec le traitement des Données à caractère personnel, les règles, principes et lignes directrices applicables en matière de protection des données du Responsable du traitement (réf. Circulaire du directeur exécutif OED 2024/002, telle que modifiée de temps à autre, et toute politique connexe du PAM) et, exclusivement en ce qui concerne le Sous-traitant, également toutes les lois et réglementations sur la protection des données et la sécurité des informations applicables au Sous-traitant et/ou à tout sous-traitant ultérieur.
- 1.5 « **Sous-traitant** » désigne une personne physique ou morale (y compris une autorité publique, une agence, une ONG ou un autre organisme) qui traite des Données à caractère

personnel pour le compte du Responsable du traitement. Le Partenaire coopérant agit en tant que Sous-traitant de toutes les Données à caractère personnel traitées dans le cadre du présent Accord.

- 1.6 « **Incidents de confidentialité** » désigne tout élément réel ou raisonnablement soupçonné : (1) accès non autorisé ou vol de Données à caractère personnel ; (2) utilisation non autorisée de Données à caractère personnel par une personne ayant un accès autorisé à ces Données à caractère personnel ; (3) divulgation ou modification non autorisée de Données à caractère personnel ; (4) destruction accidentelle ou illégale de Données à caractère personnel ; ou (5) perte de Données à caractère personnel, dans chaque cas par le Sous-traitant ou ses Sous-traitants ultérieurs.
- 1.7 « **Représentants** » désigne, en ce qui concerne le Sous-traitant et tout Sous-traitant ultérieur, les administrateurs, dirigeants, employés, personnel et sociétés affiliées de cette partie, qui sont impliqués dans la mise en œuvre des activités convenues dans le cadre du présent Accord en ce qui concerne les données à caractère personnel. Le Sous-traitant assumera l'entière responsabilité légale des actes et/ou omissions de ses Représentants et des Représentants de son Sous-traitant ultérieur en relation avec les présentes Conditions.
- 1.8 « **Sécurité** » désigne les contrôles technologiques, physiques et administratifs (y compris, mais sans s'y limiter, les politiques, procédures, structures organisationnelles, fonctions matérielles et logicielles) et les mesures de sécurité physique, dont le but est, en tout ou partie, d'assurer la confidentialité, l'intégrité et la disponibilité des Données à caractère personnel.
- 1.9 « **Sous-traitant ultérieur** » désigne tout prestataire ou agent du Sous-traitant, qui contribue aux activités de Traitement des Données à caractère personnel du Responsable du traitement en vertu du présent Accord.

2. FINALITÉS

- 2.1 Le PAM autorise par la présente le Sous-traitant à traiter certains types et catégories de Données à caractère personnel comme spécifié dans l'Accord et/ou demandé par le PAM, au nom du PAM. Un tel traitement est nécessaire à l'exécution de l'Accord par le Sous-traitant. Le Sous-traitant ne traitera que les Données à caractère personnel strictement nécessaires à l'exécution des activités décrites dans l'Accord et uniquement pendant sa durée, sauf convention contraire expresse par écrit avec le Responsable du traitement.
- 2.2 Le Sous-traitant garantit qu'il dispose d'une expertise et de compétences suffisantes pour mener les activités de traitement de données spécifiques assumées dans le cadre du présent Accord, et qu'il a mis en place des mesures techniques et organisationnelles appropriées pour se conformer aux Règles de confidentialité.

3. TRAITEMENT DES DONNÉES A CARACTERE PERSONNEL

- 3.1 Le Sous-traitant s'engage et accepte de traiter les Données à caractère personnel conformément aux Règles de confidentialité et aux présentes Conditions. Plus précisément, le Sous-traitant doit : (i) agir uniquement conformément aux instructions écrites du Responsable du traitement pour exécuter de manière adéquate les activités en vertu du présent Accord ; (ii) traiter les Données à caractère personnel uniquement dans le but de remplir ses obligations en vertu du présent Accord ; (iii) s'abstenir d'appliquer ou utiliser les Données à caractère personnel à des fins autres que celles énoncées dans le présent Accord ; (iv) s'abstenir d'utiliser les Données à caractère personnel traitées pour le compte du Responsable du traitement à ses propres fins commerciales ; (v) informer

- immédiatement le Responsable du traitement par écrit si, à son avis, une instruction fournie par le Responsable du traitement enfreint les Règles de confidentialité ; (vi) informer immédiatement le Responsable du traitement en cas de manquement à ses obligations en vertu des présentes Conditions ; et (vii) garder confidentielles et ne pas divulguer, donner accès ou partager les Données à caractère personnel avec un tiers (y compris les Sous-traitants ultérieurs) sauf autorisation expresse écrite du Responsable du traitement et uniquement dans le respect des Règles de confidentialité.
- 3.2 À la demande du Responsable du traitement, le Sous-traitant doit informer de manière claire et transparente les Personnes concernées sur le traitement de leurs Données à caractère personnel conformément aux instructions fournies par le Responsable du traitement et en conserver la preuve de la manière spécifiée par le Responsable du traitement.
- 3.3 Le Sous-traitant doit mettre en œuvre et maintenir toutes les mesures techniques et organisationnelles appropriées nécessaires pour assurer la sécurité des Données à caractère personnel qu'il traite afin d'éviter leur altération, perte, traitement ou accès non autorisé, compte tenu de l'état de la technologie, de la nature des Données à caractère personnel stockées et des risques auxquelles elles sont exposées, qu'ils soient d'origine humaine, environnementale ou naturelle. Les mesures de sécurité doivent être conformes aux Règles de confidentialité, aux normes de sécurité internationales pertinentes et au moins conformes à l'Annexe sur la sécurité des informations ci-jointe.
- 3.4 Le Sous-traitant doit conserver un dossier écrit de toutes les activités de traitement effectuées au nom du Responsable du traitement. Ce dossier doit contenir au moins (i) le nom et les coordonnées du Sous-traitant et de ses Sous-traitants ultérieurs pour le présent Accord spécifique ; (ii) les types d'activités de traitement effectuées pour le compte du Responsable du traitement, (iii) la ou les finalités de son traitement, (iv) la description des catégories de Personnes concernées et des Données à caractère personnel traitées ; (v) lorsque cela est autorisé, les transferts de Données à caractère personnel vers un pays tiers, et (vi) une description générale des mesures de sécurité techniques et organisationnelles mises en œuvre.
- 3.5 Le Sous-traitant communiquera les Données à caractère personnel aux autres Sous-traitant du Responsable du traitement conformément aux instructions écrites du Responsable du traitement.
- 3.6 Le Sous-traitant ne procédera à aucun transfert de Données à caractère personnel traitées pour le compte du Responsable du traitement vers un pays tiers sans l'autorisation écrite préalable du Responsable du traitement (y compris, sans s'y limiter, les transferts liés aux services basés sur le cloud).
- 3.7 Le Sous-traitant reconnaît qu'il n'a aucun droit de propriété sur les Données à caractère personnel qu'il traite.

4. SÉCURITÉ ET CONFIDENTIALITÉ

- 4.1 Les obligations de confidentialité conformément à la section 3.1 (vii) et à la présente section 4 prévaudront indéfiniment, même après l'expiration ou la résiliation du présent Accord. Le Sous-traitant peut fournir l'accès aux Données à caractère personnel à ses Représentants uniquement dans la mesure où cet accès est raisonnablement nécessaire à l'exécution des obligations du Sous-traitant en vertu de l'Accord, à condition que : (i) ce Représentant soit soumis à des obligations non moins onéreuses que les exigences énoncées dans les présentes conditions et l'Annexe sur la sécurité des informations, et (ii) avant d'accorder un tel accès, le Sous-traitant se soit assuré que ces exigences et les conséquences de leur non-respect sont comprises et suivies par ces Représentants.

- 4.2 Le Sous-traitant doit garantir que la Sécurité est mise en œuvre, maintenue et appliquée pour protéger les Données à caractère personnel contre les Incidents de confidentialité tout au long de la période de traitement des Données à caractère personnel dans le cadre du présent Accord. La Sécurité doit, sans limitation, être à jour et conforme aux Règles de confidentialité, aux normes industrielles pertinentes et à l'Annexe sur la sécurité des informations ci-jointe. Le plus grand soin sera également apporté à la sécurité physique. Le Sous-traitant évaluera régulièrement ses systèmes de sécurité. Cette évaluation doit être menée conformément aux normes industrielles internationales pertinentes et aux meilleures pratiques. Le Sous-traitant doit rapidement, sur demande écrite du Responsable du traitement, fournir au Responsable du traitement les résultats de cette ou ces évaluations.

5. DEMANDE DES PERSONNES CONCERNÉES ET DE TIERS

- 5.1 Le Sous-traitant coopérera avec le Responsable du traitement pour répondre à toute demande reçue d'individus qui exercent leurs droits en vertu des Règles de confidentialité, y compris, sans limitation, les demandes d'accès, de correction, de suppression ou tout autre droit, le cas échéant, concernant les Données à caractère personnel contenues dans le dossier sous la garde du Sous-traitant et du Sous-traitant ultérieur (chacune, une « Demande d'accès »). Cette coopération comprendra, sans limitation :
- a) d'informer le Responsable du traitement dans les 5 jours ouvrables suivant la réception d'une telle demande par courrier électronique détaillant (i) le type de demande, (ii) la date de réception, (iii) l'impact et la faisabilité
 - b) de consulter le PAM avant de prendre toute mesure en conséquence ou en relation avec une telle demande d'accès et
 - c) de répondre à cette demande d'accès en suivant les instructions raisonnables du Responsable du traitement.
- 5.2 Conformément aux conventions, accords et lois référencés à l'article 15 des Conditions Générales, les Données à caractère personnel soumises au présent Accord bénéficient de privilèges et d'immunités. Dans le cas où le Sous-traitant ou un Sous-traitant ultérieur reçoit une demande ou une ordonnance de divulgation de Données à caractère personnel, sous quelque forme que ce soit, de la part d'une autorité gouvernementale, le Sous-traitant devra immédiatement (mais en aucun cas plus de 24 heures après avoir reçu cette demande) informer le Responsable du traitement par écrit par courrier électronique. Cette notification doit inclure une copie de la demande ou de la commande. Le Sous-traitant s'abstiendra (et sera responsable que le Sous-traitant ultérieur s'abstienne) d'accorder l'accès demandé ou la divulgation des Données à caractère personnel, sauf autorisation écrite du Responsable du traitement.
- 5.3 Le Sous-traitant doit désigner un délégué à la protection des données (DPO) et/ou une personne de contact et informer le Responsable du traitement de son nom, de son titre et de ses coordonnées.

6. NOTIFICATION D'INCIDENTS DE CONFIDENTIALITÉ

- 6.1 Le Sous-traitant doit former tous ses Représentants et Sous-traitants ultérieurs pour identifier et répondre à un Incident de confidentialité.
- 6.2 Le Sous-traitant doit également prendre toutes les mesures nécessaires pour prévenir, contenir et atténuer l'impact d'un tel Incident de confidentialité.

- 6.3 Le Sous-traitant mènera immédiatement une enquête interne raisonnable sur les raisons et les circonstances entourant l'Incident de confidentialité et mettra en œuvre les actions préventives et correctives nécessaires pour en atténuer l'impact. Le Sous-traitant doit également collecter et conserver toutes les preuves concernant la découverte, la cause, la vulnérabilité, l'exploitation, les mesures correctives et l'impact liés à un tel Incident de confidentialité.
- 6.4 Le Sous-traitant doit fournir une notification écrite au Responsable du traitement dans les plus brefs délais par courrier électronique, mais au plus tard vingt-quatre (24) heures après que le Sous-traitant a découvert ou pris connaissance d'un Incident de confidentialité, accompagné au moins des informations suivantes :
- a) une description de la nature de l'Incident de confidentialité, y compris, dans la mesure du possible, les catégories et le nombre approximatif de personnes concernées, ainsi que les catégories et le nombre approximatif d'enregistrements de Données à caractère personnel impliqués; le moment (heure de l'Incident) et le lieu de l'Incident ;
 - b) le nom et les coordonnées du point de contact auprès duquel de plus amples informations peuvent être obtenues ;
 - c) une description des conséquences possibles de l'Incident de confidentialité; et
 - d) une description des mesures adoptées ou proposées pour remédier à l'Incident de confidentialité, y compris, le cas échéant, les mesures adoptées pour atténuer tout effet négatif possible.

En outre, il fournira des rapports écrits périodiques sur l'état/les activités réalisées concernant les mesures d'atténuation et correctives liées à chaque Incident de confidentialité, ainsi que tous les documents et/ou informations raisonnablement demandés par le Responsable du traitement concernant cet Incident de confidentialité. Lorsque les informations ne peuvent pas être fournies rapidement et simultanément, toutes les informations disponibles sont fournies progressivement mais sans retard injustifié.

- 6.5 Le Sous-traitant s'abstient de toute communication concernant ou en référence à l'Incident de confidentialité à : (i) toute Personne concernée dont les Données à caractère personnel ont été ou pourraient avoir été affectées ; (ii) toute autorité de protection des données à laquelle le Sous-traitant peut être soumis ; ou (iii) aux médias et au grand public, sans avoir convenu d'une telle communication avec le PAM.

7. SOUS-TRAITANCE

- 7.1 Chaque Sous-traitant ultérieur est un « sous-traitant » tel que mentionné à l'article 16.7 des Conditions générales du PAM de l'Accord. Le Responsable du traitement peut révoquer son approbation de retenir un Sous-traitant ultérieur à tout moment par notification.
- 7.2 Le Sous-traitant doit s'assurer que tous les Sous-traitants ultérieurs autorisés sont contractuellement liés à des obligations qui sont substantiellement similaires, mais non inférieures, à celles imposées au Sous-traitant en vertu de l'Accord et des présentes Conditions.

8. INDEMNISATION

- 8.1 Le Sous-traitant indemnifiera et dégagera le Responsable du traitement de toute

responsabilité, dans le cas où un tiers intenterait une réclamation envers le Responsable du traitement à la suite d'un acte ou d'une omission négligente ou intentionnelle du Sous-traitant (y compris ses Représentants, Sous-traitants ultérieurs et leurs Représentants) en ce qui concerne tout traitement décrit dans l'Accord.

9. RÉSILIATION, ANNULATION ET EXTINCTION

9.1 Sauf indication contraire dans les présentes, lors de la résiliation, de l'annulation ou de l'extinction de la relation contractuelle entre le Responsable du traitement et le Sous-traitant, ce dernier doit immédiatement restituer et/ou supprimer toutes les Données à caractère personnel traitées par le Sous-traitant et ses Représentants de tous les systèmes, appareils et des sources papier ou toute autre source et devra envoyer un certificat écrit confirmant cette destruction et cette suppression au Responsable du traitement une fois réalisée.

10. SURVIE

10.1 Les dispositions des présentes Conditions resteront en vigueur après la résiliation ou l'expiration de l'Accord, conformément à l'article 17.4 des Conditions générales du PAM.

ANNEXE SUR LA SÉCURITÉ DE L'INFORMATION

La présente Annexe sur la sécurité des informations fait partie intégrante de l'Accord auquel elle est annexée.

En plus des exigences énoncées dans l'Accord, le Sous-traitant doit :

1. se conformer aux instructions du PAM sur la sécurité informatique et accepter d'être soumis aux examens et/ou audits de sécurité des informations du PAM, sur demande.
2. Posséder pendant toute la durée de l'Accord :
 - 2.1. un programme documenté de sécurité des informations basé sur un ou plusieurs des cadres de sécurité des informations standard suivants : ISO, NIST, ISACA, COBIT ; ou
 - 2.2. mettre en œuvre les contrôles de sécurité appropriés pour le traitement des Données à caractère personnel et fournir au PAM, lors de la signature de l'Accord, une description de ces Contrôles de sécurité, qui comprendra au moins :
 - a) la pseudonymisation et le cryptage des Données à caractère personnel ;
 - b) la capacité d'assurer la confidentialité, l'intégrité et la disponibilité continues des systèmes et services de traitement ;
 - c) un processus permettant de tester, d'analyser et d'évaluer régulièrement l'efficacité des contrôles de sécurité mis en œuvre ;
 - d) le rétablissement rapide de la disponibilité et de l'accès aux Données à caractère personnel en cas d'Incident de confidentialité ; et
 - e) la vérification, l'évaluation et l'appréciation régulières des contrôles de sécurité. Ces mesures doivent au moins comprendre des mécanismes pour :
 1. appliquer l'authentification multifacteur pour tout accès utilisateur aux Données à caractère personnel ;
 2. assurer le cryptage de tous les appareils, y compris les appareils mobiles, les fichiers des appareils de stockage et les bases de données contenant des Données à caractère personnel, et crypter toutes les communications entre le PAM et le Sous-traitant, entre les Représentants du Sous-traitant, entre le Sous-traitant et tous les tiers (y compris Ses sous-traitants) ;
 3. veiller à ce que tous les fichiers et bases de données contenant des Données à caractère personnel soient sauvegardés quotidiennement et que les informations papier soient dûment sécurisées dans des locaux protégés ;
 4. maintenir un cadre de gouvernance des données en fonction des risques des informations consultées ;
 5. appliquer les contrôles d'accès au système, y compris l'octroi de l'accès aux utilisateurs, la recertification des accès, la révocation de l'accès des utilisateurs, l'accès administratif et la gestion des accès des utilisateurs administratifs ;
 6. veiller à ce que des contrôles d'accès/transmission/entrée/disponibilité/intégrité/ségrégation des données soient en place ; et
 7. mettre en place des contrôles d'accès physique et garantir que les mesures de sécurité physique, en particulier celles visant à protéger les Données à caractère personnel sur papier et tout autre actif physique hébergeant des Données à caractère personnel soumises à l'application du présent FLA, sont en place et sont adaptées au niveau de risque de la sécurité évaluée.