

ANNEXE 1 RGPD - PROTECTION DES DONNEES PERSONNELLES

I. Définitions :

Les termes...

« **Responsable de Traitement** » : désigne 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; lorsque les finalités et les moyens de ce Traitement sont déterminés par le droit de l'Union ou le droit d'un État membre, le responsable du Traitement peut être désigné ou les critères spécifiques applicables à sa désignation peuvent être prévus par le droit de l'Union ou par le droit d'un État membre. Pour le présent marché, le responsable de traitement au sens du RGPD est Inria.

« **Titulaire** » : désigne la personne physique ou morale, l'autorité publique, le service ou un autre organisme qui traite des Données Personnelles pour le compte, sur instruction et sous l'autorité d'Inria.

« **Destinataire** » : désigne la personne physique ou morale, l'autorité publique, le service ou tout autre organisme qui reçoit communication de Données Personnelles, qu'il s'agisse ou non d'un tiers ;

« **Données Personnelles** » ou « **Données à caractère personnel** » : désigne toute information se rapportant à une personne physique identifiée ou identifiable, 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 spécifiques propres à son identité physique, physiologique, génétique, psychique, économique, culturelle ou sociale ;

« **Finalité(s)** » : désigne l'objectif principal d'un traitement de données à caractère personnel ;

« **Personne concernée** » : désigne les personnes physiques identifiables ou identifiées dont les Données Personnelles sont collectées et intégrées dans le Traitement ;

« **Autorité(s) de contrôle** » : désigne l'(les) autorité(s) publique(s) indépendante(s) instituée(s) par chaque État membre chargée(s) de surveiller l'application du Règlement Européen sur la Protection des Données, afin de protéger les libertés et droits fondamentaux des personnes physiques à l'égard du traitement et de faciliter le libre flux des Données Personnelles au sein de l'Union européenne ;

« **Analyse d'impact** » : désigne un processus dont l'objet est de décrire le Traitement de données à caractère personnel, d'en évaluer la nécessité ainsi que la proportionnalité et d'aider à gérer les risques pour les droits et libertés des personnes physiques liés au Traitement de leurs données à caractère personnel, en les évaluant et en déterminant les mesures nécessaires pour y faire face ;

« **Traitement de données à caractère personnel** » ou « **Traitement** » : désigne toute opération ou ensemble d'opérations portant sur des Données Personnelles, quel que soit le procédé utilisé telles que la collecte, l'enregistrement, l'organisation, la conservation, l'adaptation ou la modification, l'extraction, la consultation, l'utilisation, la communication par transmission, diffusion ou toute autre forme de mise à disposition, le rapprochement ou l'interconnexion, ainsi que le verrouillage, l'effacement ou la destruction ;

« **Violation** » : désigne une faille de la sécurité entraînant, de manière accidentelle ou illicite, la destruction, la perte, l'altération, la divulgation non autorisée de Données Personnelles transmises, conservées ou traitées d'une autre manière, ou l'accès non autorisé à de telles Données Personnelles ;

« **Transfert** » : désigne toute communication, copie ou déplacement de Données Personnelles ayant vocation à être traitées dans un pays tiers à l'Union européenne et n'ayant pas un niveau de protection adéquat ou dans une organisation internationale.

« **Règlement européen sur la Protection des Données** » : désigne le règlement (UE) 2016/679 du parlement européen et du conseil du 27 avril 2016 applicable à compter du 25 mai 2018 ;

« **Marché** » : désigne le marché de support et maintenance des logiciels de contrôle des accès SIMON VOSS.

« **Délégué** » : désigne le (la) délégué(e) à la protection des Données Personnelles tel que défini par la section 8 du Règlement européen sur la Protection des Données.

II. Objet

L'Annexe 1 Protection des Données Personnelles (ci-après « l'Annexe ») a pour objet de définir les conditions dans lesquelles le Titulaire s'engage à effectuer, dans le cadre du Marché auquel elle se rattache, pour le compte, sur instruction et sous l'autorité d'Inria, les opérations de Traitement définies ci-après (en III).

Dans le cadre de leurs relations contractuelles, les Parties s'engagent à respecter la réglementation en vigueur applicable au Traitement de données à caractère personnel et, en particulier, le Règlement Européen sur la Protection des Données.

III. Description du Traitement faisant l'objet du Marché

Le Titulaire est autorisé à traiter pour le compte d'Inria et d'après ses instructions, les Données Personnelles nécessaires pour fournir le ou les services suivants : **identification des agents Inria.**

La nature des opérations réalisées sur les Données Personnelles : **identification des agents Inria.**

- Nom ;
- Prénom ;
- Adresse mail ;
- Numéro de téléphone ;
- Nom de l'entreprise.

La Finalité du Traitement est : **identification des agents Inria.**

La durée du Traitement est conditionnée à la durée du marché.

Les catégories de Personnes concernées sont : l'ensemble des collaborateurs Inria.

Pour l'exécution du service objet du Marché, Inria peut être amené à mettre disposition du Titulaire les informations nécessaires suivantes : nom, prénom, e-mail des agents.

IV. Obligations du Titulaire vis-à-vis d'Inria

- 1)** Conformément au Règlement Européen sur la Protection des Données, Inria agit en qualité de Responsable de Traitement et le Titulaire agit exclusivement pour le compte d'Inria en qualité de Sous-traitant sur la base des stipulations du Marché ainsi que des seules instructions d'Inria et conformément à ces dernières.
- 2)** Le Titulaire comprend et reconnaît que les Données Personnelles constituent des informations confidentielles et qu'il n'acquerra pas de droit de propriété ou autre sur les Données Personnelles.
- 3)** Le Titulaire s'engage à :

- a) **TRAITEMENT DES DONNES A CARACTERE PERSONNEL**

Collecter ou à traiter les Données Personnelles pendant la durée du Marché uniquement pour la ou les seule(s) Finalité(s) qui fait/font l'objet du Marché et ce, conformément aux stipulations du Marché, aux instructions d'Inria et au Règlement Européen sur la Protection des Données. Les Données Personnelles ne peuvent pas être utilisées par le Titulaire dans un but autre que celui de fournir les prestations à Inria. Elles ne peuvent être divulguées, transférées, louées ni d'une quelconque manière cédées ou exploitées commercialement ou non par le Titulaire sans l'accord préalable et écrit d'Inria. Si le Titulaire considère qu'une instruction constitue un manquement au Règlement Européen sur la Protection des Données, il en informe immédiatement Inria. En cas de modification du Règlement Européen sur la Protection des Données Personnelles ayant une incidence sur la conformité à la loi du Traitement réalisé dans le cadre du Marché, le Titulaire s'engage à en informer immédiatement Inria et à y remédier en apportant aux prestations les adaptations nécessaires au respect des nouvelles dispositions législatives/réglementaires applicables, sans surcoût pour Inria.

- b) **OBLIGATION D'INFORMATION**

Fournir toutes informations utiles à Inria sur ses activités de Traitements (usage, stockage et pays d'origine des Données Personnelles) et assister Inria afin que celui-ci puisse procéder aux notifications à l'Autorité de contrôle compétente qui lui incombent en sa qualité de Responsable de Traitement et afin que celui-ci puisse également fournir l'information aux Personnes concernées par les opérations de Traitement au moment de la collecte des Données Personnelles ;

- c) **OBLIGATION DE SECURITE**

Mettre en place et maintenir pendant toute la durée du Marché toutes les mesures techniques et organisationnelles adaptées à la nature des Données Personnelles traitées et aux risques présentés par le Traitement (i) pour assurer la pseudonymisation et le chiffrement des Données à caractère personnel (ii) pour assurer la confidentialité, la disponibilité, la résilience et l'intégrité constantes des systèmes de Traitement de données à caractère personnel , et (iii) pour rétablir la disponibilité des Données à caractère personnel et l'accès à celles-ci dans des délais appropriés en cas d'incident physique ou technique (iv) pour tester, analyser et évaluer régulièrement l'efficacité des mesures techniques et organisationnelles pour assurer la sécurité du Traitement.

d) PROTECTION DES DONNEES A CARACTERE PERSONNEL

Prendre en compte les principes de protection et de minimisation des Données Personnelles dès la conception d'outils, produits, applications ou services.

e) SOUS-TRAITANCE

A ne pas sous-traiter tout ou partie de l'exécution du Traitement de Données Personnelles sans avoir obtenu d'Inria l'acceptation de chaque sous-traitant, conformément au présent Marché.

En cas d'accord d'Inria, le Titulaire s'engage à :

-sélectionner un sous-traitant présentant des garanties suffisantes quant à la mise en œuvre de mesures techniques et organisationnelles appropriées de manière à ce que le Traitement réponde aux exigences du Règlement Européen sur la Protection des Données et de l'Annexe ;

-signer avec le sous-traitant un contrat de sous-traitance faisant référence à l'Annexe et imposant au sous-traitant les mêmes obligations en matière de protection des Données Personnelles que celles fixées dans l'Annexe.

En cas de changement prévu concernant l'ajout ou le remplacement des sous-traitants, le Titulaire doit recueillir l'autorisation écrite, préalable et spécifique d'Inria.

Le Titulaire demeure pleinement responsable vis-à-vis d'Inria et des tiers des actes du sous-traitant. Il appartient donc au Titulaire de prendre les mesures nécessaires afin de garantir le respect par le sous-traitant des dispositions du Règlement Européen sur la Protection des Données, Inria n'ayant aucun contrôle sur les sous-traitants.

f) FLUX TRANSFRONTALIERS

Traiter les Données à caractère personnel uniquement dans l'Union Européenne et à ne pas procéder ou faire procéder à des Transferts en dehors de l'Union Européenne.

g) CONFIDENTIALITÉ RENFORCÉE

Veiller à ce que ses employés, préposés, mandataires et les sous-traitants ou toute personne agissant pour son compte, qui ont accès aux Données Personnelles soient dûment autorisés, respectent les obligations du Titulaire conformément à l'Annexe et que ces personnes soient particulièrement formées et sensibilisées aux règles encadrant la protection des Données à caractère personnel et les traitent conformément à ladite Annexe.

Le Titulaire s'engage notamment à faire signer par toutes les personnes susceptibles d'accéder aux Données Personnelles dans le cadre du Marché un engagement individuel de confidentialité. Un modèle d'engagement individuel de confidentialité figure en sous-Annexe 1.

Le Titulaire doit être en mesure de confirmer le respect de cette obligation auprès d'Inria, à première demande, en communiquant la liste des personnes susceptibles d'accéder aux Données Personnelles, accompagnée de l'engagement de confidentialité signé par lesdites personnes.

Le Titulaire s'engage à former les personnes susceptibles d'accéder aux Données Personnelles dans le cadre du Marché sur les mesures de sécurité à mettre en œuvre.

Le Titulaire s'engage à ce que les éventuels sous-traitants ultérieurs soient également tenus par ces obligations spécifiques et soient en mesure d'en justifier auprès d'Inria à première demande.

h) DEMANDES D'EXERCICE DES DROITS DES PERSONNES CONCERNÉES

Informez sans délai Inria de toute requête et toute demande ou notification de la Personne concernée d'exercer ses droits en vertu du Règlement Européen sur la Protection des Données Personnelles, sans y répondre, et appliquer les instructions d'Inria concernant une telle requête, demande ou notification. Le Titulaire doit s'assurer que les sous-traitants transmettront immédiatement les requêtes, demandes ou notifications à Inria qu'ils reçoivent directement, sans y répondre.

Le Titulaire coopérera avec Inria sans délai et lui fournira les informations nécessaires afin de permettre à Inria de répondre aux Personnes concernées et notamment de respecter les droits des Personnes concernées (droit d'accès, de modification, d'opposition, à la portabilité, etc.) tels que prévus par le Règlement Européen sur la Protection des Données et afin que les Données à caractère personnel traitées soient adéquates ;

i) DROITS DES PERSONNES CONCERNÉES

De mettre en œuvre sans délai toute demande d'Inria concernant les droits des Personnes concernées relatifs aux Données à caractère personnel traitées par le Titulaire dans le cadre du Marché (droit à la portabilité, la modification, la correction ou la suppression, droit d'opposition, etc.) ;

j) DUREE DE CONSERVATION

Ne pas conserver les Données à caractère personnel au-delà de la durée de conservation fixée par Inria et en tout état de cause à ne pas les conserver après la fin du Marché sauf obligation légale auquel cas le Titulaire s'engage à archiver les Données Personnelles et à détruire ou restituer lesdites Données Personnelles dès la fin de l'obligation légale.

k) REGISTRE DES OPERATIONS DE TRAITEMENT

Tenir un registre de toutes les catégories d'activités de Traitements de données à caractère personnel effectués pour le compte d'Inria contenant : (i) le nom et les coordonnées d'Inria et du Titulaire, le cas échéant de leur représentant, et de leur Délégué ; (ii) des catégories de Traitements de données à caractère personnel effectués pour le compte d'Inria ; (iii) les informations relatives aux personnes autorisées c'est-à-dire le personnel autorisé du Titulaire et des sous-traitants qui ont accès ou traitent les Données à caractère personnel ; le registre doit permettre de contrôler et de vérifier l'identité des personnels qui ont eu accès et qui ont traité les Données à caractère personnel et présenter les mesures de sécurité et de contrôle d'accès ; et (iv) une description générale des mesures techniques et organisationnelles permettant d'assurer la sécurité des Données Personnelles. Le registre doit se présenter sous une forme écrite y compris la forme électronique. Le Titulaire doit mettre le registre à la disposition de l'Autorité de contrôle compétente et doit prévenir immédiatement Inria de cette mise à disposition.

4) AIDE ET ASSISTANCE CONCERNANT L'ANALYSE D'IMPACT

Le Titulaire aide Inria pour la réalisation d'analyse d'impact relative à la protection des Données Personnelles lorsque le Traitement de données à caractère personnel figure dans la liste des types d'opérations de traitement pour lesquelles l'Autorité de contrôle a estimé obligatoire de réaliser une analyse d'impact ou lorsque le Traitement de données à caractère personnel remplit au moins deux des neuf critères issus des lignes directrices du G29.

Le Titulaire aide Inria pour la réalisation de la consultation préalable de l'Autorité de contrôle lorsqu'une analyse d'impact indique que le Traitement des Données Personnelles présenterait un risque élevé si Inria ne prenait pas de mesures pour atténuer le risque.

5) VIOLATION

En cas de Violation ou si le Titulaire a tout lieu de croire qu'une Violation a eu lieu, le Titulaire doit dans les 48 heures notifier à Inria via l'adresse mail rssi@inria.fr cette Violation ou possible Violation.

Il doit alors transmettre à Inria : (i) la description de la nature de la Violation, y compris si possible, les catégories et le nombre approximatifs de Personnes concernées par la Violation et les catégories et le nombre approximatif d'enregistrements de Données Personnelles concernés ; (ii) le nom et les coordonnées du Délégué ou d'un autre point de contact auprès duquel des informations complémentaires peuvent être obtenues ; (iii) la description des conséquences probables de la Violation ; (iv) la description des mesures prises ou que le Titulaire propose de prendre pour remédier à la Violation, y compris le cas échéant, les mesures pour en atténuer les éventuelles conséquences négatives afin de permettre à Inria de notifier la Violation à l'Autorité de contrôle compétente.

6) AUDIT

Inria se réserve le droit de procéder à toute vérification qui lui paraîtrait utile pour constater le respect des obligations précitées en procédant à un audit de sécurité auprès du Titulaire ou directement auprès d'un sous-traitant.

Le Titulaire s'engage à répondre aux demandes d'audit d'Inria ou d'un tiers de confiance qu'Inria aura sélectionné, reconnu en tant qu'auditeur indépendant, ayant une qualification adéquate, et libre de fournir les détails de ses remarques et conclusions d'audit à Inria.

Les audits doivent permettre une analyse du respect par le Titulaire de ses obligations au titre des présentes, ainsi qu'au titre de la réglementation applicable en matière de la protection des Données Personnelles.

Inria doit aviser le Titulaire par écrit de son intention de faire procéder à un audit moyennant le respect d'un préavis minimum de trente (30) jours.

Inria communique de manière la plus précise et exhaustive possible le périmètre envisagé, la liste des opérations de contrôle et des outils de mesure qu'il envisage d'utiliser.

Le déploiement d'un outil est fait sous l'entière responsabilité d'Inria. Le Titulaire a le droit de faire analyser l'outil. Si un risque est identifié pour le système d'information et les données du Titulaire, ce dernier est en droit de refuser l'utilisation d'un tel outil.

Inria communique, le cas échéant, le nom de l'auditeur. Le Titulaire a le droit de refuser l'auditeur pour un motif légitime. En cas de désaccord après une troisième proposition, le choix de l'auditeur est fixé par le tribunal compétent. Inria est responsable des dommages causés par l'auditeur.

Le Titulaire peut refuser l'accès aux zones confidentielles, sécurisées et mutualisées et effectue, dans ce cas, l'audit et en communique les résultats à Inria.

Les résultats de l'audit sont formalisés dans un rapport qui doit être adressé au Titulaire pour qu'il puisse y insérer ses observations et réserves. Le rapport final doit nécessairement comprendre les observations du Titulaire.

Si un désaccord survient concernant des écarts de conformité, Inria est en droit de demander une mise en conformité. Toutefois, Inria ne saurait invoquer la non-réalisation de la mise en conformité pour suspendre ses engagements.

La procédure d'audit se termine par la remise par Inria d'une lettre clôturant l'audit même en cas d'audit favorable pour le Titulaire.

7) SORT DES DONNEES A CARACTERE PERSONNEL A LA FIN DU MARCHE

A l'expiration du Marché et au plus tard le dernier jour du Marché, le Titulaire a pour obligation de supprimer toutes les Données Personnelles et toutes copies existantes sauf obligation légale de conservation auquel cas le Titulaire s'engage à archiver les Données Personnelles et à détruire lesdites Données Personnelles dès la fin de l'obligation légale.

Il ne saurait y avoir de rétention de la part du Titulaire pour quelque raison que ce soit.

Concomitamment à la destruction des Données Personnelles et des copies, le Titulaire adresse à Inria une attestation de destruction de toutes les copies existantes des Données Personnelles mises à la disposition par Inria.

8) CONTROLE DE L'AUTORITE DE CONTROLE COMPETENTE

Dans le cas où Inria ferait l'objet d'un contrôle de la part de l'Autorité de contrôle compétente, le Titulaire s'engage à coopérer, et à ce que le Titulaire coopère pleinement et sans délai avec Inria et l'Autorité de contrôle, notamment en fournissant toutes informations pertinentes et l'accès à tous équipements, logiciels, données, dossiers, systèmes d'information, etc. utilisés pour la réalisation des prestations, et notamment le Traitement, et nécessaires à la réalisation du contrôle par l'Autorité de contrôle.

- 9)** Le Titulaire peut être contraint de divulguer des Données Personnelles à la demande d'une cour, agence administrative ou autorité gouvernementale, ou en vertu de toute loi, réglementation, citation à comparaître, requête, sommation ou autre processus administratif ou légal, ou par n'importe quelle enquête formelle ou informelle par n'importe quelle agence gouvernementale ou autorité ; dans ce cas, le Titulaire s'engage à (a) notifier promptement Inria de la demande de divulgation (dans la limite de ce qui est autorisé par la loi), (b), utiliser toute option légale pour contester ou s'opposer à une telle demande et, si une telle opposition n'est pas possible ou n'aboutit pas, ne divulguer que les Données Personnelles couvertes par cette demande.

10) Sous réserve de ce qui est prévu à l'Annexe, tout Traitement non autorisé, utilisation ou divulgation de Données Personnelles par le Titulaire sont strictement interdits.

11) L'Annexe est régie par le droit français conformément au Marché.

12) Tout litige lié à l'Annexe est de la compétence des juridictions françaises conformément au Marché.

V. Droits et obligations d'Inria vis-à-vis du Titulaire

Inria s'engage à :

- fournir au Titulaire certaines Données Personnelles objet du Traitement;
- fournir au Titulaire toutes les informations et instructions documentées nécessaires à la bonne exécution du Traitement des données à caractère personnel;
- indiquer au Titulaire toute évolution des Traitements des données à caractère personnel;
- fournir au Titulaire les coordonnées de son interlocuteur ou, le cas échéant, de sa Déléguée;
- notifier les Violations auprès de l'Autorité de contrôle compétente ;
- veiller, au préalable et pendant toute la durée du Traitement, au respect des obligations prévues par le Règlement Européen sur la Protection des Données de la part du Titulaire;

Inria dispose du droit de :

- demander au Titulaire, à première demande, la communication de tout élément, pièce ou documentation permettant de garantir qu'il respecte les exigences du Règlement Européen sur la Protection des Données et de l'Annexe ;
- formuler des objections et des réserves sur le sous-traitant sélectionné par le Titulaire ;
- superviser le Traitement, y compris réaliser les audits et les inspections auprès du Titulaire afin de s'assurer du respect par ce dernier des exigences du Règlement Européen sur la Protection des Données et de l'Annexe ;
- demander l'assistance du Titulaire sur la mise en œuvre d'une analyse d'impact et la mise en œuvre de l'exercice des droits des Personnes concernées, sur la coopération avec l'Autorité de contrôle, sur la mise en œuvre des moyens de sécurité du Traitement ou encore sur la mise en œuvre des notifications de Violations auprès de l'Autorité de contrôle ou des Personnes concernées.