

CAHIER DES CHARGES À L'ATTENTION DES SOUS- TRAITANTS DE F.INICIATIVAS

Principales modifications par rapport à la version précédente			
Version	Date	Rédacteur	Modifications
V0	25/05/2018	Equipe DPO	Création
V1	12/11/2018	Equipe DPO	Modification relative à la sous-traitance
V2	04/02/2019	Equipe DPO	Complément sur l'annexe Précision sur la sécurisation des échanges et la fin de la mission
V3	02/12/2019	Equipe DPO	Mise à jour de la nouvelle sur la nouvelle trame FI

F.INICIATIVAS, Société par actions simplifiée au capital de 227.000,00 euros,
 Registre du Commerce et des Sociétés de NANTERRE sous le numéro 499 154 557
 14 Terrasse Bellini, 3ème étage, 92800 PUTEAUX

Pour toutes questions, n'hésitez pas à contacter la Data Protection Officer : dpo@fi-group.com

1. Introduction

F.INICIATIVAS, société spécialisée dans le financement de l'innovation, a à cœur de respecter les obligations permettant la protection du droit des personnes.

Depuis l'adoption du règlement général sur la protection des données n° 2016/679 entré en vigueur le 24 mai 2016, les entités traitant des données personnelles doivent mettre en œuvre les moyens nécessaires afin d'être en conformité avec ce texte entré en application le 25 mai 2018 et sa transposition dans le droit interne.

À travers la responsabilisation des acteurs qui traitent des données à caractère personnel, le règlement a pour objectif de renforcer la protection et les droits des personnes concernées par les traitements des données personnelles.

Au titre de ce règlement, F.INICIATIVAS qui a accès à des données de cette nature, revêtira la qualité de responsable de traitement.

Dans ses rapports avec les prestataires et/ou fournisseurs dont les missions nécessitent la communication de données à caractère personnel, ceux-ci revêtiront la qualité de sous-traitant.

Afin de respecter ses propres obligations, F.INICIATIVAS a la possibilité de recevoir l'assistance de ses sous-traitants ainsi que la sécurité des données personnelles qui lui ont été confiées. À ce titre, les sous-traitants ne peuvent traiter les données transmises que dans le cadre des instructions délivrées par le responsable de traitement.

Dans cet esprit, le présent cahier des charges a pour objectif de permettre à F.INICIATIVAS en tant que responsable de traitement, de communiquer à ses sous-traitants les instructions à suivre dans le cadre de l'utilisation des données à caractère personnel confiées.

Vincent VILPELLET,
Président



2. Informations générales

ARTICLE 1 - DEFINITIONS

1. **Annexe au CDC** : le CDC comprend une annexe permettant l'identification et la description des Données personnelles confiées dans le cadre de la Mission prévue dans l'Engagement contractuel. Cette Annexe au CDC est en principe intégrée dans l'Engagement contractuel et est complétée par le Sous-traitant et F.INICIATIVAS.
2. **CDC** : le présent cahier des charges.
3. **CNIL** : désigne la Commission Nationale de l'Informatique et des Libertés, autorité de contrôle pour la France ayant vocation à protéger les données à caractère personnel et à contrôler la bonne application du RGPD.
4. **Donnée(s) personnelle(s)** : 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, 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.
5. **Engagement contractuel** : devis, contrat de prestation ou écrit sous quelque forme que ce soit décrivant la relation commerciale, conclu entre le Sous-traitant et F.INICIATIVAS auquel devra être annexé le présent CDC.
6. **Faible** : faiblesse dans le système de protection des Données personnelles permettant à une personne de porter atteinte à l'intégrité de ce système de protection, c'est-à-dire à son fonctionnement, à la confidentialité ou à l'intégrité des données protégées. Une faille de sécurité n'aboutit pas automatiquement à une Violation des Données personnelles.
7. **Jours ouvrés** : jour(s) du lundi au vendredi compris, à l'exclusion des jours fériés légaux.
8. **Mission** : tâches confiées au sous-traitant par F.INICIATIVAS, qui nécessitent le traitement de Données personnelles.
9. **Rapport détaillé** : rapport transmis par le Sous-traitant à F.INICIATIVAS, décrivant l'ensemble des moyens mis en œuvre par le sous-traitant pour garantir un niveau de sécurité adapté aux Données personnelles.
10. **Registre des failles** : support qui recense la description de la faille et la solution apportée.
11. **Registre des activités de traitements** : Support qui recense toutes les Données personnelles traitées ainsi que toutes les informations utiles liées à la donnée.
12. **Responsable de traitement ou "F.INICIATIVAS"** : conformément à l'article 4 du RGPD, organisme qui détermine les finalités et les moyens d'un traitement.
13. **RGPD** : le Règlement Général à la Protection des Données (UE) 2016/679 du Parlement Européen et du Conseil du 27 avril 2016 applicable depuis le 25 mai 2018.
14. **Sous-traitant** : désigne le prestataire qui traite les Données personnelles pour le compte de F.INICIATIVAS.
15. **Synthèse simplifiée** : désigne la synthèse rédigée par le Sous-traitant en cas de modification de la méthode de sécurisation des Données personnelles en cours de Mission. Le Sous-traitant y décrit les raisons et les conséquences de ce changement.

16. **Traitement** : désigne toute opération ou tout ensemble d'opérations portant sur une Donnée personnelle, quel que soit le procédé utilisé, et notamment 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.
17. **Violation** : accès non autorisé à des Données personnelles ou atteinte à leur sécurité qui entraîne de manière accidentelle ou illicite, la destruction, la perte, l'altération, la divulgation non autorisée de Données personnelles transmises, conservées ou traitées de quelque façon que ce soit.

ARTICLE 2 - OBJET DU CAHIER DES CHARGES

Le CDC a pour objet de définir les conditions dans lesquelles le Sous-traitant s'engage à effectuer pour le compte du Responsable de traitement les opérations de Traitement des Données personnelles qui lui sont confiées dans le cadre d'un Engagement contractuel.

Le Sous-traitant certifie par la présente respecter le RGPD et plus particulièrement les consignes imposées par son Responsable de traitement.

ARTICLE 3 - DUREE DES OBLIGATIONS DU CAHIER DES CHARGES

Le CDC a vocation à s'appliquer pour la durée de l'Engagement contractuel.

Au terme de l'Engagement contractuel, pour quelque cause que ce soit, le Sous-traitant s'engage à:

- Archiver uniquement les Données personnelles strictement nécessaires dans le cadre des obligations légales qui lui incombent. Une fois le délai légal expiré, les Données personnelles devront être détruites.

Dans l'hypothèse où aucune obligation légale n'imposerait au Sous-traitant de conserver les Données personnelles, celui-ci s'engage à les détruire définitivement.

Après l'expiration de l'Engagement contractuel, les obligations ayant vocation à perdurer demeureront en vigueur.

3. Informations et consignes sur le traitement des données personnelles

ARTICLE 4 - DONNEES PERSONNELLES VISEES PAR LE CDC

L'ensemble des Données personnelles communiquées au Sous-traitant dans le cadre de son Engagement contractuel est soumis au CDC.

Le Sous-traitant s'engage à identifier dans un délai d'un mois après la signature du CDC le type de Données personnelles transmis selon le modèle remis en Annexe 1.

ARTICLE 5 - TRANSMISSION ET UTILISATION DES DONNÉES

Au titre de l'Engagement contractuel, le Responsable de traitement doit communiquer à son Sous-traitant les Données personnelles sous quelque nature et sous quelque support que ce soit.

Suivant le principe de finalité, seules les données strictement nécessaires à la réalisation de la Mission doivent être collectées. À ce titre, le Sous-traitant s'engage conformément au principe de minimisation de la collecte des données à solliciter auprès de F.INICIATIVAS le minimum d'informations nécessaires et à les utiliser uniquement dans l'accomplissement de sa Mission.

Dans l'hypothèse où un Sous-traitant constaterait que les Données personnelles transmises ne sont pas ou plus utilisées, celui-ci s'engage, après avoir averti le Responsable de traitement, à leur appliquer le même sort que celui prévu à l'article 3 concernant la durée de conservation des Données personnelles au terme de l'Engagement contractuel.

ARTICLE 6 - INFORMATION ET CONTRÔLE

Un mois après la signature du CDC, et à minima tous les douze mois, le Sous-traitant s'engage à fournir à F.INICIATIVAS, un Rapport détaillé sur les moyens de sécurisation mis en œuvre. En cas de modification de la méthode de sécurisation, le Sous-traitant s'engage à fournir à F.INICIATIVAS une Synthèse simplifiée dans le mois suivant ladite modification.

Conformément au RGPD, le Sous-traitant s'engage à tenir un Registre des activités de traitements, qui doit être mis à la disposition de la CNIL. Le Sous-traitant accepte de fournir à F.INICIATIVAS son Registre des activités de traitements dans un délai de sept (7) jours ouvrés suivant demande écrite.

En cas de doute sérieux quant à la véracité des éléments communiqués, F.INICIATIVAS se réserve le droit de demander à son Sous-traitant la communication de tout document lui permettant de s'assurer du niveau de sécurité mis en place.

De plus, afin de garantir que les mesures techniques et organisationnelles mises en place par le Sous-traitant sont suffisantes, le Responsable de traitement se réserve la possibilité de conduire des audits au sein de ses locaux, sans jamais dépasser un audit par année civile.

Le Responsable de traitement devra informer le Sous-traitant quinze (15) jours avant l'audit. Le Sous-traitant aura la possibilité de repousser l'audit de quinze (15) jours si la date ne lui convient pas.

Le Sous-traitant s'engage à coopérer à de tels audits, et plus particulièrement à communiquer toutes les informations considérées comme raisonnablement nécessaires pour l'accomplissement de cet audit.

Est expressément précisé qu'un rapport d'audit ne remontant aucune irrégularité est une condition déterminante de la poursuite de l'Engagement contractuel.

En cas de non-conformité relevée dans le rapport d'audit, le Sous-traitant aura la possibilité de présenter des actions correctives dans un délai de trente jours à compter de la remise du rapport d'audit. Si celles-ci sont suffisamment convaincantes, l'Engagement contractuel se poursuivra. En revanche, si les modifications proposées sont considérées comme insuffisantes par le Responsable de traitement, l'Engagement contractuel sera résilié par LRAR sans autre formalisme.

ARTICLE 7 - AUTORISATIONS REQUISES

1) Conditions requises concernant la sous-traitance

Dans l'exercice de sa Mission, le Sous-traitant qui au moment de la signature de son Engagement contractuel ne travaillait pas avec des sous-traitants, s'interdit d'y recourir.

En cas de nécessité d'y avoir recours, le Sous-traitant doit fournir la liste du ou des sous-traitant(s) concerné(s) et demander par écrit l'autorisation du Responsable de traitement qui se réserve le droit d'accepter ou non.

Par exception à ce qui précède, dans l'hypothèse où au moment de la signature de l'Engagement contractuel, le Sous-traitant a averti le Responsable de traitement qu'il avait recours à la sous-traitance et lui a fourni la liste des sous-traitants avec lesquels il travaillait, l'accès aux Données personnelles du Responsable de traitement est autorisé. Ainsi, en cas de recours à la sous-traitance dans les conditions précitées, le Sous-traitant s'engage d'une part à porter à la connaissance de ses sous-traitants le CDC et d'autre part à veiller à ce qu'ils le respectent.

En cas de modification de la liste des sous-traitants, le Sous-traitant s'engage à avertir le Responsable de traitement un mois à l'avance de tout changement qui interviendrait afin que F.INICIATIVAS puisse s'opposer à la divulgation de ses Données personnelles à un nouveau sous-traitant. En cas de suppression d'un sous-traitant de la liste, F.INICIATIVAS se réserve le droit de se tourner directement vers celui-ci pour le mettre en demeure de respecter les obligations liées à la fin de la Mission.

2) Conditions requises concernant le traitement de la donnée lié aux droits des personnes

Le Sous-traitant s'interdit toute reproduction et/ou transfert, de Données personnelles sans l'autorisation préalable de son Responsable de traitement.

Dans ce cadre, le Sous-traitant s'interdit de donner accès, corriger, supprimer ou bloquer des Données personnelles hormis accord exprès du Responsable de traitement.

En cas de demande d'une personne physique, après avoir préalablement vérifié l'identité de la personne concernée, le Sous-traitant s'engage à transmettre la demande d'accès, de correction ou de suppression au Responsable de traitement afin que celui-ci puisse adresser les directives nécessaires au traitement de cette demande.

ARTICLE 8 - SÉCURISATION DES ÉCHANGES

Pour toutes questions générales relatives au traitement des Données personnelles, le Responsable de traitement et F.INICIATIVAS pourront se tourner vers les interlocuteurs privilégiés identifiés en Annexe 1.

Dans le cadre de la Mission, le Sous-traitant et le Responsable de traitement doivent établir conjointement à la signature du CDC par le Responsable de traitement la liste des interlocuteurs privilégiés au sein de leur service respectif vers lesquels, uniquement, les Données personnelles pourront transiter.

En cas de changement d'interlocuteurs privilégiés, le Sous-traitant et le Responsable de traitement doivent respectivement s'informer par écrit de cette modification. La Partie informée doit accuser réception de l'information.

ARTICLE 9 - MESURES DE SÉCURITÉ A LA CHARGE DU SOUS-TRAITANT

Le Sous-traitant veille à assurer une sécurisation adaptée au Traitement. Il doit à minima prévoir :

- Le verrouillage systématique du matériel informatique détenant des Données personnelles et laissé sans surveillance.
- Le changement récurrent des mots de passe pour l'ensemble des personnes ayant accès aux Données personnelles dans l'exercice de la Mission. Ce changement doit avoir lieu dans un délai en adéquation avec la criticité des Données personnelles.

- Un lieu de stockage avec un accès sécurisé dès lors que des Données personnelles seront communiquées sur un support matériel (papier, clef USB...)

Par exception à ce qui précède, le Sous-traitant reste libre de mettre en place les mesures de sécurité de son choix, sous réserve que celles-ci soient au moins égales aux mesures visées au présent article.

Le Sous-traitant s'engage à respecter et à faire respecter par son personnel la confidentialité des Données personnelles.

Le Sous-traitant s'engage à former son personnel à la sécurisation des Données personnelles.

4. Informations et consignes en cas de Violation de sécurité des Données personnelles

ARTICLE 10 - VIOLATION DES DONNÉES PERSONNELLES

Afin d'anticiper les mesures mises en œuvre en cas de Violation d'une Donnée personnelle, le Sous-traitant doit communiquer à F.INICIATIVAS la méthode suivie en cas de réalisation du risque. Cette méthode doit être relatée dans le Rapport détaillé et le cas échéant la Synthèse simplifiée. A l'appui de cette information, F.INICIATIVAS sera en mesure d'évaluer l'adaptabilité et l'efficacité des mesures appliquées.

Dans les 24 heures suivant la Violation d'une Donnée personnelle, le Sous-traitant s'engage à informer le Responsable du traitement des moyens immédiatement mis en œuvre, par l'intermédiaire d'un Registre des failles qu'il s'engage à tenir.

En cas d'identification d'un risque pouvant porter atteinte à la sécurité des Données personnelles, le Sous-traitant s'engage à avertir dans un délai de 72 heures F.INICIATIVAS. Étant expressément précisé que le Sous-traitant ne pourra se prévaloir d'un risque non survenu ou d'un niveau de faille qualifié de « faible » pour se libérer de son obligation d'avertir F.INICIATIVAS.

Dès identification du risque, le Sous-traitant s'engage à mettre en œuvre des actions correctives immédiates qui permettent d'atteindre un niveau de protection plus performant que celui initialement prévu en cas d'atteinte à la sécurité des Données personnelles.

5. Sanctions et fin de la Mission

ARTICLE 11 - SANCTIONS

En cas de manquement à une des obligations lui incombant au titre du CDC, entraînant une sanction pécuniaire de la part de la CNIL ou de toutes autres entités habilitées à sanctionner le Responsable de traitement, le Sous-traitant s'engage à rembourser la somme au Responsable de traitement qui ne pourrait se voir imputer l'inconséquence du Sous-traitant.

De même, en cas d'action, réclamation, revendication ou opposition de la part d'un tiers lié à un manquement du Sous-traitant, celui-ci s'engage à assumer pleinement sa responsabilité et à rembourser au Responsable de traitement les frais engagés sur justificatif.

F.INICIATIVAS pourra exiger la rupture de la relation avec le Sous-traitant pour manquement à une obligation essentielle et déterminante et par conséquent la résiliation immédiate et de plein droit de l'Engagement contractuel.

ARTICLE 12 - FIN DE LA MISSION

Le Sous-traitant s'engage dans un délai d'un (1) mois suivant la fin de la Mission, à respecter les obligations prévues à l'article 3 et à délivrer une attestation d'archivage / de destruction sur première demande.

L'obligation de confidentialité conserve tous ses effets pour une durée illimitée suivant le terme de la Mission.

Société.....
M.....
Mention manuscrite « bon pour accord »
Date, cachet et signature