

Accord relatif à la protection des données à caractère personnel

Cet Accord fait partie du contrat entre SINARI (ci-après le « Sous-traitant ») et le Client (ci-après le « Client ») pour la fourniture de solutions par SINARI (ci-après le " Service "). Le Sous-traitant et le Client sont collectivement dénommés ci-après « les Parties ».

Le Client conclut le présent Accord en son nom et, dans la mesure requise par les Lois et Règlements sur la protection des données, au nom et pour le compte de ses Affiliés autorisés, si et dans la mesure où SINARI traite des Données personnelles pour lesquelles ces Affiliés autorisés sont qualifiés de Responsable de traitement ou de Sous-traitant.

Tous les termes commençant par une majuscule qui ne sont pas définis au présent Accord ont la signification qui leur est donnée dans les Lois et Règlements sur la protection des données.

Dans le cadre de la fourniture du Service au Client conformément au contrat, SINARI peut traiter des Données à caractère personnel pour le compte du Client en qualité de Sous-traitant, et les parties conviennent de se conformer aux dispositions suivantes en ce qui concerne toutes les Données à caractère personnel.

Définitions

« *Autorité de contrôle* » désigne une autorité publique indépendante qui est instituée par un État membre en vertu de l'article 51 du RGPD.

« *Données à caractère personnel* » désigne toute information se rapportant à une personne physique identifiée ou identifiable.

« *Données du Client* » désigne toutes les données fournies par le Client en relation avec le Service.

« *Lois et Règlements sur la protection des données* » désigne le Règlement 2016/679 du Parlement européen et du Conseil relatif à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données et la Loi n°78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés telle que modifiée par la loi du 20 juin 2018.

« *Responsable du 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.

« *RGPD* » désigne le Règlement (UE) 2016/679 du Parlement européen et du Conseil du 27 avril 2016 relatif à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données, et abrogeant la directive 95/46/CE (Règlement général sur la protection des données).

« *Service* » désigne la prestation effectuée par le Sous-traitant.

« *Sous-traitant* » désigne la personne physique ou morale, l'autorité publique, le service ou un autre organisme qui traite des Données à caractère personnel pour le compte du Responsable du traitement.

« *Traitement* » désigne toute opération ou tout ensemble d'opérations effectuées ou non à l'aide de procédés automatisés et appliquées à des données ou des ensembles de Données à caractère

personnel, telles que la collecte, l'enregistrement, l'organisation, la structuration, la conservation, l'adaptation ou la modification, l'extraction, la consultation, l'utilisation, la communication par transmission, la diffusion ou toute autre forme de mise à disposition, le rapprochement ou l'interconnexion, la limitation, l'effacement ou la destruction.

Objet de l'Accord

SINARI fournit le Service au Client en vertu du Contrat. Dans le cadre du Service, les parties prévoient que SINARI peut traiter des Données du Client qui peuvent contenir des Données à caractère personnel.

Les parties conviennent qu'en ce qui concerne le Traitement des données personnelles, SINARI agit en tant que Sous-traitant pour le compte du Client, lequel agit soit en tant que Responsable du traitement soit en tant que Sous-traitant, auquel cas SINARI agit en qualité de Sous-traitant ultérieur.

Dans ce contexte, le présent Accord a pour objet de régler les modalités d'exécution et d'organisation du Traitement de ces Données par le Sous-traitant.

Il est entendu entre les parties que le Sous-traitant agit exclusivement pour le compte et conformément aux instructions du Responsable du traitement, et ce pendant toute la durée du présent Accord.

Le Responsable du traitement donne instruction au Sous-traitant de procéder en son nom et pour son compte au(x) traitement(s) des données à caractère personnel décrit(s) ci-après.

1 Description du ou des traitements

Les détails des opérations de traitement, et notamment les catégories de Données à caractère personnel et les finalités du traitement pour lesquelles les Données à caractère personnel sont traitées pour le compte du Responsable du traitement, sont spécifiés à l'Annexe 1 - Description du traitement de données à caractère personnel. Il convient de souligner que SINARI a créé une Annexe 1 pour chaque solution vendue par l'entité, permettant ainsi au Client de consulter l'annexe correspondant à la solution à laquelle il a souscrit au sein de la base documentaire en ligne de SINARI, accessible en suivant le lien ci-dessous :

<https://www.sinari.com/basedocumentaire/rgpd/dpa/annexe1>

2 Responsabilités du Client

Le Client doit, dans le cadre de son utilisation du Service, traiter les Données à caractère personnel conformément aux exigences des Lois et Règlements sur la protection des données, y compris toute exigence applicable pour informer les Personnes concernées du recours au Sous-traitant et obtenir les consentements nécessaires pour permettre le traitement des Données à caractère personnel par le Sous-traitant pour la durée et les finalités de l'Accord.

Le Responsable du traitement s'engage à :

- fournir au Sous-traitant les données visées au point 1 du présent Accord.
- documenter par écrit toute instruction concernant le Traitement des Données à caractère personnel par le Sous-traitant.
- veiller, au préalable et pendant toute la durée du Traitement, au respect des obligations prévues par les Lois et Règlements sur la protection des données de la part du Sous-traitant.

- superviser le Traitement, y compris réaliser les audits et les inspections auprès du Sous-traitant.

Le Responsable du traitement est le seul responsable (i) pour déterminer les finalités et les moyens du Traitement des Données à caractère personnel effectué par le Sous-traitant ; (ii) de l'exactitude, l'adéquation et de la complétude des instructions susmentionnées. De manière expresse et générale, le Sous-traitant ne détermine jamais les finalités et les moyens des traitements qui lui sont confiés par le Responsable du traitement.

3 Obligations des parties

3.1 Instructions

Le Sous-traitant ne traite les Données à caractère personnel que sur instruction documentée du Responsable du traitement, à moins qu'il ne soit tenu d'y procéder en vertu du droit de l'Union ou du droit de l'État membre auquel il est soumis. Dans ce cas, le Sous-traitant informe le Responsable du traitement de cette obligation juridique avant le traitement, sauf si la loi le lui interdit pour des motifs importants d'intérêt public. Des instructions peuvent également être données ultérieurement par le Responsable du traitement pendant toute la durée du Traitement des Données à caractère personnel.

Le Sous-traitant informe immédiatement le Responsable du traitement si, selon lui, une instruction donnée par le Responsable du traitement constitue une violation des Lois et Règlements sur la protection des données. Cette information ne doit en aucun cas être interprétée comme un conseil juridique de la part du Sous-traitant. Le Sous-traitant se réserve le droit de ne pas procéder à un Traitement de données suivant une instruction du Responsable du traitement qui violerait les Lois et Règlements sur la protection des données, sans que cette inexécution puisse être considérée comme une violation de ses obligations prévues au présent Accord.

3.2 Limitation de la finalité

Le Sous-traitant traite les Données à caractère personnel uniquement pour la ou les finalités spécifiques du Traitement, telles que définies à l'Annexe 1, sauf instruction complémentaire du Responsable du traitement.

3.3 Durée du traitement des Données à caractère personnel

Le traitement par le Sous-traitant n'a lieu que pendant la durée précisée à l'Annexe 1.

3.4 Confidentialité et sécurité du traitement de Données à caractère personnel

En application de l'article 32 du RGPD, les parties s'engagent à mettre en œuvre des mesures organisationnelles et techniques appropriées afin de garantir un niveau de sécurité adapté au Traitement. Lors de l'évaluation du niveau de sécurité approprié, les parties tiennent dûment compte de l'état des connaissances, des coûts de mise en œuvre et de la nature, de la portée, du contexte et des finalités du Traitement, ainsi que des risques pour les Personnes concernées.

Le Sous-traitant met au moins en œuvre les mesures techniques et organisationnelles précisées à l'Annexe 3 pour assurer la sécurité des Données à caractère personnel. L'Annexe 3 est accessible au sein de la base documentaire en ligne de SINARI en suivant le lien ci-dessous :

<https://www.sinari.com/basedocumentaire/rgpd/dpa/MOT>

Le Sous-traitant veille à ce que les personnes autorisées à traiter les Données à caractère personnel s'engagent à respecter la confidentialité ou soient soumises à une obligation légale appropriée de confidentialité et reçoivent la formation nécessaire en matière de protection des Données à caractère personnel.

Le Sous-traitant prend en compte, s'agissant de ses outils, produits, applications ou services, les principes de protection des données dès la conception et de protection des données par défaut.

Le Sous-traitant s'engage à enregistrer les opérations de maintenance du SI dans une main courante consultable par le Client à tout moment. Le cas échéant, chaque opération de maintenance réalisée par le Sous-traitant devra faire l'objet d'un descriptif précisant les dates, la nature des opérations et les noms des intervenants.

En cas de télémaintenance permettant l'accès à distance aux fichiers du Client, le Sous-traitant prendra toutes dispositions afin de permettre au Client d'identifier la provenance de chaque intervention extérieure. À cette fin, le Sous-traitant s'engage à obtenir l'accord préalable du Client avant chaque opération de télémaintenance dont il prendrait l'initiative.

Le Client reste pleinement responsable des mesures de sécurité organisationnelles et techniques mises en place et notamment de la confidentialité de ses mots de passe. Conformément aux standards du Sous-traitant, les mots de passe doivent respecter les recommandations suivantes :

- Imposer une longueur minimale pour les mots de passe (moyen à fort : entre 12 et 14 caractères, fort à très fort : au moins 15)
- Ne pas imposer de longueur maximale pour les mots de passe
- Mettre en œuvre des règles sur la complexité des mots de passe (utilisation de majuscules, minuscules, chiffres et caractères spéciaux)
- Choisir un mot de passe sans information personnelle ou propre à l'entreprise
- Utiliser un mot de passe différent pour chaque service
- Ne pas enregistrer les mots de passe en clair (au sein d'un fichier ou d'un mail par exemple)
- Modifier les mots de passe par défaut
- Imposer un délai d'expiration sur les mots de passe
- Révoquer immédiatement les mots de passe en cas de compromission suspectée ou avérée
- Mettre en place une politique de sécurité des mots de passe
- Mettre en place un contrôle de la robustesse des mots de passe lors de leur création ou de leur renouvellement
- Mettre à disposition un coffre-fort de mots de passe

Le Client s'engage à transmettre les mots de passe aux tiers, notamment aux sous-traitants, de façon sécurisée et à ne pas transmettre ces mots de passe en clair.

3.5 Données sensibles

Si le Traitement porte sur des Données à caractère personnel révélant l'origine raciale ou ethnique, les opinions politiques, les convictions religieuses ou philosophiques ou l'appartenance syndicale, des données génétiques ou des données biométriques aux fins d'identifier une personne physique de manière unique, des données concernant la santé ou des données concernant la vie sexuelle ou l'orientation sexuelle d'une personne physique, ou des données relatives aux condamnations pénales et aux infractions («données sensibles»), le Sous-traitant applique des limitations spécifiques et/ou des garanties supplémentaires.

3.6 Recours à des sous-traitants ultérieurs

Le Sous-traitant dispose de l'autorisation générale du Responsable du traitement pour ce qui est du recrutement de sous-traitants ultérieurs sur la base d'une liste convenue en Annexe 2 du présent Contrat. Le Sous-traitant informe spécifiquement par écrit le Responsable du traitement de tout projet de modification de cette liste par l'ajout ou le remplacement de sous-traitants ultérieurs en fournissant une communication de la mise à jour de l'Annexe 2 par e-mail au moins quinze (15) jours avant la modification, donnant ainsi au Responsable du traitement suffisamment de temps pour

pouvoir s'opposer à ce changement avant le recrutement du ou des sous-traitants ultérieurs concernés. Afin de recevoir les notifications par e-mail concernant les nouveaux Sous-traitants, le Responsable de traitement doit s'inscrire ici :

https://www.sinari.com/newsletter_sous_traitants_ulterieurs

Le Sous-traitant fournit au Responsable du traitement les informations nécessaires pour lui permettre d'exercer son droit d'opposition. En cas d'absence de réponse de la part du Responsable du traitement au terme du délai susvisé, le sous-traitant ultérieur est réputé accepté.

La liste des sous-traitants ultérieurs au jour de la signature du présent accord figure en Annexe 2 et devra être actualisée par le Sous-traitant en cours d'exécution des prestations, le cas échéant. Il convient de souligner que l'Annexe 2 répertorie, pour chaque solution vendue, les sous-traitants impliqués dans la fourniture de cette solution. Cette Annexe 2 est accessible au sein de la base documentaire en ligne de SINARI en suivant le lien ci-dessous :

<https://www.sinari.com/basedocumentaire/rgpd/dpa/annexe2>

Lorsque le Sous-traitant recrute un sous-traitant ultérieur pour mener des activités de traitement spécifiques (pour le compte du Responsable du traitement), il le fait au moyen d'un contrat qui impose au sous-traitant ultérieur, en substance, les mêmes obligations en matière de protection des données que celles imposées au Sous-traitant en vertu des présentes clauses. Le Sous-traitant veille à ce que le sous-traitant ultérieur respecte les obligations auxquelles il est lui-même soumis en vertu des présentes clauses et des Lois et Règlements sur la protection des données.

Le Sous-traitant demeure pleinement responsable, à l'égard du Responsable du traitement, de l'exécution des obligations du sous-traitant ultérieur conformément au contrat conclu avec le sous-traitant ultérieur.

3.7 Transferts de données à caractère personnel

Le Responsable du traitement convient que lorsque le Sous-traitant recrute un sous-traitant ultérieur conformément à la clause 3.6 pour mener des activités de Traitement spécifiques (pour le compte du Responsable du traitement) et que ces activités de Traitement impliquent un transfert de données à caractère personnel au sens du chapitre V du RGPD, le Sous-traitant et le sous-traitant ultérieur peuvent garantir le respect du chapitre V du RGPD en utilisant notamment les clauses contractuelles types adoptées par la Commission Européenne sur la base de l'article 46, paragraphe 2, du RGPD, pour autant que les conditions d'utilisation de ces clauses contractuelles types soient remplies.

4 Assistance du Responsable de traitement par le Sous-traitant

Le Sous-traitant prête assistance au Responsable du traitement pour ce qui est de remplir l'obligation qui lui incombe de répondre aux demandes des personnes concernées d'exercer leurs droits, en tenant compte de la nature du Traitement.

Le Sous-traitant informe dans les meilleurs délais le Responsable du traitement de toute demande qu'il a reçue de la part d'une personne concernée. Il ne donne pas lui-même suite à cette demande, à moins que le Responsable du traitement des données ne l'y ait autorisé.

Outre l'obligation incombant au Sous-traitant d'assister le Responsable du traitement en vertu des dispositions précédentes, le Sous-traitant aide en outre le Responsable du traitement à garantir le respect des obligations suivantes, compte tenu de la nature du Traitement et des informations dont dispose le Sous-traitant :

- (1) l'obligation de procéder à une évaluation de l'incidence des opérations de traitement envisagées sur la protection des Données à caractère personnel («analyse d'impact relative à la protection des données») lorsqu'un type de

traitement est susceptible de présenter un risque élevé pour les droits et libertés des personnes physiques;

- (2) l'obligation de consulter l'autorité de contrôle compétente/les autorités de contrôle compétentes préalablement au traitement lorsqu'une analyse d'impact relative à la protection des données indique que le traitement présenterait un risque élevé si le Responsable du traitement ne prenait pas de mesures pour atténuer le risque;
- (3) l'obligation de veiller à ce que les Données à caractère personnel soient exactes et à jour, en informant sans délai le Responsable du traitement si le Sous-traitant apprend que les Données à caractère personnel qu'il traite sont inexactes ou sont devenues obsolètes;
- (4) les obligations prévues aux articles 32 à 36 du RGPD.

5 Notification des Violations de Données à Caractère Personnel

Le Sous-traitant s'engage à informer le Responsable du traitement de toute Violation de Données à caractère personnel dans le cadre du Service dès que possible après avoir pris connaissance de cet événement.

En cas de Violation de Données à caractère personnel, le Sous-traitant coopère avec le Responsable du traitement et lui prête assistance aux fins de la mise en conformité avec les obligations qui lui incombent en vertu des articles 33 et 34 du RGPD en tenant compte de la nature du Traitement et des informations dont dispose le Sous-traitant.

6 Documentation et conformité

Le Sous-traitant met à la disposition du Responsable du traitement toutes les informations nécessaires pour démontrer le respect des obligations énoncées dans les présentes clauses et découlant directement des Lois et Règlements sur la protection des données.

À la demande du Responsable du traitement, le Sous-traitant permet également la réalisation d'audits des activités de traitement couvertes par les présentes clauses et y contribue, à intervalles raisonnables ou en présence d'indices de non-conformité.

Le Responsable du traitement peut décider de procéder lui-même à l'audit ou de mandater un auditeur indépendant. Les audits peuvent également comprendre des inspections dans les locaux ou les installations physiques du Sous-traitant et sont, le cas échéant, effectués moyennant un préavis raisonnable.

Les parties mettent à la disposition de l'autorité de contrôle compétente/des autorités de contrôle compétentes, dès que celles-ci en font la demande, les informations énoncées dans la présente clause, y compris les résultats de tout audit.

7 Restitution/Destruction des données traitées

Selon le choix du Responsable du traitement, le Sous-traitant supprime toutes les Données à caractère personnel ou les renvoie au Responsable du traitement au terme de la prestation de services relatifs au Traitement, et détruit les copies existantes, à moins que le droit de l'Union ou le droit de l'État membre n'exige la conservation des Données à caractère personnel.

8 Traitement des Données personnelles du Client par le Sous-traitant en qualité de Responsable de traitement

Dans le cadre du Contrat, le Sous-traitant est susceptible de traiter des Données à caractère personnel appartenant au Client en qualité de Responsable du traitement.

Les Données collectées par le Sous-traitant sont celles fournies par le Client dans le cadre de l'exécution du Contrat et de la relation commerciale entretenue entre le Client et le Sous-traitant.

Les Données à caractère personnel collectées dans ce cadre sont nécessaires à l'exécution du Contrat.

Les Données à caractère personnel du Client sont susceptibles d'être communiquées aux destinataires suivants :

- **A des destinataires internes :** c'est-à-dire aux membres du personnel du Sous-traitant habilités à accéder aux Données et qui en ont strictement besoin pour l'exercice de leurs fonctions.
- **A des prestataires de services et/ou sous-traitants**
- **A des Autorités judiciaires, publiques ou gouvernementales :** lorsque cela est nécessaire, par exemple, (i) pour que le Sous-traitant se conforme à ses obligations légales, (ii) qu'il se conforme à des demandes légitimes émanant d'autorités publiques ou gouvernementales, (iii) pour prévenir un délit ou procéder à une enquête et (iv) pour protéger les droits, la propriété ou la sécurité du Sous-traitant, de ses filiales ou de tiers.

Les Données à caractère personnel du Client sont susceptibles d'être transférées en dehors de l'Union européenne. Lorsque le Sous-traitant réalise des Transferts de Données à caractère personnel, il signe avec ses Sous-traitants des Clauses contractuelles types édictées par la Commission européenne.

Le Sous-traitant a désigné un Délégué à la Protection des Données (« **DPO** ») dont les coordonnées sont les suivantes : dpo@sinari.com.

Les personnes concernées disposent d'un droit d'accès, de rectification, d'effacement et d'un droit à la portabilité des Données à caractère personnel qui les concernent. Elles peuvent également demander la limitation du Traitement de ces Données à Caractère Personnel ou s'opposer à leur Traitement dans les conditions prévues par les Lois et Règlements sur la protection des données. Elles peuvent enfin communiquer au Sous-traitant leurs directives relatives au sort de leurs Données à caractère personnel en cas de décès lorsqu'il s'agit d'un contrat régi par la Loi française.

Si le Client considère que le Sous-traitant ne respecte pas ses obligations légales en matière de protection des Données à caractère personnel ou qu'il n'a pas répondu efficacement à sa demande, il dispose toujours d'un droit de déposer plainte auprès de l'Autorité de contrôle compétente.

Le Sous-traitant met en œuvre des mesures organisationnelles et techniques destinées à garantir la sécurité et la confidentialité des Données qu'il traite.

Le Sous-traitant ne conserve les Données à caractère personnel des Personnes concernées que pendant le temps nécessaire aux opérations pour lesquelles elles ont été collectées et dans le respect des réglementations en vigueur. D'une manière générale, les Données à caractère personnel traitées par le Sous-traitant dans le cadre du Contrat sont conservées pendant la durée de la relation commerciale puis supprimées. Certaines Données à caractère personnel sont susceptibles d'être conservées en archivage intermédiaire suivant la fin de la relation commerciale, conformément à des obligations légales auxquelles est soumis le Sous-traitant (ex : conservation des documents comptables), ou parce que ces Données à caractère personnel présentent un intérêt administratif légitime pour le Sous-traitant (ex : conservation à des fins de preuve pour les durées de prescription légales).

9 Responsabilités

Toute personne ayant subi un dommage matériel ou moral du fait de la violation des Lois et Règlements sur la protection des données a le droit d'obtenir du Responsable du traitement ou du Sous-traitant réparation du préjudice subi dans sa totalité.

Lorsque le Responsable du traitement et le Sous-traitant participent au même Traitement et qu'ils sont responsables d'un dommage causé par le Traitement, le Responsable du traitement ou le

Sous-traitant est tenu responsable du dommage dans sa totalité. Dans ce cas, celui qui a réparé totalement le dommage subi est en droit de réclamer auprès de l'autre la part de la réparation correspondant à sa part de responsabilité dans le dommage.

Le Sous-traitant ne sera tenu responsable du dommage causé par le Traitement que s'il n'a pas respecté le présent contrat, notamment lorsqu'il a agi en dehors des instructions licites du Responsable du traitement ou contrairement à celles-ci, et/ou s'il n'a pas respecté les obligations fixées par ou en vertu de la réglementation applicable sur la protection des données, sans préjudice de sa responsabilité en vertu d'autres règles.

Le Sous-traitant sera exonéré ou pourra limiter sa responsabilité, s'il prouve que le fait qui a provoqué le dommage ne lui est pas imputable. Toutefois, le Sous-traitant ne peut invoquer un manquement par un Sous-traitant ultérieur à ses obligations découlant du présent contrat pour échapper à ses propres responsabilités. En d'autres termes, le Sous-traitant est responsable devant le Responsable du traitement de la mauvaise exécution des obligations contractuelles de ses propres Sous-traitants ultérieurs.

10 Durée et résiliation

Le présent contrat est conclu pour une durée indéterminée.

Il entre en vigueur à la date de signature du Contrat principal. Chaque partie pourra en outre mettre fin au contrat en notifiant cette décision par lettre recommandée et moyennant le respect d'un délai de préavis de 1 mois.

Si, pour quelque raison que ce soit, le Sous-traitant n'est pas capable de respecter ses obligations en vertu du présent contrat, il s'engage à en informer immédiatement le Responsable du traitement, auquel cas ce dernier aura le droit de demander au Sous-traitant de suspendre les traitements de données réalisés pour son compte et/ou de résilier le contrat.

Le présent contrat est conclu en considération de la personne du Sous-traitant. De ce fait, celui-ci n'a pas le droit de céder et/ou de transférer le présent contrat et/ou les droits et obligations qui en découlent à un ou des tiers, sans l'accord écrit et préalable du Responsable du traitement.

11 Nullité d'une disposition

L'éventuelle nullité d'une disposition du présent contrat n'affecte pas la validité des autres dispositions du contrat. Les parties mettront tout en œuvre pour remplacer la disposition invalide par une disposition valide.

12 Loi applicable et juridiction compétente

Le présent contrat est régi par le droit national du lieu d'établissement principal du Sous-traitant.

Tout litige relatif à l'interprétation ou l'exécution du présent contrat sera soumis aux juridictions de ce droit national.