ACCORD RELATIF A LA PROTECTION DES DONNEES PERSONNELLES

Le présent accord relatif à la protection des données à caractère personnel (ci-après désigné le « **DPA** ») est conclu entre Smart Data et le Client qui a accepté les conditions générales societeinfo (ci-après désignées les « **Conditions Générales** »), en souscrivant un abonnement à societeinfo, ou en commandant une prestation sur mesure auprès de Smart Data.

Le DPA entrera en vigueur à la même date que les Conditions Générales, et pour la durée des Conditions Générales.

Smart Data et le Client sont ci-après dénommés collectivement les « **Parties** » et individuellement une « **Partie** ».

Au cours de l'exécution des Conditions Générales, chacune des Parties est amenée à procéder à divers traitements de données à caractère personnel.

Par le biais du DPA, les Parties souhaitent identifier lesdits traitements, les règles applicables à ces derniers et leurs rôles respectifs au regard du droit applicable à la protection des données à caractère personnel.

Article 1 Définitions

Sauf précision expresse contraire dans le DPA, les termes « **Données à Caractère Personnel** », « **Personnes Concernées** », « **Responsable du Traitement** », « **Sous-Traitant** », « **Traitement** » et « **Violation de Données à Caractère Personnel** » auront, dans le DPA, les définitions prévues par le Règlement 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 (ci-après désigné le « **RGPD** »).

En sus, il est indiqué que les termes utilisés dans le DPA avec une majuscule ont la même signification que dans le cadre des Conditions Générales.

Par ailleurs, les termes suivants auront, dans le DPA, les définitions suivantes :

1.1 « **Droit Applicable à la Protection des Données à Caractère Personnel** » désigne toutes lois, règlements et autres normes nationales, européennes et internationales, applicables au Traitement concerné, en ce compris notamment le RGPD et toute loi nationale des États membres de l'Union Européenne adoptée en complément ou en application des dispositions du RGPD, ainsi que, le cas échéant, les lois, règlements et autres normes nationales, européennes et internationales applicables au Traitement concerné.

1.2 « **Transfert de Données** » désigne tout transfert de Données à Caractère Personnel vers une personne, une entité ou un service d'une quelconque nature situé(e) dans un pays tiers ne bénéficiant pas d'une décision d'adéquation de la Commission Européenne au sens de l'article 45 du RGPD, et/ou tout accès à des Données à Caractère Personnel par une personne, une entité ou une service d'une quelconque nature situé(e) dans un tel pays.

Article 2 Objet

Le DPA a pour objet de définir les termes et conditions applicables aux Traitements mis en œuvre lors de l'exécution des Conditions Générales. Ces Traitements sont liés à l'utilisation par le Client de societeinfo et/ou à la souscription d'une Prestation sur Mesure auprès de Smart Data.

Article 3 Liste des Traitements mis en œuvre

Lors de l'exécution par le Client des Conditions Générales, les Traitements suivants peuvent avoir lieu :

N°	**Traitement**	**Personnes Concernées**	**Qualification de Smart Data**	Qualification du Client
1	Utilisation de societeinfo et mise en œuvre des Modules en vue de la collecte de Données à Caractère Personnel	Personnes physiques répondant aux critères définis par le Client au sein de societeinfo	Sous-Traitant	Responsable du Traitement
2	Réalisation de l'analyse de données à Caractère Personnel commandée par le Client	Personnes physiques répondant aux critères définis par le Client en vue de la réalisation de l'analyse demandée par Smart Data	Sous-Traitant	Responsable du Traitement

Article 4 - Description et modalités des Traitements mis en œuvre

Pour les seuls besoins de l'exécution des Conditions Générales, le Client - en qualité de Responsable du Traitement - autorise Smart Data - en qualité de Sous-Traitant - à réaliser pour son compte le(s) Traitement(s), dont les modalités sont plus précisément décrites en Annexe A.

Article 5 - Obligations des Parties

5.1 Obligation de chacune des Parties

Chacune des Parties s'engage à respecter l'ensemble des obligations légales qui s'imposent à elle en application du Droit Applicable à la Protection des Données à Caractère Personnel.

5.2 Obligations du Client

En qualité de responsable du(des) Traitement(s), le Client s'engage à ce que le(s) Traitement(s) mis en œuvre soi(en)t :

(i) réalisé(s) de manière loyale et licite ;

(ii) effectué(s) pour des finalités déterminées, explicites et légitimes ;

(iii) en respectant la nécessité de collecter des Données à Caractère Personnel (a) adéquates, pertinentes et non excessives au regard des finalités du(des) Traitement(s), (b) exactes, complètes et, le cas échéant, à jour ;

(iv) sur le fondement d'une base légale adéquate au sens du RGPD.

En outre, le Client s'engage à respecter son obligation d'information des Personnes Concernées.

5.3 Obligations de Smart Data

5.3.1 Traitement sur instruction documentée du Client

Smart Data s'engage à ne traiter des Données à Caractère Personnel que sur instruction documentée du Client, y compris en ce qui concerne les Transferts de Données, à moins que Smart Data ne soit tenue de traiter lesdites Données à Caractère Personnel en vertu du droit de l'Union européenne ou du droit d'un État membre de l'Union Européenne auquel elle est soumise. Dans une telle situation, Smart Data s'engage à informer le Client de cette obligation de traiter des Données à Caractère Personnel avant de procéder à ce Traitement,

sauf si le droit concerné interdit une telle information pour des motifs importants d'intérêt public.

Les Parties conviennent expressément de ce que le DPA, ainsi que les Conditions Générales, constituent des instructions documentées du Client au sens du paragraphe précédent.

5.3.2 Assistance fournie au Client

Conformément au Droit Applicable à la Protection des Données à Caractère Personnel, Smart Data s'engage à s'acquitter de son(ses) obligation(s) :

(i) d'aider le Client à répondre aux demandes d'exercice des droits des Personnes Concernées et de faire droit, le cas échéant, à ces demandes ;

(ii) liées à la sécurité du(des) Traitement(s) mis en œuvre et à la confidentialité des Données à Caractère Personnel collectées et traitées ;

(iii) de notification des Violations de Données à Caractère Personnel ;

(iv) de réaliser des études d'impact préalables et de consulter, lorsque nécessaire, les Autorités de Contrôle préalablement à la mise en œuvre d'un Traitement.

5.3.3 Sécurité des Traitements

Smart Data s'engage à prendre et maintenir toutes mesures techniques et organisationnelles appropriées au regard des risques présentés par le Traitement concerné afin d'assurer un niveau adéquat de sécurité du Traitement concerné et de protéger les Données à Caractère Personnel collectées et traitées dans la cadre de la mise en œuvre dudit Traitement.

Smart Data a décrit précisément en Annexe B les mesures techniques et organisationnelles mises en place à ce titre. Le Client reconnaît et accepte qu'il considère que les mesures techniques et organisationnelles décrites sont appropriées au regard des risques présentés par le(s) Traitement(s).

5.3.4 Confidentialité des Données à Caractère Personnel

Smart Data s'engage à mettre en place des procédures afin que tout tiers auquel il autorise l'accès, dans la mesure permise par le DPA, aux Données à Caractère Personnel concernées, y compris ses employés, sous-traitants et autres partenaires, soit tenu à des obligations appropriées de confidentialité à l'égard des Données à Caractère Personnel concernées.

5.3.5 Droit d'audit

Dans la limite d'un (1) par an, le Client est susceptible de réaliser ou faire réaliser, à ses frais, un audit de Smart Data visant à s'assurer du respect par cette dernière des stipulations du DPA, dans la situation où le Client constaterait un non-respect de ses engagements par Smart Data.

Si le Client souhaite faire appel à un tiers pour réaliser l'audit, ce dernier ne saurait en aucun cas être un concurrent de Smart Data et devra (i) être soumis à des obligations de confidentialité au moins aussi contraignantes que celles visées aux termes du DPA ou des Conditions Générales ; et (ii) respecter les mesures d'hygiène et de sécurité de Smart Data. Le Client se porte fort du respect par ses auditeurs des stipulations du présent article.

Le Client notifiera par écrit à Smart Data, sous un délai préalable minimal de quinze (15) jours ouvrés, sa décision de procéder à un audit en précisant son périmètre et ses modalités. Le Client s'efforcera de conduire les audits de manière à entraîner le minimum de perturbations et d'interruptions des activités de Smart Data. Les audits pourront être conduits seulement durant les heures ouvrées des bureaux de Smart Data. Smart Data s'efforcera de coopérer dans le cadre de cet audit. Si la durée et/ou la conduite de l'audit devaient impacter les activités de Smart Data en se prolongeant au-delà d'un (1) jour, cette dernière est susceptible de facturer au Client les coûts supportés par elle sur la base du temps passé par ses préposés et/ou prestataires à participer à l'audit. Dans l'hypothèse où l'audit viendrait à impacter la fourniture des services, aucun avoir ou responsabilité quelle qu'elle soit ne saurait être supporté par Smart Data de ce fait.

L'audit ne pourra concerner que les douze (12) derniers mois d'activité précédant le début de l'audit. Durant l'audit, le Client ne pourra pas accéder (i) aux données ou informations relatives à d'autres clients et prospects de Smart Data, (ii) à toute donnée interne dont Smart Data considère être propriétaire (p. ex. structure des coûts, données financières, informations comptables), ou (iii) à toute autre Information Confidentielle de Smart Data qui n'est pas directement et strictement pertinente au regard des finalités de l'audit.

Toutes les informations révélées ou échangées dans le cadre de la conduite d'un audit, de même que leurs résultats, constituent des Informations Confidentielles.

5.3.6 Sous-traitance

Smart Data peut faire appel à un autre Sous-Traitant pour mener des activités de traitement spécifiques. Dans ce cas, il informe préalablement et par écrit le Client de tout changement envisagé concernant l'ajout ou le remplacement d'autres Sous-Traitants. Le Client dispose d'un délai maximum de sept (7) jours à compter de la date de réception de cette information pour présenter ses objections.

5.3.7 Suppression/restitution des Données à Caractère Personnel

Smart Data s'engage, au terme des Conditions Générales, à procéder à la suppression définitive et irréversible de l'ensemble des Données à Caractère Personnel encore à sa possession ou à restituer l'ensemble des Données à Caractère Personnel au Client.

En l'absence d'instruction documentée du Client, Smart Data privilégiera, au titre du paragraphe précédent, la suppression des Données à Caractère Personnel concernées.

5.3.8 Avertissement du Client

Dans l'hypothèse où Smart Data estimerait qu'une instruction documentée du Client concernant les Traitements confiés pourrait être considérée comme illicite au regard du Droit Applicable à la Protection des Données à Caractère Personnel, ou risquerait d'entraîner un manquement ou une violation de ces dernières, Smart Data s'engage à en informer le Client.

Article 6 - Prévalence

En cas de conflit entre les stipulations du DPA et celles des Conditions Générales, les Parties conviennent de ce que les premières prévaudront.

Article 7 Modification

Le DPA ne peut être modifié que par accord écrit signé par l'ensemble des Parties.

Annexe A

Description et modalités des Traitements

1. Traitement n°1

Identité et coordonnées du Délégué à la Protection des Données de Smart Data	**Bao-Mi NGUYEN** Data Protection Officer - Juriste bao-mi.nguyen@explore.fr
Finalités du Traitement	Création d'un fichier de prospects du Client
Liste des Personnes Concernées	Personnes physiques occupant un poste au sein d'un prospect du Client

Liste des Données à Caractère Personnel concernées	Nom, prénom(s), adresse électronique professionnelle, profession
Liste des catégories particulières de Données à Caractère Personnel concernées	N/A
Liste exhaustive des Sous-Traitants ultérieurs	OnLine (hébergement) Debounce.io (validateur d'email)
Transferts de Données à caractère personnel	N/A
Durée de conservation	3 ans à compter de leur collecte
Sort des Données concernées au terme des Conditions Générales	Suppression définitive

2. Traitement n°2

Identité et coordonnées du Délégué à la Protection des Données de Smart Data	**Bao-Mi NGUYEN** Data Protection Officer - Juriste bao-mi.nguyen@explore.fr
Finalités du Traitement	Analyse du fichier de prospects ou de clients du Client

Liste des Personnes Concernées	Personnes physiques occupant un poste au sein d'un prospect ou d'un Client du Client
Liste des Données à Caractère Personnel concernées	Nom, prénom(s), adresse électronique professionnelle, profession
Liste des catégories particulières de Données à Caractère Personnel concernées	N/A
Liste exhaustive des Sous-Traitants ultérieurs	OnLine (hébergement) Debounce.io (validateur d'email)
Transferts de Données à caractère personnel	N/A
Durée de conservation	3 ans à compter de leur collecte
Sort des Données concernées au terme des Conditions Générales	Suppression définitive

Annexe B

Mesures de sécurité techniques et organisationnelles

---

1. Infrastructure et politique de sécurité

1.1 Infrastructure

Nous opérons notre propre infrastructure de serveurs physiques loués chez notre partenaire Scaleway.

Cette infrastructure est un cluster d'hyperviseurs KVM/QEMU sous Linux en mode silo. Les machines virtuelles sont de type Linux pour les serveurs et Freebsd pour les Firewall.

1.2 Politique de sécurité

SMART DATA maintient une politique de sécurité de l'information pour établir des garanties administratives, techniques et physiques efficaces pour les données des clients, et pour identifier, détecter, protéger contre les incidents de sécurité, y répondre et y remédier.

La politique de sécurité des informations de SMART DATA est revue et mise à jour régulièrement pour refléter les changements apportés à notre organisation, nos pratiques commerciales, notre technologie, nos services et les lois et règlements applicables.

L'Editeur s'engage à réaliser régulièrement tous les tests adéquats et contrôler préalablement les éléments informatiques mis à disposition du Client ou utilisés par l'Editeur dans le cadre du Contrat, notamment en termes de conformité aux normes de sécurité applicative. Dans ce cadre, l'Editeur répondra aux sollicitations du Client visant à définir et documenter le niveau de prise en compte des exigences prévues et, si nécessaire, à définir et mettre en œuvre des exigences complémentaires spécifiques au présent Contrat ;

1.3 **Contact sécurité**

Si vous avez des problèmes de sécurité ou des questions, vous pouvez nous contacter via vos canaux d'assistance habituels, ou en envoyant un e-mail à **security@societeinfo.com**

2. Contrôles d'accès

L'Editeur s'engage à mettre en œuvre l'ensemble des dispositifs techniques et organisationnels de sécurité physique en prévention, en détection et réaction à tout risque de sécurité (ex. intrusion) pouvant impacter les bâtiments, les salles serveurs, les locaux techniques, les lieux de stockages utilisés par les Service utilisé par le Client.

L'Editeur s'engage à prendre toutes les mesures nécessaires concernant le contrôle d'accès logique, et au minimum sans que cette liste soit limitative, celles prévues ci-dessous.

L'Editeur s'engage notamment à conserver la trace horodatée des actions réalisées (notamment flux émis et reçus, nouvelles versions applicatives, tests, erreurs, les dé-doublonnages et les purges, journaux et traces de connexions effectués par l'Editeur (par

l'intermédiaire de ses collaborateurs ou sous-traitants autorisés) à des fins de contrôle, d'audit et de preuves (les « Traces »).

L'Editeur tient à la disposition du Client, un journal d'événements sécurisés contenant les Traces, conservées de manière sécurisée et chiffrées conformément aux règles de l'art et aux exigences de l'article « Sécurité », pendant la durée du Contrat.

Sur demande du Client, l'Editeur s'engage à ce que les remontées de Traces soient réalisées directement sur les systèmes d'information du Client

L'Editeur s'interdit tout autre usage des Traces que ceux visés au présent article.

Les Traces seront communiquées sans délai au Client un format lisible par ce dernier, sur simple demande.

2.1 **Chiffrement en transit**

Tout le trafic réseau de SMART DATA est protégé par Transport Layer Security (TLS) :

- Tous les services HTTP sont uniquement accessibles en HTTPS
- Le service FTP sont uniquement accessibles en FTPS

L'implémentation de notre certificat SSL est notée A+ chez SSL Labs : https://www.ssllabs.com/ssltest/analyze.html?d=societeinfo.com&hideResults=on&latest

La zone du domaine societeinfo.com est sécurisée par le protocole DNSSEC : https://dnssec-analyzer.verisignlabs.com/societeinfo.com

2.2 **Authentification et autorisation des utilisateurs de SMART DATA**

Les clients peuvent accéder à la plate-forme societeinfo via :

- L'application Web HTTP (sous réserve de compatibilité avec le SSO de Bpifrance)
- L'API HTTP
- L'accès FTP (partenaires uniquement)

2.2.1 Application Web

Le système d'autorisation de l'application Web est standard au protocole OAuth 2.0 . Dans l'application Web, une politique de droits permet de définir l'accès des différents utilisateurs d'une même entreprise.

2.2.2 API

Les clés API sont définissables par l'utilisateur dans l'application Web. Chaque clé peut être décrite dans l'interface (DEV, PROD) générée et révoquée à tout instant.

Les clés d'API peuvent être inclues dans le header HTTP (X-API-KEY) de chaque requête pour limiter le risque d'usurpation.

2.2.3 FTPs

L'accès partenaires aux fichiers est disponible à travers un service FTPs. Ce dernier est configuré pour supporter le TLS en mode implicite (ce qui signifie que nous refusons les connections non chiffrées). L'accès FTPs est totalement indépendant des accès Web et API. Un login et un mot de passe complexe sont fournis. La politique de changement de ce mot de passe est établie en concertation.

2.3 **Audit des accès**

L'ensemble des accès HTTP est stockée en interne dans une base interne dédiée à des fins d'analyse.

Nous révoquons l'accès d'un utilisateur privilégié lorsqu'il n'est plus nécessaire. Nous enregistrons également tout accès du personnel à SMART DATA. Les journaux d'audit sont conservés pendant au moins 1 an et incluent un horodatage, un acteur, une action et une sortie. Le même principe s'applique pour les accès de nos clients à la plateforme.

Nous avons une gestion des accès au silo rigoureuse avec différents types de filtrages combinés.

3. Antivirus

L'éditeur s'engage à installer des logiciels de sécurité (anti-virus, etc.) sur tous les systèmes permettant la fourniture des Services et à les maintenir à jour par application des dernières signatures publiées par les éditeurs afin de prémunir le Client contre toute introduction de programme malveillant dans le(s) système(s) d'information du Client ou dans les Données. Si, malgré ces précautions, un Programme malveillant était introduit dans les systèmes d'information ou les Données du Client, les frais de diagnostic et de remise en état seraient imputables à l'Editeur, sauf à ce qu'il démontre son absence totale de responsabilité dans cette introduction ;

4. Sécurité dans le développement

4.1 **Cycle de vie du développement logiciel**

Notre processus de développement est basé sur la méthodologie SCRUM. Une backlog de tâches est maintenues sous JIRA. En amont de chaque début de SPRINT, la liste des tâches du SPRINT suivant est définie par l'équipe.

Un gestionnaire de source, GITLAB est utilisé pour gérer nos différentes branches de développements. Chaque projet dispose d'un ensemble de tests unitaires pour assurer les tests de non-régression.

Les développements du sprint courant sont validés par pull-request par l'équipe de développement puis comités sur la branche master du gestionnaire de source.

En interne, nous disposons d'un outil de build automatique Jenkins pour :

- Exécuter de façon automatique des tests de non-régression
- Exécuter de façon automatique des tests de qualité de code
- Déployer de manière automatique les livrables sur nos différents environnements.

En cours de sprint, en cas de validité des tests et de la pull-request, un livrable SNAPSHOT est automatiquement déployé sur notre environnement de développement.

Quelques jours avant la fin du sprint, une release versionnée est construite, avec :

- Dépôt d'un tag sur le gestionnaire de source
- Archivage d'un binaire unique dans notre référentiel de build (Nexus)

La release est enfin déployée et soumise à l'équipe dédiée à la validation afin qu'elle valide l'ensemble des tickets JIRA programmés dans le SPRINT.

Suite à la validation de l'ensemble de ces tickets JIRA, une livraison en production est programmée. Chaque livraison en production est accompagnée d'une procédure de rollback.

4.2 **Analyse des vulnérabilités**

SMART DATA effectue des analyses régulières des systèmes sous-jacents sur lesquels sont hébergés les actifs de l'entreprise accessibles sur Internet, recherche les vulnérabilités.

Des audits automatisés sont réalisés pour un certain nombre de nos clients, tel que le Vendor Security Assessment Questionnaires (VASQ) de Google.

4.3 **Correction des vulnérabilités**

SMART DATA utilise un système de billetterie central à l'échelle de l'entreprise pour suivre tous les problèmes de sécurité jusqu'à la résolution (JIRA).

L'ensemble de l'infrastructure est maintenue à jour au plus près des recommandations de sécurité (CERT-FR, CWE, etc…) en fonction de nos contraintes de production.

4.4 **Tests de pénétration et évaluations internes des risques**

Actuellement, SMART DATA ne fait pas de campagne de tests de pénétration.

5. Backup et PCA

5.1 **Politique de sauvegarde des fichiers**

SMART DATA gère une politique de sauvegarde automatisée de ses données (sur bandes virtuelles) basée sur le principe suivant :

- Sauvegarde complète mensuelle
- Différentielle hebdomadaire
- Incrémentale quotidienne

5.2 **Politique de sauvegarde des VMs**

SMART DATA sauvegarde les machines virtuelles composant son infrastructure de façon quotidienne ou hebdomadaire selon le type de service rendu par ces dernières.

5.3 **Stockage des sauvegardes**

La gestion du stockage des sauvegardes de SMART DATA est basée sur la règle du 3-2-1.

- 3 jeux de données
- 2 supports physiques différents
- 1 jeu de données externalisée

Le jeu de sauvegarde (bandes virtuelles, exports de VMs) est répliqué sur un second serveur.

Les sauvegardes sont physiquement stockées sur des serveurs physiques situés dans un datacenter différent des machines de production.

L'externalisation complète du jeu de sauvegarde chez un autre fournisseur est en cours de mise en œuvre.

5.4 **PCA**

SMART DATA a pensé son infrastructure dans un objectif de résilience grâce à des mécanismes de cluster. Néanmoins, en cas de perte totale de l'infrastructure, SMART DATA serait capable de reconstruire cette infrastructure en partant des sauvegardes.

6. Reporting

Le status d'accès à nos services est disponible sur l'url suivante : https://status.societeinfo.com/