silex | PROTECTION DES DONNÉES ET CYBERSÉCURITÉ

Livre blanc du DPA/RGPD

Le contrat de sous-traitance IT conforme au RGPD

SOMMAIRE

Partie 1 – Éléments obligatoires du contrat de sous-traitance (DPA) et fondements juridiques

Lorsqu'un responsable de traitement confie un traitement de données personnelles à un prestataire externe (sous-traitant), le **Règlement Général sur la Protection des Données (RGPD)** exige la formalisation d'un **contrat de sous-traitance** (aussi appelé *Data Processing Agreement* ou DPA). Ce contrat, conclu **sous forme écrite** (éventuellement électronique), vise à encadrer strictement les opérations réalisées pour le compte du responsable de traitement. L'absence d'un tel contrat expose les parties à des **sanctions** : le manquement à l'obligation d'encadrer la relation par un acte juridique formalisé peut entraîner une amende administrative allant jusqu'à **10 millions d'euros ou 2 %** du chiffre d'affaires annuel mondial. De plus, en cas de contrôle, la CNIL exigera systématiquement la production des contrats de sous-traitance relatifs aux traitements examinés.

Avant même la signature du contrat, le responsable de traitement doit s'assurer de sélectionner un **prestataire offrant des garanties suffisantes** en matière de protection des données. En effet, l'article 28(1) du RGPD impose de ne faire appel qu'à des sous-traitants capables de mettre en œuvre des mesures techniques et organisationnelles appropriées pour assurer la conformité au règlement et la protection des droits des personnes concernées. Ce devoir de diligence amont (vérification des compétences, certifications, fiabilité du sous-traitant, etc.) est la première étape pour réduire les risques. Ensuite, **un contrat ou acte juridique** liera le sous-traitant au responsable de traitement afin de formaliser les obligations de chaque partie. Notons que ce DPA peut être un document autonome **ou être intégré aux conditions générales** ou au contrat principal du prestataire, pourvu qu'il respecte toutes les exigences légales.

Contenu exigé par l'article 28 du RGPD

Le RGPD détaille précisément les **mentions obligatoires** que doit comporter le contrat de sous-traitance. D'abord, le contrat doit **décrire les caractéristiques du traitement confié** : il doit notamment **définir l'objet et la durée du traitement, la nature et la finalité de celui-ci, le type de données personnelles traitées et les catégories de personnes concernées**, ainsi que rappeler les **obligations et droits du responsable du traitement**. Ces éléments factuels constituent le **périmètre** de la prestation et assurent que le sous-traitant n'interviendra que dans le cadre prévu par le contrat. Le responsable de traitement doit également documenter clairement ses **instructions** au prestataire concernant le traitement des données, par exemple en annexe technique si nécessaire. En effet, l'étendue exacte de la mission du sous-traitant est délimitée par les instructions documentées du client ; le prestataire ne doit pas en diverger, sous peine d'être requalifié en responsable de traitement s'il décide lui-même des finalités et moyens du traitement.

Surtout, **l'article 28(3) du RGPD impose une série de clauses obligatoires** à inclure dans tout contrat de sous-traitance. En d'autres termes, le DPA **doit prévoir au minimum** que le sous-traitant :

- **Ne traite les données personnelles que sur instruction documentée** du responsable de traitement (y compris pour tout transfert vers un pays tiers, sauf obligation légale contraire). Autrement dit, le prestataire s'interdit toute utilisation des données en

dehors du cadre défini par le client. S'il estime qu'une instruction viole le RGPD ou le droit applicable, il en avertira immédiatement le responsable de traitement.

- **Garanti la confidentialité des données** traitées. Il doit veiller à ce que les personnes autorisées à accéder aux données s'engagent à la confidentialité ou soient tenues au secret. Cela implique par exemple de faire signer aux employés et éventuels sous-traitants ultérieurs des accords de confidentialité appropriés.
- **Prenne des mesures de sécurité appropriées** afin de protéger les données (conformément à l'article 32 du RGPD). Ce point exige la mise en œuvre de mesures techniques et organisationnelles pour assurer un niveau de sécurité adapté aux risques (pseudonymisation, chiffrement, protections physiques et logicielles, plans de reprise, etc., voir Partie 2).
- **Ne recrute pas un autre sous-traitant sans l'autorisation** écrite préalable du responsable de traitement. Le contrat doit préciser si cette autorisation est donnée de façon spécifique (au cas par cas) ou générale. En cas d'autorisation générale, le prestataire doit informer le client de tout changement (ajout ou remplacement d'un sous-traitant ultérieur) afin que celui-ci puisse émettre des objections. (Nous reviendrons en Partie 2 sur la gestion des sous-traitants ultérieurs).
- **Assiste le responsable de traitement dans la satisfaction des droits des personnes** concernées (droit d'accès, rectification, effacement, opposition, limitation, portabilité, etc.). Concrètement, le sous-traitant doit aider le client à répondre aux demandes reçues de personnes exerçant leurs droits, ou transmettre toute demande reçue directement au client selon les modalités convenues.
- **Aide le responsable de traitement à respecter ses autres obligations réglementaires**, notamment en matière de sécurité, de notification des violations de données, d'**analyses d'impact (AIPD)** et de consultation préalable de l'autorité de contrôle. Le sous-traitant doit fournir son concours pour réaliser les analyses d'impact sur la vie privée si le traitement l'exige, alerter et aider en cas de **violation de données** (voir ci-dessous), et d'une manière générale coopérer avec le client pour garantir la conformité des traitements (articles 32 à 36 RGPD).
- **Supprime ou restitue toutes les données personnelles au terme du contrat**, au choix du responsable de traitement. Le DPA doit prévoir qu'à la fin de la prestation, le sous-traitant effacera **intégralement** les données du client ou bien les renverra à ce dernier (ou à tout autre sous-traitant désigné par le client), selon la décision du responsable de traitement. La destruction des copies doit être attestée par écrit.
- **Fournisse au responsable de traitement toutes les informations nécessaires pour prouver le respect de ses obligations et permette la réalisation d'audits**. En pratique, le prestataire doit tenir à disposition du client la documentation démontrant la conformité (politiques internes, registres, rapports d'audit…), accepter que le client réalise des audits ou inspections, et contribuer activement à ces contrôles.

Ces clauses essentielles (résumées ci-dessus) **doivent figurer explicitement** dans le contrat pour se conformer à l'article 28 RGPD. À noter que le RGPD prévoit également que le sous-traitant demeure pleinement responsable vis-à-vis du responsable de traitement en cas de recours à des sous-traitants ultérieurs : le prestataire initial doit s'assurer que tout sous-traitant secondaire respecte les mêmes obligations et il reste **responsable des manquements** de celui-ci à l'égard du client. Enfin, le contrat doit mentionner, le cas échéant, le **délégué à la**

protection des données (DPO) du sous-traitant et ses coordonnées si celui-ci en a désigné un, et le sous-traitant doit déclarer tenir un **registre de ses activités de traitement** réalisées pour le compte du client, conformément à l'article 30 RGPD.

En synthèse, l'article 28 RGPD impose un véritable **cahier des charges contractuel** visant à encadrer strictement la sous-traitance de données personnelles. La liste ci-dessous récapitule les points devant impérativement figurer dans le DPA :

- ***Objet du contrat*** : portée du service confié (ex. maintenance applicative, stockage cloud…) et description précise du traitement (finalité, nature du traitement effectué, catégories de données et de personnes concernées, durée).
- ***Instructions du client*** : le sous-traitant n'agit que sur instructions écrites du responsable de traitement et l'informe immédiatement s'il estime qu'une instruction viole la réglementation.
- ***Confidentialité*** : obligation de discrétion pour le prestataire et son personnel sur les données traitées.
- ***Sécurité*** : mesures techniques et organisationnelles pour protéger les données (article 32 RGPD).
- ***Sous-traitance ultérieure*** : conditions de recours à des sous-traitants secondaires (autorisation du client, information préalable, mêmes obligations imposées aux sous-traitants ultérieurs).
- ***Aide aux droits des personnes*** : assistance du sous-traitant pour répondre aux demandes d'accès, de rectification, etc..
- ***Notification des violations*** : signalement sans délai au responsable de traitement de toute violation de données personnelles, avec les informations nécessaires (nature de l'incident, données affectées, mesures prises).
- ***Assistance conformité*** : coopération pour les analyses d'impact et consultations CNIL, et plus généralement respect des obligations des articles 32 à 36 RGPD (sécurité, notification des failles, AIPD, etc.).
- ***Sort des données en fin de contrat*** : restitution ou destruction des données traitées, au choix du client, avec garantie d'effacement complet des copies et confirmation écrite.
- ***Preuve de conformité et audits*** : mise à disposition par le prestataire de toutes les documentations nécessaires pour prouver la conformité et acceptation d'audits par le client ou un tiers mandaté.

Chacun de ces points est indispensable pour avoir un contrat conforme et protéger efficacement les données confiées. En l'absence de clauses couvrant l'ensemble de ces exigences, le contrat de sous-traitance sera jugé **non conforme**, exposant le responsable de traitement à un risque juridique sérieux (sanction RGPD, mise en demeure de la CNIL, etc.). Le DPO et les juristes devront donc vérifier systématiquement la présence de ces dispositions lors de la rédaction ou de l'audit des contrats.

Enfin, il convient de souligner que depuis juin 2021, la Commission européenne a adopté des **clauses contractuelles types** spécifiques pour les contrats de sous-traitance conformes à l'article 28 RGPD. Ces modèles officiels (dits *clauses types "responsable-sous-traitant"*) peuvent être utilisés par les entreprises pour accélérer la mise en conformité de leurs DPA. Ils

couvrent l'ensemble des obligations légales évoquées ci-dessus. Les parties conservent toutefois la liberté d'ajouter des clauses supplémentaires en fonction de leur contexte d'activité, comme nous allons le voir en Partie 2. En outre, si la prestation implique des **transferts de données hors de l'UE**, il faudra également intégrer les clauses contractuelles types de transfert international ou tout autre mécanisme de transfert adéquat (conformément au Chapitre V du RGPD), point sur lequel nous reviendrons également.

Partie 2 – Clauses contractuelles annexes importantes (sécurité, propriété intellectuelle, confidentialité, etc.)

En plus des éléments obligatoires dictés par le RGPD (Partie 1), un **contrat de sous-traitance IT complet** devrait comporter un ensemble de **clauses annexes** visant à préciser les responsabilités et à protéger au mieux les intérêts du responsable de traitement. En effet, si le contenu minimal du DPA est encadré par la loi, les parties restent libres de négocier des **dispositions complémentaires** pour adapter le contrat à leur situation particulière et couvrir des aspects non explicitement traités par le RGPD. Le Comité européen de la protection des données (CEPD) encourage d'ailleurs les responsables de traitement et sous-traitants à détailler contractuellement leurs obligations respectives au-delà du socle légal, afin de prévenir les litiges et assurer une protection effective des données.

Ainsi, un DPA négocié par un DPO ou un juriste vigilant inclura généralement des clauses supplémentaires portant notamment sur : **la sécurité renforcée des traitements**, la **confidentialité étendue** des informations, les droits de **propriété intellectuelle** sur les données et développements, la **responsabilité** et l'indemnisation en cas de manquement, le **droit d'audit** du prestataire, la gestion des **sous-traitants ultérieurs** (chaîne de sous-traitance), les conditions de **transfert international** des données, ou encore des droits de **résiliation** spécifiques liés à la conformité. Nous abordons ci-dessous ces principales clauses annexes et leur portée, en adoptant une perspective de **bonne pratique contractuelle** du point de vue du responsable de traitement.

Mesures de sécurité renforcées et gestion des incidents

Le RGPD oblige déjà le sous-traitant à prendre toutes les **mesures de sécurité** requises par l'article 32, mais il est recommandé d'insérer dans le contrat une clause détaillant les engagements de sécurité du prestataire. Cette clause peut renvoyer à une **annexe technique de mesures de sécurité** décrivant précisément les protections mises en place (pare-feu, contrôle d'accès, chiffrement des données en transit et au repos, sauvegardes, etc.), et éventuellement les **normes** ou **certifications** auxquelles le prestataire se conforme (par ex. ISO 27001, ISO 27701, HDS pour l'hébergement de données de santé, certification SecNumCloud, etc.). On rappellera que l'article 32 RGPD impose une approche par les risques : les mesures doivent garantir un niveau de sécurité adapté compte tenu de l'état de l'art, des coûts, de la nature des données et des risques pour les personnes. Sont cités en exemple : la pseudonymisation et le chiffrement des données, la capacité à assurer la confidentialité, l'intégrité, la disponibilité et la résilience des systèmes, et la capacité à restaurer les données en cas d'incident. Il est fréquent de lister dans le DPA des mesures telles que : **chiffrement** des données sensibles, **authentification forte** des utilisateurs, journalisation et **traçabilité** des accès, cloisonnement des environnements, tests d'intrusion périodiques, etc. Ces engagements doivent être adaptés à la nature de la prestation (par exemple, un infogérant infrastructure fournira des garanties de disponibilité et sauvegarde, un éditeur SaaS mettra l'accent sur le chiffrement et la gestion des accès applicatifs, etc.).

Une attention particulière doit être portée à la **répartition des responsabilités de sécurité** entre le client et le prestataire. Certaines mesures relèvent en effet du responsable de traitement (paramétrage de sécurité du logiciel, gestion des habilitations côté client, etc.) tandis que d'autres incombent au sous-traitant. Il est **recommandé de clarifier**

contractuellement la responsabilité de chaque partie pour chaque mesure de sécurité mise en œuvre. Cette précision évitera les zones d'ombre et les « angles morts » dans la sécurité du traitement. Par exemple, le contrat peut stipuler que le client est responsable de la sécurisation de son réseau et de ses postes de travail, tandis que le prestataire garantit la sécurité côté serveur (data center) et la protection applicative côté backend. En cas de manquement de l'une des parties sur son périmètre, sa responsabilité pourra alors être engagée plus facilement.

En matière de **gestion des incidents** et des **violations de données**, le contrat doit prévoir des procédures de notification efficaces. L'article 33 du RGPD impose à tout sous-traitant d'alerter **sans délai** le responsable de traitement en cas de violation de données personnelles. Dans la pratique, il est conseillé de fixer un **délai maximum contractuel** (par exemple *24 ou 48 heures*) pour la notification par le prestataire d'une faille de sécurité au client. Le DPA pourra préciser les modalités de cette notification (point de contact à alerter chez le client, informations devant être fournies dans le rapport d'incident, etc.). La notification devrait inclure **toute la documentation disponible** afin d'assister le responsable de traitement dans sa propre obligation de notifier l'autorité de contrôle (CNIL) sous 72 heures si nécessaire. Typiquement, on attend du prestataire qu'il communique la **nature de la violation**, les catégories et le volume de données concernées, les conséquences probables et les mesures correctives déjà prises ou envisagées. Une clause type pourra stipuler par exemple : *« Le Sous-Traitant notifie au Responsable de Traitement toute violation de données à caractère personnel dans un délai maximum de [X] heures après en avoir pris connaissance, par email à l'adresse de contact désignée. Cette notification comprendra au minimum : la description de la nature de la violation, les catégories et le nombre approximatif de personnes et d'enregistrements de données concernés, le nom et les coordonnées du DPO ou point de contact, les conséquences probables de la violation, et les mesures correctives prises ou envisagées. »*. Le contrat peut également prévoir qu'**avec l'autorisation du client**, le sous-traitant se charge de notifier directement la CNIL en son nom (notamment pour gagner du temps), ou de communiquer aux personnes concernées la survenance d'une violation si celle-ci est susceptible d'engendrer un risque élevé pour leur vie privée. Ces derniers points restent optionnels et à évaluer au cas par cas, le responsable de traitement préférant souvent garder la maîtrise de la communication envers l'autorité et les individus affectés.

En résumé, la clause "Sécurité" d'un DPA doit non seulement réitérer l'obligation de moyens du prestataire pour assurer la sécurité des données, mais aussi la **traduire en engagements concrets** (mesures précises, plans d'urgence, seuils de service minimum en cas d'incident, etc.), tout en définissant qui fait quoi entre le client et le fournisseur. Cette approche proactive renforce la protection des données et fournit un niveau de détail utile en cas d'audit ou de survenance d'un incident de sécurité.

Clause de confidentialité étendue

Outre la confidentialité des données personnelles elle-même (déjà obligatoire, cf. art. 28(3) et art. 29 RGPD), il est recommandé d'ajouter une **clause de confidentialité générale** couvrant **toutes les informations échangées** dans le cadre du contrat. En effet, lors d'une prestation IT, le sous-traitant aura non seulement accès à des données personnelles, mais aussi potentiellement à des informations sensibles du client : secrets d'affaires, informations techniques sur le système d'information, codes source, stratégies, etc.

Réciproquement, le client peut être exposé à certaines informations confidentielles du prestataire (par ex. méthodes propriétaires, pricing internes, etc.).

La clause de confidentialité viendra donc **engager contractuellement les parties (surtout le prestataire)** à garder strictement confidentielles toutes les informations non publiques obtenues de l'autre partie, à ne les utiliser que pour les besoins de la prestation et à ne les divulguer à aucun tiers sans autorisation préalable. Le sous-traitant devra notamment s'assurer que son personnel, ses éventuels sous-traitants ultérieurs et tous ses collaborateurs respectent également cette obligation de confidentialité élargie. Il est utile de préciser que cette obligation de confidentialité **survit après la fin du contrat**, pour une durée définie (par ex. **5 ans** après la fin de la mission, ou sans limite de durée concernant les secrets protégés tant qu'ils restent confidentiels).

On peut s'inspirer des clauses classiques de **NDA** (*No-Disclosure Agreement*) en stipulant, par exemple : *« Chaque partie s'engage à considérer comme strictement confidentielles toutes les informations, de quelque nature qu'elles soient, reçues de l'autre partie ou portées à sa connaissance à l'occasion de l'exécution du présent contrat (notamment informations commerciales, financières, techniques ou relatives aux données personnelles). Elle s'interdit de les divulguer à quiconque, directement ou indirectement, ainsi que de les exploiter pour d'autres finalités que l'exécution du contrat, sans l'autorisation écrite préalable de l'autre partie. Le Sous-Traitant garantit le respect de cet engagement par l'ensemble de son personnel et de ses éventuels sous-traitants ultérieurs. L'obligation de confidentialité demeurera en vigueur pendant toute la durée du contrat et [X] ans après son expiration, pour quelque cause que ce soit. »*

Cette clause de confidentialité générale complète utilement l'obligation de confidentialité ciblée sur les données personnelles prévue par le RGPD. Elle offre une protection plus large au responsable de traitement en couvrant *toutes* les données et informations liées au projet. En cas de violation (par exemple, divulgation non autorisée d'une information stratégique du client par un employé du prestataire), le responsable de traitement pourra agir en **responsabilité contractuelle** contre le sous-traitant sur le fondement de cette clause, indépendamment des recours prévus par le RGPD. Pour le prestataire, c'est également une garantie que le client ne divulguera pas d'informations sensibles le concernant (même si dans la plupart des cas, c'est surtout le client qui souhaite protéger ses données).

Clauses de propriété intellectuelle et « propriété » des données

Dans le contexte d'un contrat IT, il est important de clarifier les enjeux de **propriété intellectuelle (PI)** liés aux données et aux résultats de la prestation. Sur le plan du RGPD, les données personnelles ne sont pas à proprement parler une « propriété » du responsable de traitement, mais ce dernier en a la **maîtrise légale** et détermine les finalités du traitement. Il est donc légitime de prévoir dans le contrat que le responsable de traitement conserve l'**entière maîtrise et disponibilité des données** confiées. En pratique, on insère souvent une clause stipulant que **les données demeurent la propriété du client** (ou de ses propres donneurs d'ordre), le sous-traitant n'acquérant **aucun droit** sur ces données du seul fait de la prestation. Le prestataire ne peut traiter ou utiliser les données que pour exécuter le contrat et selon les instructions du client, ce qui rejoint l'obligation légale de ne pas sortir du périmètre instruit. Il est utile de rappeler explicitement cette interdiction de toute réutilisation des

données à des fins propres ou pour le compte de tiers sans autorisation écrite du responsable de traitement. La CNIL souligne qu'un sous-traitant ne peut en effet *« réutiliser des données personnelles pour son propre compte que si cette réutilisation est compatible avec le traitement initial et que le responsable de traitement lui a donné son autorisation écrite »*. Une telle clause conforte le principe que les données confiées restent sous le contrôle du client.

Du point de vue *propriété intellectuelle stricto sensu*, si la mission du prestataire inclut du développement logiciel, de l'analyse de données ou la production de livrables spécifiques, le contrat doit déterminer qui détiendra les **droits de propriété intellectuelle** afférents. Par exemple, un éditeur de logiciel SaaS restera propriétaire de sa plateforme et de tous les outils mis à disposition, le client n'ayant qu'un droit d'utilisation (licence) prévu par le contrat principal. À l'inverse, si le prestataire réalise un développement sur mesure ou un rapport à partir des données du client, ce dernier voudra s'assurer de pouvoir en disposer librement. On pourra stipuler que les **livrables** (documents, analyses, configurations, code) produits dans le cadre de la prestation sont cédés au client, ou qu'il bénéficie d'une licence d'utilisation étendue. L'objectif est d'éviter toute ambiguïté sur le point de savoir qui peut exploiter tel résultat ou tel **ensemble de données** après la fin du contrat.

Une clause PI typique pourrait articuler que *« Le Responsable de Traitement conserve la pleine et entière propriété des données à caractère personnel mises à disposition du Sous-Traitant pour les besoins du contrat. Le Sous-Traitant n'acquiert aucun droit, titre, ni intérêt sur ces données et s'interdit toute utilisation qui n'est pas strictement nécessaire à l'exécution de ses obligations contractuelles. Par ailleurs, les méthodes, savoir-faire, logiciels ou outils appartenant au Sous-Traitant et utilisés pour la prestation restent sa propriété exclusive. De son côté, le Responsable de Traitement demeure propriétaire de ses bases de données, architectures et plus généralement de tous les éléments qu'il fournit. Chaque partie reste également propriétaire des droits de propriété intellectuelle qu'elle détenait avant le début de la prestation. Les résultats spécifiques (études, développements, rapports…) issus de la prestation seront [la propriété du Responsable de Traitement / cédés au Responsable de Traitement pour les besoins de ses activités / exploités conformément aux stipulations de l'accord principal sur la PI]. »*

En somme, cette clause vise à protéger le **patrimoine immatériel** du client (ses données et tout ce qui pourrait en dériver) tout en préservant les droits du prestataire sur ses solutions techniques. Elle évite que le sous-traitant puisse revendiquer un droit sur les données ou refuser leur restitution en invoquant un droit de rétention, par exemple. Elle consolide aussi l'interdiction pour le prestataire d'exploiter les données à d'autres finalités que celles du contrat, sauf accord du client. Pour un responsable de traitement, c'est une garantie cruciale : ses données, souvent stratégiques, ne changeront pas de main ni ne seront monétisées sans son consentement.

Clauses de responsabilité et d'indemnisation

La question de la **responsabilité** en cas de manquement du sous-traitant est un enjeu majeur lors de la négociation du contrat. Juridiquement, l'article 82 du RGPD prévoit que toute personne ayant subi un dommage matériel ou moral du fait d'une violation du règlement peut obtenir réparation, le responsable de traitement et le sous-traitant pouvant être tenus pour responsables solidairement vis-à-vis de la victime dans certains cas. Toutefois, le RGPD précise

que le sous-traitant n'est responsable des dommages que s'il a **outrepassé les instructions licites** du responsable de traitement ou violé spécifiquement les obligations qui lui incombent en vertu du RGPD. En d'autres termes, le sous-traitant est exempté de responsabilité vis-à-vis des personnes concernées s'il a strictement agi sur instruction et n'a commis aucune violation du règlement de son propre fait.

Entre les parties (c'est-à-dire dans le contrat DPA lui-même), il est **possible de moduler la répartition des responsabilités**. Le contrat peut prévoir des clauses d'**indemnisation** par lesquelles le sous-traitant s'engage à indemniser le responsable de traitement si ce dernier venait à subir un préjudice ou être tenu responsable en raison d'un manquement du sous-traitant. Par exemple, le DPA peut stipuler que le prestataire indemnisera le client à hauteur de tous les coûts, amendes, dommages-intérêts, honoraires d'avocat, etc., résultant d'une violation du RGPD imputable au prestataire. Ce type de clause assure que le risque financier final retombe sur la partie fautive. Du point de vue du responsable de traitement, c'est une protection essentielle, notamment contre le risque de sanctions administratives ou de réclamations de personnes concernées déclenchées par une erreur du sous-traitant (ex. une fuite de données due à une négligence de sécurité chez le prestataire).

En pratique, les prestataires chercheront toutefois à **limiter contractuellement leur responsabilité**. Ils peuvent proposer d'insérer des plafonds d'indemnisation (par exemple limiter la responsabilité globale du sous-traitant au montant du contrat ou à un multiple de ce montant), ou exclure certains types de dommages (ex. pertes de profit, dommages indirects). Le RGPD n'interdit pas formellement de telles limitations entre responsables de traitement et sous-traitants, mais celles-ci **ne doivent pas vider de sa substance la protection des données**. La CNIL a d'ailleurs mis en garde contre des contrats « manifestement déséquilibrés » qui feraient reposer sur le sous-traitant des obligations disproportionnées ou, inversement, qui exonéreraient trop facilement le prestataire. Par exemple, une clause par laquelle le responsable de traitement renoncerait par avance à tout recours contre le sous-traitant en cas de violation du RGPD pourrait être jugée contraire à cette logique (car neutralisant l'obligation de sécurité, etc.). De même, un plafond de responsabilité dérisoire ne serait pas acceptable s'agissant d'obligations aussi fondamentales.

Le **juste équilibre** doit donc être recherché. Une approche courante consiste à aligner la responsabilité du sous-traitant sur celle prévue dans le contrat principal de service : le DPA renvoie alors aux limitations de responsabilité définies dans le contrat commercial (ex. un plafond global égal aux redevances annuelles). Toutefois, pour les aspects relatifs à la protection des données, le responsable de traitement pourra exiger un **niveau d'engagement supérieur**. Par exemple, il est fréquent d'exclure du plafond de responsabilité les violations de la confidentialité des données ou les amendes RGPD : en clair, stipuler que ces dommages-là seront intégralement supportés par le sous-traitant fautif, **sans plafond**, compte tenu de la gravité qu'ils représentent.

Il est également recommandé de prévoir que le sous-traitant possède une **assurance responsabilité civile** couvrant les risques liés à la protection des données (cyber assurance), avec un montant de garantie adéquat, et qu'il s'engage à maintenir cette assurance pendant toute la durée du contrat. Cette mention, bien qu'indirecte, offre une sécurité supplémentaire quant à la capacité du prestataire à faire face financièrement aux conséquences d'un incident.

En résumé, la clause de responsabilité doit rechercher une répartition **équitable du risque**. Le responsable de traitement voudra s'assurer qu'il dispose de voies de recours efficaces si le prestataire commet une faute entraînant un préjudice, tandis que le sous-traitant cherchera à éviter d'assumer l'intégralité des conséquences économiques d'un incident majeur hors de proportion avec sa rémunération. L'important est de **négocier clairement ces aspects en amont** et de les formaliser précisément. En cas d'incident, un contrat bien rédigé permettra de déterminer rapidement qui supporte quoi, et d'éviter des litiges longs et coûteux.

Droit d'audit et conformité documentaire

Comme évoqué en Partie 1, le responsable de traitement a le droit (et même le devoir) de **vérifier la conformité** de son sous-traitant tout au long du traitement. L'article 28(3)h) RGPD impose que le prestataire fournisse au client toute information nécessaire pour démontrer le respect de ses obligations et contribue aux audits. Dans la pratique, il est très utile de détailler dans le contrat les modalités de ce **droit d'audit**.

Une clause d'audit bien construite pourrait prévoir par exemple que *« Le Responsable de Traitement (ou tout auditeur externe qu'il aura mandaté) pourra, une fois par an au maximum, sous réserve d'un préavis écrit de [X] jours, procéder à un audit des installations, systèmes, procédures et documents du Sous-Traitant directement liés aux traitements de données personnelles effectués pour son compte, afin de vérifier le respect des exigences du présent contrat et de la réglementation applicable. Le Sous-Traitant s'engage à coopérer de bonne foi à cet audit. Les audits seront réalisés pendant les heures ouvrées normales et ne devront pas affecter de manière substantielle les activités du Sous-Traitant. Chaque partie supporte ses propres coûts liés à l'audit, à moins qu'un manquement significatif du Sous-Traitant ne soit mis en évidence, auquel cas les coûts raisonnables de l'audit pourront être mis à sa charge. »*

L'objectif est de donner un cadre clair à l'exercice du droit d'audit, pour éviter toute contestation ou mauvaise surprise. Du point de vue du responsable de traitement, il faut veiller à conserver un **accès suffisant** à l'information : par exemple, certains prestataires peuvent proposer de limiter les audits aux seuls rapports fournis par eux (certifications, audits tiers type SOC 2, etc.). Ces rapports externes sont très utiles (et le contrat peut mentionner que le prestataire fournira annuellement ses **rapports de certification** ou résultats de tests de pénétration), mais ils ne remplacent pas entièrement le droit pour le client de conduire lui-même un audit si nécessaire. En revanche, du point de vue du sous-traitant, il est légitime d'encadrer les audits pour éviter des intrusions trop fréquentes ou désorganisées dans ses opérations. La clause doit trouver un compromis entre **transparence** et **praticabilité**.

Il est également recommandé d'inclure dans le DPA une obligation pour le sous-traitant de **mettre à disposition la documentation** de conformité. Cela recouvre par exemple : la fourniture du **registre des traitements** du sous-traitant sur demande (extrait pertinent lié au contrat), la communication des politiques de sécurité internes, des preuves de formations du personnel, des plans de continuité, etc. Le prestataire doit démontrer son respect du principe d'**accountability** en prouvant qu'il a bien pris en charge les obligations RGPD. Le contrat peut lister les documents que le client peut exiger en cours de contrat (par exemple, remise annuelle d'un rapport de performance sur les mesures de sécurité et incidents survenus).

En somme, la clause d'audit et de documentation garantit au responsable de traitement un **droit de regard permanent** sur le respect des règles par son prestataire. Elle concrétise le

principe *« Trust but verify »* : on fait confiance au sous-traitant sélectionné, mais on s'assure de pouvoir vérifier concrètement cette confiance via des contrôles périodiques. Cette clause est cruciale pour les DPO et juristes, car elle conditionne leur capacité à **piloter la conformité** des opérations externalisées et à réagir vite en cas de manquement.

Gestion des sous-traitants ultérieurs (cascade de sous-traitance)

Nombre de prestations IT impliquent elles-mêmes d'autres acteurs en bout de chaîne : par exemple, un éditeur SaaS peut s'appuyer sur un hébergeur cloud, ou un prestataire faire appel à un freelance en renfort. On parle de **sous-traitance en cascade** (ou *chaîne de sous-traitance*). Le RGPD encadre strictement ce recours aux sous-traitants ultérieurs : le sous-traitant initial **ne peut en recruter un autre sans l'autorisation** du responsable de traitement (voir art. 28(2)), et il doit imposer à ce sous-traitant ultérieur les **mêmes obligations** en matière de protection des données que celles prévues dans le contrat initial (art. 28(4)). En outre, comme indiqué plus haut, le prestataire initial demeure **pleinement responsable** vis-à-vis du client en cas de manquement du sous-traitant ultérieur.

Au-delà de ces obligations minimales, une bonne pratique contractuelle est d'exiger une **transparence totale** sur la chaîne des sous-traitants. Le CEPD recommande que le responsable de traitement sache *à tout moment* **qui sont tous les sous-traitants ultérieurs** intervenant sur ses données, y compris plus loin dans la chaîne, et qu'il dispose de leurs informations d'identité et de contact. Ainsi, le DPA devrait prévoir que le prestataire fournit au client la **liste exhaustive** de ses propres sous-traitants (sous-traitance de second niveau) et des éventuels sous-traitants de ces derniers (troisième niveau, etc.), dans la mesure où ils interviennent sur les données personnelles en question. Cette liste devrait être maintenue **à jour en temps réel** et idéalement intégrée en annexe du contrat, avec une obligation pour le prestataire de notifier le client **avant toute modification** (ajout ou retrait d'un sous-traitant). C'est en effet la condition pour que le client puisse exercer son droit d'objection en toute connaissance de cause et assurer aux personnes concernées une information complète sur qui traite leurs données.

La clause de sous-traitance ultérieure précisera aussi la **procédure d'approbation** : par exemple, *« Le Responsable de Traitement accorde une autorisation générale au Sous-Traitant pour engager des sous-traitants ultérieurs aux conditions suivantes : le Sous-Traitant communiquera par écrit au Responsable de Traitement la liste initiale de ses sous-traitants agréés (annexe…), et l'informera par email au moins [X] jours ouvrés à l'avance de toute intention d'ajouter ou de remplacer un sous-traitant. Le Responsable de Traitement disposera d'un délai de [Y] jours à compter de cette notification pour émettre d'éventuelles objections. En l'absence d'objection dans ce délai, le nouveau sous-traitant sera réputé approuvé. En cas d'objection justifiée du Responsable de Traitement (par exemple si le sous-traitant proposé présente des garanties insuffisantes), les parties négocieront de bonne foi une solution alternative. Le Sous-Traitant s'engage à ce que chacun de ses sous-traitants ultérieurs respecte strictement les mêmes obligations de protection des données que celles stipulées au présent contrat, et demeure entièrement responsable envers le Responsable de Traitement de l'exécution par ceux-ci de leurs obligations. »*

Cette clause permet au responsable de traitement de garder la **maîtrise de la chaîne** et d'éviter qu'un acteur non validé manipule ses données à son insu. Elle encourage aussi le sous-

traitant à sélectionner des partenaires fiables, sachant qu'il devra rendre des comptes de leur performance. Notons qu'en vertu du principe d'accountability, le responsable de traitement reste de son côté tenu de pouvoir démontrer qu'il n'a recours qu'à des sous-traitants (directs ou indirects) offrant des garanties suffisantes. Il ne saurait donc se décharger entièrement sur le prestataire initial : il doit **vérifier et documenter** que chaque maillon de la chaîne est conforme. Le contrat peut l'y aider en imposant par exemple que le prestataire fournisse les **preuves de conformité** de ses sous-traitants (certifications, audits, etc.).

Transferts internationaux de données

Dans un contexte de sous-traitance IT, il est fréquent que les données puissent être hébergées ou accessibles **en dehors de l'Union européenne** (par exemple si le prestataire utilise des centres de données aux USA ou en Asie, ou si son support technique est international). Or, le RGPD impose des conditions strictes pour les **transferts de données hors UE** (chapitre V du RGPD). Il est donc indispensable de traiter ce point dans le contrat.

D'abord, le DPA devrait stipuler que le sous-traitant **ne transférera pas** les données personnelles hors de l'Espace Économique Européen **sans l'autorisation préalable écrite** du responsable de traitement. Cela permet au client de garder le contrôle sur la localisation de ses données. Si des transferts hors UE sont envisagés (par ex. utilisation d'un cloud public avec des serveurs aux États-Unis), le contrat doit exiger la mise en place de **garanties appropriées** conformes au RGPD : typiquement, la signature des **Clauses Contractuelles Types (CCT)** adoptées par la Commission européenne pour les transferts internationaux, ou l'adhésion à des règles d'entreprise contraignantes (BCR) validées, ou encore l'application d'une exception prévue par le RGPD (consentement explicite de la personne, etc.) dans les cas limités où c'est possible.

Les transferts vers des pays sans niveau de protection reconnu nécessitent en plus une **évaluation des risques** et des mesures additionnelles (chiffrement fort, etc.). Un contrat de sous-traitance sérieux mentionnera que le sous-traitant doit **coopérer avec le responsable de traitement** pour effectuer ces analyses d'impact transferts (*TIA*) et pour mettre en œuvre les mesures complémentaires requises le cas échéant. Par exemple : *« Le Sous-Traitant s'engage à informer le Responsable de Traitement de tout transfert de données en dehors de l'UE et à ne procéder à un tel transfert qu'après avoir mis en place un mécanisme de transfert valide (telles que les clauses contractuelles types de la Commission européenne) approuvé par le Responsable de Traitement. Il assistera le Responsable de Traitement dans la réalisation de toute évaluation d'impact relative aux transferts et dans la mise en œuvre de garanties supplémentaires visant à assurer un niveau de protection essentiel équivalent à celui garanti au sein de l'UE. »*

Par ailleurs, le contrat devrait adresser la question des **demandes d'accès étrangères** (par exemple une demande d'autorité gouvernementale américaine d'accéder aux données hébergées). Une clause de **coopération juridique** peut stipuler que le sous-traitant informera le responsable de traitement immédiatement s'il reçoit une demande légale de divulgation de données, qu'il ne donnera suite qu'après instruction du client, et qu'il épuisera les voies de recours pour s'y opposer si la demande paraît excessive ou non conforme au droit européen. Cette précaution contractuelle, apparue suite aux préoccupations liées au CLOUD Act américain, vise à protéger la souveraineté des données du client.

En résumé, la clause “Transferts internationaux” est incontournable dès lors que des données peuvent sortir de l’UE. Elle doit garantir que le responsable de traitement conserve la **mainmise sur les décisions de transfert** et que le sous-traitant respecte scrupuleusement les exigences du RGPD en la matière. Pour les directeurs juridiques et DPO, c’est un point de vigilance majeur, car la non-conformité des transferts est un motif fréquent de sanction. Un DPA robuste fournira donc un cadre clair sur ce qui est permis ou non et sur les obligations du prestataire en cas de transfert transfrontière des données.

Autres clauses utiles et clauses finales

Enfin, d’autres clauses diverses méritent d’être envisagées pour compléter le contrat de sous-traitance IT :

- **Clause de coopération avec l’autorité de contrôle** : on peut prévoir que le sous-traitant assistera le responsable de traitement en cas de contrôle ou de réquisition de la CNIL, notamment en fournissant sans tarder les informations ou documents nécessaires, et qu’il informera le client de toute interaction avec la CNIL concernant les traitements sous-traités.
- **Clause de durée et de résiliation** : généralement, la durée du DPA est alignée sur la durée du contrat de service principal. Il est utile de préciser que **la fin du contrat principal entraîne automatiquement la fin du DPA** (sauf pour les stipulations devant survivre, comme la confidentialité et le sort des données). Il peut être ajouté que le responsable de traitement peut suspendre ou résilier le DPA (et donc la prestation) en cas de **violation grave** des obligations de protection des données par le sous-traitant, sans préavis et sans indemnité pour ce dernier. Cette faculté de résiliation pour manquement RGPD constitue une garantie de dernier recours.
- **Clause de réversibilité** : en lien avec le sort des données, on peut inclure des modalités opérationnelles de réversibilité en fin de contrat (format de restitution des données, assistance fournie par le prestataire pour la migration des données vers un autre système, coûts éventuels de cette assistance). Cela garantit une transition fluide, empêche le prestataire de « retenir » les données du client et en facilite le « réemploi ».
- **Clause relative au DPO** : si le sous-traitant est tenu de désigner un DPO, mentionner ses coordonnées et s’engager à le maintenir en poste tant que requis, et à ce que le client puisse le contacter directement en cas de besoin. Côté client, si un DPO est en place, identifier aussi son contact pour faciliter les échanges.
- **Pénalités ou sanctions contractuelles** : certains contrats prévoient des pénalités financières en cas de manquement du prestataire à certaines obligations (ex. retard dans la notification d’un incident, non-respect d’un plan de sécurité convenu, etc.). Ces pénalités (soumises en droit français à des critères de proportionnalité) peuvent avoir un effet dissuasif utile, bien qu’elles ne remplacent pas les recours de droit commun.
- **Lois applicables et juridiction** : dans la plupart des cas, le DPA suivra la loi applicable du contrat principal (souvent le droit français si le client est en France, ou autre loi UE pertinente) et les litiges seront soumis aux mêmes tribunaux compétents. Il est bon de le préciser pour éviter toute confusion, surtout si le prestataire est étranger. On peut rappeler que quelles que soient les lois choisies, le sous-traitant doit **de toute façon**

respecter le RGPD dès lors qu'il traite des données de résidents de l'UE pour le compte du client.

- **Hiérarchie des documents** : si le DPA est un appendice au contrat principal ou aux CGV du prestataire, il est prudent de stipuler qu'en cas de conflit entre les dispositions, ce sont celles du DPA (spécifiques à la protection des données) qui prévaudront sur toute autre clause du contrat contraire. Cela évite que des clauses limitatives de responsabilité ou autres dispositions générales viennent contredire les obligations de protection des données.

Chaque clause additionnelle doit être calibrée selon le contexte de la prestation et les **risques identifiés**. Par exemple, un simple contrat de maintenance applicative n'appellera pas nécessairement une clause PI très poussée, tandis qu'un contrat d'externalisation de processus métier critique impliquant des données sensibles justifiera l'ensemble des clauses renforcées décrites ci-dessus. L'essentiel est de **verrouiller contractuellement tous les points névralgiques** liés à la protection des données et à la conformité RGPD, au-delà du strict minimum légal. C'est à ce prix que le responsable de traitement (et son DPO) pourra dormir sur ses deux oreilles en ayant externalisé un traitement de données : un bon contrat de sous-traitance est avant tout un filet de sécurité juridique et opérationnel.

Partie 3 – Modèle de contrat de sous-traitance (DPA) complet pour une prestation IT

Nous présentons ci-après un **modèle complet de Data Processing Agreement (DPA)** couvrant l'ensemble des obligations légales et clauses recommandées exposées précédemment. Ce modèle est fourni dans un contexte type : celui d'un responsable de traitement (client) confiant des données à un prestataire **éditeur de logiciel** (sous-traitant) dans le cadre d'une solution SaaS. Le contrat est rédigé du point de vue du responsable de traitement, incluant des clauses protectrices maximales. Bien entendu, ce modèle devra être **adapté et négocié** en fonction de la situation concrète de chaque partie (nature du service, volume de données, sensibilités particulières, etc.). Il s'inspire notamment des exemples de clauses proposés par la CNIL, enrichis de bonnes pratiques actuelles.

Pour faciliter la lecture, le terme « RGPD » désigne le Règlement (UE) 2016/679. Le contrat emploie les définitions de « Responsable de Traitement » et « Sous-Traitant » au sens de l'article 4 du RGPD. Le Responsable de Traitement est la société cliente qui détermine les finalités et moyens du traitement. Le Sous-Traitant est la société prestataire qui traite les données pour le compte du client.

Contrat de Sous-Traitance de données à caractère personnel (Data Processing Agreement)

Entre les soussignés :

- **[Nom de la société Cliente]**, située à [adresse complète], représentée par [nom, fonction], dûment habilité aux fins des présentes, (ci-après le « **Responsable de Traitement** » ou « Client »),

Et

- **[Nom de la société Prestataire]**, située à [adresse complète], immatriculée [numéro d'enregistrement], représentée par [nom, fonction], dûment habilité, (ci-après le « **Sous-Traitant** » ou « Prestataire »),

Ci-après individuellement une « Partie » et ensemble les « Parties ».

Préambule : Dans le cadre de leurs relations contractuelles, les Parties reconnaissent que le Responsable de Traitement détermine les finalités et les moyens des traitements de données personnelles confiés au Sous-Traitant dans le cadre du service défini ci-après. Le Sous-Traitant agit exclusivement pour le compte et sur instructions du Responsable de Traitement. Le présent **contrat de sous-traitance** (ci-après le « Contrat ») a pour objet de définir les conditions et modalités selon lesquelles le Sous-Traitant s'engage à traiter des **données à caractère personnel** pour le compte du Responsable de Traitement, conformément aux exigences du droit applicable et notamment du RGPD. Il constitue l'exécution de l'obligation prévue à l'article 28 du RGPD d'encadrer par un acte juridique la relation entre Responsable de Traitement et Sous-Traitant.

1. Objet du Contrat

Le présent Contrat fait partie intégrante de [***l'Accord Principal / du Contrat de service***] conclu entre les Parties en date du [***date***] (relatif à « [***titre du contrat principal***] »). Il a pour objet de définir les engagements du Sous-Traitant en matière de protection des données à caractère personnel dans le cadre de la prestation suivante : [***Description succincte de la prestation IT***].

Par exemple : « Solution logicielle en mode SaaS de gestion des ressources humaines »

Le Contrat est conclu en application de l'article 28 du RGPD et des lois nationales applicables en matière de protection des données. Il prévaut sur toute autre convention ou tout autre accord entre les Parties en ce qui concerne le traitement de données personnelles, et annule et remplace le cas échéant toute clause précédente relative à la protection des données dans la relation contractuelle des Parties.

2. Description du traitement sous-traité

2.1. Finalité(s) du traitement : Le Sous-Traitant est autorisé à traiter les données personnelles uniquement dans le but de fournir le(s) service(s) suivant(s) : **[*décrire la finalité précise du traitement confié*]**.

*Par exemple : gestion de la paie du personnel via le logiciel **X**, hébergement et sauvegarde des données RH du Client, etc.*

2.2. Nature des opérations effectuées : Le traitement sous-traité comprend les opérations suivantes **[*énumérer les opérations*].**

> *Par exemple : collecte de données via l'application, enregistrement, hébergement sur serveurs, consultations, analyses, modification, extraction, communication aux personnes autorisées, sauvegarde, et suppression/destruction en fin de contrat.*

2.3. Catégories de données personnelles traitées : [*Liste détaillée des types de données*] confiées au Sous-Traitant.

> *Par exemple : données d'identification (nom, prénom, identifiants utilisateurs), données de contact (email, téléphone), données professionnelles (poste, service, salaire), données de connexion (logs, adresses IP), etc. (Inclure aussi les catégories particulières si pertinent, ex. données de santé, avec mention du régime spécial applicable).*

2.4. Catégories de personnes concernées : [*Lister*] les personnes dont les données sont traitées dans le cadre de la prestation.

> *Par exemple : employés du Client, utilisateurs finaux de l'application, clients du Client, etc.*

2.5. Durée du traitement / Conservation : Le présent Contrat entre en vigueur à compter de sa date de signature pour la durée du Contrat principal, soit **[*durée*]**, et s'applique aussi longtemps que le Sous-Traitant traite des données personnelles pour le compte du Responsable de Traitement. Sauf instruction contraire du Responsable de Traitement, le Sous-Traitant supprimera ou restituera toutes les données personnelles traitées pour le compte du Client à l'issue du Contrat (cf. Clause 12 ci-dessous sur le sort des données). La durée de conservation des données pendant le Contrat est déterminée par le Responsable de Traitement.

> *Et indiquée éventuellement en annexe : par ex. durée du contrat + X mois pour réversibilité, ou selon les obligations légales du Responsable de Traitement.*
>
> *Les informations ci-dessus constituent les instructions initiales du Responsable de Traitement. Toute instruction additionnelle ou modification d'instruction devra faire l'objet d'un écrit (y compris courriel) du Responsable de Traitement.*

3. Obligations du Responsable de Traitement

Le Responsable de Traitement s'engage à :

3.1. Fournir au Sous-Traitant les données personnelles énumérées à l'article 2 ci-dessus, ainsi que toute information nécessaire pour la bonne exécution des services sous-traités. Il garantit que ces données sont collectées et traitées par lui-même conformément au RGPD avant d'être confiées au Sous-Traitant.

3.2. Documenter par écrit toute instruction ultérieure concernant le traitement des données par le Sous-Traitant. Le présent Contrat tenant lieu d'instruction initiale, toute instruction complémentaire ou modification (par ex. changement de finalité, transferts non prévus, etc.) devra être convenue par écrit entre les Parties.

3.3. Superviser le traitement et le respect des obligations légales. Le Responsable de Traitement s'engage à exercer un contrôle approprié sur l'exécution de la prestation, notamment en réalisant si nécessaire des audits chez le Sous-Traitant (cf. Clause 10 sur le droit d'audit) et en s'assurant pendant toute la durée du traitement du respect du RGPD par le Sous-Traitant.

3.4. Respecter ses propres obligations légales. Notamment, le Responsable de Traitement déclare et garantit que les traitements confiés au Sous-Traitant ont une base légale valable, qu'il a accompli les formalités éventuelles et qu'il n'instruit pas le Sous-Traitant d'agir d'une manière illicite ou non conforme au RGPD.

Le Responsable de Traitement demeure seul décideur des finalités et moyens du traitement. À ce titre, il reconnaît qu'il lui appartient d'évaluer les risques pour les droits et libertés des personnes concernées et de s'assurer que le niveau de sécurité mis en œuvre est approprié (en coopération avec le Sous-Traitant, voir Annexe 1). Il s'engage à notifier aux personnes concernées le recours au Sous-Traitant si la loi l'exige, et plus généralement à gérer la relation avec les personnes concernées (exercice des droits, information, etc.) sauf disposition contraire du présent Contrat.

4. Obligations du Sous-Traitant

Le Sous-Traitant s'engage, dans le cadre du présent Contrat et pour tout traitement de données personnelles effectué pour le compte du Responsable de Traitement, à respecter les obligations suivantes :

4.1. Traitement uniquement sur instruction du Responsable de Traitement : Le Sous-Traitant ne traitera les données personnelles qu'en exécution des instructions documentées du Responsable de Traitement, telles que définies dans le présent Contrat ou par tout écrit ultérieur du Responsable de Traitement. Le Sous-Traitant ne décidera en aucun cas lui-même des finalités ou des moyens du traitement. Il ne pourra pas utiliser ou exploiter les données à d'autres fins (y compris à des fins propres, commerciales ou autres) sans l'autorisation écrite préalable du Responsable de Traitement.

4.2. Alerte en cas d'instruction illicite : Si le Sous-Traitant considère qu'une instruction du Responsable de Traitement constitue une violation du RGPD ou d'autres dispositions applicables en matière de protection des données, il s'engage à en informer immédiatement et par écrit le Responsable de Traitement. Le Sous-Traitant sera alors en droit de suspendre l'exécution de l'instruction concernée dans l'attente de directives clarifiées ou conformes, ou de l'accord du Responsable de Traitement pour sa mise en œuvre malgré le risque notifié. De même, si le Sous-Traitant est tenu de procéder à un transfert de données vers un pays tiers ou à une organisation internationale en vertu du droit de l'Union ou du droit d'un État membre auquel il est soumis, il doit informer le Responsable de Traitement de cette obligation juridique avant le traitement (sauf si le droit concerné interdit une telle information pour des motifs importants d'intérêt public).

4.3. Respect de la confidentialité : Le Sous-Traitant s'engage à garantir la confidentialité des données à caractère personnel traitées pour le compte du Responsable de Traitement. Il veille à ce que les données soient traitées de manière confidentielle et ne soient ni divulguées, ni rendues accessibles à des tiers non autorisés, y compris au sein de son organisation, sans

instruction du Responsable de Traitement ou sans y être obligé par la loi. Plus particulièrement, le Sous-Traitant s'assure que toute personne autorisée à traiter les données personnelles dans le cadre du présent Contrat (par exemple ses employés, agents, collaborateurs et sous-traitants ultérieurs) : *(i)* s'est engagée par écrit à respecter la confidentialité et à ne traiter les données que dans les limites nécessaires à ses tâches, ou bien est soumise à une obligation légale appropriée de confidentialité ; et *(ii)* reçoit la formation nécessaire en matière de protection des données personnelles. Le Sous-Traitant fournit sur demande du Responsable de Traitement des preuves de ces engagements de confidentialité signés et des actions de formation menées.

4.4. Sécurité des traitements : Le Sous-Traitant s'engage à mettre en œuvre des mesures de sécurité techniques et organisationnelles appropriées afin de garantir un niveau de sécurité adapté au risque, en conformité avec l'article 32 du RGPD. Ces mesures sont détaillées en Annexe 1 « Mesures de sécurité » du présent Contrat. Elles comprennent, entre autres, selon les besoins et l'état de l'art : la pseudonymisation et le chiffrement des données, des moyens garantissant la confidentialité, l'intégrité, la disponibilité et la résilience constantes des systèmes et services, des moyens permettant de rétablir la disponibilité et l'accès aux données en temps utile en cas d'incident physique ou technique, et une procédure de test, d'analyse et d'évaluation régulière de l'efficacité des mesures de sécurité mises en place. Les Parties conviennent que les mesures listées en Annexe 1 correspondent au niveau de sécurité approprié au regard des risques identifiés par le Responsable de Traitement. Le Sous-Traitant s'engage à maintenir ces mesures pendant toute la durée du Contrat, et à les ajuster en tant que de besoin en fonction de l'évolution des risques et des bonnes pratiques. Il notifie sans délai le Responsable de Traitement en cas de modification substantielle des mesures de sécurité.

> *(Optionnel : Si le Sous-Traitant se conforme à un code de conduite ou bénéficie d'une certification en matière de protection des données, mentionner ici : par ex. « Le Sous-Traitant déclare adhérer au code de conduite [référence] approuvé en vertu de l'article 40 du RGPD / Le Sous-Traitant est certifié [nom de la certification] pour le périmètre couvert par le présent Contrat. Il s'engage à conserver et renouveler cette certification pendant la durée du Contrat. »)*

Les responsabilités respectives du Responsable de Traitement et du Sous-Traitant en matière de sécurité sont précisées en Annexe 1. En particulier, il est convenu que

> *[ex. le Responsable de Traitement est responsable de la sécurisation de ses postes clients, de la gestion de ses habilitations utilisateurs et du chiffrement de ses terminaux, tandis que le Sous-Traitant est responsable de la sécurité du système serveur, du réseau et de l'application côté serveur].*

4.5. Sous-traitance ultérieure : Le Sous-Traitant ne fera appel à aucun autre sous-traitant (ci-après « Sous-Traitant Ultérieur ») pour l'exécution des activités de traitement confiées sans avoir obtenu au préalable **l'autorisation écrite** du Responsable de Traitement. Les dispositions suivantes s'appliquent :

- **Autorisation spécifique initiale :** Le Responsable de Traitement autorise d'ores et déjà le Sous-Traitant à sous-traiter certaines opérations liées aux services, aux entités suivantes : **[Nom du sous-traitant ultérieur, adresse, activité sous-traitée]** (voir Annexe 2 *« Liste des Sous-Traitants Ultérieurs autorisés »*). Ces entités sont donc

approuvées pour intervenir dans le traitement, dans le périmètre décrit (par ex. hébergement, maintenance, support). Le Sous-Traitant garantit qu'il a vérifié que chacun de ces Sous-Traitants Ultérieurs présente des garanties suffisantes de conformité au RGPD.

- **Autorisation générale pour les futurs sous-traitants :** Pour tout ajout ou remplacement d'un Sous-Traitant Ultérieur non listé en Annexe 2, le Sous-Traitant devra informer préalablement et par écrit le Responsable de Traitement de tout changement envisagé concernant l'ajout ou le remplacement d'autres sous-traitants. Cette information comprendra l'identité du sous-traitant envisagé, son adresse, la description des activités sous-traitées, la date prévue de début de la sous-traitance et toute information utile sur les garanties qu'il présente. Le Responsable de Traitement disposera d'un délai de **[nombre]** jours ouvrés à compter de la réception de cette information pour notifier par écrit au Sous-Traitant d'éventuelles objections motivées.

  (par exemple si le sous-traitant proposé ne présente pas les garanties de sécurité ou de confidentialité requises).

  En l'absence d'objection écrite dans le délai imparti, le nouveau Sous-Traitant Ultérieur sera réputé autorisé par le Responsable de Traitement. En cas d'objection du Responsable de Traitement considérée comme légitime, les Parties négocieront de bonne foi afin de trouver une solution alternative.

  (par exemple choisir un autre sous-traitant, ou ajuster le service pour éviter cette sous-traitance).

- **Mêmes obligations imposées :** Dans tous les cas, le Sous-Traitant s'engage à ce que chaque Sous-Traitant Ultérieur soit soumis aux mêmes obligations que celles stipulées dans le présent Contrat, en particulier en ce qui concerne les garanties de confidentialité, de sécurité, d'assistance et de conformité au RGPD. Le Sous-Traitant conclura un accord écrit avec chaque Sous-Traitant Ultérieur imposant au minimum les obligations de protection des données prévues par le présent Contrat, notamment celles de la Clause 4 (Obligations du Sous-Traitant) et de l'Annexe 1 (Sécurité).

- **Responsabilité** : Le Sous-Traitant reconnaît qu'il demeure pleinement responsable vis-à-vis du Responsable de Traitement de l'exécution par le Sous-Traitant Ultérieur de ses obligations en matière de protection des données. En d'autres termes, tout manquement d'un Sous-Traitant Ultérieur sera considéré comme un manquement du Sous-Traitant lui-même à l'égard du Responsable de Traitement. Le Sous-Traitant assumera donc l'entière responsabilité des conséquences de l'intervention de ses Sous-Traitants Ultérieurs sur les données du Responsable de Traitement.

(Option additionnelle : transparence vis-à-vis des personnes concernées : « Le Responsable de Traitement pourra, pour les besoins d'information prévus aux articles 13 et 14 du RGPD, communiquer aux personnes concernées la liste des Sous-Traitants Ultérieurs amenés à traiter leurs données, telle que mise à jour par le Sous-Traitant. »)

4.6. Droit d'information des personnes concernées : Il est convenu que la responsabilité d'informer les personnes concernées des traitements de données les concernant revient au Responsable de Traitement. Le Sous-Traitant n'a pas à fournir d'information directe aux

personnes concernées, sauf si le Responsable de Traitement lui en donne instruction ou si une disposition légale l'y oblige. Si, dans des circonstances exceptionnelles, le Sous-Traitant devait collecter des données directement auprès des personnes concernées pour le compte du Responsable de Traitement, il ne le ferait qu'après avoir convenu avec le Responsable de Traitement du contenu et du format des mentions d'information à délivrer.

4.7. Assistance pour l'exercice des droits des personnes : Le Sous-Traitant s'engage à aider le Responsable de Traitement à satisfaire aux demandes d'exercice des droits des personnes concernées (accès, rectification, effacement, opposition, limitation, portabilité, etc.). Compte tenu de la nature des traitements et des informations dont il dispose, le Sous-Traitant prendra les mesures suivantes :

- Si une personne concernée adresse une demande directement au Sous-Traitant, le Sous-Traitant la transmettra sans délai (au plus sous **[nombre]** jours ouvrés) au Responsable de Traitement à l'adresse de contact suivante : **[email du DPO ou « service privacy » du Client]**, et ce sans y répondre.

- Par ailleurs, le Sous-Traitant apportera son concours au Responsable de Traitement pour répondre aux demandes, notamment en mettant à disposition les données nécessaires ou en exécutant toute opération de traitement demandée par le Responsable de Traitement. Il le fera dans les meilleurs délais compte tenu des échéances légales.

- Si le concours du Sous-Traitant est nécessaire pour permettre l'exercice effectif d'un droit (par ex. extraction des données dans un format portable, application sélective d'une restriction de traitement), le Sous-Traitant s'exécutera sur simple demande écrite du Responsable de Traitement et fournira les éléments attendus dans un délai compatible avec les obligations légales.

Le Sous-Traitant peut facturer au Responsable de Traitement les coûts raisonnables réels engagés pour des assistances particulièrement complexes ou lourdes non prévues initialement, sous réserve d'en informer préalablement le Responsable de Traitement et d'obtenir son accord.

4.8. Notification des violations de données personnelles : Le Sous-Traitant notifie au Responsable de Traitement toute violation de données à caractère personnel (failles de sécurité, accès non autorisé, perte ou destruction de données, etc.) concernant les données traitées pour le compte du Responsable de Traitement. Cette notification intervient sans délai indû et en tout état de cause dans un délai maximum de **[nombre]** heures après que le Sous-Traitant en a pris connaissance. Elle sera adressée au contact suivant du Responsable de Traitement : **[coordonnées 24/7 du destinataire des notifications d'incident côté Client]** par **[email/téléphone]**.

La notification devra décrire de manière claire et concise la nature de la violation et comporter au moins les informations suivantes (si disponibles) : *(i)* la description de la nature de la violation de données personnelles, y compris, si possible, les catégories et le nombre approximatif de personnes concernées et de dossiers de données concernés ; *(ii)* le nom et les coordonnées du délégué à la protection des données (DPO) du Sous-Traitant ou d'un autre point de contact auprès duquel des informations supplémentaires peuvent être obtenues ; *(iii)* la description des conséquences probables de la violation ; *(iv)* la description des mesures

prises ou que le Sous-Traitant propose de prendre pour remédier à la violation, y compris, le cas échéant, les mesures pour en atténuer les éventuelles conséquences négatives. Dans la mesure où toutes ces informations ne pourraient être fournies en même temps, le Sous-Traitant pourra les communiquer de manière échelonnée sans retard indu, au fur et à mesure des éléments dont il dispose, en concertation avec le Responsable de Traitement.

(Option complémentaire : notification par le ST au régulateur/aux personnes) Après accord préalable et écrit du Responsable de Traitement, le Sous-Traitant pourra notifier pour le compte du Responsable de Traitement la violation de données à l'autorité de contrôle compétente (CNIL) et, le cas échéant, aux personnes concernées lorsque celle-ci est susceptible d'engendrer un risque élevé pour leurs droits et libertés. Le Sous-Traitant préparera les éléments de notification et les soumettra au Responsable de Traitement pour validation avant envoi. En tout état de cause, le Sous-Traitant ne contactera pas l'autorité de contrôle ni les personnes concernées de sa propre initiative sans instruction du Responsable de Traitement, excepté si une obligation légale lui impose une communication directe.

4.9. Aide à la conformité du Responsable de Traitement : Le Sous-Traitant apporte son assistance au Responsable de Traitement pour garantir le respect de l'ensemble des obligations prévues aux articles 32 à 36 du RGPD, compte tenu de la nature du traitement et des informations à la disposition du Sous-Traitant. Notamment, le Sous-Traitant :

- Coopérera à la réalisation d'**analyses d'impact sur la protection des données (AIPD)** si le Responsable de Traitement doit en mener une concernant les traitements objet du présent Contrat (art. 35 RGPD). Sur demande, le Sous-Traitant fournira au Responsable de Traitement toutes les informations utiles (description technique des opérations, mesures de sécurité en place, etc.) pour mener l'AIPD. Si le Responsable de Traitement sollicite l'avis du Sous-Traitant sur l'évaluation des risques ou les mesures envisagées, le Sous-Traitant lui apportera son expertise dans la limite de ses connaissances sur les traitements.

- De même, en cas de **consultation préalable** de l'autorité de contrôle requise (art. 36 RGPD), le Sous-Traitant assistera le Responsable de Traitement dans les échanges avec la CNIL, en fournissant notamment les informations techniques demandées par celle-ci.

- Plus généralement, le Sous-Traitant s'engage à coopérer avec la CNIL sur demande du Responsable de Traitement, notamment en permettant ou facilitant toute mission de vérification (audit, investigation) initiée par la CNIL chez le Responsable de Traitement et concernant les opérations effectuées par le Sous-Traitant.

4.10. Tenue d'un registre des traitements : Le Sous-Traitant déclare tenir par écrit un registre de toutes les catégories d'activités de traitement effectuées pour le compte du Responsable de Traitement, conformément à l'article 30(2) du RGPD. Le Sous-Traitant mettra ce registre à disposition du Responsable de Traitement sur simple demande.

4.11. Documentation et audit : Le Sous-Traitant met à la disposition du Responsable de Traitement toutes les informations nécessaires pour démontrer le respect de l'ensemble de ses obligations au titre du présent Contrat et du RGPD. Il permet la réalisation d'audits et d'inspections par le Responsable de Traitement ou tout autre auditeur mandaté par celui-ci, et s'engage à y contribuer activement. Les conditions de ces audits sont détaillées à la

Clause 10 ci-après. De plus, le Sous-Traitant s'engage à fournir sur demande du Responsable de Traitement la documentation attestant de sa conformité (par ex. politiques internes, résultats de contrôles internes, certificats obtenus, rapports d'audit tiers pertinents, etc.).

5. Coordonnées des points de contact et Délégués à la Protection des Données

Pour l'exécution du présent Contrat, les Parties désignent les points de contact suivants :

- **Chez le Responsable de Traitement** : **[Nom, fonction, coordonnées (téléphone, email)]** pour toute question relative à la protection des données et à l'application du présent Contrat. ***(Si le Responsable de Traitement a désigné un DPO)*** : Le Délégué à la Protection des Données du Client est **[nom du DPO]**, joignable à **[email DPO]**.

- **Chez le Sous-Traitant** : **[Nom, fonction, coordonnées]** en tant que responsable opérationnel du suivi du présent Contrat. ***(Si DPO chez ST)*** : Le Sous-Traitant a désigné comme Délégué à la Protection des Données **[nom du DPO ST]**, joignable à **[email DPO ST]**, qui sera l'interlocuteur privilégié pour toute question relative aux données personnelles.

Les Parties s'engagent à se notifier mutuellement par écrit toute modification de ces contacts. Les notifications exigées par le présent Contrat devront être adressées aux contacts ci-dessus désignés.

6. Confidentialité

Chaque Partie s'engage, pour elle-même et pour l'ensemble de son personnel et de ses éventuels sous-traitants, à considérer comme strictement confidentielles toutes les informations (écrites ou orales, sur tout support) reçues de l'autre Partie ou auxquelles elle aura accès dans le cadre de la préparation et de l'exécution du présent Contrat. Ceci vise aussi bien les données à caractère personnel traitées (dont la confidentialité doit être maintenue conformément au RGPD et à la Clause 4.3) que toute information commerciale, technique, stratégique ou financière relative à l'autre Partie, à ses activités, ses clients, partenaires ou employés, etc.

En conséquence, chaque Partie s'interdit de divulguer lesdites informations confidentielles à quiconque, directement ou indirectement, sans l'autorisation écrite préalable de l'autre Partie. Elles ne seront communiquées qu'aux membres du personnel, sous-traitants ou conseils ayant besoin d'en connaître pour l'exécution du Contrat, et sous réserve que ces destinataires soient soumis à une obligation de confidentialité équivalente. Chaque Partie s'interdit également d'utiliser ou d'exploiter les informations confidentielles de l'autre Partie à des fins autres que la bonne exécution du Contrat ou la défense de ses droits en justice le cas échéant.

Les obligations ci-dessus ne s'appliquent pas aux informations qui seraient ou deviendraient publiquement disponibles autrement que par la faute de la Partie récipiendaire, ni aux informations déjà connues de celle-ci avant leur communication par l'autre Partie, ni à celles obtenues de bonne foi de tiers autorisés à les divulguer, ni enfin à celles qu'une Partie serait obligée de divulguer en vertu d'une disposition légale ou d'une décision de justice ou

administrative (dans ce cas, elle devra prévenir sans délai l'autre Partie de cette obligation, si légalement possible, et limiter la divulgation aux informations strictement requises).

La présente obligation de confidentialité demeurera en vigueur pendant toute la durée du Contrat et pour une période de **[durée, par ex. 5 ans]** à compter de sa date de terminaison ou d'expiration. En ce qui concerne les secrets d'affaires au sens de la loi (informations présentant une valeur commerciale du fait de leur secret et faisant l'objet de mesures de protection raisonnables), l'obligation de confidentialité restera en vigueur tant que ces informations conservent le caractère de secret d'affaires, sans limitation de durée.

En cas de violation de cette clause par une Partie, l'autre Partie pourra exiger la cessation immédiate de la divulgation ou de l'utilisation non autorisée, et se réserve le droit de réclamer des dommages-intérêts en réparation du préjudice subi.

Cette clause s'ajoute aux engagements de confidentialité spécifiques du Sous-Traitant vis-à-vis des données personnelles, énoncés à la Clause 4.3. En cas de contradiction, la disposition offrant la plus grande protection aux informations devra prévaloir.

7. Propriété des données et propriété intellectuelle

7.1. Données à caractère personnel : Le Responsable de Traitement demeure seul propriétaire des données personnelles qui sont mises à la disposition du Sous-Traitant pour les besoins de la prestation. Le Sous-Traitant reconnaît que le Responsable de Traitement conserve la pleine souveraineté sur ces données et qu'aucune disposition du présent Contrat ne saurait être interprétée comme lui transférant la propriété ou le contrôle des données. Le Sous-Traitant n'acquiert notamment aucun droit, titre, intérêt ou licence sur les données personnelles du seul fait de leur traitement dans le cadre du Contrat. Les données sont et resteront en toutes circonstances sous le contrôle du Responsable de Traitement, qui peut en demander la restitution ou la destruction conformément aux dispositions du présent Contrat.

Le Sous-Traitant s'interdit en conséquence toute utilisation des données personnelles en dehors des instructions du Responsable de Traitement, et notamment toute exploitation commerciale, revente, location, échange ou mise à disposition (même partielle) de ces données à des tiers, sauf obligation légale contraignante ou autorisation écrite préalable du Responsable de Traitement. En particulier, le Sous-Traitant ne pourra pas construire de fichiers distincts ou de profils à partir des données du Responsable de Traitement, ni les réutiliser pour son propre compte (y compris de façon anonymisée ou agrégée) sans accord. Le Sous-Traitant peut toutefois utiliser les informations agrégées découlant de l'utilisation de ses services à des fins internes d'analyse et d'amélioration de ses services, sous réserve que ces informations ne permettent pas d'identifier, même indirectement, le Responsable de Traitement ou des personnes concernées.

7.2. Autres données du Responsable de Traitement : De manière générale, tous les fichiers, documents, données, contenus ou matériaux fournis par le Responsable de Traitement au Sous-Traitant, ou accessibles par ce dernier dans le cadre de la prestation (y compris les données non personnelles), restent la propriété exclusive du Responsable de Traitement. Le Sous-Traitant n'en acquiert aucun droit hormis celui de les utiliser dans le seul but d'exécuter ses obligations contractuelles.

7.3. Éléments appartenant au Sous-Traitant : Le Sous-Traitant reste propriétaire de ses méthodes, savoir-faire, outils, logiciels, documentations techniques et plus généralement de tous les éléments qu'il met à disposition ou utilise pour fournir le service (y compris les éventuelles améliorations ou mises à jour effectuées durant la prestation, dans la mesure où elles ne sont pas spécifiques aux données du Responsable de Traitement). Le présent Contrat n'opère aucun transfert de propriété intellectuelle sur ces éléments appartenant au Sous-Traitant. Le Responsable de Traitement bénéficie uniquement d'un droit d'usage dans le cadre du service et pour la durée du Contrat, sauf stipulation contraire dans le contrat principal entre les Parties.

Si le Responsable de Traitement formule des suggestions d'amélioration, de correction ou nouvelles fonctionnalités concernant le logiciel ou les services du Sous-Traitant, il est entendu que le Sous-Traitant pourra librement les utiliser et les intégrer, et que toute propriété intellectuelle afférente aux évolutions du logiciel ou aux œuvres dérivées restera dévolue au Sous-Traitant.

7.4. Livrables et résultats spécifiques : Dans l'hypothèse où le Sous-Traitant serait amené à produire des livrables spécifiques pour le compte du Responsable de Traitement (par ex. rapports d'analyse de données, développements sur mesure, paramétrages spécifiques, etc.), les droits de propriété intellectuelle sur ces livrables sont traités dans **[le contrat principal / l'accord de développement]** liant les Parties.

> *(Si pas traité ailleurs, préciser ici la règle souhaitée : par ex. « ces livrables seront la propriété du Responsable de Traitement dès leur création, le Sous-Traitant lui cédant à titre exclusif l'ensemble des droits de propriété intellectuelle y afférents, pour le monde entier et pour toute la durée de protection » OU « le Responsable de Traitement reçoit une licence non-exclusive lui permettant d'utiliser ces livrables pour les besoins de son activité, sans limitation de durée », etc.)*.

7.5. Droits des tiers : Le Sous-Traitant garantit que les outils, logiciels ou documents qu'il utilise ou fournit dans le cadre de la prestation n'enfreignent pas les droits de propriété intellectuelle de tiers. Il indemnisera le Responsable de Traitement en cas de réclamation d'un tiers fondée sur la violation d'un droit de propriété intellectuelle résultant de l'exécution de la prestation par le Sous-Traitant, conformément aux conditions de responsabilité prévues au Contrat principal.

8. Transferts internationaux

8.1. Localisation des données : Par défaut, le Sous-Traitant s'engage à traiter et héberger les données personnelles confiées dans des centres de données situés exclusivement sur le territoire de ***[l'Union européenne/l'Espace économique européen/France].*** Tout transfert ou accès aux données en dehors de ce territoire par le Sous-Traitant, y compris par ses sous-traitants ultérieurs ou personnel, est strictement interdit sans l'autorisation écrite préalable du Responsable de Traitement.

8.2. Transfert autorisé sous conditions : Si le Responsable de Traitement autorise par écrit un transfert de données vers un pays n'offrant pas un niveau de protection adéquat au sens du RGPD, le Sous-Traitant ne pourra effectuer ce transfert qu'en respectant l'une des conditions suivantes : *(i)* mise en place de Clauses Contractuelles Types (CCT) adoptées par la Commission

européenne dûment signées entre les parties concernées du transfert, éventuellement assorties de mesures supplémentaires de protection technique et organisationnelle si requis ; *(ii)* existence d'une décision d'adéquation de la Commission européenne couvrant le pays de destination ; *(iii)* application de règles d'entreprise contraignantes (BCR) approuvées couvrant le transfert en question ; ou *(iv)* autre garantie ou dérogation légale applicable prévue par le Chapitre V du RGPD. Le choix et la mise en œuvre du mécanisme de transfert approprié devront être validés par le Responsable de Traitement avant tout transfert effectif.

8.3. Information et assistance : Le Sous-Traitant informera le Responsable de Traitement de tout projet de transfert transfrontalier non prévu initialement et coopérera avec lui pour assurer la légalité de ce transfert. À la demande du Responsable de Traitement, le Sous-Traitant fournira les informations nécessaires pour réaliser une évaluation d'impact relative au transfert (Transfer Impact Assessment) et s'engage à mettre en œuvre les mesures techniques ou organisationnelles complémentaires éventuellement identifiées comme nécessaires pour garantir un niveau de protection essentiellement équivalent à celui de l'UE (par ex. chiffrement additionnel, segmentation des données, etc.). Le Sous-Traitant consent par ailleurs à ce que le texte des clauses contractuelles types ou autres garanties mises en œuvre soit intégré en annexe du présent Contrat ou du contrat principal, afin d'être opposable et disponible pour les autorités de contrôle compétentes.

8.4. Demandes d'autorités étrangères : Dans le cas où le Sous-Traitant recevrait une demande juridiquement contraignante d'une autorité publique étrangère (police, agence gouvernementale, renseignement, etc.) visant à obtenir communication de données personnelles traitées dans le cadre du présent Contrat, il s'engage à : *(i)* en informer immédiatement le Responsable de Traitement, sauf interdiction légale d'en divulguer l'existence ; *(ii)* consulter le Responsable de Traitement sur la suite à donner ; *(iii)* utiliser les moyens légaux dont il dispose pour s'opposer à la demande ou en obtenir la limitation si elle apparaît excessive ou non conforme au droit de l'UE ; et *(iv)* ne fournir que les informations strictement requises par la réglementation applicable. Le Sous-Traitant aidera le Responsable de Traitement à évaluer la légitimité de la demande et à préparer une éventuelle réponse. Ces dispositions s'appliquent sauf si la loi interdit au Sous-Traitant d'informer le Responsable de Traitement, en quel cas le Sous-Traitant s'efforcera de demander la levée de cette interdiction pour permettre au Responsable de Traitement d'intervenir.

9. Responsabilité contractuelle et indemnisation

9.1. Répartition des responsabilités : Les Parties conviennent que chacune d'elles est responsable envers l'autre de l'exécution des obligations lui incombant en vertu du présent Contrat. Le Responsable de Traitement demeure responsable de la légalité des traitements confiés et du respect des obligations qui lui incombent en tant que responsable de traitement au titre du RGPD. Le Sous-Traitant est responsable de l'exécution conforme de ses obligations définies aux Clauses 4 à 8 ci-dessus, ainsi que du respect des instructions licites du Responsable de Traitement.

9.2. Indemnisation du Responsable de Traitement : Le Sous-Traitant indemnisera et dégagera de toute responsabilité le Responsable de Traitement contre toutes les pertes, dommages, coûts, sanctions, amendes ou dépenses (y compris les honoraires d'avocats raisonnables) encourus par le Responsable de Traitement et résultant d'une violation par le Sous-Traitant

des obligations qui lui incombent en vertu du présent Contrat ou du RGPD. Cette indemnisation couvre notamment : (a) les amendes administratives éventuellement infligées au Responsable de Traitement par une autorité de contrôle en raison d'un manquement du Sous-Traitant, (b) les dommages-intérêts mis à la charge du Responsable de Traitement vis-à-vis de tiers (y compris des personnes concernées) du fait d'une faute du Sous-Traitant, et (c) plus généralement, tous les frais engagés par le Responsable de Traitement pour remédier à un incident causé par le Sous-Traitant.

Cette obligation d'indemnisation ne s'applique pas si la faute ou le manquement en cause est exclusivement imputable au Responsable de Traitement. Dans l'hypothèse où la responsabilité conjointe des Parties serait engagée vis-à-vis d'un tiers selon l'article 82(4) du RGPD, les Parties conviennent que le Sous-Traitant assumera la part de responsabilité correspondant à sa part de faute dans la violation ayant causé le dommage, conformément à l'article 82(5) du RGPD.

9.3. Limitation de responsabilité entre Parties : Sous réserve des dispositions ci-dessus et sauf stipulation contraire dans le Contrat Principal, la responsabilité financière totale du Sous-Traitant envers le Responsable de Traitement au titre du présent Contrat, tous faits générateurs confondus, est plafonnée à ***[montant ou formule de calcul]***. En aucun cas le Sous-Traitant ne saurait exclure ou limiter sa responsabilité en cas de : (a) dommage corporel ou décès causé par sa négligence, (b) fraude ou dol, (c) violation de la loi applicable en matière de protection des données engageant sa responsabilité légale irréfragable envers les personnes concernées ou l'autorité, (d) violation de l'obligation de confidentialité (Clause 6) ou atteinte illégale aux droits de propriété intellectuelle (Clause 7), et (e) toute autre responsabilité qui ne peut légalement être limitée ou exclue.

> *(La clause de limitation doit être adaptée : souvent, les DPA renvoient au plafond du contrat principal. Par ex. « conformément aux clauses de limitation de responsabilité stipulées à l'article X du Contrat Principal » ou « plafond égal aux redevances annuelles versées ». On peut aussi prévoir qu'aucune limite ne s'applique aux obligations d'indemnisation RGPD, selon la position du responsable de traitement.)*

9.4. Responsabilité vis-à-vis des personnes concernées : Il est rappelé qu'en application de l'article 82 du RGPD, chaque Partie pourra être tenue pour responsable, en tant que de besoin, vis-à-vis des personnes concernées, du fait des violations commises dans le cadre du traitement sous-traité. En interne, les Parties s'engagent à se tenir informées mutuellement de toute réclamation ou action de personnes concernées dont elles auraient connaissance et susceptible d'engager la responsabilité de l'autre Partie, et à se coordonner dans la réponse apportée. Chaque Partie informera sans délai l'autre Partie si elle est mise en cause sur le fondement du RGPD relativement aux opérations sous-traitées.

10. Droit d'audit

Le Responsable de Traitement (ainsi que tout auditeur externe qu'il pourrait mandater à cet effet) dispose du droit de réaliser des audits de conformité chez le Sous-Traitant, afin de vérifier le respect des dispositions du présent Contrat et plus largement la conformité des opérations de traitement réalisées pour le compte du Responsable de Traitement, notamment au regard du RGPD.

Pour exercer ce droit, les Parties conviennent de la procédure suivante :

- Le Responsable de Traitement notifiera par écrit au Sous-Traitant sa décision de conduire un audit avec un préavis minimum de **[X] jours ouvrés**. Il s'efforcera de ne pas exercer ce droit plus d'une fois par an, sauf en cas de manquement avéré du Sous-Traitant ou d'incident majeur justifiant un contrôle plus fréquent.

- L'audit pourra être mené soit par le personnel interne du Responsable de Traitement, soit par un tiers indépendant mandaté, non concurrent du Sous-Traitant. Les personnes en charge de l'audit devront être soumises à une obligation de confidentialité.

- L'audit portera strictement sur les traitements effectués par le Sous-Traitant pour le compte du Responsable de Traitement et sur le respect des mesures de sécurité et procédures convenues. Il pourra inclure des vérifications documentaires (politiques, enregistrements de logs, certifications…), des entretiens avec le personnel clé du Sous-Traitant et, le cas échéant, des inspections des installations utilisées pour le traitement (centres de données, locaux…).

- Le Sous-Traitant s'engage à coopérer de bonne foi avec l'équipe d'audit. Il fournira l'accès nécessaire aux informations, systèmes et personnels pertinents, dans la limite de ce qui est raisonnablement requis pour l'audit. Si certaines informations sont couvertes par un secret de fabrication ou de sûreté, le Sous-Traitant pourra les anonymiser ou les restreindre sous forme de preuves négatives (attestation par exemple).

- L'audit se déroulera pendant les heures normales de bureau du Sous-Traitant et d'une manière à minimiser les perturbations de son activité. Le Responsable de Traitement veillera à ce que les auditeurs respectent les mesures de sécurité et les consignes internes du Sous-Traitant lors de leur présence sur site.

- À l'issue de l'audit, un rapport d'audit sera communiqué au Sous-Traitant. Celui-ci aura la possibilité de formuler des observations. Si le rapport met en lumière un manquement du Sous-Traitant aux obligations du présent Contrat ou à la réglementation, le Sous-Traitant s'engage à mettre en œuvre dans les plus brefs délais un plan d'actions correctives pour y remédier. Les Parties conviendront par écrit des mesures à prendre et du calendrier de mise en conformité.

- Les frais liés à l'audit seront supportés par le Responsable de Traitement, à l'exception des coûts internes du Sous-Traitant (temps passé du personnel, etc.). Toutefois, si l'audit révélait un manquement significatif du Sous-Traitant, ce dernier remboursera au Responsable de Traitement les frais d'audit raisonnables engagés.

En alternative à un audit sur site, le Sous-Traitant peut proposer la fourniture de certificats ou rapports d'audit tiers récents (moins de 12 mois) couvrant le périmètre du traitement sous-traité, émanant d'organismes indépendants (par ex. certificat ISO 27001, rapport SSAE 18 / ISAE 3402 type II, etc.). Si ces rapports sont jugés suffisants par le Responsable de Traitement, ils pourront dispenser d'un audit direct. Toutefois, le Responsable de Traitement se réserve le droit de procéder lui-même à un audit si des éléments objectifs le justifient (incident, mise à jour majeure, expiration de la certification…).

La présente clause n'a pas pour objet de réduire les pouvoirs des autorités de contrôle. En cas de contrôle de la CNIL chez le Sous-Traitant concernant les traitements du Responsable de Traitement, le Sous-Traitant informera ce dernier sans délai (sauf interdiction légale) et coopérera pleinement avec la CNIL, tout en permettant la participation du Responsable de Traitement si cela est pertinent.

11. Durée et fin du Contrat

Le présent Contrat entre en vigueur à la date de sa signature par les Parties et demeure en vigueur pendant toute la durée de la relation de services entre les Parties. Il prendra fin automatiquement à la date de fin ou de résiliation du contrat principal liant les Parties, sous réserve des dispositions ci-après concernant le sort des données et la survie de certaines clauses.

En cas de manquement grave ou répété du Sous-Traitant à ses obligations au titre du présent Contrat, le Responsable de Traitement pourra, après mise en demeure écrite restée sans effet pendant un délai raisonnable de **[X jours]**, procéder à la résiliation anticipée de plein droit du présent Contrat (et, si applicable, du contrat principal) sans indemnité, sans préjudice des dommages-intérêts auxquels il pourrait prétendre. Aucune période de préavis n'est requise en cas de manquement ne pouvant être remédié (ex. violation volontaire de données, falsification de rapports, etc.) ; la résiliation sera alors immédiate sur notification écrite.

Il est convenu que toute fin du présent Contrat, qu'elle qu'en soit la cause, entraîne l'obligation pour le Sous-Traitant de cesser immédiatement tout traitement de données personnelles pour le compte du Responsable de Traitement, sauf dans la mesure nécessaire à la mise en œuvre de la Clause 12 (réversibilité/destruction). La résiliation ou l'expiration du présent Contrat ne dégage pas le Sous-Traitant de ses obligations de confidentialité (Clause 6), de coopération avec le Responsable de Traitement et de protection des données jusqu'à leur restitution ou destruction.

Les Clauses 6 (Confidentialité), 7 (Propriété des données), 9 (Responsabilité), 11 (Fin du Contrat), 12 (Sort des données) et 13 (Droit applicable) survivront à l'expiration ou la résiliation du présent Contrat, ainsi que toute autre disposition qui par nature est destinée à produire effet au-delà de la fin du Contrat.

12. Sort des données en fin de contrat

Lors de l'expiration du présent Contrat ou en cas de résiliation anticipée, le Responsable de Traitement aura la possibilité de choisir entre les mesures suivantes concernant les données personnelles traitées par le Sous-Traitant pour son compte :

- **Option 1 – Restitution intégrale des données :** À la demande écrite du Responsable de Traitement, le Sous-Traitant restituera au Responsable de Traitement, ou à tout autre sous-traitant désigné par celui-ci, l'intégralité des données à caractère personnel traitées pour son compte, dans un format structuré, couramment utilisé et exploitable, accompagnées de toute documentation utile pour leur réutilisation. Cette restitution sera effectuée dans un délai maximum de **[X]** jours à compter de la fin du Contrat. Le Sous-Traitant certifiera par écrit avoir restitué toutes les données et n'en avoir

conservé aucune copie (sauf copie intermédiaire strictement nécessaire à l'export, détruite immédiatement après).

- **Option 2 – Destruction des données :** À la demande du Responsable de Traitement (ou en l'absence d'instruction explicite dans un délai de **[X]** jours après la fin du Contrat), le Sous-Traitant procédera à la destruction complète et sécurisée de toutes les données à caractère personnel traitées pour le compte du Responsable de Traitement, y compris toutes les copies de sauvegarde ou répliques sur ses systèmes. Cette destruction comprendra l'effacement des données dans les bases actives et la purge des données dans les backups, dans les délais techniquement raisonnables. Sur demande, le Sous-Traitant fournira au Responsable de Traitement un certificat de destruction confirmant que l'ensemble des données a été détruit ou rendu définitivement inutilisable.

(On peut également prévoir une Option 3 combinant restitution puis destruction : le Sous-Traitant restitue d'abord les données, puis les détruit une fois la récupération confirmée.)

Si le Sous-Traitant est tenu par la loi de conserver certaines données personnelles au-delà de la fin du Contrat, il en informera le Responsable de Traitement. Dans ce cas, il garantit qu'il continuera à assurer la protection et la confidentialité de ces données et ne les traitera que pour les fins spécifiques imposées par la loi, pendant la durée de conservation requise. Une fois ce délai légal expiré, il procédera à leur destruction comme indiqué ci-dessus.

Les coûts éventuels de restitution des données (supports, transfert) seront supportés par **[préciser : généralement inclus dans le prix, ou facturation spécifique si volumétrie exceptionnelle]**. En tout état de cause, le Sous-Traitant ne conditionnera pas la restitution ou la destruction des données à un paiement supplémentaire non prévu, ni ne retardera ces opérations de réversibilité.

13. Droit applicable et règlement des litiges

Le présent Contrat est régi par le **droit [français / de l'État membre UE]**, à l'exclusion de ses règles de conflit de lois. Il devra être interprété conformément au RGPD et aux lois nationales applicables en matière de protection des données.

Tout différend relatif à la validité, l'interprétation ou l'exécution du présent Contrat qui ne pourrait être résolu à l'amiable sera soumis à la compétence exclusive des tribunaux du ressort de **[ville]**, y compris en matière de référé ou de procédure d'urgence.

14. Dispositions finales

14.1. **Modification du Contrat :** Le présent Contrat ne peut être modifié que par un avenant écrit signé par les deux Parties, à l'exception des mises à jour de la liste des Sous-Traitants Ultérieurs (Annexe 2) effectuées selon la procédure convenue en Clause 4.5, qui seront entérinées par simple notification écrite du Sous-Traitant au Responsable de Traitement et ajout à l'Annexe 2.

14.2. **Nullité partielle :** Si une ou plusieurs dispositions du présent Contrat s'avéraient nulles, invalides ou inopposables au regard d'une règle de droit ou d'une décision de justice

définitive, elles seraient réputées non écrites, sans pour autant entraîner la nullité du Contrat dans son ensemble ni altérer la validité de ses autres stipulations. Les Parties négocieront de bonne foi une disposition de remplacement valide reflétant au mieux l'objectif initial.

14.3. **Priorité :** En cas de contradiction entre une disposition du présent Contrat et une disposition de tout autre accord conclu entre les Parties (y compris le Contrat principal ou les CGV du Sous-Traitant), les Parties conviennent que les stipulations du présent Contrat prévaudront, dans la mesure de cette contradiction, pour tout ce qui a trait au traitement de données personnelles.

14.4. **Intégralité :** Le présent Contrat et ses annexes expriment l'intégralité de l'accord des Parties quant à son objet, et remplacent tout accord ou négociation antérieur(e) – oral(e) ou écrit(e) – relatif à la sous-traitance de données entre les Parties.

14.5. **Annexes :** Sont annexés au présent Contrat et en font partie intégrante : **Annexe 1 « Mesures de sécurité techniques et organisationnelles »**, **Annexe 2 « Liste des Sous-Traitants Ultérieurs autorisés »** (y compris localisation des données), **[Éventuellement Annexe 3 « Clauses contractuelles types de transfert » si transferts hors UE]**.

Fait en deux exemplaires,

À **[lieu]**, le **[date]**

Pour le Responsable de Traitement :	Pour le Sous-Traitant :
Nom :	Nom :
……	……
Fonction :	Fonction :
……	……
Signature :	Signature :
……	……

(cachet)

(cachet)

Annexe 1 – Mesures de sécurité techniques et organisationnelles

[Exemple d'annexe sécurité – à compléter selon le contexte réel]

Le Sous-Traitant s'engage à mettre en œuvre au minimum les mesures de sécurité suivantes pour protéger les données personnelles confiées :

- **Contrôle d'accès logique :** authentification individuelle des utilisateurs (mots de passe robustes renouvelés régulièrement, gestion des droits d'accès selon le principe du moindre privilège, double authentification pour les accès sensibles), traçabilité des connexions (journaux de logs conservés X mois).
- **Chiffrement :** chiffrement des données en transit (certificats SSL/TLS, protocoles sécurisés) et chiffrement des données au repos sur les serveurs (par ex. AES-256) pour les données sensibles. Gestion sécurisée des clés de chiffrement (stockage séparé, rotation des clés).
- **Pseudonymisation :** utilisation de techniques de pseudonymisation pour limiter l'identification directe des personnes (par ex. remplacement des noms par des identifiants chiffrés dans certaines exports, si applicable).
- **Sécurité des réseaux et des systèmes :** cloisonnement des réseaux (VLAN, pare-feu), système de détection/prévention d'intrusion (IDS/IPS), antivirus et antimalware à jour sur les serveurs, mise à jour régulière des patchs de sécurité des logiciels et OS utilisés.
- **Résilience et disponibilité :** redondance des composants critiques, répartition de charge, plan de continuité d'activité (PCA) prévoyant des solutions de repli en cas de panne majeure. Sauvegardes régulières des données (fréquence : quotidienne/hebdomadaire) stockées dans un environnement séparé, avec tests de restauration effectués périodiquement (au moins tous les [X] mois). Capacité à restaurer la disponibilité des données sous [Y] heures en cas d'incident.
- **Surveillance et audit :** surveillance continue de l'infrastructure (supervision 24/7, alertes en cas d'événement anormal), audits de sécurité annuels par un tiers indépendant (tests d'intrusion, scans de vulnérabilité). Correction rapide (plan de remédiation) de toute vulnérabilité critique identifiée.
- **Mesures organisationnelles :** politique interne de sécurité de l'information (PSSI) en place, sensibilisation régulière du personnel à la protection des données (formations RGPD et sécurité au moins 1 fois par an), processus de gestion des habilitations (création, modification, suppression des comptes utilisateurs sur validation managériale).
- **Gestion des incidents :** existence d'une procédure de gestion des incidents de sécurité incluant détection, analyse, réaction (mitigation) et notification conformément à la Clause 4.8 du Contrat. Équipe d'intervention désignée (référents sécurité) mobilisable rapidement en cas d'incident majeur. Journalisation des incidents et mesures correctives conservées et partagées avec le Responsable de Traitement sur demande.
- **Locaux et accès physiques :** centres de données sécurisés avec contrôle d'accès physique (badges, biométrie), surveillance vidéo, présence d'une équipe de sécurité, protection contre les sinistres (incendie, inondation) via systèmes dédiés (extincteurs automatiques, onduleurs et générateurs électriques). Locaux du Sous-Traitant sécurisés (accès restreint aux seules personnes autorisées aux zones de travail contenant des données du Client).

- **Sous-traitance ultérieure** : imposition contractuelle de mesures de sécurité équivalentes à tous les Sous-Traitants Ultérieurs (fournisseurs cloud etc.), vérification de leurs certifications (ex. ISO 27001) et obtention régulière de rapports de sécurité de leur part.
- *(Autres mesures spécifiques le cas échéant : ex. exigence de chiffrement des sauvegardes sur bandes, interdiction d'utiliser des données de production à des fins de test sans anonymisation, procédure particulière pour l'utilisation d'ordinateurs portables ou le télétravail, etc.)*

Le Sous-Traitant reconnaît que la liste ci-dessus n'est pas exhaustive et représente un socle minimal. Il maintiendra un niveau de sécurité global conforme aux normes de l'industrie et à l'état de l'art pour des données de nature et de sensibilité équivalentes. Toute mesure de sécurité supplémentaire mise en œuvre sera documentée et communiquée au Responsable de Traitement sur demande.

Annexe 2 – Liste des Sous-Traitants Ultérieurs autorisés

[Exemple de tableau à remplir, la liste doit être tenue à jour par le ST et refléter tous les sous-traitants impliqués]

Nom du Sous-Traitant Ultérieur	Adresse (pays)	Service fourni (activité sous-traitée)	Données concernées	Garanties (certification, CCT, etc.)
ABC Hosting Ltd	Paris, France	Hébergement des serveurs et bases de données	Toutes les données	Certification ISO 27001, contrat de sous-traitance RGPD signé
XYZ Support SAS	Marseille, France	Support technique niveau 2 (heures non ouvrées)	Données d'identification et tickets support	Employés soumis NDA, accès VPN sécurisé, pas de copie locale
CloudBackup Inc.	Dublin, Irlande	Sauvegarde externalisée chiffrée	Données sauvegardées (base SQL)	CCT adoptées + ISO 27018, hébergement UE exclusivement
... (ajouter d'autres lignes selon le cas)				

(Le Responsable de Traitement autorise les entités listées ci-dessus. Toute modification sera effectuée selon Clause 4.5. Le Sous-Traitant garantit que ces entités respectent les obligations du présent Contrat.)

Conclusion générale du livre blanc

À travers ce livre blanc, nous avons examiné en détail le **contrat de sous-traitance IT** à la lumière du RGPD, en identifiant d'une part les **clauses obligatoires** imposées par la réglementation (Partie 1) et d'autre part les **clauses additionnelles** recommandées pour une meilleure protection juridique et opérationnelle (Partie 2). Nous avons finalement proposé un **modèle complet de DPA** (Partie 3) illustrant concrètement comment articuler l'ensemble de ces exigences dans un contrat à destination des directeurs juridiques, avocats et DPO.

Il ressort que le DPA est un **outil contractuel stratégique** pour maîtriser les risques liés à l'externalisation de traitements de données personnelles. Un DPA précis et robuste permet au responsable de traitement de **déléguer en confiance** tout en conservant les garanties nécessaires, et au sous-traitant de **démontrer sa conformité** et son sérieux en matière de protection des données. Dans un contexte de responsabilité partagée et d'attention croissante des autorités (la CNIL n'hésitant pas à sanctionner l'absence ou l'insuffisance des contrats de sous-traitance), il est crucial pour les professionnels du droit et de la conformité de **maîtriser la négociation et la rédaction des DPA**.

En pratique, la clé d'un bon DPA réside dans la **clarté** (définir sans ambiguïté le qui fait quoi), la **complétude** (couvrir tous les aspects légaux et opérationnels) et l'**adaptabilité** (ajuster les clauses au cas par cas selon le service et les risques spécifiques). Les directeurs juridiques et DPO devront collaborer étroitement, ainsi qu'impliquer les équipes techniques et de sécurité, pour s'assurer que le contrat reflète fidèlement la réalité des traitements et les engagements de sécurité effectivement mis en place.

Ce livre blanc vise à servir de référence et de guide pratique. Il conviendra de le tenir à jour au gré des évolutions législatives et jurisprudentielles, ainsi que des **lignes directrices du CEPD** ou de la CNIL, qui affinent régulièrement l'interprétation des obligations (on pense notamment aux précisions du CEPD sur la sous-traitance en cascade en 2024). Le DPA, document vivant, doit lui aussi pouvoir évoluer.

En définitive, la conformité d'un contrat de sous-traitance n'est pas un état statique mais un processus de vigilance continue. La rédaction initiale doit être solide, la négociation équilibrée, puis le **pilotage** dans la durée assuré (mise à jour des clauses en cas de changement de sous-traitants ou de contexte, audits réguliers, etc.). Armés de ce livre blanc, les directeurs juridiques, avocats et DPO disposent des clés pour **sécuriser leurs contrats de sous-traitance IT** et, ce faisant, protéger les données et les droits des personnes de manière efficace.

Les enjeux sont élevés, mais avec une démarche rigoureuse et collaborative, le contrat de sous-traitance peut devenir le socle d'une relation de confiance entre le responsable de traitement et son prestataire, au bénéfice de tous et dans le respect plein et entier du RGPD.

Sources : Règlement (UE) 2016/679 (RGPD), Articles 28, 32, 33, 82 ; [Lignes directrices du CEPD – notions de responsable et sous-traitant, 2020] ; [CNIL – Exemples de clauses de sous-traitance, 2017] ; [CNIL – Guide du sous-traitant, 2017] ; Sous-traitance : Exemple de clauses | CNIL