



Conditions générales Addendum RGPD

1.	Addendum	3
1.1.	PARTIES	3
1.2.	OBJET	3
1.3.	DÉFINITIONS.....	3
2.	Engagements.....	4
2.1.	OPÉRATIONS DE TRAITEMENT CONCERNÉES.....	4
2.2.	DROITS ET OBLIGATIONS DU RESPONSABLE DU TRAITEMENT.....	5
2.3.	DROITS ET OBLIGATIONS DU SOUS-TRAITANT.....	5
3.	Dispositions générales	6
3.1.	CONFIDENTIALITÉ.....	6
3.2.	MESURES DE SÉCURITÉ	7
3.3.	NOTIFICATION D'UNE VIOLATION.....	7
3.4.	DÉLÉGATION SOUS-TRAITANCE	7
3.5.	DURÉE ET FIN DE CONTRAT DE SOUS-TRAITANCE	8
4.	Mesures permanentes.....	8
4.1.	MESURES ORGANISATIONNELLES	8
4.2.	MESURES OPÉRATIONNELLES.....	9

1. Addendum

1.1. PARTIES

Art. 1 L'Addendum RGPD complète les Conditions Générales de Bisoft S.A. et fait partie intégrante de tout Contrat de Service conclu ou qui serait conclu entre les parties suivantes :

Le Client (le Responsable du traitement).
Bisoft S.A. en sa qualité de sous-traitant

Art. 2 En acceptant les Conditions Générales, ou tout autre Contrat de service de Bisoft S.A., le Client accepte expressément l'application des clauses suivantes concernant le traitement des données à caractère personnel par Bisoft S.A..

Art. 3 La personne de contact de Bisoft S.A. est :

- Le Délégué à la protection des données (Data Protection Officer ou DPO)
- privacy@Bisoft.be

1.2. OBJET

Art. 4 L'Addendum RGPD correspond à un contrat de sous-traitance qui définit les droits et les obligations respectifs des Parties conformément aux législations référencées à l'Art.5.

1.3. DÉFINITIONS

Art. 5 **Législation :**

- **Règlement général sur la protection des données ou RGPD:** le Règlement (UE) 2016/679 du Parlement européen et du Conseil du 27 avril 2016 relatif à la protection des personnes physiques à l'égard du traitement des Données à caractère personnel et à la libre circulation de ces données, applicable à partir du 25 mai 2018.
- **Autorité de contrôle :** l'Autorité de protection des données.

Art. 6 **Contrats :**

- **Contrat de service:** Tous les contrats conclus avec Bisoft S.A. pour l'implémentation de solution, les services SAAS, l'hébergement, le support, les contrats de licences et de maintenance informatique, la mise à disposition de ressources.

Art. 7 **Intervenants :**

- **Personne concernée** : la personne physique identifiée ou identifiable dont les Données à caractère personnel font l'objet des Opérations de traitement.
- **Catégories de personnes** : les clients, utilisateurs, employés sont concernées par les Opérations de traitement.
- **Responsable du traitement** : la personne physique ou morale qui a mis en place et détermine les moyens du traitement de Données à caractère personnel.
- **Sous-traitant** : la personne physique ou morale qui traite les Données à caractère personnel pour le compte et sur instruction du Responsable du traitement.
- **Personnel** : les personnes désignées par les Parties pour exécuter le contrat et qui sont placées sous leur autorité directe.

Art. 8 **Données :**

- **Données à caractère personnel** : toute information se rapportant à une personne physique identifiable par un nom, un numéro d'identification, des données de localisation, un identifiant en ligne, ou à un ou plusieurs éléments spécifiques propres à son identité.
- **Catégories de Données à caractère personnel** : Nom, prénom, adresse physique, date de naissance, adresse email, sexe, âge, adresse IP, données financières, images, etc.
- **Opération de traitement** : toute opération effectuée à l'aide de procédés manuels ou automatique et appliquée à des données ou des ensembles de données à caractère personnel, telles que la collecte, l'enregistrement, la qualification, la conservation, l'adaptation, l'extraction, la consultation, l'utilisation, la communication, la diffusion ou toute autre forme de mise à disposition, le rapprochement ou l'interconnexion, la limitation, l'effacement ou la destruction.
- **Violation de données** : toute violation de la sécurité entraînant, de manière accidentelle ou délibérée et illicite, la divulgation, la modification, la destruction ou l'accès non autorisé de données à caractère personnel.

2. Engagements

2.1. OPÉRATIONS DE TRAITEMENT CONCERNÉES

- Art. 9 Le Sous-traitant s'engage à ne traiter des Données à caractère personnel que sur la base d'instructions écrites du Responsable du traitement dans le cadre du Contrat de Service conclu.
- Art. 10 Le Sous-traitant est autorisé à traiter pour le compte du Responsable du traitement les Données à caractère personnel nécessaires pour assurer les services strictement prévus dans le Contrat de Service conclu entre les Parties.
- Art. 11 Pendant toute la durée du Contrat de sous-traitance, les Données à caractère personnel sont soumises aux Opérations de traitement recensées dans la définition de l'ART.8.

2.2. DROITS ET OBLIGATIONS DU RESPONSABLE DU TRAITEMENT

Art. 12 Le Responsable du traitement :

- est entièrement responsable des traitements de Données à caractère personnel effectués par les membres de son Personnel.
- doit fournir les informations mentionnées aux articles 13 et 14 du RGPD aux personnes concernées par les Opérations de traitement.
- tient un registre des activités de traitement effectuées sous sa responsabilité, conformément aux modalités prévues à l'article 30(1) du RGPD.

Art. 13 Le Responsable du traitement :

- met à la disposition du Sous-traitant les Données à caractère personnel faisant l'objet du présent Contrat de sous-traitance. Il détermine les moyens et les finalités du traitement.
- garantit en outre la licéité du traitement, notamment le transfert des Données à caractère personnel au Sous-traitant.
- met à la disposition du Sous-traitant ses instructions écrites concernant le traitement. Il garantit la conformité de ses instructions à la Législation sur la protection des données personnelles.
- conserve la propriété des Données à caractère personnel, des informations et du matériel mis à la disposition du Sous-traitant dans le cadre de l'exécution du Contrat de sous-traitance.
- notifie à l'autorité de contrôle la Violation de Données à caractère personnel.

2.3. DROITS ET OBLIGATIONS DU SOUS-TRAITANT

Art. 14 Le Sous-traitant :

- ne traite que les Données à caractère personnel strictement nécessaires à l'exécution du Contrat de service et uniquement pour les finalités définies dans le Contrat de sous-traitance et déterminées par le Responsable du traitement.
- s'engage à traiter les Données à caractère personnel conformément aux instructions écrites du Responsable du traitement et aux dispositions du présent Contrat de sous-traitance.
- Vérifie que les accès des personnes désignées et autorisées à traiter les données personnelles sont strictement limité aux nécessités liées à l'exécution du Contrat de Service et que ces personnes sont sensibilisées à la protection des données à caractère personnel.
- informe le responsable de traitement lorsqu'une instruction constitue une violation de la législation.
- ne peut effectuer aucune opération de traitement en dehors de l'Espace Economique Européen.
- transfère immédiatement les demandes des personnes concernées exerçant leurs droits au Responsable du traitement qui se chargera du traitement ultérieur de la demande.

- traite les Données à caractère personnel aussi longtemps que nécessaire dans l'exécution de ses obligations contractuelles. Il veillera ensuite à mettre fin à tout traitement des Données à caractère personnel, autre que la suppression ou la remise des données au Responsable du traitement à sa demande.

Art. 15 Le sous-traitant s'engage à assurer les missions suivantes contre rémunération convenue avec le Responsable de traitement dans le volet financier du Contrat de Service :

- Réalisation de copies et/ou back-ups des Données à caractère personnel si cela s'avère nécessaire à l'exécution du Contrat principal. Les Données à caractère personnel concernées jouissent de la même protection que les Données à caractère personnel d'origine.
- Assistance au Responsable du traitement pour la réalisation d'analyses d'impact relative à la protection des données et pour la réalisation de la consultation préalable de l'autorité de contrôle et les réponses aux demandes de l'autorité de contrôle ou au DPO désigné par le Responsable du traitement ou toute autre personne physique ou morale mandatée par le Responsable du traitement.
- Dans le cadre de Contrat de Service couvrant la mise en place d'applications Web, le Sous-traitant s'engage à aider le Responsable du traitement à s'acquitter de son obligation de donner suite aux demandes d'exercice des droits des personnes concernées : droit d'accès, de rectification, d'effacement, et d'opposition, droit à la limitation du traitement, droit à la portabilité des données, droit de ne pas faire l'objet d'une décision individuelle automatisée (y compris le profilage).
- Le Sous-traitant tient par écrit un registre des activités de traitement effectuées pour le compte du Responsable du traitement. Ce registre doit contenir toutes les informations visées à l'article 30(2) du RGPD.

3. Dispositions générales

3.1. CONFIDENTIALITÉ

Art. 16 Le Sous-traitant s'engage à informer son Personnel à propos de la Législation relative à la protection des données personnelles et des dispositions du Contrat de sous-traitance.

Art. 17 Le Sous-traitant est tenu à une obligation de confidentialité concernant toutes les Données à caractère personnel traitées et communiquées au Sous-traitant dans le cadre du Contrat de sous-traitance.

Cette obligation de confidentialité s'applique de la même manière au personnel du Sous-traitant et aux éventuels Sous-traitants et à leur propre personnel.

Cette obligation de confidentialité prend effet dès la négociation du Contrat de Service et n'est pas limitée dans le temps.

Art. 18 Cette obligation de confidentialité ne s'applique pas lorsque :

- le Sous-traitant est tenu de communiquer les Données à caractère personnel à l'Autorité de contrôle.
- l'information est déjà connue du public.
- la communication des Données à caractère personnel a été autorisée par le Responsable du traitement qui assure avoir les bases légales pour ce faire.

3.2. MESURES DE SÉCURITÉ

- Art. 19 Le Responsable du traitement et le Sous-traitant s'engagent à mettre en œuvre des Mesures de sécurité garantissant un niveau maximum pour protéger les Données à caractère personnel contre la destruction accidentelle ou délibérée et illicite, la diffusion, l'accès, la collecte ou tout traitement ultérieur non-autorisé et en particulier lorsque le traitement comprend la transmission de données dans un réseau.
- Art. 20 Le Sous-traitant est tenu d'informer le Responsable du traitement des adaptations des Mesures de sécurité et de leurs coûts lorsque des modifications importantes doivent être apportées aux technologies utilisées pour sécuriser les données.

Si le Responsable du traitement refuse l'exécution de ces mesures, le Sous-traitant ne pourra pas être tenu pour responsable en cas de violation des données imputable à une omission dans le chef du Responsable du traitement. Le Responsable du traitement sera entièrement responsable du paiement de toute amende administrative et/ou indemnité qui en découlerait.

Le sous-traitant ne peut pas être tenu responsable de la perte, de la corruption des données ou du vol d'identité qui ont notamment été causés par des virus ou des chevaux de Troie, des injonctions SQL ou toute autre attaque (contre les systèmes informatiques ou les portails cloud) indépendante de sa volonté.

Néanmoins, et conformément au Règlement, nous sommes tenus de documenter et de communiquer à l'autorité de contrôle compétente, dans les délais fixés par le Règlement, toute brèche de sécurité susceptible de représenter un risque pour les droits et libertés des personnes concernées.

3.3. NOTIFICATION D'UNE VIOLATION

- Art. 21 Le Sous-traitant notifie au Responsable du traitement toute Violation de Données à caractère personnel dans les plus brefs délais, et au plus tard 24 heures après en avoir pris connaissance sauf si indication contraire du Responsable du traitement par écrit avant la signature du contrat. Le délai est porté à 48 heures lorsque la violation n'engendre aucun risque pour les droits et libertés des personnes concernées.
- Art. 22 Dans une seconde étape, le Sous-traitant communique toute documentation utile pour permettre au Responsable du traitement de notifier cette violation à l'autorité de protection des données et/ou aux personnes concernées dont notamment :

- la nature de la Violation de Données à caractère personnel ;
- les catégories et le nombre approximatif de personnes concernées ;
- les catégories et le nombre approximatif de Données à caractère personnel concernées ;
- le nom et les coordonnées du délégué à la protection des données ou d'un autre point de contact auprès duquel des informations supplémentaires peuvent être obtenues ;
- les conséquences probables de la Violation de Données à caractère personnel ;
les mesures prises pour remédier à la Violation de Données à caractère personnel ou pour en atténuer les éventuelles conséquences négatives ;

- Art. 23 La décision d'informer ou non les Personnes concernées d'une Violation de Données à caractère personnel incombe au Responsable du traitement.

3.4. DÉLÉGATION SOUS-TRAITANCE

- Art. 24 Le Sous-traitant peut déléguer l'ensemble ou une partie de ses obligations à un autre Sous-traitant uniquement avec l'autorisation écrite, préalable et spécifique du Responsable du traitement.

Le Responsable du traitement ne peut refuser la demande du Sous-traitant que s'il invoque des motifs légitimes.

Art. 25 Le Sous-traitant reste le point de contact du Responsable du traitement et demeure pleinement responsable vis-à-vis du Responsable du traitement de l'exécution de ses obligations.

Art. 26 Les engagements prévus au chapitre 2 s'appliquent intégralement au Sous-traitant. Ces obligations sont stipulées par écrit dans un Contrat de sous-traitance.

Les catégories d'engagements concernent :

- Respect des exigences
- Sécurité des données et accès
- Procédures
- Collaboration avec d'autres sous-traitants
- Centre de données
- Audit, enregistrement, contrôle et documentation

3.5. DURÉE ET FIN DE CONTRAT DE SOUS-TRAITANCE

Art. 27 Le Contrat de Sous-traitance entre en vigueur en même temps que le premier Contrat de Service et prend fin en même temps que le dernier Contrat de Service.

Art. 28 Au terme du dernier Contrat de service conclu avec le Responsable du traitement, le Sous-traitant devra renvoyer au Responsable du traitement toutes les Données à caractère personnel. Il lui fournit également toutes les informations et la documentation nécessaires au traitement ultérieur de ces données.

Art. 29 Après le renvoi des Données à caractère personnel au Responsable du traitement, le Sous-traitant met immédiatement fin à tout traitement des Données à caractère personnel et détruit toutes les copies existantes dans ses systèmes d'information sauf si instruction contraire du Responsable. La seule exception concernerait les backups sur support amovibles dont la période de rétention d'une partie des informations ne permettrait pas la destruction globale du contenu.

3.6. MODIFICATION DE L'ADDENDUM RGPD

Art. 30 Bisoft S.A. se réserve le droit de compléter ou préciser l'Addendum RGPD de sa propre initiative avec les obligations suivantes :

- Ne supprimer aucun des engagements.
- Publier une nouvelle version en conservant l'historique accessible au Client.
- Prévenir le Client.

4. Mesures permanentes

4.1. MESURES ORGANISATIONNELLES

Art. 31 La liste non exhaustive suivante reprend les mesures mises en place par le Sous-traitant :

- Une équipe déléguée à la protection des données a été désignée pour prendre en charge la protection des données et des modalités de mise en œuvre du RGPD.
- L'équipe pour la protection des données est assistée par un comité d'experts dans divers domaines : juridique, méthodologique, technique, gouvernance et gestion du risque informatique.
- Tous les collaborateurs sont sensibilisés pour respecter la réglementation et les procédures.
- Un registre reprenant toutes les activités de traitement des données personnelles est
Bisoft S.A. | Avenue Thomas Edison 95 | B-1402 Nivelles | Tél +32 2 880 12 00 |
www.bisoft.be | info@bisoft.be | TVA: BE-0459.160.980

constitué, selon le modèle proposé par l'ancienne commission pour la protection de la vie privée, devenue l'Autorité pour la Protection des Données le 25 mai 2018. Ce registre est consolidé et maintenu en permanence à jour.

- Une analyse d'impact relative à la protection des données (AIPD) est effectuée pour chaque activité susceptible de comporter un risque pour les données personnelles
- Des recommandations sont identifiées et revues en permanence pour réduire les risques de non-conformité.
- Pour chaque nouvelle recommandation, un projet d'implémentation est géré par le DPO.
- Une Charte Vie Privée disponible sur le site internet du sous-traitant.

4.2. MESURES OPÉRATIONNELLES

Art. 32 Des dispositifs de sécurité ont été mis en place tant au niveau physique (protection des bâtiments et du data center), organisationnel (procédures, respect de directives) que technique pour prévenir ou déceler rapidement tout incident et de le traiter conformément aux dispositions du RGPD.

Elles s'inscrivent dans la politique de gestion de la sécurité gérée par le responsable de la sécurité du Sous-traitant.

Art. 33 La liste non exhaustive suivante reprend les principales procédures internes opérationnelles relatives à la sécurité des données du Client :

- Procédure « Access management »
- Procédure « Information Security management »
- Procédure « Gestion historique des accès physiques aux datacenters »

Ces procédures sont conformes et complémentaires à celles des gestionnaires des datacenter auxquels sont sous-traités les hébergements et accès.

Art. 34 Le sous-traitant utilise les moyens nécessaires pour garantir la confidentialité, l'intégrité, la disponibilité et la résilience constantes des systèmes et des services de traitement des données :

- La confidentialité : l'accès aux bases de données est restreint et contrôlé.
- L'intégrité : des backups sont réalisés de manière automatique et fréquente ;
- La disponibilité : un export des données peut être fourni à première demande ;
- La résilience : les données peuvent être rétablies de manière rapide.

Art. 35 La liste des dispositifs et mesures mis en place par le Sous-traitant pour la sécurité de son infrastructure et de celle mise à disposition du Client figure dans le Contrat de services concerné.

Art. 36 Le Sous-traitant utilise une procédure de test, d'analyse et d'évaluation régulière de l'efficacité des mesures techniques et organisationnelles pour assurer la sécurité du traitement des données.