

ANNEXE DONNEES A CARACTERE PERSONNEL

1. Dans le cadre de l'exécution du Contrat, le Prestataire pourra être amené à avoir accès à et/ou traiter des données à caractère personnel dont le Client est responsable ou sous-traitant au sens de la réglementation applicable (ci-après les « **Données** »).

2. Un tel accès et/ou traitement s'effectue par le Prestataire pour le compte du Client, en qualité de sous-traitant, la communication des Données au Prestataire valant instruction documentée du Client de traiter lesdites données dans le cadre du Contrat.

3. Les traitements dont l'exécution est susceptible d'être ainsi confiée par le Client au Prestataire présentent les caractéristiques suivantes :

Données concernées	Catégorie(s) de personnes concernées par les données	Nature des opérations effectuées sur les données par le Prestataire	Finalité du traitement effectué par le Prestataire	Durée de conservation par le Prestataire*
Données de suivi des tickets incidents	Utilisateurs (le personnel du Client)	Suivi des tickets incidents	Gestion des incidents	Durée du contrat
Données présentes sur l'appareil de l'utilisateur	Utilisateurs	Accès	Opérations d'assistance et/ou de maintenance et/ou de télémaintenance**	N/A
Données présentes sur les Équipements gérés par le Prestataire, le cas échéant	Utilisateurs	Accès	Opérations d'assistance et/ou de maintenance et/ou de télémaintenance	N/A
Données hébergées sur les plateformes Cloud/SaaS tiers telles que Microsoft 365 (Exchange, SharePoint, OneDrive, Teams...), OVHcloud, Google, etc..	Utilisateurs	Accès indirect via les outils d'administration ou d'assistance	Gestion, administration et support des services Cloud/SAS pour le compte du Client	N/A
Logs de connexion des Équipements installés chez le Client	Utilisateurs	Accès	Gestion des logs opérés sur les systèmes du Client, à des fins probatoires	N/A

* Au terme du présent contrat, le Prestataire s'engage à supprimer les Données à l'issue des délais d'archivage définis, au-delà des délais de conservation précisés ci-dessus, (i) pour la durée des délais de prescription applicables, à des fins de preuve, pour l'établissement, l'exercice ou la défense de ses droits et/ou (ii) en application d'une exigence légale ou réglementaire.

** Sauf nécessité absolue pour les besoins d'une intervention d'assistance, l'utilisateur concerné est tenu de (i) s'assurer, préalablement à l'accès au système concerné par le Prestataire, qu'aucune Donnée présente sur le système concerné n'est visible par le Prestataire et (ii) superviser à cette fin l'intervention du Prestataire sans interruption jusqu'à la fin de l'intervention. Le Client s'engage à fournir aux utilisateurs toute information nécessaire à cet égard.

4. Le Client garantit au Prestataire que :

- les données auxquelles le Prestataire aura ainsi accès ont été collectées et traitées en conformité avec la réglementation applicable et le seront pour toute la durée du Contrat ;
- le Client a préalablement fourni aux personnes concernées par les Données toute information pertinente et/ou recueilli les consentements requis, y compris s'agissant des accès et/ou traitements effectués par le Prestataire, et plus généralement s'acquittera, pendant toute la durée du Contrat, de l'ensemble de ses obligations à l'égard des personnes concernées par les Données.

A ce titre, le Client garantit le Prestataire contre toutes réclamations, émanant de tout tiers invoquant la violation d'un droit quelconque, et supportera tous les frais et dommages intérêts y afférent.

En outre, le Client s'engage pour toute la durée du Contrat à fournir au Prestataire toute information utile afin de lui permettre de respecter ses obligations en ce qui concerne les Données.

5. De son côté, le Prestataire s'engage à :

- dans le cadre des opérations de télémaintenance, informer l'utilisateur de son intervention et obtenir l'accord de l'utilisateur du Client avant toute intervention ;
- utiliser les Données aux seules fins des finalités énumérées au paragraphe 3 ci-dessus, dans le respect des instructions du Client et des stipulations du Contrat ;
- préserver la confidentialité des Données à caractère personnel du Client et veiller à ce que les personnes autorisées à traiter les Données s'engagent à respecter la confidentialité ou soient soumises à une obligation légale appropriée de confidentialité ;
- prendre toutes les mesures requises afin de mettre en œuvre, compte tenu de l'état des connaissances, des coûts de mise en œuvre et de la nature, de la portée, du contexte et des finalités du traitement ainsi que des risques pour les droits et libertés des personnes physiques, les mesures techniques et organisationnelles appropriées afin de garantir un niveau de sécurité des Données qu'il traite adapté au risque ;
- tenir compte de la nature du traitement, aider le Client, par des mesures techniques et organisationnelles appropriées, dans toute la mesure du possible, à s'acquitter de son obligation de donner suite aux demandes dont les personnes concernées qui le saisissent en vue d'exercer leurs droits prévus par la réglementation applicable. En cas de demande d'exercice de leurs droits par les personnes concernées auprès du Prestataire, le Prestataire y répondra

directement, s'agissant des traitements faisant l'objet du Contrat, au nom et pour le compte du Client et dans les délais requis par la réglementation applicable ;

- contribuer, pour ce qui le concerne et en fonction des informations dont il dispose sur les traitements du Client, aux analyses d'impact que le Client réalise et l'assister, en tant que de besoin, pour la consultation préalable de l'autorité de contrôle ;
- notifier au Client toute violation de données à caractère personnel dans un délai maximum de vingt-quatre (24) heures après en avoir pris connaissance. Cette notification est accompagnée de toute information et documentation utile afin de permettre au Client, si nécessaire, de notifier cette violation à l'autorité de contrôle compétente. Il appartient au Client de déterminer : (i) si la violation de données doit ou non être notifiée à toute personne, autorité de régulation, autorité administrative ou à toute autre personne en vertu de la réglementation applicable et (ii) le contenu de ladite notification.

Dans le cadre des opérations de maintenance, de diagnostic ou de support, le Prestataire peut être amené à transporter et conserver temporairement, pour les stricts besoins de l'intervention, des équipements appartenant au Client et susceptibles de contenir des Données à caractère personnel.

Le Prestataire s'engage à mettre en œuvre, dans ce contexte, des mesures de sécurité adaptées, incluant notamment :

- la limitation de la durée de conservation du matériel hors des locaux du Prestataire,
- la protection contre les accès non autorisés,
- le verrouillage physique des équipements lors de leur transport,
- et, lorsque cela est possible techniquement et économiquement au regard des moyens du Prestataire, le chiffrement des supports de stockage.

En cas de perte, de vol ou de compromission d'un équipement susceptible de contenir des Données à caractère personnel, le Prestataire s'engage à notifier le Client dans les conditions prévues à l'article 5 des présentes et à coopérer pleinement pour l'évaluation du risque et, le cas échéant, la notification aux autorités compétentes et/ou aux personnes concernées, conformément aux articles 33 et 34 du RGPD.

6. Chacune des parties s'engage en tout état de cause à respecter la réglementation applicable.

7. Si le Prestataire considère qu'une instruction constitue une violation de la réglementation applicable relative à la protection des données, il en informe immédiatement le Client. En outre, si le Prestataire 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 de l'Etat membre auquel il est soumis, il doit informer le responsable du traitement de cette obligation juridique avant le traitement, sauf si le droit concerné interdit une telle information pour des motifs importants d'intérêt public.

8. Le Prestataire déclare tenir par écrit un registre de toutes les catégories d'activités de traitement effectuées pour le compte du Client, dans les formes requises par la réglementation applicable.

9. Le Client demeure seul responsable de la licéité, de la qualité, du contenu et de la sécurité des données qu'il traite, conserve ou héberge dans le cadre des services fournis.

Le Prestataire ne saurait être tenu responsable d'une perte, d'une altération, d'une indisponibilité ou d'une violation de données résultant d'un dysfonctionnement, d'une maintenance, d'une interruption de service ou d'un incident imputable à un prestataire tiers, notamment à un fournisseur de services cloud ou SaaS (tels que Microsoft 365, OVHcloud, Google Workspace ou tout autre hébergeur), ni d'un usage inapproprié ou d'une mauvaise configuration imputable au Client.

10. Le Prestataire est expressément autorisé à faire appel, pour tout ou partie des opérations dont il a la charge dans le cadre de l'exécution du Contrat, à un ou plusieurs sous-traitants, au sens de la réglementation applicable. Le(s) sous-traitant(s) sera(ont) tenu(s) de respecter les obligations mentionnées dans la présente Annexe « Données à caractère personnel ». Le Prestataire demeure en tout état de cause pleinement responsable du respect de ses obligations par le ou les sous-traitant(s). L'identité et les coordonnées du ou des sous-traitants au(x)quel(s) le Prestataire fait ainsi appel sont disponibles sur demande du Client adressée à dpo@comete-informatique.com, de sorte que le Client puisse formuler ses objections à l'intervention desdits sous-traitants. Cette information doit indiquer clairement les activités de traitement sous-traitées, l'identité et les coordonnées du sous-traitant et les dates du contrat de sous-traitance. Le Client dispose d'un délai de quinze (15) jours à compter de la date de réception de cette information pour notifier ses objections au Prestataire par lettre recommandée avec accusé de réception. En cas d'objection, les parties se rapprocheront afin d'étudier de bonne foi une solution préservant, dans le respect de la réglementation applicable, leurs intérêts respectifs. A défaut d'accord sur une telle solution dans un délai de quinze (15) jours à réception de la notification de l'objection, le Prestataire pourra à son tour notifier au Client, par lettre recommandée avec accusé de réception, mettre fin aux Prestations et ce, sans indemnité de part ni d'autre.

11. Sauf autorisation expresse spécifique contraire du Client, le Prestataire s'engage à traiter les Données exclusivement sur le territoire de l'Union européenne. En cas de transfert hors UE imposé par la loi ou requis pour la prestation, le Prestataire mettra en œuvre un mécanisme conforme (clauses contractuelles types, garanties appropriées, etc.).

12. Le Prestataire met à la disposition du Client la documentation nécessaire pour démontrer le respect de ses obligations au titre de la présente annexe « Données à caractère personnel » et pour permettre la réalisation d'audits par le Client ou un auditeur mandaté par le Client (i) soumis à de strictes obligations de confidentialité et (ii) préalablement agréé de bonne foi par le Prestataire. De tels audits devront être réalisés au frais du Client et hors des locaux du Prestataire. Ils porteront sur les documents fournis par le Prestataire afin d'attester du respect de ses engagements au titre de la présente annexe « Données à caractère personnel », notamment les procédures mises en œuvre afin d'assurer le respect par le Prestataire desdits engagements. Le rapport d'audit devra être communiqué au Prestataire, afin de lui permettre de formuler ses observations.

13. EN DEHORS DES CAS LIMITATIVEMENT ENUMERES AU PARAGRAPHE 3 CI-DESSUS, LE PRESTATAIRE N'A EN AUCUN CAS ET DE QUELQUE MANIERE QUE CE SOIT A CONNAITRE, ACCEDER OU TRAITER DES DONNEES A CARACTERE PERSONNEL DU CLIENT. DES LORS, IL APPARTIENT AU CLIENT DE PRENDRE TOUTES LES DISPOSITIONS QUI S'IMPOSENT AFIN D'EVITER QUE LE PRESTATAIRE N'AIT ACCES AUXDITES DONNEES A CARACTERE PERSONNEL DU CLIENT. SI UN TIERS (EN CE COMPRIS UNE AUTORITE DE CONTROLE FRANÇAISE OU ETRANGERE) ENGAGEAIT LA RESPONSABILITE DU PRESTATAIRE EN RELATION AVEC DES DONNEES A CARACTERE PERSONNEL DU CLIENT, AUXQUELLES LE PRESTATAIRE N'A PAS ACCEPTE PREALABLEMENT ET PAR ECRIT D'AVOIR ACCES, LE CLIENT S'ENGAGE A PRENDRE EN CHARGE LE PAIEMENT DE TOUTE SOMME (EN CE COMPRIS NOTAMMENT TOUTS DOMMAGES ET INTERETS, FRAIS DE PROCEDURE ET D'AVOCATS ENGAGES PAR LE PRESTATAIRE), QUE LE PRESTATAIRE SERAIT AMENE A DEBOURSER EN CONSEQUENCE D'UNE TELLE ACTION.

14. En cas de non-respect de l'une quelconque de ses obligations par le Client, non réparé par le Client dans un délai de quinze (15) jours de la notification adressée par le Prestataire au Client, le Prestataire pourra, par lettre recommandée avec accusé de réception, mettre fin aux Prestations et ce, sans indemnité à la charge du Prestataire.

15. Les parties désignent les interlocuteurs suivants, afin de centraliser toutes les informations et être le point de contact de l'autre partie pour toute question portant sur des données à caractère personnel :

Pour le Prestataire : son Délégué à la Protection des Données, 11, rue de Gavrinis, 35170 BRUZ, téléphone : 02 99 42 80 82, adresse email : dpo@comete-informatique.com

Chacune des parties s'engage à prévenir l'autre partie dans les meilleurs délais en cas de changement d'interlocuteur.

DATE + CACHET & SIGNATURE
CLIENT