ADAT
Agence
Départementale
d'Appui aux Territoires

Règlement d'exécution de la prestation « Pack CyberSécurité »

Préambule

L'agence départementale d'appui aux territoires (ADAT) , établissement public administratif au sens du Code Général des Collectivités Territoriales (CGCT), propose à ses adhérents (collectivités territoriales et établissements publics) une prestation « Pack CyberSécurité ». Cette offre regroupe un ensemble de services visant à renforcer la sécurité de leur système d'information.

Le présent règlement, adopté par le Conseil d'Administration de l'ADAT, fixe les conditions d'abonnement, d'exécution, de gestion et de résiliation de cette prestation. Il est consultable sur le site de l'ADAT https://adat-doubs.fr ou adressé sur simple demande. Il est systématiquement joint à toute demande de devis.

1. Objet

Le présent règlement définit les modalités selon lesquelles l'ADAT fournit la prestation « Pack CyberSécurité » à ses adhérents.

Pour l'exécution de ces prestations, l'ADAT fait appel à des prestataires spécialisés. Les techniciens de l'ADAT assurent, quant à eux, l'installation, le paramétrage, la maintenance et l'accompagnement à la prise en main des solutions mises à disposition.

Les outils du Pack CyberSécurité visent à renforcer au maximum le niveau de protection informatique, cependant aucun système d'information n'est totalement infaillible.

2. Description des prestations

Le détail actualisé des prestations et leurs spécificités techniques sont consultables sur le site https://adat-doubs.fr/. Le « Pack CyberSécurité » inclut notamment :

- ***Antivirus avec protection proactive supervisé***

L'ADAT assure l'installation, le paramétrage et le suivi d'un logiciel antivirus sur les postes de travail désignés par l'adhérent. Cette solution inclut les mises à jour et est compatible avec les logiciels Berger-Levrault.

L'adhérent est invité à signaler à l'ADAT tout dysfonctionnement ou message suspect dans les meilleurs délais.

L'antivirus contribue à réduire les risques mais ne protège pas contre les usages inappropriés ou des défaillances extérieures au dispositif.

- ***Gestion du nom de domaine Internet de la collectivité en .fr***

L'ADAT prend en charge, pour le compte de l'adhérent, la réservation, le transfert et le renouvellement de noms de domaine. L'adhérent demeure seul responsable du choix du nom enregistré. À ce titre, il doit veiller à ce que le nom de domaine :

- soit correctement orthographié, sachant que toute erreur lui sera imputable,
- ne contrevienne à aucune disposition légale ou réglementaire ;
- respecte les droits des tiers (propriété intellectuelle, nom patronymique, etc.) ;
- ne présente aucun caractère illicite ou contraire aux bonnes mœurs.

Pour plus de sécurité, il est recommandé à l'adhérent de vérifier que le nom de domaine qu'il souhaite enregistrer ne correspond ni à une marque déjà déposée, ni à la raison sociale d'une personne morale existante. Pour cela, il convient d'effectuer une vérification auprès du Registre National des Marques (RNM) et du Registre National du Commerce et des Sociétés (RCS).

Il est précisé que l'ADAT agit en tant qu'intermédiaire technique et ne peut garantir l'attribution effective du nom de domaine choisi. Elle ne saurait être tenue responsable en cas d'impossibilité d'attribution du nom de domaine choisi par l'adhérent.

L'adhérent reste propriétaire du nom de domaine de sa structure.

En cas de transfert, l'opération nécessite le code d'autorisation détenu par l'ancien prestataire. À défaut, le transfert ne pourra être effectué.

- ***Coffre-fort numérique de mot de passe***

Ce service consiste à fournir une solution sécurisée pour stocker et gérer des mots de passe. Le coffre-fort est conçu pour protéger les informations sensibles grâce à des technologies de chiffrement avancées, de stockage protégé et de génération de mot de passe robuste.

L'ADAT assure la maintenance, les mises à jour de la solution ainsi qu'une assistance en cas de problème d'accès ou de dysfonctionnement. Sa responsabilité est limitée aux aspects techniques du service. En cas d'usage inadapté ou de perte de données, la responsabilité de l'ADAT ne saurait être engagée. L'adhérent reste responsable de la sécurité physique de ses équipements.

Les données sont hébergées en Europe, dans le respect du Règlement général sur la protection des données (RGPD). Pour garantir la confidentialité, le mot de passe « maître » permettant d'accéder au coffre-fort est défini par l'adhérent et n'est connu que de lui. En conséquence, en cas de perte de ce mot de passe, l'ADAT ne dispose d'aucun moyen technique pour en permettre la récupération ou déverrouiller le coffre-fort.

En cas d'incident de sécurité, il est vivement recommandé de modifier son mot de passe « maitre ».

- ***Boites aux lettres personnalisées à votre domaine Internet***

Selon les options choisies, l'ADAT procède à la création des adresses e-mail rattachées au nom de domaine de l'adhérent, ainsi qu'au transfert des anciennes boîtes mail. Toute modification (création, suppression, redirection) est incluse dans l'abonnement pendant la durée de l'abonnement.

- ***Protection antispam & antivirus des mails liée à la boite aux lettres personnalisée***

Des dispositifs de filtrage permettent de bloquer les e-mails indésirables (spam, phishing, malveillants), afin de protéger la messagerie.

L'ADAT assure le paramétrage et la maintenance de ces outils.

- ***Sauvegarde des données***

L'ADAT met à disposition un espace de stockage sécurisé permettant des sauvegardes automatiques quotidiennes, avec une conservation de l'historique sur 365 jours. L'adhérent détermine les données à sauvegarder et la capacité de stockage adaptée à ses besoins.

Conformément au règlement général de la protection des données (RGPD) les données sont hébergées sur des serveurs en France ou en Europe et sont chiffrées.

Les techniciens de l'ADAT contrôlent le bon déroulement des sauvegardes et informent l'adhérent en cas d'anomalie. Pour toute restauration de données, l'adhérent prend contact avec l'ADAT durant les horaires d'ouverture du support (voir article 3). L'agent de l'ADAT, qui intervient sur les données à la demande de l'adhérent, est soumis à une obligation de confidentialité. Toutes les actions effectuées sur la console sont horodatées dans un journal d'évènement qui peut être transmis à l'adhérent sur simple demande.

- ***Pare-feu matériel installé sur site***

Pour renforcer la sécurité informatique, un pare-feu physique peut s'avérer nécessaire afin de contrôler les flux de données et réduire les risques d'intrusion.

Les techniciens de l'ADAT assurent l'installation et le paramétrage initial du parefeu, ainsi que les ajustements nécessaires en cas d'évolution des services utilisés par l'adhérent pendant la durée de l'abonnement.

3. Assistance et maintenance

- **Assistance informatique**

L'assistance est accessible via le formulaire dédié dans l'onglet « Espace adhérents » du site internet de l'ADAT. Un technicien interviendra par mail, téléphone, via une prise en main à distance (télémaintenance) ou sur site.

Ce service est disponible du lundi au vendredi de 9h à 12h et de 14h à 17h.

- **Maintenance**

La maintenance comprend les opérations nécessaires au bon fonctionnement des services inclus dans le Pack CyberSécurité : mises à jour logicielles, corrections de bugs, et résolution de problèmes techniques. Elle peut être préventive, corrective ou évolutive.

L'ADAT s'engage à intervenir dans des délais raisonnables à la suite d'une demande d'intervention et à maintenir la compatibilité des systèmes avec les mises à jour nécessaires.

Les limites d'intervention

L'ADAT se réserve le droit de refuser l'intervention et/ou de cesser l'exécution de la prestation si les équipements et/ou logiciels fournis ne correspondent plus aux prérequis en vigueur. De même, toute modification apportée à l'initiative de l'adhérent au système d'information sans information préalable de l'ADAT pourra entrainer la suspension immédiate du service et des obligations associées.

- **Prise en main à distance (télémaintenance)**

La prise en main à distance des équipements constitue le mode d'intervention principal. L'adhérent accepte ce mode d'intervention pour chaque service proposé.

L'ADAT s'engage à en informer l'adhérent au préalable et à obtenir son consentement explicite. Les connexions sont sécurisées par chiffrement.

- **Intervention sur site**

Lorsqu'une intervention sur site est nécessaire, les agents de l'ADAT s'engagent à respecter les règles internes en vigueur dans les locaux visités.

4. Modalités financières

Chaque demande de prestation fait l'objet d'un devis. La signature de ce devis par l'adhérent vaut acceptation du présent règlement.

Les tarifs des services sont fixés par délibération du Conseil d'administration et peuvent être révisés en fonction de l'évolution des coûts des prestataires sous-traitants.

Les frais de mise en service sont facturés une fois l'installation terminée (service fait). L'abonnement est facturé annuellement à terme à échoir. En cas de souscription ou de résiliation en cours d'année, un prorata temporis sera appliqué à partir de la date d'installation.

6. Exécution des prestations

Les prestations sont réalisées selon un calendrier défini avec l'adhérent. En cas de retard dû à un cas de force majeure ou à des circonstances indépendantes de la volonté de l'ADAT, la responsabilité de cette dernière ne saurait être engagée.
L'adhérent s'engage à fournir toutes les informations et accès nécessaires à la bonne exécution des prestations.

7. Durée et résiliation

L'abonnement aux prestations est conclu pour une durée de 12 mois à partir de la date d'installation. Il est reconduit par tacite reconduction par périodes successives d'un an, sauf dénonciation par lettre recommandée par l'une des parties avec un préavis de 3 mois avant la date d'échéance (date anniversaire de l'installation de la prestation).

L'ADAT se réserve la possibilité de résiliation anticipée pour manquement grave (défaut de paiement, non-coopération ...).

8. Garantie et responsabilité

8.1 Responsabilités de l'adhérent

L'adhérent s'engage à :

- utiliser les services conformément aux recommandations de l'ADAT ;
- informer l'ADAT en amont de tout changement dans son système d'information (changement de fournisseur Internet, de matériel, de serveur, modification du paramétrage, ajout d'équipements ou de nouveaux services, etc.).
- assurer la sécurité de ses accès (identifiants, mots de passe, etc.) ;
- veiller à la mise à jour régulièrement de l'ensemble du système d'information ;
- assister aux démonstrations des logiciels et/ou matériels pour acquérir une autonomie raisonnable dans leur utilisation ;
- signaler sans délai à l'ADAT tout incident ou faille de sécurité, en fournissant le maximum d'informations sur les causes, afin de permettre une intervention rapide et efficace

L'ADAT décline toute responsabilité en cas de dysfonctionnement lié à l'infrastructure Internet, à des équipements non fournis par ses soins, à un usage inapproprié des services, ou à la divulgation par l'adhérent d'informations confidentielles à des tiers.

8.2 Responsabilité de l'ADAT

L'ADAT s'engage à effectuer les prestations en mettant tout en œuvre pour satisfaire l'adhérent. Elle est tenue à une obligation de moyens, non de résultats. En cas de contestation, la charge de la preuve incombe à l'adhérent.

Les prestations du « pack CyberSécurité » consistent en un accompagnement et une expertise technique s'appuyant sur des outils fournis par d'autres prestataires.

Toutefois, la responsabilité de l'ADAT sera exclue en cas d'intrusions extérieures dues à une action ou une inaction du prestataire tiers ou du bénéficiaire du service, d'un usage inadapté des services et plus généralement de toute panne ou incident sur des éléments non fournis par l'ADAT.

9. Sous-traitance et co-traitance

L'ADAT se réserve le droit de sous-traiter et de co-traiter l'exécution des prestations à des tiers de confiance. La liste des sous-traitants figure en annexe 1 du présent règlement. L'ADAT reste responsable de la bonne exécution des services, y compris ceux confiés à des sous-traitants.

10. Confidentialité et protection des données

L'ADAT et les adhérents s'engagent à respecter les normes françaises et européennes en vigueur applicables au traitement de données à caractère personnel et, en particulier, la loi Informatique et Libertés de 1978 dans sa version modifiée et le Règlement (UE) 2016/679 adopté par le Parlement européen et le Conseil en date du 27 avril 2016, qui est applicable depuis le 25 mai 2018 (ci-après, **« le RGPD »**).

Les dispositions relatives au traitement des données personnelles sont précisées dans l'**Annexe 2 « Protection des Données Personnelles ».**

11. Force majeure

La responsabilité de l'ADAT ne pourra pas être mise en œuvre si la non-exécution ou le retard dans l'exécution de l'une des obligations décrites dans le présent règlement découle d'un cas de force majeure, au sens du droit administratif (événement extérieur, imprévisible et irrésistible).

12. Modification du présent règlement

Toute modification du présent règlement est soumise à l'approbation du Conseil d'Administration et notifiée par email aux adhérents concernés.

13. Litiges

Tout litige pouvant survenir dans le cadre de l'application du présent règlement relèvera de la compétence du Tribunal administratif de Besançon. Les parties s'engagent toutefois à rechercher préalablement une solution amiable au litige.

ANNEXE 1

Liste des prestataires référencés pour la prestation « pack CyberSécurité »

en vigueur au 1er juillet 2025

Nom du prestataire	**Lieu hébergement**	**Ville**
Microsoft (boites mail)	France	Paris ou Marseille
Scaleway (sauvegarde)	France	Vitry sur Seine - Saint Ouen - Paris
OVH (sauvegarde)	France	Roubaix - Strasbourg - Gravelines
Kiwi Backup (sauvegarde)	France	Strasbourg
CFI (coffre-fort mot passe)	France	Marseille
ALTOSPAM Oktey (antispam)	France	Bordeaux
Synology (coffre-fort et sauvegarde)	Allemagne	Düsseldorf
TeamViewer (prise en main à distance)	Allemagne	Göppingen

ANNEXE 2

PROTECTION DES DONNEES PERSONNELLES

La présente Annexe Protection des données personnelles a pour objet de définir les conditions dans lesquelles l'ADAT (ci-après, « ***le Sous-Traitant*** ») s'engage à effectuer pour le compte de l'adhérent (ci-après, « ***le Responsable de Traitement*** ») les opérations de traitement de données personnelles, objet du Règlement.

Dans le cadre de leurs relations contractuelles, l'ADAT et les adhérents s'engagent à respecter les normes françaises et européennes en vigueur applicables au traitement de données personnelles et, en particulier, le RGPD.

Article 1. Définitions

Les définitions ci-après, telles que rédigées par le RGPD, s'appliquent au Règlement susvisé :

Données à caractère personnel ou Données ou données personnelles : désigne toute information se rapportant à une personne physique identifiée ou identifiable (ci-après dénommée « personne concernée ») ; est réputée être une « personne physique identifiable » une personne physique qui peut être identifiée, directement ou indirectement.

Responsable de Traitement : désigne la personne physique ou morale, l'autorité publique, le service ou un autre organisme qui, seul ou conjointement avec d'autres, détermine les finalités et les moyens du traitement ; lorsque les finalités et les moyens de ce traitement sont déterminés par le droit de l'Union ou le droit d'un État membre, le Responsable de Traitement peut être désigné ou les critères spécifiques applicables à sa désignation peuvent être prévus par le droit de l'Union ou par le droit d'un État membre.

Sous-Traitant : désigne la personne physique ou morale, l'autorité publique, le service ou un autre organisme qui traite des Données personnelles pour le compte du Responsable de Traitement.

Traitement : désigne toute opération ou tout ensemble d'opérations effectuées ou non à l'aide de procédés automatisés et appliqués à des Données ou des ensembles de Données personnelles.

Article 2. Description du Traitement faisant l'objet de la sous-traitance

2.1 Le Sous-Traitant est autorisé à traiter pour le compte du Responsable de Traitement les données personnelles nécessaires pour fournir le ou les service(s) définis dans le présent Règlement.

2.2 Pour l'exécution du service objet du Règlement, le Responsable de Traitement met à la disposition du Sous-Traitant les références du Délégué à la Protection des Données du Responsable de Traitement :

Agence Départementale d'Appui Aux Territoires
Délégué à la Protection des données
1 rue de Ronde du Fort Griffon
25 000 BESANCON
rgpd@adat-doubs.fr - 03.81.61.84.85

Article 3. Obligations du Sous-Traitant vis-à-vis du Responsable de Traitement

Le Sous-Traitant s'engage à :

3.1 Traiter les données uniquement pour la ou les seule(s) finalité(s) qui fait/font l'objet de la sous-traitance ;

3.2 Traiter les données conformément aux instructions documentées du Responsable de Traitement ou par tout autre document accepté par les Parties.

Si le Sous-Traitant considère qu'une instruction constitue une violation du RGPD ou de toute autre disposition du droit des Etats membres de l'Union Européenne relative à la protection des Données, il s'engage à en informer le Responsable de Traitement.

Dans l'hypothèse où le Sous-Traitant serait tenu de procéder à un Traitement de données personnelles en vertu d'une disposition impérative résultant du droit européen ou du droit de l'Etat membre de l'Union Européenne auquel il est soumis, le Sous-Traitant informera le Responsable de Traitement de cette obligation juridique avant le Traitement des Données, sauf si le droit concerné interdit une telle information pour des motifs importants d'intérêt public.

3.3 En cas de transfert de données personnelles vers un pays tiers, n'appartenant pas à l'Union Européenne, ou vers une organisation internationale, le Sous-Traitant devra, sauf motifs importants d'intérêt public et transfert nécessaire à la constatation, à l'exercice ou à la défense de droits en justice, obtenir l'accord préalable écrit du Responsable de Traitement. Si cet accord est donné, le Sous-Traitant s'engage à coopérer avec le Responsable de Traitement afin d'assurer :

- le **respect des procédures** permettant de se conformer à la réglementation des données personnelles, par exemple dans le cas où une autorisation de la part de l'autorité de contrôle compétente apparaîtrait nécessaire ;
- si besoin, la **conclusion d'un ou plusieurs contrats** permettant d'encadrer les flux transfrontières de données personnelles. Le Sous-Traitant s'engage en particulier, si nécessaire, à signer de tels contrats avec le Responsable de Traitement et/ou à obtenir la conclusion de tels contrats par ses Sous-Traitants Ultérieurs. Pour ce faire, il est convenu entre les Parties que les Clauses Contractuelles Types publiées par la Commission européenne, dans leur version en vigueur, seront utilisées pour encadrer les flux transfrontières de Données. Si cela n'est pas suffisant pour assurer une protection effective des données personnelles, le Sous-Traitant mettra également en œuvre toutes les mesures techniques et organisationnelles appropriées.

3.4 Garantir la confidentialité des données personnelles traitées dans le cadre du présent Règlement.

3.5 Veiller à ce que **les personnes autorisées à traiter les données personnelles** en vertu du présent Règlement:

- s'engagent à respecter la confidentialité ou soient soumises à une obligation légale appropriée de confidentialité ;
- soient sensibilisées à la protection des données personnelles.

3.6 Prendre en compte, s'agissant de ses outils, produits, applications ou services, **les principes de protection des données personnelles dès la conception** et par défaut.

3.7 Faire appel éventuellement à un autre sous-traitant (ci-après, « le Sous-Traitant Ultérieur ») pour mener des activités de Traitement spécifiques. Les Sous-Traitants Ultérieurs autorisés à intervenir dans le cadre du présent Règlement sont listés en Annexe 1.
Toute modification de la liste des Sous-Traitants Ultérieurs figurant en Annexe 1 est soumise à l'approbation préalable du Conseil d'Administration.
Le Sous-Traitant Ultérieur est tenu de respecter les obligations du Règlement, et de ne traiter des données personnelles que pour le compte et selon les instructions du Responsable de Traitement.
Il appartient au Sous-Traitant initial de s'assurer que le Sous-Traitant Ultérieur présente les mêmes garanties suffisantes quant à la mise en œuvre de mesures techniques et organisationnelles

appropriées de manière à ce que le Traitement réponde aux exigences du RGPD.

Si le Sous-Traitant Ultérieur ne remplit pas ses obligations en matière de protection des données personnelles, le Sous-Traitant initial demeure pleinement responsable à l'égard du Responsable de Traitement de l'exécution par le Sous-Traitant Ultérieur de ses obligations, notamment en ce qui concerne la notification des violations de données personnelles.

3.8 Permettre l'exercice des droits des personnes. Dans la mesure du possible, le Sous-Traitant doit aider le Responsable de Traitement à s'acquitter de son obligation de donner suite aux demandes d'exercice des droits des personnes concernées au titre de la règlementation sur la protection des données personnelles, à savoir principalement : droit d'accès, de rectification, d'effacement et d'opposition, droit à la limitation du traitement, droit à la portabilité des données personnelles. Il appartient au Responsable de Traitement de fournir l'information aux personnes concernées par les opérations de Traitement au moment de la collecte des données personnelles.

Lorsque les personnes concernées exercent auprès du Sous-Traitant des demandes d'exercice de leurs droits, le Sous-Traitant doit adresser ces demandes dès réception par courrier électronique à la personne désignée par le Responsable de Traitement. Le Sous-Traitant ne pourra répondre directement à la demande d'une personne concernée que sur instruction du Responsable de Traitement.

3.9 Notifier des violations de données personnelles. Une violation de données personnelles s'entend de toute violation de la sécurité entraînant, de manière accidentelle ou illicite, la destruction, la perte, l'altération, la divulgation non autorisée de données personnelles transmises, conservées ou traitées d'une autre manière, ou l'accès non autorisé à de telles données personnelles.
Lors d'une violation de données personnelles, le Sous-Traitant s'engage à procéder à toutes investigations utiles sur les manquements aux règles de protection afin d'y remédier dès que possible et de diminuer l'impact de tels manquements sur les personnes concernées.

Le Sous-Traitant notifie au Responsable de Traitement toute violation de données personnelles dans les meilleurs délais et, en tout état de cause, dans un délai maximum de quarante-huit (48) heures après en avoir pris connaissance. Cette notification est accompagnée de toute documentation utile afin de permettre au Responsable de Traitement, si nécessaire, de notifier cette violation à l'autorité de contrôle compétente.

La notification doit contenir au moins :

- la description de la nature de la violation de données personnelles y compris, si possible, les catégories et le nombre approximatif de personnes concernées par la violation et les catégories et le nombre approximatif d'enregistrements de données personnelles concernés;
- 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 ;
- la description des conséquences probables de la violation de données personnelles ;
- la description des mesures prises ou que le Responsable de Traitement propose de prendre pour remédier à la violation de données personnelles, y compris, le cas échéant, les mesures pour en atténuer les éventuelles conséquences négatives.

Si, et dans la mesure où il n'est pas possible de fournir toutes ces informations en même temps, les informations peuvent être communiquées de manière échelonnée sans retard indu. En tout état de cause, le Sous-Traitant s'engage à informer le Responsable de Traitement de ses investigations sur les manquements aux règles de protection ayant entraîné la violation de données personnelles, de l'évolution de la nature et des conséquences de la violation, ainsi que des mesures prises ou envisagées pour diminuer l'impact des manquements identifiés, et ce de manière régulière.

Le Sous-Traitant s'engage à collaborer activement avec le Responsable de Traitement pour qu'ils soient en mesure de répondre à leurs obligations réglementaires et contractuelles respectives. Seul le Responsable de Traitement peut notifier la violation des données personnelles à l'autorité de contrôle compétente et communiquer des informations sur cette violation aux personnes concernées ; le Sous-Traitant s'interdit en conséquence, de procéder à une telle notification et à une telle communication.

3.10 Collaborer avec le Responsable de Traitement pour l'aider à respecter ses obligations. Le Sous-Traitant aide le Responsable de Traitement pour la réalisation d'analyses d'impact relatives à la protection des Données que le Responsable de Traitement déciderait d'effectuer.

Le Sous-Traitant aide le Responsable de Traitement dans le cadre de la consultation préalable de l'autorité de contrôle, suite à la réalisation des analyses d'impact.

3.11 Prendre les mesures de sécurité appropriées. Sans préjudice des dispositions du corps du Règlement, le Sous-Traitant met en œuvre toutes les mesures techniques et organisationnelles appropriées pour protéger les données personnelles, en prenant en compte l'état des connaissances, les coûts de mise en œuvre et la nature, portée, contexte et les finalités du Traitement ainsi que les risques, dont le degré de probabilité et de gravité varie, pour les droits et libertés des personnes physiques, afin de garantir un niveau de sécurité adapté au risque.

Le Sous-Traitant s'engage ainsi, notamment, à prendre toutes précautions utiles au regard de la nature des Données et des risques présentés par le Traitement, pour préserver la sécurité des Données des fichiers et notamment empêcher toute déformation, altération, endommagement, destruction de manière fortuite ou illicite, perte, divulgation et/ou tout accès par des tiers non autorisés préalablement.

Les moyens mis en œuvre par le Sous-Traitant destinés à assurer la sécurité et la confidentialité des Données incluent notamment les mesures suivantes telles que :

- les moyens permettant de garantir la confidentialité, l'intégrité, la disponibilité et la résilience constantes des systèmes et des services de Traitement,
- les moyens permettant de rétablir l'accès et la disponibilité des données personnelles dans les délais appropriés/définis en cas d'incident physique ou technique,
- une procédure visant à tester, à analyser et à évaluer régulièrement l'efficacité des mesures techniques et organisationnelles pour assurer la sécurité du Traitement.

Le Sous-Traitant s'engage à maintenir ces moyens tout au long de l'exécution du Règlement et, à défaut, à en informer immédiatement le Responsable de Traitement.

En tout état de cause, le Sous-Traitant s'engage en cas de changement des moyens visant à assurer la sécurité et la confidentialité des données personnelles et des fichiers, à les remplacer par des moyens d'une performance supérieure. Aucune évolution ne pourra conduire à une régression du niveau de sécurité.

3.12 Agir de manière raisonnable à l'issue de la prestation de services relatifs au traitement de ces Données. Le Sous-Traitant s'engage notamment à:

- restituer toutes les données personnelles et les fichiers au Responsable de Traitement dans un format exploitable et dans les conditions spécifiées par le Responsable de Traitement
- ou adresser les données personnelles au sous-traitant désigné par le Responsable de Traitement, et ensuite
- détruire toutes les données personnelles et les fichiers manuels ou informatisés comportant les informations collectées dans un délai de deux (2) mois après la restitution, afin de permettre au Client de disposer du temps nécessaire pour vérifier que les Données restituées sont exploitables et lisibles, sauf disposition impérative contraire résultant du droit européen ou du droit d'un Etat membre de l'Union Européenne applicable aux Traitements objets des présentes.

Le renvoi doit s'accompagner de la destruction de toutes les copies existantes dans les systèmes d'information du Sous-Traitant. Une fois détruites, le Sous-Traitant doit justifier par écrit de leur destruction au plus tard dans le délai d'un (1) mois.

3.13 Communiquer au Responsable de Traitement le nom et les coordonnées de son délégué à la protection des données, conformément à l'article 37 du RGPD.

3.14 Tenir par écrit un registre de toutes les catégories d'activités de Traitement effectuées pour le compte du Responsable de Traitement.

3.15 Mettre à la disposition du Responsable de Traitement la documentation nécessaire pour démontrer le respect de toutes ses obligations au titre du présent Règlement. Dans la mesure nécessaire à la protection des secrets d'affaires ou d'autres informations confidentielles, y compris les données personnelles, le Sous-Traitant peut expurger des textes de la documentation avant diffusion.

Le Responsable de Traitement pourra réclamer auprès du Sous-Traitant des explications complémentaires si les documents fournis ne lui permettent pas de vérifier le respect des obligations du Sous-Traitant. Le Responsable de Traitement formule alors une demande écrite auprès du Sous-Traitant, dans laquelle il justifie et documente sa demande d'explication complémentaire. Le Sous-Traitant s'engage à apporter une réponse dans les meilleurs délais.

3.16 Ne pas insérer dans les fichiers des données étrangères ; **consulter, traiter des Données autres que celles concernées** par les présentes et ce, même si l'accès à ces Données est techniquement possible ; **divulguer**, sous quelque forme que ce soit, tout ou partie des données personnelles exploitées ; **prendre copie ou stocker**, quelles qu'en soient la forme et la finalité, tout ou partie des informations ou données contenues sur les supports ou documents qui lui ont été confiés ou recueillies par lui au cours de l'exécution du Règlement, en dehors des cas couverts par les présentes.

Article 4. Obligation du Responsable de Traitement vis-à-vis du Sous-Traitant

Le Responsable de Traitement s'engage à :

- Fournir au Sous-Traitant les données nécessaires à l'exécution de la prestation
- Documenter par écrit toute instruction concernant le Traitement des Données par le Sous-Traitant
- Veiller, au préalable et pendant toute la durée du Traitement, au respect des obligations prévues par le RGPD à la charge du Sous-Traitant
- Superviser le Traitement

Article 5. Coopération en cas de contrôle

En cas de contrôle d'une autorité compétente, les Parties s'engagent à coopérer entre elles et avec l'autorité de contrôle.

Dans le cas où le contrôle mené ne concernerait que les Traitements mis en œuvre par le Sous-Traitant en tant que Responsable de Traitement, le Sous-Traitant fera son affaire du contrôle et s'interdira de communiquer ou de faire état des données personnelles du Responsable de Traitement, sauf demande d'une autorité compétente ayant des prérogatives de puissance publique.

Dans le cas où le contrôle mené chez le Sous-Traitant concernerait les Traitements mis en œuvre au nom et pour le compte du Responsable de Traitement, le Sous-Traitant s'engage à en informer immédiatement le Responsable de Traitement et à ne prendre aucun engagement pour elle.

En cas de contrôle d'une autorité compétente chez le Responsable de Traitement portant notamment sur les prestations délivrées par le Sous-Traitant, ce dernier s'engage à coopérer avec le Responsable de Traitement et à lui fournir toute information dont il pourrait avoir besoin ou qui s'avèrerait nécessaire.