

ANNEXE 5 : GESTION DES DONNÉES À CARACTÈRE PERSONNEL

TABLE DES MATIÈRES

Table des matières	1
I. Objet	2
II. Description des traitements	2
III. Durée des Clauses.....	2
IV. Obligations générales du Titulaire du marché	3
V. Obligations particulières du Titulaire du marché.....	6
VI. Obligations de l'Acheteur vis-à-vis du Titulaire du marché	7
VII. Pénalités et résiliation.....	7

Dans la suite du document, le Titulaire du marché est le prestataire qui remportera le marché à l'issue de la consultation. L'Acheteur est la SPL ALEC de la Grande Région Grenobloise.

I. OBJET

Les présentes clauses ont pour objet de définir, conformément à l'article 28.3 du RGPD, les conditions dans lesquelles le Titulaire du marché s'engage à effectuer pour le compte de l'Acheteur, les opérations de traitement de données à caractère personnel définies ci-après.

II. DESCRIPTION DES TRAITEMENTS

Le Titulaire du marché est autorisé à traiter pour le compte de l'Acheteur les données à caractère personnel nécessaires à l'exécution du présent contrat, à savoir :

Finalités du traitement	Mise en place d'un Active Directory Peuplement du tenant Microsoft 365 et mise en place des règles de sécurité Migration de la messagerie Zimbra vers Outlook 365 Migration du fonds documentaire vers Sharepoint et Teams Formation et support des contributeurs de la SPL ALEC pour la prise en main de la plateforme O365
Catégories de données à caractères personnel	État civil, identité, données d'identification, images... Vie personnelle (habitudes de vie, situation familiale, etc.) Vie professionnelle (CV, diplômes, formation, fonction, lieu de travail, etc.) Informations d'ordre économique et financier (revenus, situation financière, situation fiscale, etc.) Données de connexion (adresse IP, logs, etc.) Données de localisation (déplacements, données GPS, GSM, etc.) Numéro de Sécurité Sociale (ou NIR) Données révélant l'appartenance syndicale Données relatives à des condamnations pénales ou infractions
Catégories de personnes concernées	Les contributeurs de la SPL ALEC Les commanditaires, les fournisseurs et les partenaires de la SPL ALEC Les bénéficiaires des accompagnements réalisés par la SPL ALEC
Provenance des données	Les données sont transmises par le service Moyens Généraux et Système d'Information pour la configuration des accès. Les données sont présentes dans les outils qui font l'objet de la migration (serveur, messagerie).
Catégorie de destinataire des données	Le titulaire n'est pas autorisé à donner accès à ces données, sauf en cas de co-traitance / sous-traitance prévue lors de la réponse au marché, et exclusivement pour la réalisation des traitements listés ci-dessus.

III. DURÉE DES CLAUSES

Les clauses s'appliquent pour la durée de la prestation impliquant le traitement de données à caractère personnel.

IV. OBLIGATIONS GÉNÉRALES DU TITULAIRE DU MARCHÉ

1. Limitation des Finalités

Conformément au principe de limitation des finalités (art. 5 RGPD), le Titulaire du marché s'engage à traiter les données à caractère personnel uniquement pour la ou les seule(s) finalité(s) indiquées au titre II – Description du traitement.

2. Instructions du responsable de traitement

Le Titulaire du marché s'engage à traiter les données conformément aux instructions documentées de l'Acheteur.

Si le Titulaire du marché considère qu'une instruction constitue une violation du règlement européen sur la protection des données ou de toute autre disposition du droit de l'Union ou du droit des Etats membres relative à la protection des données, il en informe immédiatement l'Acheteur.

3. Confidentialité

Le Titulaire du marché s'engage à garantir la confidentialité des données à caractère personnel traitées dans le cadre du présent contrat.

En particulier, le Titulaire du marché veille à ce que les personnes autorisées à traiter les données à caractère personnel en vertu du présent contrat :

- s'engagent à respecter la confidentialité ou soient soumises à une obligation légale appropriée de confidentialité ;
- figurent sur une liste limitée de personnes autorisées à traiter les données ;
- reçoivent la formation nécessaire en matière de protection des données à caractère personnel.

4. Protection des données dès la conception et par défaut

Le Titulaire du marché s'engage à prendre en compte les principes de protection des données dès la conception et de protection des données par défaut :

- Dès la conception, les outils, produits, applications ou services offerts doivent intégrer de façon effective les principes relatifs à la protection des données.
- Par défaut, les outils, produits, applications ou services doivent garantir un traitement limité aux données nécessaires à la finalité du traitement au regard de la quantité de données collectées, de l'étendue de leur traitement, de la durée de conservation et du nombre de personnes qui y a accès.

Ces principes impliquent en particulier la mise en œuvre de mécanismes permettant :

- de limiter la collecte aux données strictement nécessaires à la finalité du traitement ;
- de purger automatiquement et sélectivement les données d'une base active à l'issue d'une certaine durée ou d'en permettre l'archivage ;
- de gérer des habilitations et droits d'accès informatiques « donnée par donnée » ou sur demande des personnes concernées.

5. Sous-traitance

Le Titulaire du marché peut faire appel à un autre prestataire (ci-après, « le sous-traitant ») pour mener des activités de traitement spécifiques. Dans ce cas, il informe préalablement et par écrit l'Acheteur de tout changement envisagé concernant l'ajout ou le remplacement d'autres prestataires. 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. L'Acheteur dispose d'un délai minimum de 30 jours à compter de la date de réception de cette information pour présenter ses objections. Cette sous-traitance ne peut être effectuée que si l'Acheteur n'a pas émis d'objection pendant le délai convenu.

Le sous-traitant est tenu de respecter les obligations du présent contrat pour le compte et selon les instructions de l'Acheteur. Il appartient au Titulaire du marché de s'assurer que le sous-traitant 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 règlement général sur la protection des données. Si le sous-traitant ne remplit pas ses obligations en matière de protection des données, le Titulaire du marché demeure pleinement responsable devant l'Acheteur de l'exécution par le sous-traitant de ses obligations.

6. Notification des violations de données à caractère personnel

Le Titulaire du marché notifie au l'Acheteur toute violation de données à caractère personnel dans un délai maximum de 72 heures après en avoir pris connaissance et par l'envoi d'un courriel avec accusé de réception et de haute importance, à l'adresse suivante : dpo.rgpd@alec-grenoble.org.

Cette notification est accompagnée de toute documentation utile afin de permettre à l'Acheteur, si nécessaire, de notifier cette violation à l'autorité de contrôle compétente et de porter plainte auprès des autorités compétentes.

7. Aide du Titulaire du marché dans le cadre du respect par l'Acheteur de ses obligations

Le Titulaire du marché aide l'Acheteur pour la réalisation d'analyses d'impact relative à la protection des données.

Le Titulaire du marché aide l'Acheteur pour la réalisation de la consultation préalable de l'autorité de contrôle.

8. Mesures de sécurité relatives aux traitements de données à caractère personnel

Le Titulaire du marché s'engage à mettre en œuvre des mesures de sécurité garantissant un niveau de sécurité adapté aux risques engendrés par les traitements.

Si l'exécution des prestations repose sur des outils numériques, le Titulaire du marché s'engage à respecter l'arrêté du 18 septembre 2018 portant approbation du cahier des clauses simplifiées de cybersécurité (CCSC).

En cas d'incapacité à se conformer à certains articles du CCSC, le Titulaire du marché explique les raisons de cette incapacité pour les articles concernés dans son mémoire technique.

9. Transfert des données

Toute transmission de données à des tiers, y compris au bénéfice d'entités établies hors de l'Union européenne, qui ne serait pas strictement conforme à la réglementation en vigueur est formellement prohibée.

Tous les transferts de données à caractère personnel vers des pays tiers ou des organisations internationales doivent être réalisés en conformité avec les principes du chapitre V du RGPD.

Les transferts de données effectués par le Titulaire du marché doivent être réalisés sur la base des instructions documentées de l'Acheteur.

Si l'Acheteur ne fournit pas d'instructions documentées, il est interdit au Titulaire du marché, dans le cadre de ces clauses :

- De traiter et ou de transférer les données à caractère personnel d'un pays tiers à l'Union européenne ou à une organisation internationale ;
- De faire appel à un sous-traitant basé dans un pays tiers à l'Union européenne ou à une organisation internationale.

Il est en outre recommandé :

- D'utiliser des services de cloud fournissant des garanties quant à la localisation géographique des données ;
- De s'assurer que l'hébergement des données soit soumis à des conditions légales appropriées ;
- De se référer aux recommandations de la CNIL en la matière.

10. Sort des données

Au terme de la prestation de services relatifs au traitement de ces données, le Titulaire du marché s'engage à renvoyer toutes les données à caractère personnel à l'Acheteur ou sur demande de l'Acheteur, à renvoyer les données à caractère personnel à un autre Titulaire de marché désigné par l'Acheteur.

Le renvoi doit s'accompagner de la destruction de toutes les copies existantes dans les systèmes d'information du Titulaire du marché. Une fois détruites, le Titulaire du marché doit justifier par écrit de la destruction au délégué à la protection des données.

11. Registre des catégories d'activités de traitement

Le Titulaire du marché déclare tenir par écrit un registre de toutes les catégories d'activités de traitement effectuées pour le compte du l'Acheteur comprenant :

- le nom et les coordonnées de l'Acheteur pour le compte duquel il agit, des éventuels sous-traitants ; et, le cas échéant, du délégué à la protection des données ;
- les catégories de traitements effectués pour le compte de l'Acheteur ;
- le cas échéant, les transferts de données à caractère personnel vers un pays tiers ou à une organisation internationale, y compris l'identification de ce pays tiers ou de cette organisation internationale et, dans le cas des transferts visés à l'article 49, paragraphe 1, deuxième alinéa du règlement européen sur la protection des données, les documents attestant de l'existence de garanties appropriées ;

- dans la mesure du possible, une description générale des mesures de sécurité techniques et organisationnelles, y compris entre autres, selon les besoins :
 - la pseudonymisation et le chiffrement des données à caractère personnel ;
 - des moyens permettant de garantir la confidentialité, l'intégrité, la disponibilité et la résilience constantes des systèmes et des services de traitement ;
 - des moyens permettant de rétablir la disponibilité des données à caractère personnel et l'accès à celles-ci dans des délais appropriés 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.

12. Documentation

Le Titulaire du marché met à la disposition de l'Acheteur la documentation nécessaire pour démontrer le respect de toutes ses obligations et pour permettre la réalisation d'audits, y compris des inspections, par l'Acheteur ou un autre auditeur qu'il a mandaté, et contribuer à ces audits.

V. OBLIGATIONS PARTICULIÈRES DU TITULAIRE DU MARCHÉ

1. Droit d'information des personnes concernées

Le Titulaire du marché, au moment de la collecte des données, doit fournir aux personnes concernées par les opérations de traitement l'information relative aux traitements de données qu'il réalise. La formulation et le format de l'information doivent être convenus avec le Délégué à la protection des données de l'Acheteur avant la collecte de données.

L'information doit être conforme aux articles 13 et 14 du RGPD. Des exemples de mentions d'information sont disponibles sur le site Internet de la CNIL.

Si le marché implique des prestations liées à une application (maintenance, assistance, hébergement de données, sécurité, reprise des données), il appartient à l'Acheteur de fournir l'information aux personnes concernées par les opérations de traitement au moment de la collecte des données.

2. Exercice des droits des personnes

Dans la mesure du possible, le Titulaire du marché doit aider l'Acheteur 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 Titulaire du marché doit répondre, au nom et pour le compte de l'Acheteur et dans les délais prévus par le règlement général sur la protection des données aux demandes des personnes concernées en cas d'exercice de leurs droits, s'agissant des données faisant l'objet de la sous-traitance prévue par le présent contrat.

Si le marché implique des prestations liées à une application (maintenance, assistance, hébergement de données, sécurité, reprise des données), lorsque les personnes concernées exercent auprès du

Titulaire du marché des demandes d'exercice de leurs droits, le Titulaire du marché doit adresser ces demandes dès réception par courrier électronique avec accusé de réception et de haute importance

à dpo.rgpd@alec-grenoble.org. Cette notification est accompagnée de toute documentation utile afin de permettre à l'Acheteur de répondre aux demandes des personnes concernées.

3. Délégué à la protection des données

Le Titulaire du marché indique dans l'acte d'engagement le nom et les coordonnées de son délégué à la protection des données, s'il en a désigné un conformément à l'article 37 du règlement général sur la protection des données. A défaut, il communique les données de son référent en matière de protection des données. L'absence de mention implique la désignation de la personne habilitée à engager l'entreprise en tant que référent pour les besoins du contrat.

VI. OBLIGATIONS DE L'ACHETEUR VIS-À-VIS DU TITULAIRE DU MARCHÉ

L'Acheteur s'engage à :

- fournir au Titulaire du marché les données visées au II des présentes clauses
- documenter par écrit toute instruction concernant le traitement des données par le Titulaire du marché
- veiller, au préalable et pendant toute la durée du traitement, au respect des obligations prévues par le règlement général sur la protection des données de la part du Titulaire du marché
- superviser le traitement, y compris réaliser les audits et les inspections auprès du Titulaire du marché

VII. PÉNALITÉS ET RÉSILIATION

En cas de violation des mesures énoncées dans la présente annexe, le titulaire s'expose à une pénalité égale à 2 % du montant exécuté du marché public à la date de constatation du fait générateur appliquées dans les conditions prévues au CCAG-TIC.

En cas de constatation de plusieurs faits générateurs, les pénalités ainsi établies sont appliquées de façon cumulative.

En cas de manquement grave par le titulaire ou son sous-traitant à ses obligations légales et contractuelles relatives à la protection des données personnelles, le marché peut être résilié pour faute.