

Annexe au CCAP - Sécurité et protection des données

1. Définitions applicables

Marché : on entend par Marché le présent document et ses annexes, notamment le CCTP.

Données Personnelles : désigne les données qui, au sens du RGPD, correspondent à toute information ou ensemble d'informations se rapportant à une personne physique identifiée ou identifiable.

Responsable du traitement : 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.

Sous-traitant : la personne physique ou morale, l'autorité publique, le service ou un autre organisme qui traite des données personnelles au nom et pour le compte du responsable du traitement.

Traitement de données personnelles : désigne toute opération ou tout ensemble d'opérations effectuées ou non à l'aide de procédés automatisés et appliquées à des données ou des ensembles de données personnelles, telles que notamment une collecte, une utilisation, ou encore suppression de données.

Violation de données personnelles : tout événement portant sur une violation de la sécurité organisationnelle ou technique, entraînant, de manière accidentelle ou encore 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.

2. Instructions

Dans le cadre de leurs relations contractuelles, les parties s'engagent à respecter la réglementation en vigueur applicable au traitement de données personnelles nécessaires à la réalisation du Marché.

Le fournisseur Titulaire du Marché est considéré comme sous-traitant de l'UGECAM Alsace pour les traitements de données personnelles nécessaires à l'exécution du présent Marché. Le fournisseur Titulaire demeure responsable de traitement pour l'ensemble des traitements de données personnelles mis en œuvre par lui, et pour lesquels aucune instruction documentée de l'UGECAM Alsace ne lui saurait communiquée.

Pour l'exécution du service, objet du présent contrat, le Titulaire s'engage notamment au respect des obligations suivantes :

- Traiter les données uniquement pour les finalités de la prestation (conformément à la description des fonctionnalités exigées dans le CCTP) qui font l'objet du Marché ;
- Traiter les données conformément aux instructions documentées de l'UGECAM Alsace, à moins qu'il ne soit tenu d'y procéder en vertu du droit de l'Union ou du droit de l'Etat membre auquel il est soumis. Si le Titulaire 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'UGECAM Alsace. En outre, si le Titulaire 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 l'UGECAM Alsace de cette obligation juridique avant le traitement, sauf si le droit concerné interdit une telle information pour des motifs impérieux d'intérêt public ;
- Garantir la confidentialité des données personnelles traitées dans le cadre du présent contrat ;
- Veiller à ce que les personnes autorisées à traiter les données personnelles en vertu du présent contrat :
 - s'engagent à respecter la confidentialité ou soient soumises à une obligation légale appropriée de confidentialité ;
 - reçoivent la formation nécessaire en matière de protection des données personnelles.
- Prendre en compte, s'agissant de ses outils, produits, applications ou services, les principes de Protection des données dès la conception et par défaut de protection des données ;
- Demander l'autorisation préalable à l'UGECAM Alsace pour faire appel à un sous-traitant ultérieur pour mener des activités de traitement spécifiques nécessaires au présent Marché. Dans un tel cas, il doit informer préalablement et par écrit l'UGECAM Alsace de tout changement envisagé concernant l'ajout ou le remplacement d'autres 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. L'UGECAM Alsace dispose d'un délai minimum de 15 jours, à compter de la date de réception de ces informations, pour présenter ses objections.
- S'engage à tenir un registre des traitements pour tout traitement de données personnelles effectué dans le cadre du présent Marché ;
- Fournir assistance et collaboration pour la mise en place, le cas échéant, de tout traitement de données personnelles nécessaire pour l'exécution du présent Marché ainsi que pour l'ensemble des documentations et autres éléments permettant le respect des dispositions relatives à la protection des données, y compris assistance dans la réalisation d'analyses d'impacts relatives à la protection des données et, le cas échéant, la réalisation de la consultation préalable ou tout autre contrôle de l'autorité de contrôle compétente ;
- Collaborer et fournir assistance à l'UGECAM Alsace pour la réalisation d'analyses d'impact relatives à la protection des données ainsi que pour la réalisation, le cas échéant, des consultations préalables de l'autorité de contrôle ;
- Informer sans délai l'UGECAM Alsace en cas de requête provenant d'une autorité administrative ou judiciaire reçue par le Titulaire.

3. Désignation d'un Délégué à la Protection des Données

Le Titulaire s'engage à communiquer à l'UGECAM Alsace le nom et les coordonnées du délégué à la protection des données, s'il en a désigné un conformément à l'article 37 du Règlement Européen.

4. Droits d'informations des personnes concernées

Le Titulaire, au plus tard 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 doit être convenue avec l'UGECAM Alsace avant la collecte de données. Cette information ne sera pas due en cas de connaissance préalable et suffisante en accord avec les règles de protection des données personnelles des personnes concernées des traitements de données personnelles visés par le présent Marché.

5. Exercice des droits des personnes

Le Titulaire doit aider l'UGECAM Alsace 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) ainsi que le droit de disposer de ses données après la mort.

En cas de demande directe exercée auprès du Titulaire par une personne concernée par un traitement de données personnelles ayant pour finalité la réalisation des prestations (conformément à la description des fonctionnalités exigées dans le CCTP) qui font l'objet du contrat, le Titulaire s'engage à recueillir les instructions documentées de l'UGECAM Alsace afin de satisfaire cette demande dans les délais légaux. Dans tous les cas, le Titulaire informe sans délai le responsable du traitement de toute demande qu'il a reçue de la part de la personne concernée. Il ne donne pas lui-même suite à cette demande, à moins que le responsable du traitement des données ne l'y ait expressément autorisé et seulement sur instruction documentée.

6. Données sensibles

Si le traitement porte sur des données personnelles révélant l'origine raciale ou ethnique, les opinions politiques, les convictions religieuses ou philosophiques ou l'appartenance syndicale, ainsi que des données génétiques ou des données biométriques aux fins d'identifier une personne physique de manière unique, des données concernant la santé ou des données concernant la vie sexuelle ou l'orientation sexuelle d'une personne physique, ou des données relatives aux condamnations pénales et aux infractions («données sensibles»), le Titulaire applique des limitations spécifiques et/ou des garanties supplémentaires, qu'il documentera et justifiera auprès de l'UGECAM Alsace.

Le Titulaire se conformera à toute instruction donnée par l'UGECAM Alsace quant au traitement de ce type de données.

7. Notification des violations de données personnelles

Le Titulaire notifie à l'UGECAM Alsace toute violation de données personnelles dans un délai maximum de 48 heures après en avoir pris connaissance.

Cette notification est accompagnée de toute documentation utile afin de permettre à l'UGECAM Alsace, si nécessaire, de notifier cette violation à l'autorité de contrôle compétente.

La documentation utile ci-avant visée contient 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 l'UGECAM Alsace 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. Tout retard dans la fourniture des éléments ci-avant décrits, et pour tout élément supplémentaire demandé par l'UGECAM Alsace, devra être dûment justifié par le Titulaire, dans les conditions édictées par la réglementation relative à la protection des données personnelles.

Seulement après accord écrit de l'UGECAM Alsace, le Titulaire pourra notifier à l'autorité de contrôle compétente, au nom et pour le compte de l'UGECAM Alsace, les violations de données personnelles dans les meilleurs délais et, si possible, 72 heures au plus tard après en avoir pris connaissance, à moins que la violation en question ne soit pas susceptible d'engendrer un risque pour les droits et libertés des personnes physiques.

Seulement après accord écrit de l'UGECAM Alsace, le Titulaire communique, au nom et pour le compte de l'UGECAM Alsace, la violation de données personnelles à la personne concernée dans les meilleurs délais, lorsque cette violation est susceptible d'engendrer un risque élevé pour les droits et libertés de la personne physique concernée.

La communication à la personne concernée décrit, en des termes clairs et simples, la nature de la violation de données personnelles et contient 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 l'UGECAM Alsace 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.

8. Mesures de sécurité

Dans le cadre de ses attributions, et compte tenu du contexte réglementaire et légal applicable, le Titulaire fait partie prenante de la sécurité informatique de l'UGECAM Alsace.

Le Titulaire s'engage à mettre en œuvre les mesures de sécurité techniques et organisationnelles garantissant un niveau de sécurité adapté aux risques, notamment les règles de sécurité élémentaires telles que communiquées par les autorités ou autres agences gouvernementales compétentes, y compris, entre autres :

- La mise en place de mesures contractuelles garantissant la confidentialité et la sécurité des données traitées dans le cadre du présent Marché ;
- La pseudonymisation et le chiffrement des données personnelles ;
- 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 la disponibilité des données personnelles 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,
- Toute mesure de sécurité physique, technique et organisationnelle, notamment : la gestion et la traçabilité des accès physiques des personnes sur les sites du Titulaire ou de l'UGECAM Alsace, la mise en œuvre de moyens et dispositifs de protection physique des biens et des personnes, etc.

Le Titulaire s'engage à mettre en œuvre les mesures de sécurité de l'UGECAM Alsace présentes et à venir, et celles définies par lui-même en interne et à tenir à disposition de l'UGECAM Alsace toute preuve ou documentation appuyant la mise en place de telles mesures. En particulier, le Titulaire s'engage à informer l'UGECAM Alsace de toute anomalie qu'il détectera ayant pour effet une altération, destruction, ou indisponibilité des données qu'il pourra traiter pour son compte ou pour le compte de l'UGECAM Alsace.

En cas de données sensibles, le Titulaire s'engage à respecter toute instruction relative à la sécurité informatique de l'UGECAM Alsace, en particulier les mesures de sécurité techniques et organisationnelles en place pour la protection de ces données.

9. Audits du Titulaire

Dans le cadre des activités de traitements faisant partie du présent Marché, le Titulaire tient à la disposition de l'UGECAM Alsace toute documentation relative à la sécurité des systèmes d'informations ainsi que tout élément permettant de démontrer, appuyer ou contrôler le respect des dispositions en vigueur, en particulier celles relatives à la protection des données personnelles et à la sécurité des systèmes d'informations. Le Titulaire mettra à disposition toute information nécessaire, et apportera toute son assistance, sa collaboration et sa contribution pour la réalisation d'audits, inspections ou demandes de documentations auprès de l'UGECAM Alsace ou tout autre auditeur qu'il aura mandaté.

L'UGECAM Alsace procédera à la communication des modalités de ces audits, inspections ou demandes de documentation auprès du Titulaire, qui s'engage à les respecter. Le cas échéant, l'UGECAM Alsace communiquera les résultats d'audit par la rédaction d'un rapport et présentant les anomalies ou recommandations à faire suivre d'actions correctives et suivies par le Titulaire.

Tout audit, inspection ou demande de documentation pourra se réaliser :

- à distance, notamment sur demande écrite de l'UGECAM Alsace, par mail, courrier ou tout autre moyen de communication qu'elle jugera adéquat ;
- sur site, dans les locaux du Titulaire, tels qu'identifiés par la comparution des parties du présent Marché ;
- sur instruction documentée de l'UGECAM Alsace, par mail, courrier, ou tout autre moyen de communication qu'elle jugera adéquat.

10. Non-respect des clauses et résiliation

Sans préjudice des dispositions du règlement (UE) 2016/679 et/ou du règlement (UE) 2018/1725, en cas de manquement du sous-traitant aux obligations qui lui incombent en vertu du présent Marché, le responsable du traitement peut donner instruction au sous-traitant de suspendre le traitement des données personnelles jusqu'à ce que ce dernier se soit conformé aux présentes clauses ou jusqu'à ce que le contrat soit résilié. Le sous-traitant informe dans les meilleurs délais, qui ne sauraient excéder 72h le responsable du traitement s'il n'est pas en mesure de se conformer aux présentes clauses, pour quelque raison que ce soit.

Le responsable du traitement est en droit de résilier le contrat dans la mesure où il concerne le traitement de données personnelles conformément aux présentes clauses si :

- le traitement de données personnelles par le sous-traitant a été suspendu par le responsable du traitement et le respect des présentes clauses n'est pas rétabli dans un délai raisonnable et, en tout état de cause, dans un délai d'un mois à compter de la suspension ;
- le sous-traitant est en violation grave ou persistante des présentes clauses ou des obligations qui lui incombent en vertu du règlement (UE) 2016/679 et/ou du règlement (UE) 2018/1725, de manière constatée notamment par un audit ou des demandes de documentations non satisfaites en application du présent Marché ;

- le sous-traitant ne se conforme pas à une décision contraignante d'une juridiction compétente ou de l'autorité de contrôle compétente/des autorités de contrôle compétentes concernant les obligations qui lui incombent en vertu des présentes clauses ou du règlement (UE) 2016/679 et/ou du règlement (UE) 2018/1725.

11. Sort des données

Le Titulaire s'engage à ne conserver les données, y compris les données personnelles, au-delà de la durée de conservation, soit fixée par l'UGECAM Alsace, soit par les réglementations en vigueur, et, dans tous les cas, pour une durée qui ne saurait excéder la réalisation des finalités pour lesquelles elles ont été traitées dans le cadre du présent Marché.

Au terme du contrat, le Titulaire perd sa qualité de sous-traitant pour l'ensemble des traitements de données personnelles nécessaires à la réalisation du présent Marché.

À la suite de la résiliation du contrat, le sous-traitant supprime, selon le choix du responsable du traitement, toutes les données personnelles traitées pour le compte du responsable du traitement et certifie auprès de celui-ci qu'il a procédé à cette suppression, ou renvoie toutes les données personnelles, dans un format ouvert et interopérable tels que défini par l'état de l'art, au responsable du traitement et détruit les copies existantes, à moins que le droit de l'Union ou le droit national n'impose de les conserver plus longtemps. A défaut de choix du responsable de traitement, le Titulaire procédera à la suppression de toutes les données personnelles dans les conditions décrites dans le présent Marché. Le sous-traitant continue de veiller à la conformité aux présentes clauses jusqu'à la suppression ou à la restitution des données.

Le Titulaire doit justifier par écrit les destructions de données.