Délégué à la protection des données

FICHE 5 – Insertion de clauses de protection des données personnelles pour la commande publique

Introduction : Depuis le 25 mai 2018, le RGPD impose des **obligations spécifiques** aux **sous-traitants** (organismes qui traitent des données personnelles pour le compte d'un autre organisme), **dans le cadre d'un service ou d'une prestation**. Sont notamment concernés :

- les prestataires de services informatiques (hébergement, maintenance, …),
- les intégrateurs de logiciels,
- les sociétés de sécurité informatique,
- les entreprises de service du numérique et/ou d'ingénierie en informatique qui ont accès aux données,
- les agences de marketing ou de communication qui traitent des données personnelles pour le compte de leurs clients

Quelles obligations pour les sous-traitants?

Les sous-traitants sont tenus de respecter des obligations spécifiques en matière de :
- protection des données dès la conception du service ou du produit et par défaut,
- protection optimale des données par mise en œuvre de mesures techniques et organisationnelles,
- sécurité, confidentialité et documentation de leur activité,
- conseil et aide des clients à la mise en œuvre de certaines obligations du règlement : étude d'impact sur la vie privée, notification de violation de données, contribution aux audits,
- tenue du registre des activités de traitement pour le responsable de traitement,
- désignation d'un délégué à la protection des données (DPO).

Délégué à la protection des données

Quelles clauses obligatoires relatives à la protection des données?

Il est fondamental de respecter les prescriptions de l'article 28 du RGPD lors de la passation d'un contrat afin de définir :

- l'objet, la durée du traitement, la nature et la finalité du traitement, le type de données à caractère personnel et les catégories de personnes concernées, qui constituent les instructions du responsable de traitement,

- les obligations et droits de la collectivité en lien avec le RGPD.

L'objectif est de s'assurer que le sous-traitant auquel la métropole recourt :

- présente des garanties suffisantes concernant la mise en œuvre de mesures techniques et organisationnelles adaptées afin que le traitement réponde aux exigences du RGPD et garantisse la protection des droits des personnes,
- recourt lui-même à un sous-traitant uniquement avec autorisation préalable du responsable de traitement.

Dans quelles pièces des marchés insérer les clauses?

Dans le CCAP : Intégrer l'annexe 1

Conformément à l'article 38 du RGPD, le DPO associé dès la conception du traitement, préconise l'insertion de ces clauses pour les marchés concernés.

NB / La plate-forme Marco web est opérationnelle depuis le 1er avril pour insérer ces clauses dans tous les marchés (supérieurs à 90 000 €).
Pour les marchés sous ce seuil et hors Marcoweb, l'annexe est jointe en tant que de besoin.

Dans le CCTP : Intégrer l'annexe 2

Les critères Informatique et Libertés peuvent permettre de juger de la qualité des offres.
Pénalités et sanctions doivent être prévues en cas de déficience en matière de protection des données personnelles.

Délégué à la protection des données

Contacter les responsables de la protection des données en cas de questionnement sur la protection des données ou la sécurité informatique

- ✓ **Les DPO (Data Protection Officer) : Régine MAGNE ou Fabien MALLERET**
  Téléphone : 06-13-76-47-33 ou 06-49-82-38-78
  Mail : cnil@grandnancy.eu

- ✓ **Les RSSI (Responsable de la Sécurité des Systèmes d'Information) : Jean-Marc KOZIAR ou Djamal BOUDJI**

  Téléphone : 06-24-93-01-31 ou 06-45-11-36-90
  Mail : rssi@grandnancy.eu

- ✓ **La CDO (Chief Data Officer) pour Nancy : Tiphaine NOUGUE**
  Téléphone : 03-54-50-60-79

Annexe 1 - Clauses Informatique et Liberté

(à insérer dans les CCAP des marchés)

1) Objet

Les présentes clauses ont pour objet de définir les conditions dans lesquelles le sous-traitant s'engage à effectuer pour le compte du responsable de traitement les opérations de traitement de données à caractère personnel définies ci-après.

Dans le cadre de leurs relations contractuelles, les parties s'engagent à respecter la réglementation en vigueur applicable au traitement de données à caractère personnel et, en particulier, le règlement (UE) 2016/679 du Parlement européen et du Conseil du 27 avril 2016 applicable depuis le 25 mai 2018 ainsi que la loi n° 2018-493 du 20 juin 2018 relative à la protection des données personnelles.

2) Description du traitement faisant l'objet de la sous-traitance

Le sous-traitant (ST) est autorisé à traiter pour le compte du responsable de traitement (RT) les données à caractère personnel nécessaires pour fournir le ou les service(s) suivant(s) [...] *(décrire l'activité)*.
La nature des opérations réalisées sur les données est […] *(Décrire les opérations de traitement*, exemple : hébergement, maintenance, etc.).
La ou les finalité(s) du traitement sont [...] *(décrire ce pour quoi le traitement est mis en place).*
Les données à caractère personnel traitées sont […] *(décrire la nature des données traitées et leur éventuelle sensibilité).*
Les catégories de personnes concernées sont […] *(décrire les catégories de personnes ayant confié leurs données).*
Pour l'exécution du service objet du présent contrat, le RT met à la disposition du ST les informations nécessaires suivantes […].
Règlement européen sur la protection des données personnelles - Guide du sous-traitant -Edition septembre 2017.

3) Durée du contrat

Le présent contrat entre en vigueur à compter du […] pour une durée de […].

4) Obligation du sous-traitant vis-à-vis du responsable de traitement

Le ST s'engage à :
1. traiter les données uniquement pour la ou les seule(s) finalité(s) qui fait/font l'objet de la sous-traitance,

2. traiter les données conformément aux instructions documentées du RT.

Si le ST 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 le RT. En outre, si le ST est tenu de procéder à un transfert de données vers un pays tiers ou à une organisation internationale, il doit en informer le RT avant le traitement, sauf si le droit concerné interdit une telle information pour des motifs importants d'intérêt public.

3. garantir la confidentialité des données à caractère personnel traitées dans le cadre du présent contrat.

4. veiller 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,
- ✓ reçoivent la formation nécessaire en matière de protection des données à caractère personnel.

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

6. Sous-traitance

Choisir l'une des deux options

Option A (autorisation générale)

Le ST peut faire appel à un autre ST (« le sous-traitant ultérieur ») pour mener des activités de traitement spécifiques. Dans ce cas, il informe préalablement et par écrit le RT de tout changement envisagé concernant l'ajout ou le remplacement d'autres sous-traitants (formulaire DC4). Cette information doit indiquer clairement les activités de traitement sous-traitées, l'identité et les coordonnées du ST et les dates du contrat de sous-traitance. Le RT dispose d'un délai de 21 jours à compter de la date de réception de cette information pour présenter ses objections. Cette sous-traitance ne peut être effectuée que si le RT n'a pas émis d'objection pendant ce délai.

Option B (autorisation spécifique)

Le ST est autorisé à faire appel à l'entité […] (ci-après, le « sous-traitant ultérieur ») pour mener les activités de traitement suivantes : […]

En cas de recrutement d'autres ST ultérieurs, le ST doit recueillir l'autorisation écrite, préalable et spécifique du RT.

Le ST ultérieur est tenu de respecter les obligations du présent contrat pour le compte et selon les instructions du RT. Il appartient au ST initial de s'assurer que le ST 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 règlement européen sur la protection des données. Si le ST ultérieur ne remplit pas ses obligations en matière de protection des données, le ST initial demeure pleinement responsable devant le RT de l'exécution par l'autre ST de ses obligations.

7. Droit d'information des personnes concernées

Choisir l'une des deux options

Option A

Il appartient au RT de fournir l'information aux personnes concernées par les opérations de traitement au moment de la collecte des données.

Option B

Le ST, 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 le RT avant la collecte de données.

8. Exercice des droits des personnes

Dans la mesure du possible, le ST doit aider le RT 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 profilage).

Choisir l'une des deux options

Option A

Lorsque les personnes concernées exercent auprès du ST des demandes d'exercice de leurs droits, le sous-traitant doit adresser ces demandes dès réception par courrier électronique à la mission DPO mutualisée du Grand Nancy à cnil@grandnancy.eu .

Option B

Le ST doit répondre, au nom et pour le compte du RT et dans les délais prévus par le règlement européen sur la protection des données aux demandes des personnes concernées en cas d'exercice de leurs droits.

9. Notification des violations de données à caractère personnel

Option A

Le ST notifie au responsable de traitement toute violation de données à caractère personnel dans un délai maximum de 48 heures après en avoir pris connaissance et par courrier électronique à la mission DPO mutualisée du Grand Nancy à cnil@grandnancy.eu.

Cette notification est accompagnée de toute documentation utile afin de permettre au RT, si nécessaire, de notifier cette violation à l'autorité de contrôle compétente (la CNIL).

Option B

Après accord du RT, le ST notifie à l'autorité de contrôle compétente (la CNIL), au nom et pour le compte du RT, les violations de données à caractère personnel 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.

La notification contient au moins :

- ✓ la description de la nature de la violation de données à caractère personnel 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 à caractère personnel concernés ;
- ✓ le nom et les coordonnées du délégué à la protection des données ou d'un autre point de contact du ST auprès duquel des informations supplémentaires peuvent être obtenues ;
- ✓ la description des conséquences probables de la violation de données à caractère personnel ;
- ✓ la description des mesures prises ou que le ST propose de prendre pour remédier à la violation de données à caractère personnel, 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.

Après contact du RT, le ST peut être amené à communiquer la violation de données à caractère personnel à la personne concernée dans les meilleurs délais, lorsque cette violation est susceptible d'engendrer un risque élevé pour les droits et libertés d'une personne physique.

10. Aide du sous-traitant dans le cadre du respect par le responsable de traitement de ses obligations

Le ST aide le RT pour la réalisation d'analyses d'impact relative à la protection des données.

Le ST aide le RT pour la réalisation de la consultation préalable de l'autorité de contrôle.

11. Mesures de sécurité

Le ST s'engage à mettre en œuvre les mesures de sécurité suivantes adaptées aux risques, y compris, entre autres :

- ✓ 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 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 ;
- ✓ la pseudonymisation et le chiffrement des données à caractère personnel ;
- ✓ un code de conduite, une certification.

(Dans la mesure où l'article 32 du règlement européen sur la protection des données prévoit que la mise en œuvre des mesures de sécurité incombe au responsable du traitement et au sous-traitant, il est recommandé de déterminer précisément les responsabilités de chacune des parties au regard des mesures à mettre en œuvre).

12. Sort des données

Au terme de la prestation de service relative au traitement des données, le ST s'engage à convenir avec le RT du sort de restitution et du format.

Au choix des parties :

- ✓ détruire avec l'autorisation du service d'archive compétent toutes les données à caractère personnel, certificat de destruction à l'appui ;
- ✓ à renvoyer toutes les données à caractère personnel devant être conservées plus longtemps au RT ou au ST désigné par le RT dans un format préalablement validé avant la fin du contrat. Le renvoi doit s'accompagner de la destruction de toutes les copies existantes dans les systèmes d'information du ST, certificat de destruction à l'appui.

13. Délégué à la protection des données

Le ST communique au RT 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 européen sur la protection des données.

14. Registre des catégories d'activités de traitement

Le ST déclare tenir par écrit un registre de toutes les catégories d'activités de traitement effectuées pour le compte du RT comprenant :

- ✓ le nom et les coordonnées du RT pour le compte duquel il agit, des éventuels ST et, le cas échéant, du délégué à la protection des données;
- ✓ les catégories de traitements mis en œuvre pour le compte du RT;
- ✓ 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 les documents attestant de l'existence de garanties appropriées;
- ✓ dans la mesure du possible, une description générale des mesures de sécurité techniques et organisationnelles décrites au 11) mises en œuvre.

15. Documentation

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

5) Obligations du responsable de traitement vis-à-vis du sous-traitant

Le RT s'engage à :

1. fournir au ST les données visées par les présentes clauses,
2. documenter par écrit toute instruction concernant le traitement des données par le ST,
3. veiller, au préalable et pendant toute la durée du traitement, au respect des obligations prévues par le règlement européen sur la protection des données de la part du ST,
4. superviser le traitement, y compris réaliser en tant que de besoin les audits et les inspections auprès du ST.

6) Cas de la résiliation

Le prestataire reconnait que tout manquement à ses obligations de sécurité et de confidentialité est de nature à entraîner la fin imminente de sa relation avec l'acheteur sans indemnité. La responsabilité du prestataire sera également susceptible d'être engagé sur la base des articles 226-13 et 226-17 du code pénal.

Annexe 2 - Clauses Informatique et Liberté

(à insérer dans les CCTP des marchés)

1) Conditions d'exécution des contrats de la commande publique portant sur des prestations de traitement de données à caractère personnels ou faisant intervenir, dans le cadre de leur exécution, un tel traitement.

Les clauses insérées dans le CCTP ont pour objet de définir précisément les conditions dans lesquelles le ST s'engage à effectuer pour le compte du RT les opérations de traitement de données à caractère personnel.

2) Critères de sélection des offres

Dans la partie « critères techniques », une sous-partie cotant pour la protection des données personnelles peut être prévue.

-