Guide de remplissage de l'annexe RGPD de description des traitements effectués par le Titulaire

Le tableau de description des traitements mis en œuvre par le Titulaire est annexé aux pièces de **tout marché public** traitant des données à caractère personnel (DCP).

Le Titulaire, en tant que Sous-traitant en termes RGPD (ST) doit renseigner les rubriques du tableau, selon les traitements de données à caractère personnel **qu'il réalise, est susceptible de réaliser ou confie à une autre société**.

Il peut communiquer tout document ou justification qu'il juge utile, notamment dans le cadre des mesures de sécurité techniques et organisationnelles qu'il met en place.

La collectivité, en tant que Responsable de traitement en termes RGPD (RT), peut également demander tout document ou justification susceptible de démontrer les mesures prises par le ST.

Table des matières

1. Terminologie 2
2. Tableau descriptif des traitements sous-traités 4
3. Liste des sous-traitants ultérieurs 4
4. Transfert de données hors UE 5
5. Mesures de sécurités du sous-traitant 5
6. Coordonnées du délégué à la protection des données 6

1. Terminologie

1.1. Données à caractère personnel (DCP)

Toute information qui permet d'identifier une personne physique directement ou indirectement par recoupement d'informations.

Exemples : nom, prénom, coordonnées postales, téléphoniques ou électroniques, adresse IP, numéro de matricule, photos, vidéos, etc.

1.2. Traitement

Toute opération ou tout ensemble d'opérations, effectuées ou non à l'aide de procédés automatisés et appliquées à des données à caractère personnel. Il est à retenir que **la simple consultation, sans aucune autre intervention, est un traitement de DCP**. À partir du moment où le Titulaire a connaissance de DCP, il réalise un traitement.

Le traitement de données à caractère personnel concerne à la fois les supports papier et les supports numériques.

Exemples: consultation, modification, utilisation, diffusion, extraction, interconnexion, organisation, conservation, suppression, anonymisation de DCP.

1.3. Finalité de traitement

C'est l'objectif principal de l'utilisation des données à caractère personnel. La finalité du traitement permet de répondre à la question "Pourquoi les DCP sont traitées ?"

Exemples : maintenance d'une application, hébergement d'une base de données, réalisation d'enquêtes nominatives, etc.

1.4. Responsable de traitement

C'est une personne physique ou morale, une autorité publique, un service ou un organisme qui détermine les finalités et les moyens de traitement des données à caractère personnel. Autrement dit, le Responsable de traitement définit pourquoi (finalités) et comment (moyens) les données à caractère personnel seront traitées.

Il s'agit selon le cas de la Ville ou de l'Eurométropole de Strasbourg

1.5. Sous-traitant

C'est une personne physique ou morale, une autorité publique, un service ou un organisme qui traite des données à caractère personnel pour le compte du Responsable du traitement et sur instruction(s) documentée(s) de ce dernier.

Il s'agit du Titulaire du marché public, qui traite des DCP pour le compte et sur instruction(s) de la Ville ou de l'Eurométropole de Strasbourg.

1.6. Sous-traitant ultérieur

Le Sous-traitant peut faire appel à un autre sous-traitant (« le Sous-traitant ultérieur ») pour mener des activités de traitement spécifiques. Les clauses conclues entre le Responsable de traitement et le Sous-traitant doivent être imposées contractuellement au Sous-traitant ultérieur. Le Sous-traitant est responsable envers le Responsable de traitement des actions réalisées par le sous-traitant ultérieur et de leur conformité à la règlement applicable en matière de données à caractère personnel.

Il s'agit des sociétés auxquelles le Titulaire fait appel pour mettre en œuvre des traitements objets du marché public.

Exemple : le Titulaire traite des données personnelles dans le cadre de la mise à disposition d'une plateforme à l'Eurométropole et fait appel à une société pour l'hébergement de cette plateforme. En termes RGPD, le Titulaire a la qualité de Sous-traitant et la société d'hébergement la qualité de Sous-traitant ultérieur.

1.7. Personne concernée

C'est la personne physique dont les DCP sont traitées. Il ne s'agit pas de la personne qui traite les DCP.

Exemples : agents, usagers, utilisateurs, administrés, etc.

1.8. Transferts de données hors de l'Union européenne

Toute communication, copie ou déplacement de données personnelles ayant vocation à être traitées dans un pays tiers à l'Union européenne.

Exemples : hébergement de données dans un centre de données en Suisse, recours à un support informatique basé aux États-Unis, etc.

1.9. Pseudonymisation

La pseudonymisation est un traitement de données personnelles réalisé de manière à ce qu'on ne puisse plus attribuer les données relatives à une personne physique sans information supplémentaire telle qu'une table de correspondance.

La pseudonymisation permet ainsi de traiter les données d'individus sans pouvoir identifier ceux-ci de façon directe. En pratique, il est toutefois bien souvent possible de retrouver l'identité de ceux-ci grâce à des données tierces : les données concernées conservent donc un caractère personnel. **L'opération de pseudonymisation est réversible**.

Exemple : remplacer les noms et prénoms de personnes physiques par un numéro de matricule ou un trigramme.

1.10. Anonymisation

L'anonymisation est un traitement qui consiste à utiliser un ensemble de techniques de manière à rendre impossible, en pratique, toute identification de la personne par quelque moyen que ce soit et de manière **irréversible**, contrairement à la pseudonymisation.

Exemple : remplacer les noms et prénoms de personnes physiques par « XXX »

2. Tableau descriptif des traitements sous-traités

Éléments à renseigner	Précisions	*Exemple*
Objet du traitement	Il s'agit de l'objet du marché	*Maintenance d'un logiciel, hébergement de données personnelles, réalisation de prestations intellectuelles nécessitant le traitement de DCP*
Nature des opérations réalisées sur les données	Correspond à toute opération que le Titulaire est susceptible de réaliser sur les DCP	*Consultation, extraction, enregistrement, analyse, modification, transfert, suppression, anonymisation, etc.*
Finalité du traitement	Signifie l'objectif principal de la prestation objet du marché. En d'autres termes, il s'agit de pourquoi les DCP sont traitées par le Titulaire	*Réaliser des enquêtes, gestion du parc de véhicules, création d'une plateforme, transport de personne, etc.*
Durée du traitement	Équivaut à la durée pendant laquelle les opération sur les DCP sont susceptibles d'être réalisées	*Durée du marché public, durée du contrat de maintenance, autre durée spécifique convenue*
Catégories de personnes concernées	Il s'agit des **personnes physiques** dont les DCP sont traitées. Ne doit pas être confondu avec les personnes qui traitent les DCP.	*Agents de la collectivité, prestataires, usagers*
Type de données traitées	Ce sont les données traitées **par le Titulaire** dans le cadre des missions qu'il réalise ou est susceptible de réaliser	*Nom, prénom, numéro de téléphone, adresse postale, courriel, matricule, tout autre numéro d'identification*
Délai de rétention des sauvegardes	Cet élément n'est applicable que pour les hébergement en SaaS	*Nombre de jours, semaines ou mois*

3. Liste des sous-traitants ultérieurs

Éléments à renseigner	Précisions	*Exemple*
Identité de la société et coordonnées du DPO	Nom de l'entreprise, adresse postale et coordonnées du délégué à la protection des données ou de tout autre point de contact	
Objet du traitement	Correspond à la prestation confiée par le Titulaire à son ou ses Sous-traitant(s), dits Sous-traitants ultérieurs en termes RGPD	*Maintenance d'un logiciel, hébergement de données, support informatique téléphonique, etc.*
Nature des opérations réalisées	Il s'agit du ou des types d'opérations effectuées sur les DCP	*Consultation, extraction, enregistrement, analyse, modification, transfert, suppression*
Finalité du traitement	Signifie l'objectif principal de la prestation objet du marché. En d'autres termes, il	*Réaliser des enquêtes, mise à disposition/hébergement d'un logiciel ou de données personnelles*

	s'agit du pourquoi les DCP sont traitées par le sous-traitants ultérieurs	
Durée du traitement	Équivaut à la durée pendant laquelle les opérations sur les DCP sont susceptibles d'être réalisées	*Durée du marché public, durée du contrat entre le titulaire et son prestataire, autre durée spécifique*
Type de données à caractère personnel traitées	Il s'agit des données traitées par le sous-traitant ultérieur dans le cadre des missions qu'il réalise ou est susceptible de réaliser et qui lui ont été confiées par le Titulaire du marché public	*Nom, prénom, numéro de téléphone, adresse postale, courriel, matricule, etc.*
Catégories de personnes concernées	Il s'agit des **personnes physiques** dont les DCP sont traitées. Ne doit pas être confondu avec les personnes qui traitent les DCP.	*Agents de la collectivité, prestataires, usagers*

4. Transfert de données hors UE

Cette partie est à compléter si un transfert de DCP hors UE est réalisé par le Sous-traitant. Dans ce cas, vous veillerez à préciser les **mesures prises conformément à la législation pour que ce transfert soit licite.**

Liste non exhaustive de mesures permettant de justifier la licéité du transfert :

- Décision d'adéquation
- Clauses contractuelles types (CCT)
- Règles d'entreprise contraignantes (BCR)
- Code de conduite
- Mécanisme de certification

5. Mesures de sécurités du Sous-traitant

Veuillez compléter ce paragraphe en décrivant les différentes mesures de sécurité existantes dans le cadre de cette sous-traitance de données. Vous pouvez également joindre votre PSSI (Politique de Sécurité des Systèmes d'Information), votre PAS (Politique Assurance Sécurité) ou tout autre document à cette annexe au marché.

Vous trouverez ci-dessous des éléments de description que vous pouvez indiquer dans cette partie.

5.1. Dans le cas d'un hébergement SaaS

- Mesures de sécurité de l'application elle-même
- Lieu d'hébergement et redondances : enjeux transfert de données hors U.E.
- Type de données traitées : si données de santé, nécessité d'un agrément HDS
- Mesures de sécurité du centre de stockage des données
- Mesures de sécurité du prestataire
- Sensibilisation des utilisateurs / personnels à la protection des données
- Mesures de protection des données : anonymisation ou pseudonymisation (le cas échéant décrire le type de procédé)
- Authentification des utilisateurs (gestion des accès, gestion des mots de passe, authentification forte)

- Gestion des habilitations
- Sécurité des postes de travail
- Sécurité des serveurs et des réseaux
- Sécurité des opérations de maintenance
- Sécurité des échanges de données

5.2. Dans le cas d'un hébergement On Premise (prestation de maintenance du prestataire)

- Mesures de sécurité de l'application en elle-même
- Mesures de sécurité lors de la maintenance
- Accès à distance à la base de données
- Outil sécurisé et conforme au RGPD : chiffrement de bout en bout de la communication (VPN, connexion sécurisée)
- Enregistrement main-courante de l'intervention (traçabilité des accès)
- Transmission copie base de données
- Transmission via outil sécurisé et conforme au RGPD
- Chiffrement du fichier avant envoi
- Anonymisation des données avant envoi
- Mesures de sécurité dans les locaux du prestataire
- Sensibilisation des utilisateurs / personnels à la protection des données
- Mesures de protection des données : anonymisation ou pseudonymisation
- Authentification des utilisateurs (gestion des accès, gestion des mots de passe, authentification forte)
- Gestion des habilitations
- Sécurité des postes de travail
- Sécurité des serveurs et des réseaux
- Sécurité des opérations de maintenance
- Sécurité des échanges de données

6. Coordonnées du Délégué à la Protection des Données (DPD/DPO)

Veuillez compléter ce paragraphe en indiquant les coordonnées de contact de votre Délégué à la Protection des Données (identité, adresse postale et électronique, numéro de téléphone) ou de votre point de contact pour les sujets liés à la protection des données à caractère personnel.