

Annexe RGD

**Règlement général
de protection des
données**

**École normale
supérieure Paris-
Saclay**

Protection des données à caractère personnel et exigences de sécurité informatique

1. Obligations générales.....	3
2. Sécurité des échanges et des supports.....	3
3. Notification d'incident	3
4. Réversibilité et fin de marché	4
5. Référents RGPD et sécurité	4
6. Interdictions.....	4

La présente annexe s'inscrit dans le respect du **Règlement (UE) 2016/679 du Parlement européen et du Conseil du 27 avril 2016** relatif à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données (ci-après « le RGPD »), ainsi que de la **loi n° 78-17 du 6 janvier 1978 modifiée**, dite « Informatique et Libertés ». Elle en détaille les obligations.

Conformément au RGPD et aux fins du présent document :

- les **données à caractère personnel** désignent toute information se rapportant à une personne physique (identifiée ou identifiable) ;
- le **Responsable de traitement (RT)** est la personne morale ou physique qui détermine les finalités et les moyens du traitement de données à caractère personnel ; en l'espèce, **l'acheteur public**
- le **Sous-traitant (SST)** est toute entité traitant des données à caractère personnel pour le compte du responsable de traitement.

Dans le cadre de l'exécution du présent marché, il n'est pas prévu que le titulaire soit chargé de traiter des données à caractère personnel pour le compte de l'acheteur public. Le marché ne confie ni directement ni indirectement de mission de sous-traitance de données à caractère personnel au titulaire.

Cependant, en raison de la nature des prestations et des interactions avec les services de l'acheteur, le titulaire peut être amené à accéder à des informations ou documents contenant incidemment des données à caractère personnel (ex. : coordonnées d'agents, de référents techniques, d'usagers, d'intervenants). À ce titre, l'acheteur impose le respect des règles minimales suivantes, tant en matière de confidentialité que de sécurité des systèmes d'information.

1. Obligations générales

Le titulaire s'engage à respecter la confidentialité de l'ensemble des informations portées à sa connaissance dans le cadre du marché, qu'elles soient ou non formellement identifiées comme sensibles ou confidentielles.

Aucun fichier, document ou extrait contenant des informations relatives à l'acheteur, ses agents ou ses usagers ne peut être copié, transféré ou réutilisé hors des besoins stricts de l'exécution du marché.

Le titulaire s'engage à ne pas effectuer de traitement de données à caractère personnel de l'acheteur. Si le titulaire considère qu'une opération demandée par l'acheteur peut être qualifiée de traitement de données à caractère personnel, il en avise sans délai l'acheteur, afin que celui-ci lui délivre une autorisation écrite préalable et spécifique à titre exceptionnel.

À défaut, si le titulaire traite des données à caractère personnel des personnels ou usagers de l'acheteur sans instruction écrite préalable et documentée de ce dernier, il endosse alors la qualité de responsable de traitement au sens de l'article 4, point 7 du RGPD, en application de l'article 28⁽¹⁰⁾. Il engage de ce fait sa propre responsabilité quant au respect de l'ensemble des obligations légales applicables aux responsables de traitement. Le non-respect desdites obligations peut exposer le titulaire à des sanctions administratives pouvant aller jusqu'à 20 millions d'euros ou, dans le cas d'une entreprise, jusqu'à 4 % du chiffre d'affaires annuel mondial (article 83 du RGPD), sans préjudice de poursuites par l'acheteur.

2. Sécurité des échanges et des supports

Toute communication, même ponctuelle, contenant des données de personnes doit obligatoirement se faire via des canaux sécurisés (espace de dépôt sécurisé, chiffrement, etc.). L'envoi par messagerie électronique non chiffrée est interdit.

Les équipements techniques utilisés par le titulaire (ordinateurs, terminaux, supports amovibles, etc.) doivent être sécurisés : système d'exploitation à jour, antivirus actif, chiffrement des données sensibles, verrouillage automatique après inactivité, etc.

Les accès aux systèmes ou environnements de l'acheteur, lorsqu'ils existent, doivent être strictement individualisés, non partagés, et protégés par des mots de passe forts.

3. Notification d'incident

En cas d'incident de sécurité (accès non autorisé, perte de données, suspicion de compromission, etc.), le titulaire s'engage à :

- informer l'acheteur dans un délai maximal de 24 heures après en avoir pris connaissance ;
- transmettre toute information utile à l'analyse de l'incident et aux mesures correctives.

4. Réversibilité et fin de marché

À l'issue du marché, le titulaire doit :

- restituer à l'acheteur, sur demande, l'ensemble des documents ou fichiers reçus ou produits ;
- supprimer de façon sécurisée toute copie ou trace de ces documents, sauf au titre de ses propres obligations légales de conservation.

Un procès-verbal de restitution ou de destruction peut être exigé.

5. Référents RGPD et sécurité

Afin d'assurer un dialogue efficace en cas de question relative à la protection des données ou à la sécurité informatique, le titulaire doit être en capacité de fournir, sur simple demande de l'acheteur public les éventuels contact de tout DPO ou Référent RGPD et de tout RSSI ou Référent sécurité du titulaire. L'acheteur désigne ses référents comme suit :

- Délégué à la protection des données (DPO) de l'acheteur : dpd@ens-paris-saclay.fr
- Responsable de la sécurité des systèmes d'information (RSSI) de l'acheteur : rssi@ens-paris-saclay.fr

6. Interdictions

Il est interdit au titulaire :

- de rédiger, publier ou diffuser tout document, support, notice, communication ou livrable faisant référence, de manière explicite ou implicite, à la conformité au RGPD de l'acheteur, ou engageant celui-ci à ce titre ;
- de répondre directement à une personne physique (agent, usager, tiers) exerçant un droit prévu par les articles 15 à 22 du RGPD (accès, rectification, opposition, effacement, limitation, portabilité...) ; toute telle demande doit être immédiatement transmise à l'acheteur sans y répondre ;
- de réaliser au nom de l'acheteur une quelconque formalité ou démarche auprès de la CNIL (ou de toute autre autorité de contrôle), notamment :
 - réponse à une mise en demeure ou à un contrôle,
 - notification de violation de données,
 - désignation d'un DPO,
 - demande d'autorisation préalable.

Toute demande ou situation relevant de la protection des données doit être immédiatement signalée à l'acheteur, seul responsable de leur traitement et des obligations qui en découlent.