|  |  |
| --- | --- |
| **ANNEXE 1.** | **LE RGPD - Traitement des données à caractère personnel et à la libre circulation de ces données** |

**Obligations du titulaire vis-à-vis de l’HIAL(article 28.3 du RGPD)**

Le titulaire du marché public s'engage, notamment, à :

1. traiter les données uniquement pour la ou les seule(s) finalité(s) qui fait/font l'objet du présent marché public ;
2. traiter les données conformément aux instructions documentées de HIALl'HIALfigurant au CCTP du présent marché public. Si le titulaire considère qu'une instruction est donnée en violation du règlement général 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'HIAL ;
3. si le titulaire est tenu de procéder à un transfert de données vers un pays tiers (hors de l'Union européenne) 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 HIALl'HIAL de cette obligation juridique avant le traitement, sauf si le droit concerné interdit une telle information ;
4. garantir la confidentialité des données à caractère personnel traitées dans le cadre du présent marché public ;
5. veiller à ce que les personnes autorisées à traiter les données à caractère personnel en vertu du présent marché public :
6. s'engagent à respecter la confidentialité ou soient soumises à une obligation légale appropriée de confidentialité ;
7. reçoivent la formation nécessaire en matière de protection des données à caractère personnel.
8. 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.

**Sous-traitance des activités de traitement (articles 28.2 et 28.4 du RGPD)**

Lorsque le titulaire fait appel à un sous-traitant pour mener des prestations du marché, il informe préalablement et par écrit l'le pouvoir adjudicateur 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 marché public.

Afin d'obtenir l'acceptation et l'agrément ddu pouvoir adjudicateur, le titulaire doit présenter son sous-traitant par le biais de l'acte spécial de sous-traitance} dont les formalités sont comprises dans le formulaire DC4 ou tout autre document équivalent (téléchargeable sur <http://www.economie.gouv.fr/daj/formulaires-declaration-candidat>).

**Droit d'information et exercice des personnes concernées par le traitement (articles 13 à 15 du RGPD)**

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

La formulation et le format de l'information doivent être convenus avec l'HIAL avant la collecte de données.

Le titulaire doit répondre, au nom et pour le compte de l'HIAL 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.

**Notification des violations de données à caractère personnel (article 33 du RGPD)**

Le titulaire notifie à l'HIAL toute violation de données à caractère personnel dans un délai de 72 heures après en avoir pris connaissance et par courriel (cf. annexe 1 du présent CCTP).

Cette notification est accompagnée de toute documentation utile afin de permettre à l'HIAL, si nécessaire, de notifier cette violation à l'autorité de contrôle compétente (en l'occurrence, à la Commission nationale de l'informatique et des libertés, CNIL) si possible 72 heures au plus tard après en avoir pris connaissance. 

Après accord écrit de l'HIAL, le titulaire notifie à l'autorité de contrôle compétente, au nom et pour le compte de l'HIAL, les violations de données à caractère personnel dans un délai maximum de 72 heures 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 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 l'HIAL 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 accord écrit de l'HIAL, le titulaire communique, au nom et pour le compte de l'HIAL, 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.

La communication à la personne concernée décrit, en des termes clairs et simples, la nature de la violation de données à caractère personnel et 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 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 l'HIAL 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.

**Aide du titulaire dans le cadre du respect par l'HIAL de ses obligations**

Le titulaire aide l'HIAL :

* à la réalisation d'analyses d'impact relative à la protection des données ;
* la réalisation de la consultation préalable de l'autorité de contrôle.

**Mesures de sécurité**

Le titulaire met en œuvre notamment les mesures de sécurité suivantes :

* *garantir la confidentialité, l'intégrité, la disponibilité et la résilience constantes des systèmes et des services de traitement ;*
* *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 ;*
* *tester, analyser et évaluer régulièrement l'efficacité des mesures techniques et organisationnelles pour assurer la sécurité du traitement.*

**Sort des données (article 28.3.g du RGPD)**

Dans le cadre d'une éventuelle sous-traitance, celui-ci s'engage à renvoyer toutes les données à caractère personnel au titulaire.

Le renvoi doit s'accompagner de la destruction de toutes les copies existantes dans les systèmes d'information du sous-traitant. Une fois détruites, le sous-traitant doit justifier par écrit de la destruction.

Pour rappel, les données doivent être conservées par le titulaire pour une durée maximum de 30 ans.

**Délégué à la protection des données (articles 37 à 39 du RGPD)**

Le titulaire communique à l'HIALHIAL dès la notification du marché public 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, ou, à défaut, l'identité et les coordonnées d'un point de contact dédié à ces questions.

**Registre des activités de traitement (article 30 du RGPD)**

Le titulaire tient par écrit Un registre de toutes les activités de traitement effectuées pour le compte de l'HIALHIAL comprenant :

1. le nom et les coordonnées de l'HIALHIAL pour le compte duquel il agit, des éventuels sous-traitants et, le cas échéant, du délégué à la protection des données ;

1. les catégories de traitements effectués pour le compte de l'HIALHIAL ;
2. 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 général sur la protection des données, les documents attestant de l'existence de garanties appropriées ;
3. dans la mesure du possible, une description générale des mesures de sécurité techniques et organisationnelles, notamment, 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.*



**Documentation (article 28.3.h du RGPD)**

Le titulaire met à la disposition de l'HIALHIAL la documentation nécessaire pour démontrer le respect de toutes ses obligations et pour permettre, le cas échéant, la réalisation d'audits, y compris des inspections, par l'HIALHIAL ou un auditeur mandaté par lui, et contribuer à ces audits.

**Obligations de l'HIALHIAL vis-à-vis du titulaire**

L'HIALHIAL s'engage à :

* documenter par écrit toute instruction concernant le traitement des données par le titulaire ;
* veiller, au préalable et pendant toute la durée du traitement, au respect des obligations prévues par le RGPD et par la loi Informatique et Libertés de la part du titulaire ;
* superviser le traitement, y compris réaliser les audits et les inspections auprès du titulaire.