GHT Drôme Ardèche Vercors

ANNEXE 4 – SECURISATION DES SYSTEMES DE DONNEES

TRAVAUX HDJ SV - CHDV

I. REGLEMENT GENERAL POUR LA PROTECTION DES DONNEES PERSONNELLES

1. Conformité au RGPD

Le prestataire s'engage à être en conformité avec les exigences du RGPD.

A ce titre il est informé que le respect de la réglementation en matière de protection des données à caractère personnel est un élément fondamental pour le pouvoir adjudicateur.

Le prestataire s'engage à fournir les coordonnées de son Délégué à la Protection des Données au pouvoir adjudicateur:

Nom Prénom	Adresse mail	Téléphone

2. Clause de protection des données personnelles

Dans le cadre des missions de son marché le prestataire est amené à traiter des données à caractère personnel pour le compte du pouvoir adjudicateur. A ce titre le prestataire s'engage à :

- Traiter les données à caractère personnel confiées par le pouvoir adjudicateur dans le respect de la réglementation, du marché et des éventuelles instructions et dispositions prévues ;
- Présenter toutes les garanties suffisantes quant à la mise en œuvre des mesures techniques et organisationnelles appropriées de manière à ce que le traitement réponde aux exigences du RGPD et garantisse la protection des droits de la personne concernée ;
- Disposer d'une politique informatique conforme au RGPD.

3. Clause de protection des données personnelles

- « Données à caractère personnel » : désigne toute information se rapportant à une personne physique identifiée ou identifiable, directement ou indirectement, notamment par référence à un identifiant, tel qu'un nom, un numéro d'identification, des données de localisation, un identifiant en ligne, ou à plusieurs éléments spécifiques propres à son identité physique, physiologique, génétique, psychique, économique, culturelle ou sociale ;
- « Traitement de données à caractère personnel » : désigne toute opération ou ensemble d'opérations portant sur des données à caractère personnel, quel que soit le procédé utilisé tel que la collecte, l'enregistrement, l'organisation, la conservation, l'adaptation, ou la modification, l'extraction, la consultation, l'utilisation, etc…
- « Violation de données à caractère personnel » : désigne une violation de la sécurité entraînant, de manière accidentelle ou illicite, la destruction, la perte, l'altération, la divulgation non autorisée de données à caractère personnel transmises, conservées ou traitées, ou l'accès non autorisé à de telles données.

4. Sous-traitance ultérieure

Le prestataire est autorisé à faire appel à des sous-traitants dans le cadre des traitements de données à caractère personnel réalisés pour le compte du pouvoir adjudicateur.

Le prestataire devra se conformer à l'article « SOUS TRAITANCE » du présent marché, et en préalable, soumettre systématiquement ceux-ci à acceptation et agrément.

Sur première demande, le prestataire devra :

- Fournir la liste des sous-traitants au pouvoir adjudicateur ;
- S'assurer que les sous-traitants présentent des garanties suffisantes quant à la mise en œuvre des mesures techniques et organisationnelles appropriées de manière à ce que les traitements répondent aux exigences du RGPD.

Le prestataire demeure pleinement responsable vis-à-vis du pouvoir adjudicateur et des tiers des actes de son sous-traitant.

5. Droits et obligations du responsable de traitement

Le pouvoir adjudicateur, en tant que responsable du traitement, dispose du droit de :

- Demander au prestataire, en première intention, la communication de tout élément, pièce ou documentation permettant de garantir qu'il respecte les exigences du RGPD.
- Demander toutes précisions, formuler des objections et des réserves concernant les sous-traitants envisagés par le prestataire.
- Réaliser des audits ou des inspections auprès du prestataire afin de s'assurer du respect par ce dernier des exigences du RGPD.
- Demander l'assistance du prestataire sur la mise en œuvre d'une analyse d'impact, sur la mise en œuvre de l'exercice des droits des personnes concernées, sur la coopération avec la CNIL, sur la mise en œuvre des moyens de sécurité du traitement ou encore la mise en œuvre des notifications de violation de données auprès de la CNIL ou des personnes concernées.

Le responsable de traitement s'engage à :

- Fournir les instructions nécessaires à la bonne exécution du traitement ;
- Indiquer au prestataire les évolutions de traitement ;
- Fournir au prestataire les coordonnées de son Délégué à la Protection des Données

Etablissement	Coordonnées
Centre Hospitalier de Valence	dpo@ch-valence.fr
Hôpitaux Drôme Nord	
Centre Hospitalier Drôme Vivarais	
Centre hospitalier Intercommunal Vercors Isère	
Centre Hospitalier de Crest	
Centre Hospitalier de Die	
Centre Hospitalier de Tournon sur Rhône	
Centre Hospitalier du Cheylard	
Centre Hospitalier de Lamastre	
Groupement hospitalier Portes de Provence	
Centre hospitalier d'Ardèche Méridionale	
Centre hospitalier Privas Ardèche	
Centre hospitalier de Villeneuve de Berg	
Centre hospitalier des Cévennes Ardéchoises	
Centre hospitalier de Bourg-Saint-Andéol-Viviers	
Centre hospitalier de Rocher Largentière	
Centre hospitalier Nyons	
Centre hospitalier de Buis-les-Baronnies	

- Notifier les violations de données auprès de l'autorité compétente ;
- Respecter ses obligations en matière de protection des données.

6. Flux transfrontaliers

Aucun transfert de données à caractère personnel ne peut intervenir en dehors de l'Union Européenne sans l'accord préalable, exprès et spécial du responsable de traitement.

En cas d'accord, le prestataire s'engage à respecter l'ensemble des obligations en matière de transfert de données à caractère personnel vers un pays tiers et notamment à conclure un acte juridique contraignant avec le destinataire des données et d'en justifier auprès du responsable de traitement.

7. Confidentialité

Le prestataire s'engage à faire signer par toutes les personnes susceptibles d'accéder aux données à caractère personnel du responsable du traitement un engagement individuel de confidentialité.

Le prestataire doit être en mesure de confirmer le respect de cette obligation auprès du responsable du traitement, à première demande, en communiquant la liste des personnes susceptibles d'accéder aux données à caractère personnel, accompagnée des engagements de confidentialités signés par lesdites personnes.

Le prestataire s'engage à former les personnes susceptibles d'accéder aux données à caractère personnel du responsable de traitement sur les mesures de sécurité à mettre en œuvre. Le plan de formation annuel pourra être remis au responsable de traitement à première demande.

Le prestataire s'engage à ce que d'éventuels sous-traitants soient également tenus par ces obligations.

8. Obligation de sécurité

Le prestataire est tenu de mettre en œuvre les mesures organisationnelles et techniques de nature à lutter contre la destruction, la perte, l'altération, la divulgation non autorisée de données à caractère personnel transmises, conservées ou traitées d'une autre manière, ou de l'accès non autorisé à de telles données, de manière accidentelle ou illicite.

9. Violation de données

Il appartient au responsable de traitement et à lui seul de notifier les éventuelles violations de données à caractère personnel à la CNIL.

Le prestataire s'engage à notifier au responsable de traitement, sans délai, après en avoir pris connaissance, toute violation de données à caractère personnel qu'il aurait subi.

La violation de données est communiquée au responsable de traitement ou au Délégué à la protection des données du pouvoir adjudicateur à l'adresse correspondante

Etablissement	Coordonnées
Centre Hospitalier de Valence	dpo@ch-valence.fr
Hôpitaux Drôme Nord	
Centre Hospitalier Drôme Vivarais	
Centre hospitalier Intercommunal Vercors Isère	
Centre Hospitalier de Crest	
Centre Hospitalier de Die	
Centre Hospitalier de Tournon sur Rhône	
Centre Hospitalier du Cheylard	
Centre Hospitalier de Lamastre	
Groupement hospitalier Portes de Provence	
Centre hospitalier d'Ardèche Méridionale	
Centre hospitalier Privas Ardèche	
Centre hospitalier de Villeneuve de Berg	
Centre hospitalier des Cévennes Ardéchoises	
Centre hospitalier de Bourg-Saint-Andéol-Viviers	
Centre hospitalier de Rocher Largentière	
Centre hospitalier Nyons	
Centre hospitalier de Buis-les-Baronnies	

La notification doit préciser :

- La nature de la violation de données, y compris, si possible, les catégories et le nombre approximatif de personnes concernées, le type de données concerné ;
- Le nom et les coordonnées du délégué à la protection des données du prestataire, ou d'un point de contact auprès duquel des informations supplémentaires peuvent être obtenues ;
- Les conséquences probables de la violation de données ;
- Les mesures déjà prises ou celles qui sont proposées.

En cas de violation le prestataire prend, sans délai, toutes les mesures nécessaires pour remédier et diminuer l'impact de la violation et en informe le responsable de traitement.

Le prestataire s'engage à collaborer activement et de bonne foi avec le responsable de traitement pour qu'il soit en mesure de répondre à ses obligations réglementaires et contractuelles et notamment pour répondre aux interrogations de la CNIL.

10. Aide et assistance du responsable du traitement

Le prestataire s'engage à aider et assister le responsable de traitement concernant :

- Les droits des personnes concernées.
- La sécurité du traitement de données.
- La détection, la notification des violations de données.

- La réalisation d'analyse d'impact.

11. Contrôle de la CNIL

Le responsable du traitement et le prestataire sont tenus de coopérer avec la CNIL, à la demande de celle-ci.

Dans le cas où le contrôle est mené auprès du prestataire, les traitements mis en œuvre au nom et pour le compte du responsable de traitement, le prestataire s'engage à informer immédiatement le responsable de traitement et à ne prendre aucun engagement pour lui.

En cas de contrôle de la CNIL auprès du responsable de traitement portant sur les prestations délivrées par le prestataire, ce dernier s'engage à coopérer avec le responsable de traitement et à lui fournir toute information dont la CNIL pourrait avoir besoin sans délai.

Dans le cas où le prestataire fait l'objet d'une mise en demeure, d'un avertissement ou d'une condamnation de la CNIL, même dispensée de publication, ce dernier est tenu d'en informer le responsable de traitement sans délai. Il est précisé que le prestataire en assumera seul les conséquences.

12. Registre des traitements

Le prestataire assure la tenue du « registre des opérations de traitements ». Il est tenu de justifier de l'existence de son registre à première demande du responsable de traitement.

13. Responsabilité

Aux termes de l'article 82 du RGPD, le prestataire est tenu responsable du dommage causé par le traitement dès lors :

- Qu'il n'a pas respecté les obligations prévues par le RGPD, ou ;
- Qu'il a agi en dehors des instructions licites du responsable de traitement, ou ;
- Qu'il a agi contrairement aux instructions licites du responsable du traitement.

14. Contraintes informatiques pour la cybersécurité

Le titulaire du marché est tenu de respecter l'arrêté du 18 septembre 2018 **portant approbation du cahier des clauses simplifiées de cybersécurité consultable via le lien suivant :**

https://www.legifrance.gouv.fr/eli/arrete/2018/9/18/ECOP1825228A/jo/texte

Au titre de l'arrêté susmentionné le titulaire du présent marché devra notamment :

- Respecter les prescriptions des politiques de sécurité des systèmes d'information (PSSI) du pouvoir adjudicateur.
- Présenter en cours de marché à la demande du pouvoir adjudicateur tous labels et certificats afin de démontrer de manière économique la réalité de leurs efforts pour sécuriser les composants impliqués dans le marché.
- Fournir à première demande la documentation nécessaire à la sécurisation de leurs fournitures dans les systèmes d'information, la protection des données du pouvoir adjudicateur et aux démonstrations du respect de leurs obligations par les bénéficiaires du marché. Et, si l'emploi sécurisé du produit ou du service nécessite des actions particulières de la part des bénéficiaires du marché, elles doivent être clairement identifiées dans un chapitre « Sécurité » du mémoire technique
- Mettre à jour les composants logiciels afin de maintenir le niveau de sécurité et, d'autre part, d'information des événements et changements impactant la sécurité.
- Fournir à première demande fournir la preuve de la conformité à aux standards et référentiels pour les services et objets numériques que le titulaire inclut dans son offre de fournitures afin de permettre au pouvoir adjudicateur d'être rassuré sur le niveau de cybersécurité dont il bénéficie.

Lu et approuvé,

A , le

Signature et cachet du titulaire