# Annexe au CCTP

## Clauses VNF liées à la sécurité dans le cadre de missions de prestations informatiques avec accès au SI VNF

*Sommaire :*


**1 Objet ..... 2**

**2 Sécurité du SI ..... 2**

2.1 Exigences communes ..... 2

*2.1.1 Confidentialité ..... 2*
*2.1.2 Gestion de l'organisation ..... 3*
*2.1.3 Disponibilité et continuité d'activité ..... 3*
*2.1.4 Gestion des incidents ..... 3*
*2.1.5 Conformité ..... 4*
*2.1.6 Certifications ..... 5*
*2.1.7 Contrôle et audit ..... 5*
*2.1.8 Fin de contrat et réversibilité ..... 5*

2.2 Prestation nécessitant un accès au SI de VNF ..... 5

*2.2.1 Respect des règles d'utilisation du SI ..... 5*
*2.2.2 Utilisation du matériel VNF ..... 5*
*2.2.3 Utilisation de matériel externe ..... 6*

2.3 Prestation nécessitant un accès aux locaux de VNF ..... 6

*2.3.1 Gestion des biens VNF ..... 6*
*2.3.2 Hygiène et sécurité ..... 6*

2.4 Prestation de type acquisition ou développement de logiciel ..... 6

*2.4.1 Respect des bonnes pratiques de développement ..... 6*
*2.4.2 Tests ..... 8*
*2.4.3 Maintenance ..... 8*

**3 Protection des données ..... 9**

3.1 Objet ..... 9
3.2 Obligations du titulaire vis-à-vis du Responsable de traitement ..... 9
3.3 Sous-traitance ultérieure ..... 10
3.4 Violation, incident ..... 10
3.5 Sort des données ..... 10
3.6 Délégué à la protection des données ..... 11
3.7 Documentation ..... 11
3.8 Responsabilité ..... 11

# 1 Objet

Ce document présente les clauses liées à la sécurité qui s'appliquent à l'ensemble des projets liés au Système d'Information de VNF.

Le cas échéant, le CCTP indique les règles de sécurité spécifiques applicables à un marché public.

Afin de respecter les clauses définies ci-dessous, le candidat indiquera dans son offre les renseignements suivants :

- Responsable Sécurité du candidat (ou référent sécurité) pour ce marché : nom et fonction interne ;
- Interlocuteur privilégié du candidat pour VNF (ou Directeur de projet) : nom et fonction interne ;
- Délégué du candidat à la protection des données, s'il en a désigné un conformément à l'article 37 du règlement européen sur la protection des données : nom et fonction interne ;
- Logiciel d'antivirus utilisé chez le candidat (nom et version), pour ses postes de travail et ses serveurs informatiques ;
- Localisation des données traitées pour VNF (interne aux locaux du prestataire, en mode SaaS en France, pays de l'UE ou hors UE)

La remise d'une offre dans le cadre d'un marché de VNF pour lequel les présentes « Clauses VNF liées à la sécurité » sont annexées au CCTP impose tacitement l'acceptation complète des clauses définies dans ce document.

Le titulaire devra en outre se mettre en conformité avec l'ensemble des exigences de sécurité de VNF au travers d'un plan d'assurance sécurité (PAS) au démarrage du marché.

# 2 Sécurité du SI

## 2.1 Exigences communes

### 2.1.1 Confidentialité

Clause de confidentialité

Le prestataire s'engage à ne pas communiquer sur toute information non publique envoyée par VNF ou élaborée pour VNF, y compris en phase précontractuelle.

Sont concernés tous les documents ou informations (techniques, informatiques, commerciales, financières, économiques, sociales etc.) ainsi que les fichiers, annuaires et messages.

Cette obligation reste valable pour toute la durée du contrat signé et pendant 5 ans après sa cessation, quelle qu'en soit la cause.

Cette obligation concerne aussi bien le prestataire, son personnel et les sous-traitants éventuels. VNF peut exiger des engagements nominatifs en fonction de la criticité des informations accessibles. Dans ce cas, les engagements de confidentialité comporteront :

- La signature des deux parties (VNF et le prestataire, représentée par un mandataire social ou une personne officiellement déléguée).
- La signature des différents intervenants indiquant que ces derniers ont bien compris les termes de l'engagement et acceptent les conséquences en cas de divulgation intentionnelle ou de manquement à une procédure de sécurité.

L'intégralité des documents remis doit être restituée à la fin du contrat.

L'utilisation de toute information autrement que pour l'exécution du contrat et la diffusion de tout document à des personnes n'ayant pas de lien avec la prestation sont interdites.

Confidentialité des échanges

Les échanges d'informations concernant la mission, entre VNF et le prestataire, se font selon une méthode définie et formalisée.

Le prestataire s'engage à suivre les procédures suivantes :

- Toute donnée sensible (déclarée confidentielle ou secrète) échangée doit être chiffrée quelque que soit le réseau utilisé.
- Cette méthode est basée sur l'utilisation de la cryptographie assurant la confidentialité et l'intégrité des messages électroniques échangés conformément à la politique de sécurité de VNF.

### 2.1.2 Gestion de l'organisation

Référent sécurité

Le titulaire du marché identifiera un responsable de la sécurité du système d'information, ou à défaut un référent sécurité, pour les prestations réalisées pour VNF afin de garantir la mise en œuvre des mesures de sécurité.

Suivi de la prestation

Un comité sera établi afin d'assurer le suivi de la prestation. Il sera composé de différents représentants au sein de VNF et du prestataire. Les aspects sécurité seront abordés régulièrement au cours de ces comités, le prestataire devra démontrer notamment que les mesures de sécurité sont bien appliquées, en produisant par exemple des tableaux de bord.

Gestion des sous-traitants

Le prestataire informe VNF s'il fait appel à des sous-traitants pour la réalisation de tout ou partie de sa mission. Par ailleurs, l'ensemble des règles applicables au prestataire le sont également pour ses sous-traitants. Le prestataire est responsable des activités et des agissements de ses sous-traitants.

Information et sensibilisation des intervenants

Le prestataire s'assure que l'ensemble de ses personnels et sous-traitants ont été sensibilisés aux risques liés à la sécurité du système d'information de VNF. Il s'engage à prendre toutes les mesures nécessaires au respect des obligations mentionnées dans le présent document par l'ensemble des intervenants.

Changement de poste ou départ d'un intervenant

Le prestataire prévient VNF, dès qu'il en a connaissance, de tout changement de poste d'un de ses salariés, prestataires ou intérimaires en relation avec VNF.

### 2.1.3 Disponibilité et continuité d'activité

Le prestataire garantit la disponibilité des ressources matérielles et humaines nécessaires à la réalisation des missions pour VNF. Dans le contrat, les parties s'entendent sur :

- Le respect des charges prévues ;
- Le taux d'indisponibilité du service, réseau, application, etc. ;
- Les pénalités associées ;
- La garantie de temps de rétablissement (services) ;
- La garantie de la mise à disposition dans un délai à définir, de personnel de remplacement en cas d'indisponibilité des salariés du prestataire.

Le prestataire présentera les mesures mises en œuvre afin de garantir la continuité des activités, en cas d'incident majeur, pour les services qu'il fournit à VNF (ex : redondance matérielle, solutions dégradées, etc.).

### 2.1.4 Gestion des incidents

Déclaration des incidents de sécurité

En cas d'incident de sécurité subi par le titulaire du marché ou par un de ses sous-traitants, et susceptible d'impacter VNF, le titulaire s'engage à informer, dans les plus brefs délais, ledit incident au Responsable de la Sécurité du Système d'Information et à son interlocuteur privilégié VNF.

Le prestataire participe au maintien du niveau de sécurité de VNF et déclare tout incident qu'il pourrait constater, sans tenter d'en faire la démonstration.

Assurances

Le titulaire du marché doit être assuré contre les risques inhérents à ses activités qui pourraient causer des préjudices financiers ou opérationnels à VNF.

### 2.1.5 Conformité

Respect des lois et réglementations

D'une manière générale, le prestataire s'engage à respecter les lois et réglementations sectorielles inhérentes aux activités de VNF, notamment :

- La loi Informatique et Libertés (loi n°78-17 du 6 janvier 1978 modifiée). En particulier, il assure la sécurité des données à caractère personnel qui pourraient lui être confiées par VNF en les protégeant contre toute destruction accidentelle ou illicite, perte accidentelle, altération, diffusion ou accès non autorisés. De plus, le prestataire ne peut sous-traiter tout ou partie des prestations sans accord préalable écrit de VNF.
- Le secret des communications (Article 9 du code civil et loi n° 91-646 du 10 juillet 1991 relative au secret des correspondances émises par la voie des télécommunications).
- La protection de la propriété intellectuelle et la protection des logiciels (Article L111-1 et L113-9 du code de la propriété intellectuelle)
- La fraude informatique et cybercriminalité (Loi n°88-19 du 5 janvier 1988 relative à la fraude informatique).
- La cryptologie (Décret n°98-101 du 24 février 1998 définissant les conditions dans lesquelles sont souscrites les déclarations et accordées les autorisations concernant les moyens et prestations de cryptologie).
- La signature électronique (Loi n°2000-230 du 13 mars 2000 portant sur l'adaptation du droit de la preuve aux technologies de l'information et relative à la signature électronique)
- La loi de sécurité quotidienne du 15 Novembre 2001 portant sur la lutte contre le terrorisme et notamment sur la conservation des données de connexion.

Respect des normes et des standards

Selon le contexte de la prestation, VNF peut exiger de son prestataire d'appliquer les exigences ou mesures de sécurité définies par :

- Le RGS (Référentiel Général de Sécurité) qui fixe les règles que doivent respecter les fonctions des systèmes d'information contribuant à la sécurité des informations échangées par voie électronique entre les administrations ou avec des tiers (usagers, collectivités, autres organismes…).
- Le RGI (Référentiel Général d'Interopérabilité) qui a pour objectif de guider les autorités administratives dans l'adoption de normes, standards et bonnes pratiques, afin de favoriser l'interopérabilité de leurs systèmes d'information.
- Le RGAA (Référentiel Général d'Accessibilité pour les Administrations) qui a pour objectif de favoriser l'accessibilité des contenus diffusés sous forme numérique à travers les canaux Web, Téléphonie, Télévisuel.
- Le standard PCI-DSS (Payment Card Industry Data Security Standard) pour la protection des données de cartes bancaires.
- La norme ISO 27002 concernant les bonnes pratiques de sécurité.

Application des plans gouvernementaux

Dans le cadre d'application de plans gouvernementaux, le premier ministre peut décider la mise en œuvre de mesures spécifiques destinées à lutter contre les attaques visant les systèmes d'information et de communication des opérateurs d'intérêts vitaux.

Dans le cadre de ses prestations, le titulaire du marché pourrait être concerné par ces alertes décidées au niveau gouvernemental, et s'engage à appliquer les consignes de sécurité données par VNF. Ces

mesures sont susceptibles d'évoluer et les modifications seront régulièrement transmises durant l'exécution du marché.

Exigence de traçabilité

Le prestataire assure la traçabilité des actions qu'il réalise dans le cadre de sa mission pour VNF. VNF se réserve le droit de demander, à tout moment, les traces conservées par le prestataire concernant sa mission.

### 2.1.6 Certifications

Le prestataire précisera les éventuelles certifications dont il dispose sur le périmètre concerné par les services proposés (ex : Certification ISO 27001). Le prestataire s'engage à maintenir pendant toute la durée du contrat les critères permettant de répondre aux exigences des certifications obtenues.

En cas de perte de certification, le prestataire s'engage à en informer VNF dans les plus brefs délais.

### 2.1.7 Contrôle et audit

VNF se réserve le droit de diligenter des audits afin de vérifier que les consignes d'usage et les règles de sécurité sont bien appliquées sur les ressources du système d'information concernées par la prestation. L'audit pourra être réalisé par des auditeurs internes ou par un cabinet d'audit externe.

Sauf cas d'urgence où ce délai pourra être réduit à la discrétion de VNF, l'audit pourra être réalisé après que le prestataire en ait été avisé avec un préavis de 15 jours. Cela permet au prestataire de s'organiser, réunir la documentation demandée, s'assurer de la disponibilité des personnes concernées.

Si les résultats de l'audit font ressortir des carences du prestataire en matière de sécurité des systèmes d'information, le prestataire s'engage à y remédier sans délai et à supporter le coût de l'audit.

### 2.1.8 Fin de contrat et réversibilité

En cas d'expiration ou de résiliation de tout ou partie des services ou du contrat pour quelque motif que ce soit, le prestataire s'engage à :

- Eviter toute interruption et baisse de qualité des services
- Assurer les opérations qui permettront à VNF d'avoir toute la maitrise nécessaire afin de reprendre ou faire reprendre les services par un tiers (transfert de compétences, documents explicatifs, etc.)
- A restituer ou, selon les souhaits de VNF, à détruire de manière sécurisée tous les biens matériels et immatériels de VNF qui lui ont été confiés au cours de la période couverte par le contrat entre le prestataire et VNF.

## 2.2 Prestation nécessitant un accès au SI de VNF

### 2.2.1 Respect des règles d'utilisation du SI

Le prestataire s'engage à respecter les règles d'usage du Système d'Information.

Le prestataire n'utilise ses habilitations, au sein de VNF, que dans le cadre de la mission.

Le prestataire protège les identifiants de connexion que lui fournit VNF. Tout incident les concernant doit immédiatement être porté à l'attention du RSSI.

En cas d'abus, le prestataire est responsable des méfaits commis avec ces identifiants, s'il n'a pas préalablement déclaré l'incident.

### 2.2.2 Utilisation du matériel VNF

Le prestataire s'interdit d'utiliser le matériel fourni à d'autres fins que celles prévues dans le cadre de ses prestations. Il s'engage notamment à utiliser le matériel de VNF en l'état, sans y apporter aucun changement de quelque nature que ce soit.

### 2.2.3 Utilisation de matériel externe

En cas d'utilisation par le prestataire de son propre matériel, le prestataire devra veiller à ce que le matériel utilisé dispose des mesures de sécurité nécessaires à la protection du Système d'Information de VNF : utilisation d'un antivirus à jour, application des derniers patchs de sécurité critiques, désactivation des services non utilisés, utilisation de codes d'accès robustes, verrouillage de la session en cas d'absence, etc.

## 2.3 Prestation nécessitant un accès aux locaux de VNF

### 2.3.1 Gestion des biens VNF

Le prestataire s'engage à prendre soin des biens qui lui sont confiés et à les restituer en fin de contrat. Le prestataire s'interdit d'utiliser les biens à d'autres fins que celles prévues aux termes de ses prestations et ce exclusivement dans le cadre de projets convenus d'un commun accord par écrit avec VNF.

### 2.3.2 Hygiène et sécurité

En cas d'intervention sur site, le prestataire est tenu de respecter les procédures d'accès aux locaux et d'appliquer toutes les mesures permettant d'assurer tant l'hygiène et la sécurité de ses salariés, que la sécurité publique ainsi que la protection des biens et de l'environnement.

D'une manière générale, le personnel du prestataire devra respecter le règlement intérieur de VNF, et ses évolutions durant la période de ses prestations.

Le prestataire s'engage à observer scrupuleusement les règles d'intervention des entreprises extérieures sur le site VNF et, d'une manière générale, à s'imposer toutes les prescriptions applicables au sein de sa propre entreprise.

Ainsi, le prestataire veillera à ce que l'ensemble de ses intervenants porte des badges afin d'être identifiés comme des prestataires extérieurs.

## 2.4 Prestation de type acquisition ou développement de logiciel

### 2.4.1 Respect des bonnes pratiques de développement

Lors de l'acquisition et du développement d'applications, le prestataire est tenu d'assurer la sécurité des développements conformément à l'état de l'art dans chacune des technologies mises en oeuvre.

Pour la mise en oeuvre de technologies web, les développements pourront notamment s'appuyer sur les recommandations de l'OWASP (Open Web Application Security Project).

Le prestataire s'engage sur le respect d'un plan qualité projet qu'il décrira en précisant notamment les mesures de sécurité prises en compte lors des étapes suivantes :

- Conception
- Développement
- Test
- Documentation
- Maintenance

#### *2.4.1.a.1 Gestion des droits et des accès*

L'application devra disposer d'un système d'authentification et de gestion des habilitations en cohérence avec le niveau de sensibilité des données et des fonctionnalités.

L'application devra proposer des fonctionnalités permettant de mettre en oeuvre une gestion des droits dans le respect de la politique de mots de passe de l'établissement :

- Interface éventuelle avec un annuaire externe
- Mise à disposition d'un paramétrage de la politique de mot de passe :
  - Complexité du mot de passe (nombre de caractère minimum, comprenant des minuscules, majuscules, chiffres et caractères spéciaux)
  - Durée d'expiration du mot de passe,
  - Nombre de tentatives d'accès infructueuses avant verrouillage du compte.
- Mise à disposition d'une fonctionnalité de changement de mot de passe pour l'utilisateur.
- Paramétrage des droits des utilisateurs au travers de profils ou rôles en respectant le principe du moindre privilège
- Gestion de profils utilisateurs et de profils administrateurs (fonctionnels et techniques)
- Possibilité de vérifier facilement les droits attribués aux utilisateurs

Le prestataire documentera le processus de gestion des habilitations relatif au projet.

#### *2.4.1.a.2 Protection des données d'application*

En fonction du niveau de confidentialité des données exprimé par VNF, le prestataire précisera les mesures de sécurité mises en place afin de garantir la sécurité des données lors de leur stockage (ex: chiffrement en base) et des échanges (ex : chiffrement des flux).

En fonction du niveau d'intégrité des données exprimé par VNF, le prestataire précisera les mesures de sécurité mises en place afin de garantir la fiabilité des données (contrôles lors de la saisie, contrôles lors des échanges, etc.)

#### *2.4.1.a.3 Disponibilité et continuité*

En fonction du niveau de disponibilité attendue par l'application, le prestataire présentera les mesures mises en place afin de garantir la continuité des activités en cas d'incident ou d'opération de maintenance : procédure de sauvegarde, procédure de bascule, mise en place d'une procédure dégradée, etc.

#### *2.4.1.a.4 Traçabilité*

L'application doit permettre de générer les traces relatives aux :

- Accès à l'application (réussite ou échec)
- Actions réalisées au sein de l'application (consultation, modification)
- Opérations d'administration (suppression de comptes, modification de droits, etc.) et de maintenance

Chaque trace comportera à minima les informations suivantes : Identifiant utilisateur, date/heure, action réalisée.

Une documentation précisera les opérations de maintenance relatives aux traces générées (stockage, sauvegarde, etc.).

#### *2.4.1.a.5 Respect des règles constructeur*

Le prestataire respecte les recommandations des constructeurs en ce qui concerne le développement et la maintenance du Système d'Information. La version de la solution proposée par le prestataire devra intégrer les derniers correctifs de sécurité (systèmes, applicatifs, etc.). Le prestataire documentera les procédures de mise à jour.

#### *2.4.1.a.6 **Protection du code source***

Le prestataire cède à VNF, la totalité des codes sources des développements, et informe VNF des sources qui seraient soumis à licence ou droits d'exploitation.

Le prestataire s'engage à commenter et documenter son code conformément aux bonnes pratiques de sécurité et de développement.

### 2.4.2 Tests

#### *2.4.2.a.1 **Phase de test et de recette***

Le prestataire présentera le processus de test qu'il s'engage à mettre en oeuvre avant toute livraison d'une version ou d'un correctif. Le prestataire s'engage à respecter la méthodologie de recette de VNF. Lors de la conduite des tests de validation ou de déploiement sur le SI VNF, le prestataire s'engage à:

Ne pas provoquer des perturbations sur le SI de production ;

Remettre en l'état initial les systèmes testés et réinitialiser le matériel sensible (effacement sécurisé des disques ayant recueilli des données sensibles, etc.).

Les jeux de test utilisés devront être anonymisés. Ils ne devront contenir aucune information dont le niveau de confidentialité n'est autre que public.

#### *2.4.2.a.2 **Contrôle du code et audit***

VNF se réserve le droit de faire auditer par tout moyen qu'il aurait à sa disposition, ou par l'intermédiaire d'un tiers, tout ou partie du code fournit par le prestataire ainsi que les infrastructures de développement. Les mesures correctives issues des préconisations de l'audit devront être systématiquement mises en place.

Avant toute mise en production d'une application contenant des données sensibles, un audit pourra être réalisé. Les mesures correctives issues des préconisations de l'audit devront être systématiquement mises en place.

### 2.4.3 Maintenance

#### *2.4.3.a.1 **Intervention de maintenance***

Les interventions de maintenance en environnement de production (application de routine de correction, accès direct aux bases de données) ne doivent se faire qu'avec l'autorisation de la maitrise d'ouvrage.

#### *2.4.3.a.2 **Gestion des évolutions***

Les évolutions fonctionnelles ou techniques ne doivent pas remettre en cause le respect des exigences de sécurité ou compromettre une éventuelle opération de réversibilité.

# 3 Protection des données

## 3.1 Objet

Dans le cadre de son contrat établi avec VNF, le prestataire pourra être amené à accéder et à traiter des données à caractère personnel au titre du développement, de la maintenance ou de la récupération des données.

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 à compter du 25 mai 2018 (ci-après, « le règlement européen sur la protection des données – RGPD- ») et la Loi n° 78-17 du 6 janvier 1978 modifiée, relative à l'informatique, aux fichiers et aux libertés (ci-après, la « Loi informatique et libertés »).

A ce titre, VNF est qualifié de Responsable de traitement.

## 3.2 Obligations du titulaire vis-à-vis du Responsable de traitement

Pendant toute la durée du marché, le titulaire est autorisé à accéder et à traiter de la donnée à caractère personnel pour exécuter et réaliser les prestations définies dans le CCTP.

A ce titre, le titulaire s'engage à :

1. Accéder et traiter les données uniquement pour les seules besoins et finalités, tels que décrits dans le CCTP.
2. Traiter les données conformément aux instructions documentées du Responsable de traitement. Si le titulaire considère qu'une instruction constitue une violation du RGPD 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 Responsable de traitement. En outre, si le titulaire est tenu de procéder à un transfert de données vers un pays tiers 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 VNF de cette obligation juridique avant le traitement, sauf si le droit concerné interdit une telle information pour des motifs importants d'intérêt public.
3. Prendre des mesures organisationnelles permettant de garantir la protection et la confidentialité des données traitées en soumettant ses employés à une obligation légale appropriée de confidentialité et veiller à ce qu'ils reçoivent la formation nécessaire en matière de protection des données à caractère personnel.
4. Prendre en compte, s'agissant de ses outils, produits, applications ou services, les principes de protection des données dès la conception des solutions, et de mettre en place les moyens permettant de garantir la confidentialité, l'intégrité, la disponibilité et la résilience constante des systèmes et des services. Le titulaire fournira en outre 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. Il mettra en place une procédure visant à tester, à analyser et à évaluer régulièrement l'efficacité des mesures techniques et organisationnelles pour assurer cette sécurité.
5. Collaborer avec le Responsable de traitement pour aider celui-ci à démontrer qu'il respecte ses obligations légales et réglementaires relatives à la protection des données à caractère personnelles et notamment le RGPD et la loi Informatique et Libertés. Le titulaire aide le responsable de traitement pour la réalisation de la consultation préalable de l'autorité de contrôle.
6. Assister, le Responsable du traitement, dans la mesure du possible, à s'acquitter de son obligation de donner suite aux demandes des personnes concernées (accès, rectification, effacement, opposition etc).

## 3.3 Sous-traitance ultérieure

Le titulaire s'engage à demander l'autorisation écrite de VNF pour le recours à un Sous-traitant, dont il communiquera les noms et coordonnées à VNF et dont il précisera les activités sous-traitées. Cette saisine peut s'effectuer par messagerie avec accusé réception au responsable de marché VNF. Toute sous-traitance doit être obligatoirement et explicitement validée par VNF.

Le Sous-traitant validé est tenu de respecter les obligations définies dans le présent document ainsi que les exigences du RGPD sur la protection des données et le droit national applicable en la matière.

Le titulaire du marché demeure pleinement responsable vis-à-vis du Responsable du traitement de l'exécution de ses obligations par le Sous-traitant validé par VNF.

## 3.4 Violation, incident

Le titulaire du marché s'engage à alerter VNF en cas de suspicion, ou de violation de la sécurité des données personnelles notamment en cas de détournement, de vol ou de divulgation de données dans un délai maximum de 4 heures après en avoir pris connaissance en contactant le Responsable de traitement par le biais du responsable VNF de ce marché, ainsi qu'à lui fournir tout élément d'environnement, de contexte et de volume.

Cette notification est accompagnée de toute documentation utile afin de permettre au Responsable de traitement, si nécessaire, de notifier cette violation à l'autorité de contrôle compétente.

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 ;
- 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 le responsable du traitement 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 du responsable de traitement, le titulaire communique, au nom et pour le compte du responsable de traitement, 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. Cette communication décrit la nature de la violation de données à caractère personnel, 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 ainsi que la description des mesures prises ou à 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.

## 3.5 Sort des données

Au terme de la prestation réalisée dans le cadre du présent marché, et en commun accord avec VNF, le titulaire s'engage à :

- Soit détruire toutes les données à caractère personnel
- Soit à renvoyer toutes les données à caractère personnel au responsable de traitement
- Soit à renvoyer les données à caractère personnel à un prestataire tiers désigné par le responsable de traitement

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

## 3.6 Délégué à la protection des données

Le titulaire communique au responsable de traitement 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

## 3.7 Documentation

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

## 3.8 Responsabilité

Le titulaire sera tenu responsable en cas de manquement exclusivement imputable à lui et/ou à ses sous-traitants à leurs obligations en vertu du présent Contrat, du RGPD et de la Loi Informatique et Libertés.