



MARCHÉ PUBLIC TECHNIQUES DE L'INFORMATION ET DE LA COMMUNICATION

**Hébergement et administration des serveurs dédiés aux sites
« cnil.fr » et prestations associées**

Consultation n°25_CNIL_01

**CAHIER DES CLAUSES TECHNIQUES PARTICULIERES
(CCTP)**

Le marché est lancé dans le cadre d'une procédure adaptée en application de l'article R.2123-1 1° du Code de la commande Publique.

SOMMAIRE

ARTICLE 1 -	GLOSSAIRE TECHNIQUE ET ABRÉVIATIONS	4
ARTICLE 2 -	PRÉSENTATION ET MISSION DE LA CNIL	7
ARTICLE 3 -	CONTEXTES, ENJEUX ET OBJECTIFS DU MARCHÉ	8
ARTICLE 4 -	OBJET DU MARCHÉ	9
ARTICLE 5 -	PRÉSENTATION DE L'ENVIRONNEMENT TECHNIQUE ET APPLICATIF	10
	5.1 PRESENTATION GENERALE DES ENVIRONNEMENTS	10
	5.2 SPECIFICATIONS DES MACHINES VIRTUELLES	11
	5.3 ENVIRONNEMENT DES PARES-FEUX « FW », PROXY INVERSE « RP » ET REDIRECTIONS	11
	5.4 LA PLATEFORME DE PRODUCTION	12
	5.5 LA PLATEFORME DE PREPRODUCTION	13
	5.6 SOCLE DES LOGICIEL TIERS (HORS SYSTEME D'EXPLOITATION DEBIAN).....	14
	5.7 NOMS DE DOMAINES, SERVEURS DE NOMS DE DOMAINES « DNS » ET CERTIFICATS « TLS RGS »	14
ARTICLE 6 -	VOLUMÉTRIE	15
ARTICLE 7 -	PRESTATIONS ATTENDUES	16
	7.1 POSTE 1 - INITIALISATION	17
	<i>UO1 Lancement du projet</i>	<i>17</i>
	7.2 POSTE 2 - MISE EN PLACE	18
	<i>UO2 Mise en place de la plateforme de gestion technique.....</i>	<i>18</i>
	<i>UO3 Mise en place des environnements de production et de préproduction</i>	<i>19</i>
	<i>UO4 Reprise de l'existant</i>	<i>20</i>
	7.3 POSTE 3 - EXPLOITATION	21
	<i>UO5 Suivi opérationnel (infogérance) des environnements</i>	<i>21</i>
	<i>UO6 Mise à jour des environnements de production et de préproduction</i>	<i>22</i>
	<i>UO7 Installer un serveur physique.....</i>	<i>23</i>
	<i>UO8 Suivi opérationnel (infogérance) d'un serveur physique et des « VM » associées</i>	<i>24</i>
	<i>UO9 Installer une machine virtuelle « VM » additionnelle.....</i>	<i>25</i>
	<i>UO10 Suivi opérationnel (infogérance) d'une machine virtuelle « VM » additionnelle</i>	<i>26</i>
	<i>UO11 Installer un logiciel tiers</i>	<i>27</i>
	<i>UO12 Montée de version majeure d'un logiciel tiers</i>	<i>28</i>
	<i>UO13 Etude d'architecture.....</i>	<i>30</i>
	7.4 POSTE 4 - REVERSIBILITE.....	31
	<i>UO14 Réversibilité</i>	<i>32</i>
ARTICLE 8 -	EXIGENCES TECHNIQUES.....	33
	8.1 CENTRE DE DONNEES (DATACENTER) ET SERVEURS PHYSIQUES.....	33
	8.2 BANDE PASSANTE	33
	8.3 ÉCO RESPONSABILITE DU CENTRE D'HEBERGEMENT	34
	8.4 DISPONIBILITE	35
	8.5 CARTOGRAPHIE DES SYSTEMES D'INFORMATION	37
	8.6 DEVOIR DE CONSEIL	37
	8.7 PLAN DE REPRISE D'ACTIVITE.....	37
	8.8 JOURNALISATION.....	37
	8.9 SAUVEGARDES	38
	8.10 GESTION DES FLUX ET FILTRAGES PAR ADRESSES IP	38
	8.11 MAINTIEN EN CONDITION DE SECURITE	38
	8.12 MISE A JOUR DES PLATEFORMES	39
	8.13 LICENCES LOGICIELLES	40
ARTICLE 9 -	EXIGENCES DE SECURITE	41
	9.1 GESTION DES BIENS.....	41
	9.2 SECURITE PHYSIQUE	42
	9.3 SECURITE DES RESEAUX ET EXPLOITATION	43
	9.4 SECURITE DU POSTE DE TRAVAIL	47
	9.5 TRAITEMENT DES INCIDENTS	47

9.6 ENVIRONNEMENT DE TRAVAIL SECURISE ET TRAÇABILITE DES ACTIONS	48
9.7 SECURITE DES SERVEURS	48
9.8 PROTECTION CONTRE LES DENIS DE SERVICE DISTRIBUES	48
9.9 SURVEILLANCE DES INCIDENTS ET DES VULNERABILITES	49
9.10 SUPERVISION ET ADMINISTRATION DES PLATEFORMES.....	49
9.11 AUDIT DE SECURITE.....	49
9.12 OBLIGATIONS RELATIVES AUX ASTREINTES	50
9.13 OBLIGATIONS SPECIFIQUES LIEES A LA PRESTATION D'HEBERGEMENT.....	51
9.14 CERTIFICATION DU TITULAIRE	51
ARTICLE 10 - ORGANISATION, PILOTAGE ET SUIVI DES PRESTATIONS	52
10.1 ORGANISATION DE L'EQUIPE PROJET « EPROJ » DE LA CNIL.....	52
10.2 ORGANISATION DE L'EQUIPE PROJET DU TITULAIRE	52
10.3 PILOTAGE ET SUIVI DES PRESTATIONS.....	52
ARTICLE 11 - CONFORMITE RGAA	53

ARTICLE 1 - GLOSSAIRE TECHNIQUE ET ABRÉVIATIONS

Terme (en Français)	Abréviation	Définition
Comité de pilotage	COPIL	Réunion de pilotage : réunion de suivi en présence de l'équipe projet « EPROJ » et du titulaire, pendant toute la durée du marché.
Composant technique	CT	Terme utilisé dans le cadre des installations ou des mises à jour : matériel physique, logiciel dans le cadre des hyperviseurs de type 1 (actuellement ProxMox), système d'exploitation installés sur les machines virtuelles « VM », applications (CMS, LMS), logiciel tiers (Apache, nginx, MediaWiki, etc.)
Déni de service	DDoS	Distributed Denial of Service : attaque par déni de service en vue de surcharger les serveurs (HTTP/DNS) ou d'inonder les infrastructures reliant le réseau avec un trafic inutile (pipeline UDD, SYN, NTP, etc.) par des requêtes. Ces attaques volumétriques ou applicatives peuvent être distribuées ou non.
Domaine de premier niveau	TLD	Top Level Domain : un domaine Internet de premier niveau est le suffixe du nom de domaine, c'est-à-dire la partie venant après le dernier point (exemple « .fr »).
Equipe projet	EPROJ	L'équipe projet, est composée de chefs de projets au sein de la DSI de la CNIL, d'agents au sein des services métiers, travaillant sur l'hébergement des sites, incluant la hiérarchie ainsi que le RSSI de la CNIL.
Garantie du temps d'intervention	GTI	Temps imparti pour la prise en compte d'un incident ou d'un dysfonctionnement des sites hébergés.
Garantie du temps de rétablissement	GTR	Temps imparti pour la résolution d'un incident ou d'un dysfonctionnement des sites hébergés.
Gestion de contenu	CMS	Content Management System : logiciel applicatif permettant de gérer du contenu informatif (ex. Wordpress, Drupal, etc.)
Interface de programmation d'application	API RESTful	Interface que deux systèmes informatiques utilisent pour échanger des informations en toute sécurité sur le réseau Internet en utilisant le protocole http ou HTTPS.
Intelligence Artificielle Générative	GenAI	Generative Artificial Intelligence : type de système d'intelligence artificielle permettant de générer du contenu (textes, images, vidéos, etc.) en réponses à des invites, prompts en Anglais. Exemples : Claude, ChatGPT, DeepSeek, Grok, Le Chat, Perplexity, etc.

Terme (en Français)	Abréviation	Définition
Hyperviseur type 1	HV1	Logiciel s'exécutant directement sur un serveur physique et permettant d'héberger des machines virtuelles « VM ». Il utilise les instructions de virtualisation matérielle des processeurs le supportant (AMD-V et Intel VT).
Pare-feu	FW	Firewall : permet de définir des règles de filtrage réseau, pour contrôler le flux de données entre différentes zones de confiance.
Pare-feu applicatif	WAF	Web Application Firewall : aide à protéger les applications en surveillant et en filtrant le trafic réseau HTTP entre une application et le réseau Internet.
Plan d'Assurance Qualité	PAQ	Document permettant de définir l'organisation, les méthodes, et les activités permettant d'obtenir la qualité des livrables avec les différents acteurs du projet.
Plan d'Assurance Sécurité	PAS	Document permettant de présenter les mesures de sécurité techniques et organisationnelles que le titulaire met en œuvre pour assurer la sécurité des sites institutionnels « cnil.fr ».
Plateforme d'apprentissage	LMS	Learning Management System : logiciel applicatif permettant de gérer un parcours pédagogique avec pour objectif de proposer de l'auto-évaluation.
Proxy inverse	RP	Reverse Proxy : permet aux usagers d'accéder aux serveurs frontaux du réseau interne pour permettre l'exposition des pages des sites institutionnels.
Référentiel général de sécurité (certificats)	RGS	Ce type de certificat est utilisé pour assurer la sécurité des échanges entre les sites de l'institution et les usagers.
Règlement général sur la protection des données personnelles	RGPD	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.
Sécurité de la couche transport	TLS	Protocole de sécurisation des échanges entre les clients et les serveurs.
Serveur de stockage en réseau	NAS	Network Attached Storage : serveur de stockage de fichiers en volume centralisé.
Support à long terme	LTS	Long Term Support : les éditeurs logiciels proposent une version spécifique dont le support, et les corrections des failles de sécurité, sont assurés pour une période de temps plus longue que la normale. Cette version permet d'aborder plus sereinement la migration vers la dernière version.

Terme (en Français)	Abréviation	Définition
Système de nom de domaine	DNS	Service distribué permettant d'associer les noms de domaines internet, exemple de « www.cnil.fr » avec leurs adresses IP ou d'autres types d'enregistrements (MX, TEXT, etc.)
Vérification d'aptitude	VA	Permet de constater l'aptitude des prestations, livrées ou exécutées, conforme aux caractéristiques techniques.
Vérification de service régulier	VSR	Permet de constater que les prestations fournies sont capables d'assurer un service régulier dans les conditions normales d'exploitation prévues dans ce document.

ARTICLE 2 - PRÉSENTATION ET MISSION DE LA CNIL

PRESENTATION DE LA CNIL

Créée par la loi Informatique et Libertés du 6 janvier 1978, la Commission Nationale de l'Informatique et des Libertés est une autorité administrative indépendante chargée de veiller à la protection des données personnelles contenues dans les fichiers et traitements informatiques, aussi bien publics que privés.

LES MISSIONS DE LA CNIL

La CNIL est chargée de veiller au respect des droits et libertés des personnes à l'égard des traitements de données personnelles et des usages du numérique. Elle s'assure que ces traitements sont conformes aux prescriptions du RGPD et de la loi du 6 janvier 1978 modifiée, dite loi informatique et libertés.

À ce titre, elle dispose d'un pouvoir de contrôle et de sanction, ainsi qu'un rôle d'alerte et de conseil. Elle a pour mission de veiller, à ce que le développement des nouvelles technologies et des usages numériques ne porte atteinte, ni à l'identité humaine, ni aux droits de l'homme, ni à la vie privée, ni aux libertés individuelles ou publiques.

La loi confie à la CNIL les missions suivantes :

- ✓ Réguler, recenser les traitements de données personnelles et autoriser les traitements les plus sensibles avant leur mise en place.
- ✓ Contrôler, en instruisant les plaintes qu'elle reçoit, en procédant à des vérifications directement dans les traitements de données et en sanctionnant le cas échéant.
- ✓ Informer les personnes de leurs droits et obligations, et garantir leur droit d'accès à leurs données qu'elles soient personnelles ou non.
- ✓ Conseiller les personnes et les organismes qui exploitent des données personnelles, et répondre aux consultations des pouvoirs publics et des juridictions.
- ✓ Recenser et animer le réseau des Délégués à la Protection des Données (DPO).
- ✓ Accompagner les usagers par les outils de la conformité.

La CNIL peut aussi proposer au Gouvernement toutes mesures législatives ou réglementaires de nature à adapter la protection des libertés et de la vie privée à l'évolution des techniques.

Elle collabore avec ses homologues européens dans le cadre de l'application du RGPD.

Par ailleurs, la CNIL est investie d'une mission générale de réflexion prospective. Elle se tient informée de l'évolution des technologies, et analyse les effets de leur utilisation sur le droit à la protection de la vie privée, l'exercice des libertés et le fonctionnement des institutions.

ARTICLE 3 - CONTEXTES, ENJEUX ET OBJECTIFS DU MARCHÉ

La CNIL souhaite s'associer les services d'un opérateur économique dans le but de garantir la continuité de sa visibilité sur le réseau Internet.

Cette visibilité est représentée sous la forme des sites « cnil.fr » existants, en permettant plus précisément :

- D'informer et d'aider les particuliers à maîtriser leurs données personnelles.
- D'accompagner les professionnels dans leur mise en conformité au RGPD.
- De partager les réflexions de l'institution sur les tendances émergentes et nouvelles d'usage du numérique des données.
- De conduire des projets d'expérimentation et de prototypage d'outils, de services ou de concepts autour des données personnelles.

Les principaux enjeux de ce marché sont de :

- Garantir une haute disponibilité des différents sites institutionnels.
- Garantir une sécurité optimale contre les attaques par déni de service distribuée « DDoS » sur les différentes couches réseaux et protocoles.
- Disposer de centres d'hébergements sécurisés et redondés en appliquant les règles de sécurité selon les exigences définies aux [articles 8](#) et [9](#).
- Fournir et héberger physiquement les serveurs dédiés, les solutions de sauvegardes et les infrastructures du centre de données sur le territoire d'un État membre de l'Union européenne.
- Infogérer les infrastructures, serveurs physiques et machines virtuelles « VM » constituant le socle matériel et logiciel des sites institutionnels.
- Gérer la réservation des noms de domaines actuels et futurs de l'institution, pour éviter le vol de nom de domaines.
- Adapter les prestations actuellement en fonction, en cas d'évolution des besoins d'infrastructures ou applicatifs, pour mettre à disposition de nouveaux sites web (HTML statiques ou basés sur un CMS) ou d'autres applications.

L'objectif de ce marché est de répondre aux besoins institutionnels en respectant les contraintes et les enjeux définis aux articles 5 à 9.

ARTICLE 4 - OBJET DU MARCHÉ

Le présent marché a pour objet, l'exécution des prestations permettant l'hébergement et l'administration des serveurs dédiés aux sites de « cnil.fr » et de prestations associées.

Les prestations d'hébergement concernent à la fois :

- Des logiciels libres de gestion de contenus « CMS », préparé et configurés dans le cadre d'une tierce maintenance applicative « TMA », gérée par une société mandatée par la CNIL.
- Des sites web statiques dédiés, principalement fournis par le laboratoire d'innovation numérique (LINC) de notre l'institution.

Le titulaire assurera les prestations décrites à l'article 7 ci-après, et organisées en quatre grands postes, répartis dans les différents articles référencés dans le tableau suivant.

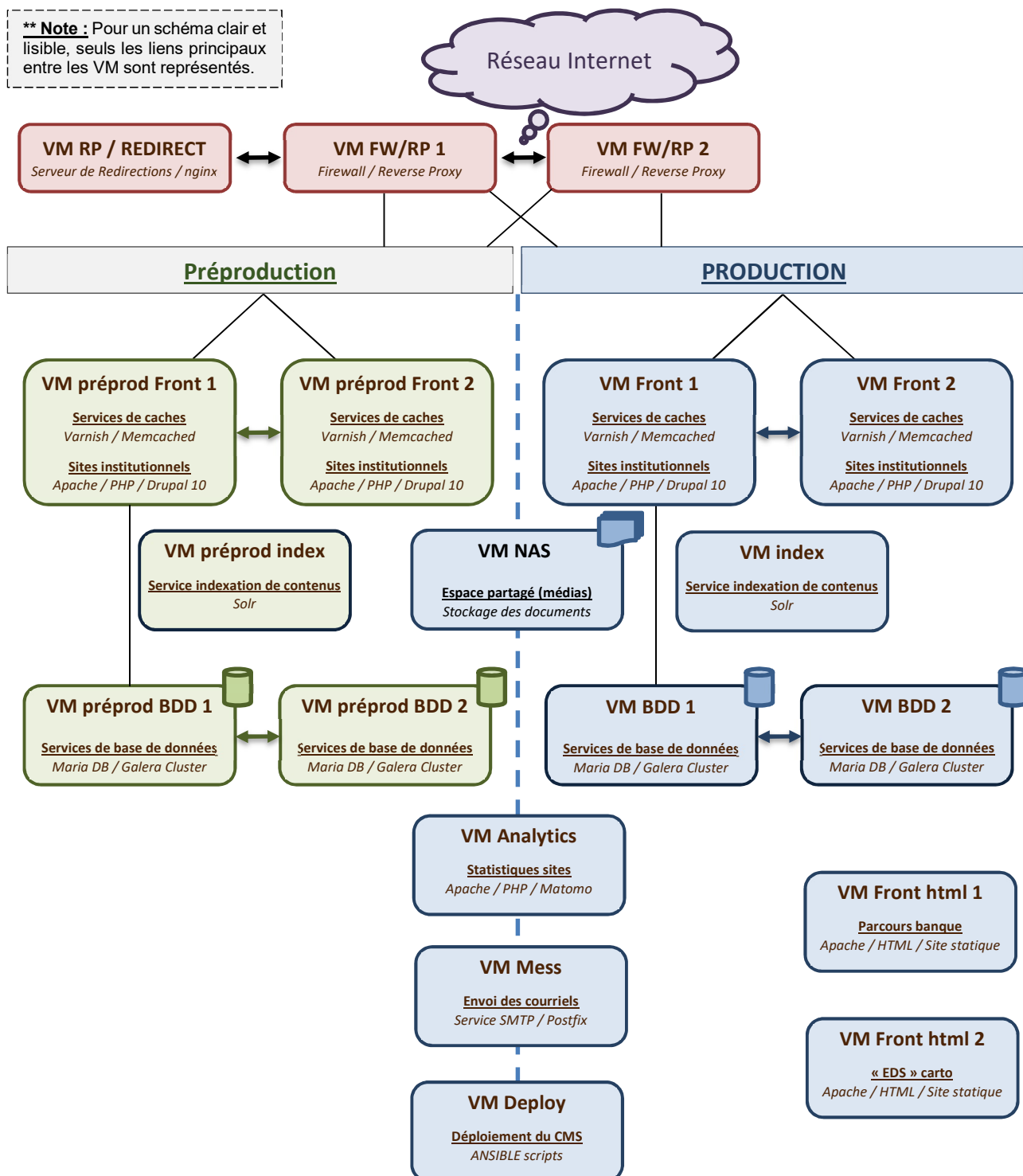
La colonne « résumé des prestations attendues », permet une description générale et non exhaustive des prestations, des contraintes et des exigences qui permettent de répondre aux besoins de ce marché d'hébergement.

Poste de prestation	Articles du CCTP	Résumé des prestations attendues
Poste 1 - Initialisation UO1	5 et 10	Lancer l'exécution du marché avec une réunion de lancement, la présentation des équipes, la définition de l'organisation et du pilotage et l'appropriation du périmètre du marché.
Poste 2 - Mise en place UO2 à UO4	5, 6, 7, 8, 9 et 10	Mettre en place un ou plusieurs logiciels de gestion de contenus « CMS », avec les bases de données associées, afin d'assurer la disponibilité des sites « cnil.fr » institutionnels (contenus et paramètres fournis par la CNIL ou la société en charge de la « TMA » des sites institutionnels).
Poste 3 - Exploitation UO5 à UO13	5, 6, 7, 8, 9 et 10	Garantir la mise à jour, l'évolution et le maintien en condition opérationnelle des sites de l'institution. Garantir la sécurité des infrastructures en appliquant nos exigences de disponibilité des sites institutionnels. Effectuer des études d'architectures.
Poste 4 - Réversibilité UO14	5 et 10	Préparer un dossier complet contenant toutes les informations (<i>paramétrages et documents inclus</i>) relatives à l'installation, la reprise de l'existant et de l'état actuel des plateformes techniques permettant le transfert des compétences vers la CNIL ou vers un nouveau titulaire.

5.1 Présentation générale des environnements

Les sites institutionnels de la CNIL sont hébergés sur **trois serveurs physiques dédiés** répartis sur **deux centres de données distants**. La vingtaine de machines virtuelles « VM » sont réparties sur les trois serveurs physiques où sont installés des hyperviseurs de type 1, actuellement ProxMox.

Le schéma** ci-dessous, représente les différentes plateformes de production et de préproduction des sites institutionnels.



5.2 Spécifications des machines virtuelles

Ce tableau présente les ressources minimales des machines virtuelles « VM », ainsi que leur quantité, pour que les plateformes de production et de préproduction s'exécutent dans les meilleures conditions opérationnelles.

Les spécifications techniques demandées dans ce tableau, sont les valeurs minimales exigées en termes de nombre de processeurs « CPU », mémoire vive « RAM », ou espace disque « system/data ».

Si des ressources doivent être augmentées, la priorité est mise sur le nombre de processeurs « CPU » et sur la capacité de la mémoire vive « RAM » des différentes machines virtuelles.

Machine virtuelle	Qté	CPU	RAM	HDD (system/data)
Pares-feux, proxy inverse et redirections				
Firewall / Reverse Proxy	2	2	2 Go	4 Go / 20 Go
Redirections	1	2	2 Go	4 Go / 20 Go
Plateforme de production				
Frontaux	2	10	16 Go	8 Go / 120 Go
Base de données Maria DB	2	4	8 Go	8 Go / 240 Go
Indexation	1	2	4 Go	8 Go / 40 Go
Stockage des fichiers	1	2	4 Go	8 Go / 240 Go
Envoi de courriel « SMTP »	1	2	4 Go	4 Go / 20 Go
Analyse de trafic « Matomo »	1	2	4 Go	4 Go / 20 Go
Frontal « EDS Carto »	1	2	8 Go	4 Go / 20 Go
Frontal « Parcours Banque »	1	2	8 Go	4 Go / 20 Go
Déploiement	1	2	2 Go	4 Go / 20 Go
Plateforme de préproduction				
Frontaux	2	4	8 Go	8 Go / 60 Go
Base de données « MariaDB »	2	4	8 Go	8 Go / 120 Go
Indexation	1	2	2 Go	8 Go / 20 Go

5.3 Environnement des pares-feux « FW », proxy inverse « RP » et redirections

Le couple des machines virtuelles « VM FW/RP » dédiées sous Debian réalise le filtrage en entrée des plateformes et permet la gestion des états de connexion pour une meilleure protection des intrusions (pare-feu à états ou stateful firewall).

En sus de la protection par filtrage, le logiciel open source « HA Proxy » permet également de jouer le rôle de proxy inverse « RP » et de répartition de charge. La disponibilité de ces deux machines virtuelles « VM FW/RP » est assurée par une redondance dans un mode « actif / actif ».

Les caractéristiques de ces machines virtuelles « VM » sont les suivantes :

- ✓ Système d'exploitation Debian.
- ✓ Filtrage des flux réseaux « FW ».
- ✓ Filtrage applicatif des requêtes « WAF ».
- ✓ Répartition de charge et proxy inverse « RP » avec le logiciel open source « HA Proxy ».

La machine virtuelle « VM RP / REDIRECT » est un serveur de redirection avec « nginx » sous Debian permettant de réaliser des redirections des noms de domaines réservés, comme par exemple « cnil.ai », « cnil.eu ». Fonctionnellement, cela permet à l'institution de faire du parking de nom de domaine pour éviter le vol en vue d'une utilisation frauduleuse des noms de domaines.

Les caractéristiques de la « VM » est la suivante :

- ✓ Système d'exploitation Debian.
- ✓ Logiciel libre « nginx » pour la gestion des redirections.

Tous ces équipements ont également un rôle de terminateur TLS.

5.4 La plateforme de production

Elle permet de fournir un accès aux services hébergés dans les meilleures conditions de disponibilité, de qualité et de sécurité pour les sites « cnil.fr » et « linc.cnil.fr ».

Elle est composée de 11 serveurs virtuels sous Debian :

- Deux frontaux « VM Front » en mode « actif-actif » :
 - Logiciel libre Apache.
 - Deux instances Drupal 10 séparées pour gérer les sites institutionnels précités.
 - Les logiciels libres de cache « Varnish » et « Memcached ».
- Deux serveurs « VM BDD » de base de données avec Maria DB « Galera Cluster ».
- Un serveur « VM index » pour l'indexation des documents et des contenus avec Apache Solr.
- Un serveur « VM NAS » de stockage pour les fichiers multimédia avec un montage de type GlusterFS.
- Un serveur « VM Mess » d'envoi de courriel.
- Un serveur « VM Analytics » d'analyse de trafic web des serveurs avec le logiciel libre « matomo ».
- Deux serveurs « VM Front html » pour les sites web statiques « EDS Carto » et « Parcours Banque » :
 - Logiciel libre Apache ou nginx
 - Pages web simple en utilisant HTML/CSS/javascript.
- Un serveur « VM Deploy » de déploiement pour les mises à jour Drupal 10 avec ANSIBLE.

Le site principal « cnil.fr » accède à d'autres ressources externes à l'aide des API RESTful.

Tous les flux échangés entre le navigateur Internet des usagers et les serveurs sont sécurisés, avec des certificats « TLS RGS » fournis par la CNIL et déposés sur les serveurs. Le titulaire sera sollicité pour la création des clefs nécessaires à la génération des dits certificats.

Cette plateforme de production est susceptible d'évoluer pour héberger d'autres sites institutionnels indépendants les uns des autres, que ce soit avec un « CMS » ou des sites statiques.

5.5 La plateforme de préproduction

Elle est utilisée par l'équipe projet « EPROJ » ainsi que les sociétés tierces intervenant dans le cadre de la maintenance « TMA » et du développement des nouvelles fonctionnalités des sites institutionnels mis à disposition.

Cette plateforme a pour but d'assurer la bonne qualité des livrables des deux sites principaux, « cnil.fr » et « linc.cnil.fr ». Elle permet à l'équipe projet « EPROJ » de réaliser la recette avant le déploiement sur la plateforme de production.

En dehors du serveur de stockage « VM NAS », de l'analyse du trafic web « VM Analytics », et du serveur d'envoi de courriels « VM Mess », la plateforme est la copie exacte de la production à tous les niveaux : machines virtuelles, système d'exploitation, composants logiciels, applications et bases de données.

Un filtrage par IP par liste blanche est mis en place pour n'autoriser que les adresses IP fournies par la direction des systèmes d'information « DSI » de la CNIL. De ce fait, la plateforme de préproduction ne peut pas être référencée par les moteurs de recherche.

L'équipe projet « EPROJ », ou les sociétés tierces intervenant dans le cadre de la maintenance « TMA » peuvent demander la mise à niveau des sites de préproduction, du lundi au vendredi, de 9^h à 18^h, hors jours fériés, à partir de l'exécution de scripts depuis le serveur « VM Deploy ».

La plateforme de préproduction est composée de cinq serveurs sous Debian 11 :

- Deux frontaux « VM préprod Front » en mode « actif-actif » :
 - Logiciel libre Apache.
 - Deux instances Drupal 10 pour gérer les sites de préproduction.
 - Les logiciels libres de cache « Varnish » et « Memcached ».
- Deux serveurs « VM préprod BDD » de base de données Maria DB « Galera Cluster ».
- Un serveur « VM préprod index » pour l'indexation des documents et des contenus avec Apache Solr.

La plateforme de préproduction accède à d'autres ressources externes en utilisant des services web RESTful.

5.6 Socle des logiciel tiers (hors système d'exploitation Debian)

À la demande de la CNIL des logiciels tiers pourront être installés à partir d'un document d'installation fourni par l'équipe projet « EPROJ ». Ces logiciels tiers viennent en complément du socle logiciel de base défini dans la liste ci-dessous.

Concernant son devoir de conseil défini au [paragraphe 8.6](#), le titulaire est tenu à une obligation permanente de conseil et de mise en garde, relative aux logiciels tiers installés dans le cadre de la « TMA » et aux prestations fournies à la CNIL.

Pour que les sites fonctionnent de façon optimale, en dehors des systèmes d'exploitation, les logiciels suivants sont installés sur les machines virtuelles :

- ✓ Varnish.
- ✓ HA Proxy.
- ✓ Memcached.
- ✓ Base de données Maria DB « Galera Cluster ».
- ✓ Serveur Web Apache et nginx en fonction des serveurs.
- ✓ Apache Solr.
- ✓ PHP.
- ✓ CMS Drupal.
- ✓ Ansible.
- ✓ Matomo.

5.7 Noms de domaines, serveurs de noms de domaines « DNS » et certificats « TLS RGS »

Des serveurs de noms de domaine sont mis à disposition par le titulaire afin d'assurer une visibilité de tous les noms de domaines réservés, dont « cnil.fr » et tous les sous-domaines afférents.

Le titulaire doit pouvoir assurer la gestion des domaines DNS/DNSSEC et garantir une disponibilité permanente des services critiques :

- Gestion administrative des noms de domaines de la CNIL : enregistrement, renouvellement avant expiration et transfert. Douze extensions sont actuellement utilisées : `.ai`, `.com`, `.eu`, `.fr`, `.info`, `.io`, `.net`, `.org`, `.paris`, `.pro`, `.tech` et `.tv`.
- Configuration et mise à jour de la zone « DNS » pour tous types d'enregistrement (A, AAAA, TXT, CNAME, MX, etc.).
- La mise en place du ou des certificats « TLS RGS » fournis par la CNIL sur les différents serveurs, conformément aux exigences de configuration de la CNIL.

La liste des noms de domaines actuellement réservés et actifs, est fournie « `noms-de-domaines.xlsx` » en annexe 1 du CCTP.

ARTICLE 6 - VOLUMÉTRIE

De tous les sites de l'institution, la volumétrie du site principal « cnil.fr » est celle qui est la plus élevée. Est présenté ci-dessous le nombre de visite « non unique » des usagers du site principal.

Notre outil « Matomo Analytics », est par ailleurs configuré de telle sorte que :

- Les adresses IP sont anonymes et masquées sur 2 octets (192.168.xxx.xxx).
- Le respect des entêtes « ne pas suivre » (DNT) des navigateurs est activé.

De ce fait, bon nombre de visites ne sont pas comptabilisées dans ce qui est présenté ci-après.

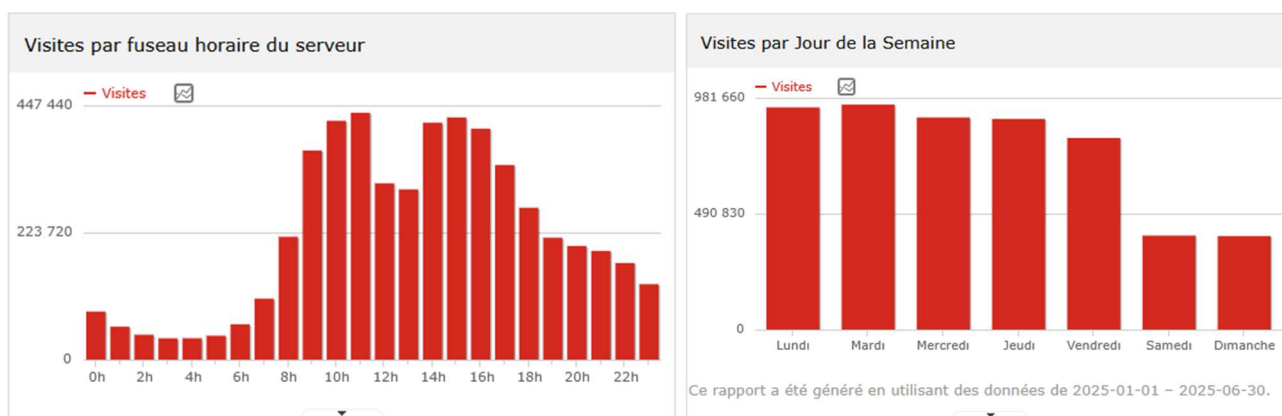
Sur les douze derniers mois, entre juin 2024 et juin 2025, nous avons en moyenne par mois :

- 1 000 000 de visites.
- Soit entre 40 000 et 200 000 visites par jour :
 - Au maximum, 300 000 visites dans le cadre d'une journée exceptionnelle.
 - Au minimum, 40 000 visites les jours non ouvrés (samedis, dimanches et jours fériés).
- 2 500 000 pages vues, 60 000 téléchargements de documents.
- Pour une durée moyenne de 2 minutes.

Récapitulatif des différentes métriques, par année, de janvier 2020 à fin juin 2025 :

Années	2020	2021	2022	2023	2024	2025 (juin)
Visites	9 251 074	10 534 474	10 867 734	10 993 370	11 434 814	5 291 247
Pages vues	19 908 246	21 545 127	21 427 271	24 919 299	30 807 732	14 695 538
Téléchargements	635 276	659 582	610 191	605 117	569 160	315 189

En complément, entre janvier et fin juin 2025, est présenté ci-après le graphique du nombre de visites total, réparti par jour de la semaine et par heure de la journée (heure de Paris) :



Toutes les volumétries indiquées ci-dessus sont données à titre purement indicatif et sans engagement contractuel.

ARTICLE 7 - PRESTATIONS ATTENDUES

Les prestations objet du marché sont définies sous la forme d'unité d'œuvres « UO » dans cet article et sont découpées en quatre postes, définis à l'article 4. Les prestations sont exécutées conformément aux exigences techniques et de sécurité figurant aux articles 8 et 9 du présent CCTP.

Le délai de réalisation des prestations des postes d'initialisation et de mise en place, commence à courir à l'issue de la réunion de lancement, au plus tard, 10 jours ouvrés après la notification du début du marché, et devront être réalisées dans un délai maximum de trois mois (60 jours ouvrés).

Ces prestations sont exécutées pendant la période de réversibilité du marché en cours sans interruption de service des sites de « cnil.fr ».

7.1 Poste 1 - Initialisation

La prestation demandée dans ce poste est relative au démarrage du projet : organisation, pilotage et appropriation du périmètre incluant la création de comptes rendus et de documents techniques.

UO1 Lancement du projet

Lors de la réunion de lancement, et conformément aux dispositions de l'article 13.8 du CCAP, la clause sociale de formation sous statut scolaire est abordée (confirmation des contacts inscrits dans la « Fiche entreprise », rappel des spécificités du public concerné, adaptabilité des missions, etc.)

Objectifs	Appropriation du périmètre de la prestation (analyse de l'existant). Définition de l'organisation du projet et des modalités de pilotage.
Prérequis	Documentation technique fournie par la CNIL transmise en amont la réunion de lancement.
Tâches à réaliser	Réunion de lancement dans les <u>10 jours ouvrés</u> après la notification du début du marché. Présentation de l'équipe projet du titulaire à l'équipe projet CNIL « EPROJ ». Définition de l'organisation du projet. Appropriation du projet par le titulaire. Rédaction d'un dossier d'architecture technique décrivant les hébergements proposés en se basant sur la réversibilité du titulaire précédent. Rédaction de la version finale du plan assurance qualité « PAQ » et du plan assurance sécurité « PAS ». En collaboration avec la CNIL, réalisation de la matrice « RACI » finale pour la mise en œuvre et l'exécution du marché <u>et</u> actualisation du planning prévisionnel d'exécution des prestations. Planning prévisionnel d'exécution des prestations
Livrables en sortie	Compte-rendu de la réunion de lancement. Dossier d'architecture technique. Plan assurance qualité « PAQ » en version finale. Plan assurance sécurité « PAS » en version finale. Matrice « RACI » pour la mise en œuvre et l'exécution du marché. Planning prévisionnel d'exécution des prestations relatif au marché validé par les parties prenantes. Guide de reprise de l'existant avec la réversibilité du titulaire précédent.
Délai de démarrage	<u>10 jours ouvrés</u> après la notification du début du marché.
Durée de réalisation	10 jours ouvrés

7.2 Poste 2 - Mise en place

Les prestations demandées dans ce poste, sont de mettre à disposition une infrastructure matérielle avec l'installation de serveurs physique dédiés, incluant la création des machines virtuelles conforme à la documentation technique et aux exigences prévues aux articles [8](#) et [9](#) du présent.

Ce poste de mise en place permet d'assurer la continuité de service des sites institutionnels de « [cnil.fr](#) » lors du passage de témoin avec le titulaire du marché précédent. L'objectif de ce poste est de ne pas avoir d'interruption de services des sites institutionnels.

UO2 Mise en place de la plateforme de gestion technique

Cette unité d'œuvre correspond à la mise en place de la plateforme de gestion technique de supervision des machines virtuelles « VM », de gestion des DNS et des réservations des noms de domaines et des tickets, permettant à la CNIL d'échanger avec le titulaire et de suivre les installations pendant toute la durée du marché.

Objectifs	Mise à disposition d'une plateforme de gestion technique et de supervision.
Prérequis	-
Tâches à réaliser	Mise à disposition d'une plateforme dédiée chez le titulaire, hébergée sur le territoire d'un État membre de l'Union européenne permettant à l'équipe projet « EPROJ » : <ul style="list-style-type: none">- De créer des comptes nominatif et sécurisé.- De gérer les habilitations d'accès aux différents modules (supervision par exemple).- De gérer les incidents et des nouvelles demandes (tickets).- De gérer les noms de domaines et des enregistrement DNS (Cf annexe 1 du CCTP - liste des noms de domaines existants).- Permettre de superviser les serveurs physiques dédiés, la bande passante, et les machines virtuelles « VM » de l'infrastructure des sites institutionnels.- D'avoir un système de remontées d'alertes incidents (réseaux, sécurité, etc.- D'avoir un système d'aide en ligne permettant de prendre en main l'outil.
Livrables en sortie	Plateforme de gestion technique disponible et utilisable par la CNIL avec les comptes nominatif de l'équipe « EPROJ » créés.
Délai de démarrage	<u>10 jours ouvrés</u> après la notification du marché.
Durée de réalisation	5 jours ouvrés

UO3 Mise en place des environnements de production et de préproduction

Cette unité d'œuvre correspond à la mise en place des plateformes d'hébergement présentées dans l'[article 5](#).

Le titulaire délivre toutes les prestations du centre de données, garantissant le fonctionnement optimal des équipements et la continuité des services hébergés en fonction de nos exigences techniques et de sécurités présentés aux articles [8](#) et [9](#) avec entre autres :

- Serveurs physiques dédiés à la CNIL.
- Alimentation sécurisée et climatisation.
- Redondance des équipements, sauvegardes et protection des données.
- Dispositifs anti intrusion et protection contre la malveillance incluant le « DDoS ».
- Supervision des services et administration.

Objectifs	Installation des plateformes de production et de préproduction.
Prérequis	Matrice « RACI » et planning prévisionnel des prestations.
Tâches à réaliser	<p>En collaboration avec l'équipe projet « EPROJ » de la CNIL, ajustement de la matrice « RACI » et ajustement du planning prévisionnel des prestations.</p> <p>Installer et paramétrer les équipements matériels (serveurs physiques dédiés, routeurs, DNS, ...) conformément au dossier d'architecture technique.</p> <p>Installer les hyperviseurs de type 1 choisi par le titulaire et en accord avec l'équipe projet « EPROJ ».</p> <p>Créer les machines virtuelles « VM ».</p> <p>Installer, configurer et sécuriser les systèmes d'exploitation.</p> <p>Installer et configurer les logiciels tiers utilisés par le CMS Drupal 10 et toute l'infrastructure logicielle existante et requise pour la mise en ligne des sites institutionnels (Varnish, HA Proxy, Memcached, Maria DB « Galera Cluster », Apache, nginx, Apache Solr, PHP, Ansible, Matomo).</p> <p>Mise en place d'un système de protection anti DDoS.</p> <p>Installation des outils de supervision sur les plateformes de production et de préproduction.</p>
Livrables en sortie	<p>Planning d'installation ajusté et matrice RACI suivie à jour.</p> <p>Le dossier d'architecture technique mis à jour et tout document associé à la mise en place des environnements.</p> <p>Les plateformes de préproduction et de production installées et opérationnelles.</p>
Délai de démarrage	<u>10 jours ouvrés</u> après la notification du début du marché.
Durée de réalisation	20 jours ouvrés

UO4 Reprise de l'existant

Cette unité d'œuvre correspond à la reprise de l'existant incluant la bascule effective des sites institutionnels, sur les environnements de production et de préproduction présentées dans l'[article 5.](#), vers le nouveau titulaire.

A cet effet, l'équipe projet « EPROJ » de la CNIL, met à disposition :

- Les fichiers du cœur du CMS Drupal et ses modules additionnels.
- Les scripts Ansible et les fichiers de configuration pour les livraisons.
- Les sauvegardes des bases de données associées et les fichiers physiques (médias).
- Les fichiers des sites « statiques » existants et les fichiers physiques associés (médias).
- Les documents techniques d'installation et de mise à jour.
- Toutes les informations nécessaires pour le transfert des noms de domaines.

Objectifs	Installation et mise en ligne des sites institutionnels et de l'ensemble des services.
Prérequis	Fourniture d'une matrice RACI détaillée par l'équipe projet « EPROJ » de la CNIL comprenant toutes les tâches pour la réalisation de cette prestation.
Tâches à réaliser	Collaboration avec l'équipe projet « EPROJ » de la CNIL sur la modification et le suivi de la matrice RACI détaillée pour la bonne réalisation. Installation des sites institutionnels « cnil.fr » et l'ensemble des services : <ul style="list-style-type: none">- Installation et exécution des scripts Ansible pour les MEP.- Installation des fichiers Drupal et les modules spécifiques associés.- Restauration des bases de données.- Transfert des noms de domaines et gestion des DNS avec le transfert complet des sites institutionnels.
Livrables en sortie	Planning d'installation ajusté et matrice RACI suivie à jour. Les sites institutionnels opérationnels en production et préproduction. Gestion du transfert des DNS et des noms de domaines réalisé. Dossier des documents technique de la reprise de l'existant. Dossier des documents d'architecture technique mis à jour.
Délai de démarrage	Commence au début de la mise en place des environnements « UO3 ».
Durée de réalisation	10 jours ouvrés

7.3 Poste 3 - Exploitation

Les prestations présentées ci-après permettent de garantir le maintien en condition opérationnelle « MCO » et de sécurité « MCS » des sites.

Les prestations d'achat et de renouvellement des noms de domaines sont exécutées dans les conditions 5) et 6) prévues à l'article 12.1.2 du CCAP.

UO5 Suivi opérationnel (infogérance) des environnements

Cette unité d'œuvre **récurrente** correspond au suivi opérationnel (infogérance) et au bon fonctionnement des sites institutionnels, présentées dans l'[article 5](#).

Le titulaire délivre le suivi opérationnel (infogérance), incluant la résolution des incidents réseaux, matériel ou logiciel des plateformes d'hébergement, garantissant le fonctionnement optimal des équipements et la continuité des services hébergés en fonction des exigences techniques et de sécurités prévues aux articles [8](#) et [9](#) du présent CCTP.

Objectifs	Suivi opérationnel des plateformes de production et de préproduction.
Prérequis	Poste 2 « Mise en place » terminé et admis
Tâches à réaliser	Utilisation de la plateforme de gestion technique pour les échanges avec l'équipe projet « EPROJ » pour les demandes administratives ou techniques. Réagir et corriger les incidents conformément aux exigences techniques de disponibilité (GTR/GTI définies au paragraphe 8.4). Superviser les plateformes de production et de préproduction en termes de disponibilité et de sécurité (machines virtuelles « VM »).
Livrables en sortie	Suivi des incidents via la plateforme de gestion technique fournie par le titulaire. Comité de pilotage « COPIL » trimestriel puis semestriel (paragraphe 10.3). Communication techniques générales sur l'infrastructure générale du titulaire. Compte rendu mensuel de l'état de la disponibilité de l'ensemble de l'infrastructure (production et de préproduction). Compte rendu mensuel de l'état de la sécurité de l'ensemble de l'infrastructure (production et préproduction) incluant les attaques DDoS.
Délai de démarrage	Sans délai à partir de la fin de la bascule opérationnelle des sites.
Réurrence	Exécution récurrente pendant la durée d'exécution du marché.

UO6 Mise à jour des environnements de production et de préproduction

Cette unité d'œuvre **récurrente** correspond la mise à jour des composants techniques « CT » dans des versions « stables et maintenues » en restant dans le support à long terme « LTS ».

Le titulaire effectue les mises à jour des environnements en fonction des exigences techniques et de sécurités prévues aux articles [8](#) et [9](#) du présent CCTP :

- A la demande de l'équipe projet « EPROJ ».
- Où à son initiative dans le cadre de sa veille de sécurité des composants techniques « CT » sous sa responsabilité.

Concernant les logiciels tiers fortement dépendant des sites institutionnels, ils seront mis à jour à la demande de la CNIL. Seule la mise à jour des versions mineures est réalisée dans le cadre de cette unité d'œuvre. La mise à jour des versions majeure est définie dans l'unité d'œuvre « UO12 ».

Objectifs	Mise à jour des environnements.
Prérequis	-
Tâches à réaliser	Mise à jour des versions maintenues, mineures et majeures : <ul style="list-style-type: none">- Des hyperviseurs de type 1 (actuellement ProxMox).- Des systèmes d'exploitation des machines virtuelles « VM » (Debian).- Bases de données (Maria DB « Galera Cluster »).- Logiciels tiers ayant une dépendance limitée avec les sites institutionnels (HA Proxy, Apache, nginx, Ansible). Mise à jour des versions maintenues, mineures seulement pour le périmètre : <ul style="list-style-type: none">- Logiciels tiers ayant une dépendance forte avec les sites institutionnels (Varnish, Memcached, Apache Solr, PHP, Matomo, Drupal).
Livrables en sortie	Suivi des mises à jour des environnements via la plateforme de gestion technique fournie par le titulaire. Compte rendu technique des mises à jour.
Délai de démarrage	Sans délai à partir de la fin de la bascule opérationnelle des sites.
Récurrance	Exécution récurrente pendant la durée d'exécution du marché.

UO7 Installer un serveur physique

Cette unité d'œuvre **ponctuelle** correspond à une demande de mise en place d'un serveur physique dédié, conformément aux exigences techniques et de sécurités, et correspondant aux spécifications demandées par l'équipe projet « EPROJ ». Elle fera l'objet d'une demande de devis dans les conditions définies à l'article 13.1 du CCAP.

Cette installation inclus la mise en place du logiciel d'Hyperviseur de type 1 (actuellement ProxMox) choisi par le titulaire en accord avec l'équipe projet « EPROJ ». Elle peut être associée à une prestation de mise en place d'une machine virtuelle supplémentaire « VM » défini ci-après.

Une fois la mise en place effectuée, le serveur passe en exploitation et entre dans le suivi opérationnel (infogérance) et de mise à jour des environnements décrit dans les « UO5 » et « UO6 ».

Objectifs	Installer un serveur physique et son logiciel hyperviseur de type 1 associé															
Prérequis	-															
Spécifications techniques	<p>Cette unité d'œuvre permet le choix d'un serveur suivant les trois niveaux de ressources matérielles, avec au minimum dans chacun des niveaux :</p> <table><tr><td>UO7.N1</td><td><u>Niveau 1</u></td><td>CPU 16 cœurs</td><td>RAM 64 Go</td><td>HDD 512 Go</td></tr><tr><td>UO7.N2</td><td><u>Niveau 2</u></td><td>CPU 24 cœurs</td><td>RAM 128 Go</td><td>HDD 1 To</td></tr><tr><td>UO7.N3</td><td><u>Niveau 3</u></td><td>CPU 32 cœurs</td><td>RAM 256 Go</td><td>HDD 2 To</td></tr></table>	UO7.N1	<u>Niveau 1</u>	CPU 16 cœurs	RAM 64 Go	HDD 512 Go	UO7.N2	<u>Niveau 2</u>	CPU 24 cœurs	RAM 128 Go	HDD 1 To	UO7.N3	<u>Niveau 3</u>	CPU 32 cœurs	RAM 256 Go	HDD 2 To
UO7.N1	<u>Niveau 1</u>	CPU 16 cœurs	RAM 64 Go	HDD 512 Go												
UO7.N2	<u>Niveau 2</u>	CPU 24 cœurs	RAM 128 Go	HDD 1 To												
UO7.N3	<u>Niveau 3</u>	CPU 32 cœurs	RAM 256 Go	HDD 2 To												
Tâches à réaliser	<p>Planification et organisation de l'installation dans le centre de données.</p> <p>Mise en place du serveur physique avec son raccordement à l'infrastructure dédiée à la CNIL.</p> <p>Installer les hyperviseurs de type 1 choisi par le titulaire et en accord avec l'équipe projet « EPROJ ».</p> <p>Intégrer le nouvel hyperviseur à l'environnement existant.</p> <p>Mise en place des exigences techniques et de sécurité.</p> <p>Installation des outils de supervision.</p>															
Livrables en sortie	<p>Le serveur physique installé et configuré.</p> <p>Le dossier d'architecture technique mis à jour et tout document associé à la mise en place du logiciel tiers ou de sa mise à jour majeure.</p>															
Délai de démarrage	A la notification du bon de commande.															

UO8 Suivi opérationnel (infogérance) d'un serveur physique et des « VM » associées

Cette unité d'œuvre **récurrente** correspond au suivi opérationnel (infogérance) d'un serveur physique nouvellement installé dans le cadre d'une « UO7 », conformément aux exigences techniques et de sécurités des articles [8](#) et [9](#) incluant les mises à jour logicielles. Elle fera l'objet d'une demande de devis dans les conditions définies à l'article 13.1 du CCAP.

En sus du suivi opérationnel (infogérance) du serveur physique, cette unité d'œuvre inclus le suivi opérationnel (infogérance) de 4 « quatre » VM.

Objectifs	Suivi opérationnel (infogérance) d'un serveur physique et de <u>4 machines virtuelles</u> « VM » associées.																		
Prérequis	« UO7 » installer un serveur physique.																		
Spécifications techniques	<p>Cette unité d'œuvre concerne le suivi opérationnel (infogérance) d'un serveur physique incluant les quatre machines virtuelles « VM » également infogérées :</p> <table><tr><td>UO8.N1</td><td>Niveau 1</td><td>8 VM (*)</td><td>CPU 16 cœurs</td><td>RAM 64 Go</td><td>HDD 512 Go</td></tr><tr><td>UO8.N2</td><td>Niveau 2</td><td>12 VM (*)</td><td>CPU 24 cœurs</td><td>RAM 128 Go</td><td>HDD 1 To</td></tr><tr><td>UO8.N3</td><td>Niveau 3</td><td>16 VM (*)</td><td>CPU 32 cœurs</td><td>RAM 256 Go</td><td>HDD 2 To</td></tr></table> <p>(*) Le nombre de machines virtuelles « VM » infogérées indiqué est le nombre maximal recommandé (nombre de cœurs du niveau « N » divisé par deux).</p>	UO8.N1	Niveau 1	8 VM (*)	CPU 16 cœurs	RAM 64 Go	HDD 512 Go	UO8.N2	Niveau 2	12 VM (*)	CPU 24 cœurs	RAM 128 Go	HDD 1 To	UO8.N3	Niveau 3	16 VM (*)	CPU 32 cœurs	RAM 256 Go	HDD 2 To
UO8.N1	Niveau 1	8 VM (*)	CPU 16 cœurs	RAM 64 Go	HDD 512 Go														
UO8.N2	Niveau 2	12 VM (*)	CPU 24 cœurs	RAM 128 Go	HDD 1 To														
UO8.N3	Niveau 3	16 VM (*)	CPU 32 cœurs	RAM 256 Go	HDD 2 To														
Tâches à réaliser	<p>Utilisation de la plateforme de gestion technique pour les échanges avec l'équipe projet « EPROJ » pour les demandes administratives ou techniques.</p> <p>Réagir et corriger les incidents conformément aux exigences techniques de disponibilité (GTR/GTI définies au paragraphe 8.4)</p> <p>Superviser le serveur physique et les machines virtuelles « VM » associées en termes de disponibilité et de sécurité.</p> <p>Mise à jour des versions maintenues, mineures et majeures des systèmes d'exploitation et des logiciels tiers Logiciels tiers ayant une dépendance limitée avec les sites institutionnels (HA Proxy, Apache, nginx, Ansible).</p>																		
Livrables en sortie	<p>Suivi des incidents via la plateforme de gestion technique fournie par le titulaire.</p> <p>Communication techniques générales sur l'infrastructure générale du titulaire.</p> <p>Compte rendu mensuel de l'état de la disponibilité du serveur physique et des 4 « quatre » machines virtuelles « VM » associées.</p> <p>Compte rendu mensuel de l'état de la sécurité de l'ensemble du serveur physique et des machines virtuelles « VM » associées incluant les attaques DDoS.</p>																		
Délai de démarrage	A la notification du bon de commande.																		
Récurrance	Exécution récurrente à partir de la commande et ce pendant la durée d'exécution du marché.																		

UO9 Installer une machine virtuelle « VM » additionnelle

Cette unité d'œuvre **ponctuelle** correspond à une demande de mise en place d'une nouvelle machine virtuelle « VM » sur un des serveurs physiques dédiés dont les ressources matérielles sont suffisantes pour l'héberger. Elle fera l'objet d'une demande de devis dans les conditions définies à l'article 13.1 du CCAP.

Cette installation inclus la mise en place du système d'exploitation choisi par le titulaire en accord avec l'équipe projet « EPROJ ». Elle peut être associée à une prestation de mise en place d'un logiciel tiers nouveau.

Objectifs	Installer une nouvelle machine virtuelle « VM »
Prérequis	-
Tâches à réaliser	Planification et organisation de l'installation de la machine virtuelle « VM ». Installer, configurer et sécuriser le système d'exploitation sur la plateforme cible de production ou de préproduction. Ajout de la machine virtuelle « VM » au système de protection anti DDoS Installation des outils de supervision.
Livrables en sortie	Planning d'installation. La machine virtuelle « VM » installée et correctement configurée sur la plateforme cible de production ou de préproduction. Le dossier d'architecture technique mis à jour et tout document associé à la mise en place du logiciel tiers ou de sa mise à jour majeure.
Délai de démarrage	A la notification du bon de commande.

UO10 Suivi opérationnel (infogérance) d'une machine virtuelle « VM » additionnelle

Cette unité d'œuvre **récurrente** est associée l'installation d'une nouvelle machine virtuelle « UO9 ». Elle correspond à au suivi opérationnel (infogérance) », conformément aux exigences techniques et de sécurités des articles [8](#) et [9](#) incluant les mises à jour logicielles. Elle fera l'objet d'une demande de devis dans les conditions définies à l'article 13.1 du CCAP.

Le titulaire effectue les mises à jour des environnements en fonction des exigences techniques et de sécurités prévues aux articles [8](#) et [9](#) du présent CCTP :

- A la demande de l'équipe projet « EPROJ ».
- Où à son initiative dans le cadre de sa veille de sécurité des composants techniques « CT » sous sa responsabilité.

Concernant les logiciels tiers fortement dépendant des sites institutionnels, ils seront mis à jour à la demande de la CNIL. Seule la mise à jour des versions mineures est réalisée dans le cadre de cette unité d'œuvre. La mise à jour des versions majeure est définie dans l'unité d'œuvre « UO12 ».

Objectifs	Mise à jour d'une machine virtuelle « VM ».
Prérequis	« UO9 » installer une machine virtuelle « VM ».
Tâches à réaliser	Utilisation de la plateforme de gestion technique pour les échanges avec l'équipe projet « EPROJ » pour les demandes administratives ou techniques. Réagir et corriger les incidents conformément aux exigences techniques de disponibilité (GTR/GTI définies au paragraphe 8.4) Superviser la machine virtuelle « VM » en termes de disponibilité et de sécurité. Mise à jour des versions maintenues, mineures et majeures des systèmes d'exploitation et des logiciels tiers Logiciels tiers ayant une dépendance limitée avec les sites institutionnels (HA Proxy, Apache, nginx, Ansible).
Livrables en sortie	Suivi des mises à jour des environnements via la plateforme de gestion technique fournie par le titulaire. Compte rendu technique des mises à jour. Compte rendu mensuel de l'état de la disponibilité de la machine virtuelle « VM ». Compte rendu mensuel de l'état de la sécurité de la machine virtuelle « VM ».
Délai de démarrage	A la notification du bon de commande.
Récurrance	Exécution récurrente à partir de la commande et ce pendant la durée restante d'exécution du marché.

UO11 Installer un logiciel tiers

Cette unité d'œuvre **ponctuelle** correspond à une demande d'installation d'une nouvelle application ou d'un logiciel tiers répondant à un besoin futur. Elle fera l'objet d'une demande de devis dans les conditions définies à l'article 13.1 du CCAP.

Toute la partie de configuration liée à l'infrastructure existante dont la sécurité, en conformité avec les autres éléments installés, est à la charge du titulaire. La configuration de l'application ou du logiciel tiers est établie par l'équipe projet « EPROJ » et est envoyée avant l'installation.

En fonction de la complexité de l'installation du logiciel tiers, une durée de l'UO pour réaliser la prestation ainsi que la séniorité du profil « Administrateur Système et Réseau » est indiquée. La liste « non exhaustive » des logiciels sont données à titre indicatif par rapport à la difficulté d'installation et de paramétrage.

En définitive, ce tableau met en exergue la corrélation étroite entre la complexité des logiciels à installer, les profils, ainsi que la durée d'exécution de l'unité d'œuvre estimée :

Référence de la commande	Niveau de complexité	Type de logiciels (Liste non exhaustive)	Profils	Durée
UO11.1	simple	Apache,nginx, etc.	Administrateur Système et Réseau (0 à 2 ans d'expérience)	1 jour ouvré
UO11.2	Intermédiaire	Mediawiki, etc.	Administrateur Système et Réseau Confirmé (3 à 10 ans d'expérience)	3 jours ouvrés
UO11.3	Elevé	CMS, LMS, etc	Administrateur Système et Réseau Sénior (+10 ans d'expérience)	5 jours ouvrés

Objectifs	Installer une application ou un logiciel tiers
Prérequis	Fourniture d'un document d'installation du logiciel tiers, incluant les exigences de sécurité en sus de la sécurité pratiquée par le titulaire et son paramétrage, par l'équipe projet « EPROJ » de la CNIL.
Profils	Administrateur Système et Réseau (Junior, Confirmé ou Sénior) en fonction de la typologie de logiciel (voir tableau ci-dessus)
Tâches à réaliser	Planification et organisation de l'installation du logiciel tiers. Installation d'un logiciel tiers nouveau sur une machine virtuelle « VM » existante ou sur une machine virtuelle « VM » nouvelle. Application du paramétrage applicatif. Application des exigences de sécurités demandés dans le document fourni.

Livrables en sortie	Planning d'installation. Le logiciel tiers installé et correctement configuré sur les plateformes de préproduction et de production. Le dossier d'architecture technique mis à jour et tout document associé à la mise en place du logiciel tiers ou de sa mise à jour majeure.
Délai de démarrage	A la notification du bon de commande de cette unité d'œuvre.
Durée de réalisation	A déterminer en fonction de la difficulté de l'installation (voir tableau ci-dessus).

UO12 Montée de version majeure d'un logiciel tiers

Cette unité d'œuvre **ponctuelle** correspond à une demande de mise à jour d'une version majeure d'une application existante ou d'un logiciel que ce soit à l'initiative de l'équipe projet « EPROJ » ou du titulaire dans le cadre d'un environnement technique maintenu. Elle fera l'objet d'une demande de devis dans les conditions définies à l'article 13.1 du CCAP.

Toute la partie de configuration liée à l'infrastructure existante dont la sécurité, en conformité avec les autres éléments installés est à la charge du titulaire. La configuration de l'application ou du logiciel tiers est établie par l'équipe projet « EPROJ » et est envoyée avant la mise à jour.

En fonction de la complexité de la montée de version du logiciel tiers, une durée de l'UO pour réaliser la prestation ainsi que la séniorité du profil « Administrateur Système et Réseau » est indiquée. La liste « non exhaustive » des logiciels sont données à titre indicatif par rapport à la difficulté d'installation et de paramétrage.

En définitive, ce tableau met en exergue la corrélation étroite entre la complexité des logiciels à installer, les profils, ainsi que la durée d'exécution de l'unité d'œuvre estimée :

Référence de la commande	Niveau de complexité	Type de logiciels (Liste non exhaustive)	Profil	Durée
UO12.1	simple	Apache,nginx, etc.	<i>Inclus dans « UO6 » s'agissant d'une montée de version mineure</i>	
UO12.2	Intermédiaire	Mediawiki, etc.	Administrateur Système et Réseau Confirmé (3 à 10 ans d'expérience)	3 jours ouvrés
UO12.3	Elevé	CMS, LMS, etc	Administrateur Système et Réseau Sénior (+10 ans d'expérience)	5 jours ouvrés

En fonction de l'exigence de disponibilité ([paragraphe 8.4](#)), cette montée de version sera associée à la duplication de l'application ou du logiciel tiers pour éviter les interruptions de service, et garantir la disponibilité maximale. Une fois la montée de version réalisée, l'ancienne version pourra être décommissionnée dans le cadre de machines virtuelles « VM ».

Objectifs	Mise à jour d'une version majeure d'une application ou d'un logiciel tiers.
Prérequis	Fourniture d'un document de mise à jour de l'application ou du logiciel tiers, incluant les exigences de sécurité et son paramétrage, par l'équipe projet « EPROJ » de la CNIL.
Profils	Administrateur Système et Réseau (Confirmé ou Sénior) en fonction de la typologie de logiciel (voir tableau ci-dessus)-
Tâches à réaliser	Planification et organisation de l'installation ou de la mise à jour majeure. Mise à jour majeure d'un logiciel tiers existant sur une machine virtuelle « VM » existante ou sur une machine virtuelle « VM » nouvelle. Application du paramétrage applicatif à périmètre équivalent. Application des exigences de sécurités demandées dans le document fourni.
Livrables en sortie	Planning de mise à jour. La montée de version correctement effectuée et configurée sur les plateformes de préproduction et de production. Le dossier d'architecture technique mis à jour et tout document associé à la montée de version majeure de l'application ou du logiciel tiers.
Délai de démarrage	A la notification du bon de commande
Durée de réalisation	A déterminer en fonction de la difficulté de l'installation (voir tableau ci-dessus).

UO13 Etude d'architecture

Ces prestations ponctuelles (UO13.1 et UO13.2) correspondent à une étude d'architecture, répondant à un besoin nouveau, allant au-delà du simple devoir de conseil de l'[article 8.6](#). Elles feront l'objet d'une demande de devis dans les conditions définies à l'article 13.1 du CCAP.

Les prestations relatives aux études d'architecture sont décomposées comme suit :

Référence de la commande	Niveau de complexité	Type d'étude	Profil	Durée
UO13.1	Intermédiaire	Besoin futur	Architecte des SI Confirmé (3 à 10 ans d'expérience)	5 jours ouvrés
UO13.2	Elevé	Migration complète de l'infrastructure	Architecte des SI Senior (+10 ans d'expérience)	5 jours ouvrés

Le titulaire délivre un dossier d'architecture pour un besoin futur, ou une migration de l'infrastructure conservant la continuité des services hébergés et en fonction des exigences techniques et de sécurité (articles 8 et 9 du CCTP).

Une fois l'étude d'architecture réalisée, dans le cadre de la réalisation et de mise en place du besoin, des unités d'œuvres opérationnelles sont commandées : exemple des unités d'œuvres pour la mise en place d'un serveur physiques « UO7 » et « UO8 », d'installation d'une nouvelle machine virtuelle « UO9 », d'installation d'un logiciel tiers « UO10 », etc.

Objectifs	Etude d'architecture.
Prérequis	Expression de besoin détaillée fournie par l'équipe projet « EPROJ ».
Profils	Architecte des Systèmes d'Information, dont le niveau d'expérience est soit : <ul style="list-style-type: none"> - Confirmé (3 à 10 ans d'expérience). - Senior (+10 ans d'expérience).
Tâches à réaliser	Etudes et analyse du besoin. Réunions d'échanges avec l'équipe projet « EPROJ ». Prise en compte de l'architecture et des performances existantes.
Livrables en sortie	Rédaction d'un document ou dossier d'architecture technique conforme au besoin en prenant en compte les exigences techniques et de sécurité. En adéquation avec le marché, proposition d'un devis pour la mise en place opérationnel du besoin en utilisant les unités d'œuvres existantes.
Délai de démarrage	A la notification du bon de commande.
Durée de réalisation	5 jours ouvrés

7.4 Poste 4 - Réversibilité

À la fin du marché, le titulaire doit mettre en œuvre l'ensemble des moyens permettant le transfert des compétences vers la CNIL ou vers le nouveau titulaire.

Il s'agit de préparer le transfert à l'aide de toutes les informations relatives à l'installation, la reprise de l'existant et de l'état actuel des plateformes techniques permettant le transfert des compétences vers la CNIL ou vers un nouveau titulaire.

- Le titulaire doit proposer un plan de reprise de données et des fonctionnalités et tenir compte des délais.
- Ressources nécessaires.
- Actions de maintenance à mener avant la fin du contrat.

Pendant la réversibilité, le titulaire s'engage à :

- Maintenir tous les services en conditions opérationnelles maximales.
- Mettre à disposition des profils nécessaires à cette reprise.
- Fournir toutes les procédures d'installation et d'exploitation.
- Fournir l'inventaire exhaustif des composants de l'application.

Le titulaire met en œuvre des mesures techniques et organisationnelles pour garantir la sécurité des données et des applications qui lui sont confiées, lors du transfert des prestations vers la CNIL ou le nouveau prestataire, en conformité avec les réglementations applicables.

Durant la phase de transfert, l'assurance de la sécurité réside notamment dans :

- La gestion des accès, habilitations.
- Le transfert de responsabilités.
- La fourniture d'informations nécessitant des mesures de protection adaptées.
- La gestion de la continuité de l'activité.

L'unité d'œuvre « UO14 » de ce poste de réversibilité est engagée au plus tard 60 jours ouvrés (3 mois calendaires) avant la fin du marché pour garder une marge de manœuvre sur les délais.

Cette prestation ponctuelle sera commandée :

- ✓ Si le Titulaire du présent marché n'est pas le Titulaire Entrant du marché suivant,
- ✓ En cas de non-reconduction du marché,
- ✓ En cas d'incapacité avérée du titulaire d'exécuter les prestations du marché.

UO14 Réversibilité

Cette unité d'œuvre correspond à la préparation du transfert en amont de la fin du marché et de maintenir en condition opérationnelle et de sécurité les sites institutionnels de « cnil.fr » jusqu'au transfert complet vers le nouveau titulaire.

Objectifs	Fournir toutes la documentation, fichiers, sauvegardes et du site cnil.fr et l'ensemble des plateformes de production et de préproduction.
Prérequis	-
Tâches à réaliser	Installation des sites institutionnels « cnil.fr » et l'ensemble des services
Livrables en sortie	Dossier de réversibilité comprenant : Les fichiers du cœur du CMS Drupal et ses modules additionnels. Les fichiers de configuration. Les sauvegardes des bases de données associées. La sauvegarde des fichiers physiques (médias). Les fichiers des sites « statiques » existants et leurs médias associés. Toutes les procédures d'installation et de mise à jour. Toutes les informations nécessaires pour le transfert des noms de domaines. Dossier d'architecture technique mis à jour. Plan de reprise des données et des fonctionnalités. Toute la documentation permettant la mise en place des plateformes de production et de préproduction par le nouveau titulaire.
Délai de démarrage	À engager au plus tard, 60 jours ouvrés (trois mois calendaires) avant la fin du marché.
Durée de réalisation	20 jours ouvrés

ARTICLE 8 - EXIGENCES TECHNIQUES

8.1 Centre de données (datacenter) et serveurs physiques

Conformément aux dispositions de l'article 13.6 du CCAP, le titulaire s'engage dans le cadre de l'exécution du marché à ce que :

- le centre de données (data center) comprenant l'ensemble des serveurs physiques dédiés ainsi que les solutions de sauvegardes pour le stockage et l'hébergement des données, soient localisés sur le territoire d'un État membre de l'Union européenne,
- cette localisation -soit maintenue sur la durée totale d'exécution du marché. Et à informer sans délai la CNIL de tout changement affectant ladite localisation.

De plus, le ou les centres de données (datacenters) doivent avoir des équipements redondés, avec des alimentations sécurisées permettant de garantir une continuité de service des sites de « cnil.fr » (groupes électrogènes, onduleurs, alimentation des équipements matériels doublées).

Les équipement réseaux et les liens doivent être redondées pour permettre au titulaire de répondre favorablement aux exigences de l'article 8.4 concernant la disponibilité des plateformes.

8.2 Bande passante

Pour déterminer la bande passante nous nous basons sur le fonctionnement nominal du site principal « cnil.fr » qui est notre site à plus fort trafic (voir l'[article 6](#) concernant la volumétrie).

Nous constatons une **utilisation moyenne** de **250 Mbits/sec.** en sortie sur deux ans entre juin 2023 et juin 2025.

Sur la même période nous avons eu **5 pics exceptionnels** : deux de 400 Mbits/sec., un de 500 Mbits/sec., un de 700 Mbits/sec. et enfin un de 900 Mbits/sec.

Pour faire suite à ces mesures, la bande passante minimale demandée est de :

- 1 Gbits / sec, pour la connectivité entre les serveurs et les machines virtuelles « VM » que ce soit sur des sites distants ou non.
- 500 Mbits/sec., pour la connectivité des serveurs vers le réseau Internet, dédiée et garantie.
- Absorption de pics exceptionnels de 1 Gbits/sec. ou supérieur.

8.3 Éco responsabilité du centre d'hébergement

Dans le cadre des démarches de développement durable de la CNIL, le titulaire doit proposer un centre d'hébergement écoresponsable.

Les exigences présentées dans cette liste, sont à minima :

- Recyclage total des déchets liés aux infrastructures (se référer au [paragraphe 9.1](#) pour le cas particulier des supports de stockage hébergeant des données de la CNIL).
- Température du centre d'hébergement supérieure ou égale à 20°C. La température doit être adaptée aux spécifications matérielles des infrastructures (serveurs, composants réseau, onduleurs, générateurs de secours,
- Le PUE (Power Usage Effectiveness) demandé est au maximum de 1.5, qui est calculé avec la formule* suivante :

$$E = \frac{W(\text{datacenter})}{W(it)}$$

***W(datacenter)**, étant la consommation d'énergie totale du centre d'hébergement*

***W(it)**, étant la consommation d'énergie des équipements informatiques (serveurs)*

* la formule de calcul du PUE a été développée par le consortium [The green Grid](#) en 2007.

8.4 Disponibilité

La CNIL ne tolère qu'une interruption mensuelle continue de service inférieur à 1 heure sur incident. La durée se décompte à partir du signalement de l'incident par l'équipe projet « EPROJ » ou l'équipe d'astreinte de la CNIL.

Dans ce cas, le titulaire est tenu de délivrer un rapport d'incident détaillant les interventions et présentant des dispositions préventives pour s'assurer que le problème ne se reproduise plus.

Tous les trimestres, le titulaire présente un taux de disponibilité du service accompagné d'un rapport sur les incidents survenus sur la période trimestrielle précédente.

Le **taux de disponibilité mensuel minimal** demandé est de **99,86 %** pour l'environnement de **production** (l'indisponibilité s'entend par l'inaccessibilité du site aux usagers).

Sur l'environnement de production uniquement et au-delà de la durée maximale d'indisponibilité d'une heure, le titulaire du marché encourt une pénalité de 20% du montant de l'unité d'œuvre « UO5 Suivi opérationnel (infogérance) des environnements » par heure d'indisponibilité, tel que cela est défini au paragraphe 10.2 du CCAP.

Par ailleurs, la CNIL se réserve le droit d'appliquer ces pénalités, voir une résiliation du marché pour faute dans les conditions prévues au CCAP.

Le titulaire du marché met à disposition de la CNIL les moyens de communication, depuis une plateforme de supervision, messagerie ou téléphone, de lui rapporter une anomalie constatée (inaccessibilité, dysfonctionnement ponctuel, dégradation du service, ...) avec des informations concernant le niveau de prise en compte nécessaire (résolution immédiate, urgente, sous 4 heures, dans la journée, etc.)

Tout constat d'anomalie, d'où qu'il provienne, fait l'objet d'un accusé réception transmis aux parties concernées et d'un suivi de résolution notamment lors du retour au fonctionnement nominal. À cette occasion, la fin d'incident mentionne les causes constatées et les actions résolutives entreprises.

Récapitulatif mensuel du temps de disponibilité et du nombre maximal d'indisponibilité :

Plateformes	Disponibilité mensuelle minimale	Nombre max. d'indisponibilités mensuelle	GTI Durée max. avant prise en charge	GTR Durée max. de l'indisponibilité
Production	99,86 %	1	30 minutes	1 heure
Préproduction	98,90 %	2	1 heure	4 heures

Pour le calcul, nous cherchons à connaître le pourcentage de la disponibilité mensuelle des différents sites, en effectuant les calculs à partir du nombre d'heures dans le mois.

Détails et calculs de la disponibilité mensuelle en fonction de la criticité du type de la plateforme :

- Pour tous les sites de **Production** :
 - Période d'intervention : **24 / 7**
 - **GTR de 30 minutes**
 - **GTR de 1 heure**
 - **Disponibilité minimale de la plateforme de production : 99,86 %**

Formule de calcul détaillé :

$$d = 1 - \frac{\text{incidents} \times \text{GTR}}{\text{heures par jour} \times \frac{\text{nb jrs annuel}}{\text{nb mois année}}} = 1 - \frac{1 \times 1}{24 \times \frac{365,25}{12}} = 1 - \frac{1}{730,5} = 0,998631$$

incidents, nombre maximal d'indisponibilités mensuelles

GTR, étant la Garantie du Temps de Rétablissement en heure

heures par jour, étant le nombre d'heure dans une journée

nb jrs annuel, étant le nombre de jours moyen dans une année (avec les années bissextiles)

nb mois année, étant le nombre de mois dans une année

Pour tous les sites de **Préproduction** :

- Période d'intervention : jours ouvrés, soit du lundi au vendredi : **9^h – 18^h**
- **GTR de 1 heure**
- **GTR de 4 heures**
- **Disponibilité minimale de la plateforme de Préproduction : 98,90%**

Formule de calcul détaillé :

$$d = 1 - \frac{\text{incidents} \times \text{GTR}}{\text{heures par jour} \times \frac{\text{nb jrs annuel}}{\text{nb mois année}}} = 1 - \frac{2 \times 4}{24 \times \frac{365,25}{12}} = 1 - \frac{8}{730,5} = 0,989049$$

incidents, nombre maximal d'indisponibilités mensuelles

GTR, étant la Garantie du Temps de Rétablissement en heures

heures par jour, étant le nombre d'heure dans une journée

nb jrs annuel, étant le nombre de jours moyen dans une année (avec les années bissextiles)

nb mois année, étant le nombre de mois dans une année

Pour ses sites principaux de production, « www.cnil.fr » et « linc.cnil.fr », l'équipe projet « EPROJ » utilise un service d'analyse tiers, lui permettant d'obtenir les métriques « GTR » en temps réel, et sur un mois glissant.

L'équipe projet « EPROJ » se réserve le droit de comparer cette métrique « GTR » avec celle fournie par le titulaire dans le cadre de sa prestation du suivi opérationnel des environnements « UO5 ».

8.5 Cartographie des systèmes d'information

Le titulaire dispose d'un inventaire et d'une cartographie des systèmes d'information dont il a la charge et doit les maintenir, selon les préconisations de l'ANSSI issues du guide « [cartographie des systèmes d'information](#) ».

L'inventaire et la cartographie comprennent également la liste des « briques » matérielles et logicielles utilisées, ainsi que leurs versions exactes avec leur configuration. Ils comportent une base de données de configuration. La cartographie est livrée à la demande de l'équipe projet « EPROJ » une fois par an.

8.6 Devoir de conseil

Le titulaire est tenu à une obligation permanente de conseil et de mise en garde, relative aux matériels, systèmes d'exploitation, logiciels tiers installés dans le cadre de la « TMA » et aux prestations fournies à la CNIL.

Dans ce cadre, le titulaire notifie à la CNIL toute information permettant d'améliorer le niveau de sécurité du système d'information et signaler les difficultés et risques encourus sur les effets de bord que certains choix peuvent entraîner.

Dans l'hypothèse où le titulaire ne respecte pas cette obligation, il ne peut se prévaloir d'une incohérence dans le marché pour s'exonérer de ses obligations contractuelles.

8.7 Plan de reprise d'activité

Le titulaire doit définir un plan de reprise d'activité qui assurera la reconstruction des environnements et la reprise de tous les services en cas de défaillance ou de sinistre majeur.

Le titulaire doit mettre en place :

- Un mode de fonctionnement dégradé afin d'assurer les services indispensables, plus précisément l'accès aux sites « www.cnil.fr » et « linc.cnil.fr ».
- Les procédures et les moyens de reprise d'activité (redondances, sauvegardes, etc.).

8.8 Journalisation

Le mécanisme de journalisation mis en place par le titulaire comprend à la fois la journalisation des actions des administrateurs et des requêtes des usagers vers les sites web.

La journalisation applicative doit comprendre au moins l'horodatage de l'accès (date et heure), la ressource « URL » accédée, l'adresse IP du client et un entête « User-Agent ». La durée de rétention du mécanisme de journalisation est au moins pour une période d'un an.

Les modalités de cette journalisation sont abordées au [paragraphe 9.3](#) alinéa m.

8.9 Sauvegardes

Le titulaire doit mettre en place un système de sauvegarde permettant la sauvegarde des données de la prestation hébergées sur les serveurs du titulaire conformément aux besoins de sauvegarde exprimés par la CNIL.

Les modalités de gestion de ces sauvegardes sont abordées au [paragraphe 9.3](#) alinéa f.

8.10 Gestion des flux et filtrages par adresses IP

Toute ouverture d'un flux entrant ou sortant des environnements doit faire l'objet d'une validation de la CNIL, entre le RSSI du titulaire et l'équipe projet « EPROJ ». Les flux uniquement nécessaires au fonctionnement des sites déposés et de ses services associés sont autorisés.

Le titulaire doit maintenir un tableau de suivi recensant tous les flux entrants et sortants de l'environnement de la CNIL.

Le titulaire doit mettre en place une politique de filtrage par adresses IP pour les plateformes de Préproduction, depuis la plateforme d'hébergement et des adresses que l'équipe projet « EPROJ » fournira. La politique est également validée par le RSSI de la CNIL.

En cas de besoin exceptionnel, et à la demande de la CNIL, un tunnel VPN respectant les conditions de sécurité définie par l'équipe projet « EPROJ », pourra être proposé par le titulaire afin de sécuriser les échanges entre les locaux de la CNIL et la plateforme d'hébergement (détaillé dans le cadre des astreintes dans le [paragraphe 9.12](#)).

8.11 Maintien en condition de sécurité

En complément du traitement des obsolescences définie à l'article 40.1 du CCAG-TIC, ajout de précisions sur le **traitement des obsolescences** de tous les composants, permettant de clarifier le maintien en condition de sécurité « MCS » :

a. Matériels physiques

Le titulaire utilise uniquement matériel d'infrastructures sous garantie et à jour prenant en compte les différentes failles de sécurité corrigées sur les dits matériels.

Les matériels « obsolètes » qui ne sont plus supportés par l'éditeur doivent faire l'objet d'une migration avec une montée de version majeure, sauf indication contraire de la CNIL, principalement pour des raisons de compatibilité.

b. Systèmes d'exploitation et Hyperviseurs

Le titulaire utilise uniquement des systèmes d'exploitation ou des hyperviseurs de type 1 maintenus suivant leur cycle de vie.

- Sauf avis contraire de la CNIL, principalement pour des raisons de compatibilité logicielle, la mise à jour doit être réalisée pour les hyperviseurs de type 1 (actuellement ProxMox) et les systèmes d'exploitation des machines virtuelles « VM » (Debian) :
 - Obsolètes qui ne sont plus supportés par l'éditeur (fin de vie).
 - Rapidement pour ceux qui sont dans la phase « LTS », de support à long terme.

Pendant toute la durée du marché, le titulaire s'engage à maintenir les hyperviseurs de type 1 (actuellement ProxMox) ainsi que les systèmes d'exploitation des machines virtuelles « VM » (Debian) à jour vers des solutions maintenues.

c. Logiciels tiers installés à la demande de la CNIL

À la demande la CNIL, ou dans le cadre de la « TMA », le titulaire installe les logiciels tiers en utilisant son devoir d'alerte dans le cas des demandes d'installation de logiciels tiers obsolètes.

Les logiciels tiers sont maintenus par la « TMA » qui demande régulièrement au titulaire d'opérer des livraisons sur l'infrastructure.

Pour des raisons de compatibilité logicielle, et pour une durée temporaire avant une migration de version, l'équipe projet « EPROJ » de la CNIL s'octroie le droit de demander au titulaire l'installation de logiciels tiers obsolète. Cette demande exceptionnelle n'intervient que dans un cas précis de migration de version et pour une durée temporaire.

Pendant toute la durée du marché, le titulaire s'engage à maintenir les logiciels tiers à jour vers des solutions maintenues.

d. Correctifs de sécurité

La CNIL représentée par l'équipe projet « EPROJ », définit les fréquences des livraisons en coordination avec les équipes d'exploitation du titulaire, en fonction des différentes criticités des vulnérabilités concernées. Le titulaire s'assure que l'application des correctifs de sécurité ne modifie pas les performances ou les fonctionnalités du système, en modifiant celui-ci à ses frais, pour maintenir le niveau de performance suite à l'application des correctifs de sécurité.

Une vérification d'aptitude (VA) ou une vérification de service régulier (VSR) peut être refusée si les mises à jour de sécurité des composants ne sont pas réalisées depuis un délai supérieur à 3 mois.

8.12 Mise à jour des plateformes

Le titulaire du marché entreprend des mises à niveau de ces composants techniques « CT » utilisés par les plateformes de production et de préproduction, s'il le juge utile, à condition qu'elles n'interfèrent pas avec le bon fonctionnement des services et logiciels hébergés.

Toute intervention de maintenance opérée sur les plateformes de production doit préalablement être reproduite sur la plateforme de préproduction. En toute bonne logique l'opération devrait avoir été préalablement menée sur la plateforme de préproduction.

En cas d'effets suspectés, il s'assure formellement de l'accord de la CNIL et se soumet à la procédure définie, et plus particulièrement aux conditions d'un retour à la situation antérieure que ce soit sur les plateformes de pré production ou de production

Toute manipulation non autorisée expressément par la CNIL, précisément par l'équipe projet « EPROJ », est susceptible d'entraîner la résiliation pour faute dans les conditions définies infra en cas de pertes de données ou de conséquences graves sur le fonctionnement des sites institutionnels.

Dans cette exigence de mise à jour des composants techniques « CT », différentes prestations sont déclinées en unité d'œuvre « UO6 » pour les mises à jour mineures dans le cadre du maintien en condition de sécurité « MCS » et l'unité d'œuvre « UO12 » pour les versions majeures.

8.13 Licences logicielles

Le titulaire s'assure de la bonne validité des licences des logiciels et des systèmes d'exploitation qu'il met à disposition de son personnel ou de l'institution dans le cadre de ce marché.

Les logiciels tiers utilisés par la CNIL pour sa visibilité sur le réseau Internet sont des CMS et outils open source du type : Varnish, HA Proxy, Memcached, Maria DB « Galera Cluster », Apache, nginx, Apache Solr, PHP, Ansible, Matomo, etc.

L'équipe projet « EPROJ » et la CNIL, encourage vivement le titulaire d'utiliser des logiciels open source sous licence GPL, GNU, BSD, Apache, etc.

ARTICLE 9 - EXIGENCES DE SECURITE

9.1 Gestion des biens

a. Séparation des données de la CNIL et des données d'autres clients

Le titulaire conserve et traite les données de la CNIL de manière séparée de ses propres données ou de données d'autres clients du titulaire. Le titulaire doit restreindre l'accès aux données de la CNIL suivant le principe de restriction au besoin d'en connaître.

b. Protection de la documentation de l'administration sur support papier

Le titulaire assure la protection de la documentation de l'administration sur support papier au sein des locaux, en la stockant dans des armoires ou des coffres fermés à clé/code par exemple, et sa destruction à la fin de la prestation.

c. Modalités d'échanges d'informations

Le titulaire garantit que les modalités de stockage et d'échanges d'informations par mail permettent d'en assurer la confidentialité et l'intégrité.

d. Échange de supports physiques

Le titulaire garantit que les supports échangés (clés ou disques externes) ou à connecter sur un SI de l'administration n'intègrent aucun code malveillant et ont fait l'objet d'un test d'innocuité positif au moyen d'une attestation à fournir à l'administration avant l'échange effectif des supports.

e. Supports de stockage hébergeant des données de la CNIL

Le titulaire conserve en lieu sûr les supports de stockage de données en fin de vie (supports amovibles ou disques serveurs) hébergeant des données de la CNIL, en attendant de procéder à leur effacement de bas niveau, sans récupération possible avec quelque logiciel que ce soit, ou à leur destruction avec des moyens adaptés visant à s'assurer qu'aucune donnée ne puisse être récupérée (voir le [paragraphe 8.3](#) pour le recyclage total des matériels).

Le cas échéant, le titulaire ne met pas au rebut ou ne fait pas emporter par une société de maintenance, ou encore ne réutilise ces supports de sauvegarde à d'autres fins que celles prévues initialement sans l'autorisation expresse de la CNIL.

f. Maintien à jour et mise à disposition des données relatives à la prestation

Le titulaire maintient à jour et est en mesure de mettre à disposition de la CNIL toutes les données relatives à la prestation.

g. Maintien à jour et mise à disposition des documents techniques relatifs à la prestation

Le titulaire maintient à jour et est en mesure de mettre à disposition de l'administration tous les documents techniques relatifs à la prestation. Le titulaire fournit systématiquement toute la documentation technique créé dans le cadre de la prestation à l'administration.

9.2 Sécurité physique

a. Changement de localisation géographique de l'hébergement

En cas de changement de localisation de l'hébergement, quand bien même celui-ci reste conforme à la localisation définie au [paragraphe 8.1](#) concernant la localisation du centre de données, le titulaire en informe préalablement l'administration.

b. Hébergement de données

À la première demande de l'administration, le titulaire identifie tous les sous-traitants techniques hébergeant ou stockant les données et leurs copies, utilisées ou échangées en cours de marché ainsi que leur localisation.

c. Contrôle d'accès physique aux bâtiments du titulaire

Les bâtiments du titulaire hébergeant son personnel dans le cadre de la prestation doivent être équipés d'un dispositif de contrôle d'accès individuel. Les accès physiques aux bâtiments en question doivent être restreints aux stricts besoins opérationnels des différentes populations présentes dans les locaux du titulaire.

Le titulaire dispose d'une procédure de gestion des accès physiques aux bâtiments du titulaire. Celle-ci précise au minimum les modalités de gestion des demandes et de suppressions d'accès.

Le titulaire dispose d'une organisation relative à la gestion et au suivi des autorisations d'accès pour les bâtiments du titulaire.

d. Contrôle des accès aux ressources techniques du titulaire

Le titulaire garantit que les accès physiques aux salles informatiques sont strictement restreints aux besoins opérationnels des différentes populations présentes sur les sites utilisés dans le cadre de la prestation. Les accès sont équipés d'un dispositif de contrôle d'accès individuel.

Le titulaire dispose d'une procédure de gestion des accès physiques aux locaux techniques du titulaire. Celle-ci précise au minimum les modalités de gestion des demandes et suppressions d'accès.

Le titulaire dispose d'une organisation relative à la gestion et au suivi des autorisations d'accès pour les locaux hébergeant des ressources de l'administration et les équipements de sûreté.

e. Protection intrusion physique des locaux techniques du titulaire

Les locaux du titulaire qui hébergent ses ressources techniques (serveurs, équipements informatiques, équipements réseaux / télécoms, etc.) sont équipés de moyens de :

- Protection contre l'intrusion et les effractions ;
- Détection d'intrusion et d'effraction reliés à un système de surveillance centralisé ;
- Réaction en cas d'intrusion ou d'effraction.

Ces équipements sont opérationnels 24h/24h et 7j/7j. Les moyens de protection sont adaptés aux moyens de détection et de réaction.

En particulier, toutes les portes donnant sur l'extérieur du bâtiment ont une méthode automatique de détection d'ouverture. De plus, toute fenêtre raisonnablement accessible est protégée contre les intrusions.

f. Accompagnement des visiteurs

Le titulaire dispose d'une procédure spécifique à l'accueil des personnes étrangères à l'organisme. Il dispose également d'une procédure pour l'accès des véhicules au site.

En particulier, les personnes extérieures nécessitant un accès aux salles hébergeant des ressources informatiques (techniciens, visiteurs, maintenance, etc.) sont accompagnées par une personne habilitée.

g. Protection des plateaux mutualisés

En cas de mutualisation de ses plateaux, le titulaire met en place les mesures pour protéger les espaces attribués pour la prestation effectuée pour l'administration (accès au poste par badge, blocage session automatique après un certain temps d'inutilisation, câble de sécurité pour le matériel fourni par l'administration, etc.).

h. Étanchéité physique des ressources informatiques

Les salles hébergeant les ressources informatiques utilisées dans le cadre de la prestation ne partagent pas le même bâtiment avec d'autres fonctions, particulièrement des bureaux n'appartenant pas à l'organisation. Si l'espace doit être mutualisé pour des raisons économiques, alors la salle hébergeant des ressources informatiques utilisées dans le cadre de la Prestation de la CNIL n'a pas de murs adjacents à d'autres bureaux.

Le titulaire met en place des moyens garantissant une étanchéité physique ou logique (par exemple avec des VLAN dédiés) entre les infrastructures dédiées à la CNIL de celles des autres clients au sein du centre de données.

9.3 Sécurité des réseaux et exploitation

a. Cloisonnement des environnements informatiques

Le titulaire est garant du bon cloisonnement (physique ou logique) des environnements utilisés dans le cadre de la prestation.

b. Sécurisation des flux d'administration

Le titulaire chiffre tous les flux d'administration (système et fonctionnelle) par des procédés fiables et à l'état de l'art garantissant la confidentialité et l'intégrité des données. Par ailleurs, les postes d'administration utilisés pour la prestation doivent être dédiés et n'avoir accès ni à Internet, ni aux infrastructures bureautiques du titulaire.

c. Règles de sécurité et d'exploitation

L'installation, l'exploitation et l'administration des moyens mis en œuvre dans le cadre des prestations sont conformes à l'état de l'art pour les règles de sécurité et d'exploitation.

d. Anti-virus opérationnel et à jour

Le titulaire s'assure de la bonne installation et mise à jour d'un logiciel anti-virus sur tous les serveurs dont il est responsable dans le cadre de la prestation. La désactivation, même temporaire, d'un antivirus sur un serveur utilisé dans le cadre de la prestation devra avoir été préalablement notifiée à la CNIL.

e. Gestion des mises à jour

Le titulaire gère les mises à jour et l'application des correctifs de sécurité et des mises à jour antivirus, pour assurer le maintien en condition opérationnelle de l'ensemble de ses équipements pour les services fournis à la CNIL.

f. Sauvegarde des données

Le titulaire propose la mise en place d'un système de sauvegarde dématérialisé, ou sous la forme de support physique, sur deux sites au minimum et dans un environnement sécurisé.

Parmi ces sauvegardes, une sauvegarde devra être :

- Isolée hors ligne des serveurs actifs.
- Conservée physiquement sur un lieu géographique distinct de celui où se trouve les serveurs actifs.

Dans le cas où le titulaire conserve les sauvegardes sur support physique, le titulaire les protège en les stockant dans un coffre étanche et ignifuge.

À minima, la sauvegarde des environnements de préproduction et de production est quotidienne, sous la forme d'une sauvegarde incrémentale, et mensuelle sous la forme d'une sauvegarde complète. Une antériorité de six mois est conservée.

À la demande de la CNIL, une restitution doit pouvoir être produite sous 4 heures ouvrées.

À la demande, et sous 48 heures ouvrées, un exemplaire de la sauvegarde la plus récente doit pouvoir être fournie, sous la forme d'un conteneur sécurisé.

Le contenu de ce conteneur sécurisé comporte la sauvegarde des fichiers en clair, pour l'ensemble de la solution de gestion de contenu :

- Le code source et les modules des sites Drupal.
- Les fichiers de paramétrage et de configuration.
- Le contenu des différentes bases de données afférentes (exportation en clair).
- Ensemble des fichiers « médias » du CMS (PDF, JPEG, PNG, etc.)

Un défaut de restitution des données est susceptible d'entraîner une résiliation pour faute dans les conditions définies infra. Les modalités d'exécution de cette prestation sont définies par le titulaire dans son offre technique.

Des tests périodiques (a minima semestriels) de restauration des sauvegardes effectuées sur les données contenues dans les serveurs du titulaire sont formalisés et effectués.

g. Comptes individuels

Le titulaire s'assure que son personnel devant accéder à des ressources informatiques ou réseau dans le cadre de la prestation (qu'elles soient hébergées chez le titulaire ou chez la CNIL) dispose d'un compte individuel qui peut être :

- Soit un compte nominatif qui lui est personnel et qui ne sera utilisé uniquement par cette personne tout au cours de la vie du compte ;
- Soit un compte individualisé qui pourra être attribué à des personnes différentes au cours de la vie du compte tout en n'étant toujours attribué qu'à une seule personne à la fois.

h. Comptes obsolètes ou par défaut

Le titulaire s'assure de la suppression de tous les comptes inutiles ou obsolètes. De même, les mots de passe par défaut d'usine devront être systématiquement modifiés.

i. Comptes techniques

Dans le cadre de la cartographie du système d'information prévue au [paragraphe 8.5](#), le titulaire doit fournir un inventaire justifié des comptes techniques (le compte propriétaire du fichier de la base de données, des données des serveurs web, ...) nécessaires au fonctionnement du système.

j. Recensement des comptes d'accès

Le titulaire tient à jour la liste exhaustive des comptes d'accès au SI de la CNIL existants ainsi que des rôles et privilèges qui y sont associés.

Il fournit cette liste à la CNIL sur demande de l'équipe projet « EPROJ » ou du RSSI.

Le titulaire effectue et formalise une revue périodique des comptes d'accès aux serveurs et autres ressources du titulaire utilisées dans le cadre de la prestation.

k. Politique du moindre privilège

Le titulaire s'assure que tous les comptes (accès Windows et autres...) des intervenants dans le cadre de la prestation sont habilités selon le principe du moindre privilège.

l. Attaques par force brute sur les secrets d'authentification

Les moyens d'authentification mis en place par le titulaire (sur ses serveurs, applications et postes de travail) incluent une protection contre les attaques par force brute sur les mots de passe et les clés de chiffrements (secrets d'authentification).

m. Journalisation des actions

Le titulaire conserve de manière exploitable, sur une durée d'un an à partir de l'événement journalisé, la trace des actions d'administration ou de connexion aux équipements à des fins d'administration, des requêtes des utilisateurs vers les sites hébergés et des erreurs rencontrées par les logiciels configurés sur les plateformes.

Les enregistrements des journaux se rapportant aux actions d'administration ou de connexion aux équipements à des fins d'administration doivent être horodatés (date et heure), nominatif (auteur) et incluant le détail de l'opération réalisée.

Les enregistrements des journaux se rapportant aux requêtes des utilisateurs vers les sites hébergés doivent être horodatés (date et heure) et au moins inclure l'adresse IP de l'utilisateur, l'URL accédé, ainsi que les entêtes « User-Agent » et « Referer ».

Les enregistrements des journaux se rapportant aux erreurs rencontrées par les logiciels doivent être horodatés (date et heure) et inclure une description de l'erreur.

Les journaux doivent être protégées contre toute perte, altération ou modification par des moyens adaptés. Les journaux doivent par ailleurs être horodatés selon une référence horaire commune à l'ensemble des équipements des plateformes.

Ces journaux pourront être consultés par la CNIL. Dans le cas où une demande de journaux est transmise au titulaire par la CNIL, les journaux nécessaires à l'action de la CNIL seront transmis par le titulaire sous 48 heures ouvrées et sous la forme d'un conteneur sécurisé.

n. Gestion des traces

Le titulaire prévoit dans sa procédure de traitement d'incident un chapitre sur la préservation des traces en cas de suspicion d'attaque.

Cette procédure pourra également comprendre une section concernant la préservation des traces volatiles. Une trace volatile est une trace potentiellement utile pour l'analyse forensique d'une attaque informatique mais qui ne peut pas, par nature, être journalisée (contenu de la RAM, du swap, journal des transactions d'un système de fichier, divers dates liées aux fichiers, clés de registres...)

La procédure établit comment limiter au maximum les activités malveillantes ou accidentelles susceptible de détruire les traces.

o. Politique de mot de passe

Le titulaire respecte les recommandations de sécurité de la CNIL relatives aux mots de passe, notamment la délibération CNIL n° 2022-100 du 21 juillet 2022 portant adoption d'une recommandation relative aux mots de passe et autres secrets partagés, pour l'ensemble des comptes d'accès utilisateurs et administrateurs aux postes de travail sous la responsabilité du titulaire.

Si vous avez besoin de critères précis pour les secrets d'authentification, vous pouvez vous reporter aux critères C32.09 et suivants de :

https://www.cnil.fr/sites/cnil/files/2024-12/projet_de_referentiel_certification_des_sous-traitants.pdf

9.4 Sécurité du poste de travail

a. Protection contre le vol des postes de travail

Le titulaire met en place des mécanismes de protection pour prévenir le vol des postes de travail. Le titulaire met notamment en place des câbles antivol de façon systématique.

b. Chiffrement du poste de travail

Une solution de chiffrement, si possible qualifiée, est mise à disposition par le titulaire à ses intervenants afin de chiffrer les données stockées sur les postes de travail ou les supports amovibles.

c. Utilisation des IA génératives

Le titulaire s'engage à ne pas transmettre des données personnelles ou techniques propres à l'infrastructure des sites de la CNIL à des IA génératives hébergées sur des services tiers au titulaire, comme par exemple : Claude, ChatGPT, Copilot, DeepSeek, Gemini, Grok, Mistral « Le Chat » ou Perplexity (liste non exhaustive).

Dans le cadre de génération de documents ou de comptes rendus, l'utilisation d'IA génératives locales avec ou sans utilisation de GPU embarqués est autorisée dans la mesure où le titulaire s'engage à ne transmettre des données personnelles ou techniques propres à l'infrastructure des sites de la CNIL entre l'IA générative locale et un autre service d'IA générative hébergée sur des services tiers au titulaire.

9.5 Traitement des incidents

a. Supervision et remontée d'alerte

Le titulaire doit mettre en place des sondes de détection d'incidents de sécurité et doit disposer d'un système de remontée d'alertes à l'administration, afin de détecter tout comportement anormal sur un périmètre SI lié à la prestation (ex : montée en charge du réseau).

b. Enregistrement et traçabilité et gestion des incidents de sécurité

Le titulaire assure l'enregistrement et la traçabilité des incidents de sécurité et dispose d'un processus formalisé et opérationnel de gestion des incidents de sécurité sur son domaine SI.

c. Traitement des incidents de sécurité

Le titulaire contacte les interlocuteurs sécurité de l'administration désignés pour signaler tout incident de sécurité SI susceptible d'affecter les données ou le SI de l'administration. De plus :

- Si cet incident a lieu sur le SI de l'administration, le titulaire participera à la demande de l'administration au traitement de l'incident.
- Si cet incident a lieu sur le SI du titulaire, le titulaire autorisera l'administration ou un tiers désigné à participer au traitement de l'incident (si l'administration le souhaite).

En outre, des réunions périodiques d'analyse post-incident devront être planifiées avec l'administration (traitement des causes profondes).

d. Base de connaissance

Le titulaire capitalise les procédures de résolution des problèmes techniques récurrents dans une base de connaissance dédiée qu'il fournit à l'administration sur demande.

9.6 Environnement de travail sécurisé et traçabilité des actions

Le Référentiel Général de Sécurité (RGS) a été élaboré conjointement par l'ANSSI et le Secrétariat général pour la modernisation de l'action publique (SGMAP) pour sa version 2, publié par arrêté du 13 juin 2014. Il contient un ensemble de règles et de recommandations applicables aux téléservices des administrations.

La CNIL doit se conformer au RGS et cette conformité se traduit par l'application d'une part, de règles relatives au cadre pour gérer la sécurité des systèmes d'information et, d'autre part, de règles relatives aux fonctions de sécurité mises en œuvre.

En particulier, les moyens d'authentification gérées par le titulaire et permettant d'accéder aux plateformes de production et de préproduction devront être conservées de manière sécurisée. En particulier, la CNIL recommande que ces moyens d'authentification soient conservés sur des supports chiffrés, avec un chiffrement conforme RGS.

Le titulaire doit recourir à des moyens d'authentification multi-facteur, notamment pour les accès distants des administrateurs aux plateformes en utilisant un « VPN ».

9.7 Sécurité des serveurs

Les serveurs des plateformes de production et de pré production sont sécurisés conformément à l'état de l'art. En particulier, le titulaire se conforme aux à la Politique de Sécurité des Systèmes d'Information de l'État (PSSIE), ainsi qu'aux recommandations de la CNIL et de l'Agence Nationale de la Sécurité des Systèmes d'Information (ANSSI). Celles-ci devront être respectées et toute dérogation à ces règles et recommandations devra faire l'objet d'une autorisation du chef de projet ou du RSSI de la CNIL.

En particulier, les serveurs sont tenus à jour. Les vulnérabilités connues sont corrigées selon la procédure décrite au paragraphe 8.11 alinéa d.

9.8 Protection contre les dénis de service distribués

Le titulaire du marché propose à la CNIL un ou plusieurs outils permettant de lutter efficacement contre les attaques par « déni de service » simples ou distribués (attaques DDoS), de type volumétrique et applicatif.

9.9 Surveillance des incidents et des vulnérabilités

Pour les prestations, produits et services fournis dans le cadre du marché, le titulaire met à disposition un dispositif d'information dédié à la sécurité informatique (notamment flux RSS/ATOM, liste de diffusion par courriel ou autre).

Ce dispositif vise à tenir la CNIL informé des événements et changements impactant la sécurité, notamment liés à la connaissance d'une vulnérabilité impactant le système (annonce de correctif, attaque en cours, violation de données à caractère personnel si le traitement de données est sous-traité au titulaire), et des mesures correctives ou conservatoires à appliquer.

Le titulaire doit informer sans délai l'équipe projet « EPROJ » et la CNIL, et plus particulièrement son RSSI de toute détection d'incident.

Le titulaire doit intégrer les correctifs de vulnérabilités selon la procédure décrite au [paragraphe 8.11](#) alinéa d.

En cas d'incidents de sécurité (exploitation de vulnérabilité, fuite de données, etc.) ciblant les plateformes de production ou de préproduction, le titulaire doit produire à la CNIL tous les éléments nécessaires à la compréhension de l'incident (éléments à l'origine de la vulnérabilité, défaillances, données ayant fuité, mesures prises immédiatement et mesures planifiées).

9.10 Supervision et administration des plateformes

Le titulaire présente dans son offre l'organisation mise en œuvre assurant la supervision « 24/7 » des plateformes de production et de préproduction afin de prévenir les failles de sécurité, détecter la dégradation des performances, envisager et appliquer les mesures correctives.

Le titulaire offre à la CNIL un accès direct à un outil sécurisé de supervision affichant entre autres les périodes d'indisponibilité, les incidents, les charges des serveurs, etc.

Les charges des serveurs restituent celles relatives : au processeurs (CPU), l'occupation de la mémoire (RAM), le volume de mémoire « swap », les espaces disques, la bande passante, le nombre de requêtes sur la base de données, le temps de réponse aux requêtes, etc.

L'administration opère en outre sur l'adaptation de la configuration technique aux besoins (espaces mémoire, adaptation des volumes, surveillance de la réplication, adaptation des débits, ...)

9.11 Audit de sécurité

La CNIL peut effectuer ou faire effectuer un audit de sécurité auprès du titulaire, ou le cas échéant, de ses sous-traitants afin de s'assurer de la mise en place effective du niveau de sécurité requis par la CNIL.

Le titulaire est informé 15 jours calendaires à l'avance (date de l'audit, modalités financières pour la CNIL et le titulaire, etc.)

La CNIL, ou l'organisme mandaté à cette fin, peut alors, pendant une période de trois mois à compter de la fin ou de la résiliation du marché, exercer un contrôle dans les locaux du titulaire et, le cas échéant, dans ceux de ses sous-traitants afin de vérifier que les dispositions en matière de destruction des données ont été effectivement appliquées.

9.12 Obligations relatives aux astreintes

a. Astreinte

Le titulaire prévoit un dispositif garantissant les services d'astreinte nécessaires à la continuité de service et à la tenue des engagements définis au [paragraphe 8.4](#) concernant la disponibilité. Les cas de force majeure doivent également être couverts.

b. Sécurisation des flux d'astreinte

Le titulaire met en œuvre un tunnel sécurisé avec chiffrement des communications (ex. VPN IPSec) pour la connexion à distance aux réseaux utilisés dans le cadre de la Prestation (que ce soient ceux du titulaire, ceux de la CNIL ou les deux). Le personnel du titulaire devra explicitement lancer la connexion et s'authentifier nominativement pour obtenir l'accès aux SI hébergés par le titulaire à distance (connexion authentifiée non permanente).

c. Chiffrement des postes d'astreinte

Le titulaire met en œuvre le chiffrement intégral du ou des postes de travail utilisés en astreinte.

d. Authentification multi facteur

Le titulaire rend obligatoire l'utilisation de l'authentification multi facteur (hors SMS) au poste de travail utilisé en astreinte si celui-ci est en dehors des locaux du titulaire.

e. Connexion distante

Le titulaire restreint la connexion distante aux personnels d'astreinte, aux horaires d'astreintes définis (ex. connexion non autorisée en horaires ouvrés), et aux ressources nécessaires en astreinte uniquement.

f. Suivi des interventions

Le titulaire est capable de fournir à la CNIL, sur demande, la liste de son personnel avec son nom, prénom et adresse mail, qui est intervenu à un instant donné sur les services hébergés chez le titulaire dans le cadre d'une astreinte.

9.13 Obligations spécifiques liées à la prestation d'hébergement

a. Exigences liées à la maintenance

Dans le cadre d'une opération de maintenance, le titulaire s'engage à chiffrer ou effacer de manière sécurisée toutes les données avant l'envoi en maintenance externe de toute ressource informatique opérée pour la CNIL.

Si les données ne sont pas sensibles, et si elles ne peuvent être chiffrées ou effacées en totalité (par exemple : disque dur défectueux sous garantie), l'envoi en maintenance externe ne peut se faire que sous couvert d'un engagement de confidentialité de la part du mainteneur, ou bien dans le cadre d'une réparation sur site en présence d'un membre de l'équipe locale chargée des systèmes d'information.

Si les données sont sensibles et si elles ne peuvent être chiffrées ou effacées en totalité, l'envoi en maintenance externe est alors de ce fait interdit.

Pour toutes les opérations liées à la maintenance externe, concernant des données stockées sur toute ressource informatique opérée pour la CNIL, l'équipe projet « EPROJ », incluant le RSSI, devra être informée.

9.14 Certification du titulaire

a. Certification ISO/IEC 27001:2022 ou équivalent

À titre de recommandation (mais non obligatoire), le titulaire pourra démontrer la maîtrise de son système de management de la sécurité de l'information (SMSI) via une certification ISO/IEC 27001:2022 ou équivalente.

Cette certification ISO/IEC 27001:2022 sera considérée comme pertinente si elle couvre :

- Le périmètre du système d'information du titulaire.
- Ou le périmètre des services d'hébergement objet du présent marché.

ARTICLE 10 - ORGANISATION, PILOTAGE ET SUIVI DES PRESTATIONS

10.1 Organisation de l'équipe projet « EPROJ » de la CNIL

La CNIL dispose d'une équipe projet « EPROJ » composée de chefs de projets de la DSI, la direction des systèmes d'information, d'agents au sein SCOM, le service de la communication, le responsable de la sécurité des systèmes d'information, RSSI, ainsi que le délégué à la protection des données, DPO de la CNIL, pour tout ce qui concerne la conformité au RGPD.

En dehors de la hiérarchie de la DSI de la CNIL et de son RSSI, un interlocuteur unique est désigné pour s'assurer de la bonne exécution des prestations. Le chef de projet de projet désigné, permettra également de fluidifier la communication entre le titulaire et d'autres prestataires.

10.2 Organisation de l'équipe projet du titulaire

Le titulaire propose dans son offre une équipe d'intervenants qui maîtrisent les technologies utilisées dans le cadre de ce marché.

Le titulaire désigne un interlocuteur principal expérimenté pour assurer le pilotage de l'ensemble des prestations.

Ponctuellement, pour la réalisation d'une prestation, le titulaire peut désigner un interlocuteur différent de l'interlocuteur habituellement désigné pour la réalisation de ladite prestation.

Pendant toute la durée du marché, le titulaire sensibilise l'équipe projet ainsi que tout personnel intervenant dans le cadre des prestations, à la sécurité de l'information, des systèmes d'information en respectant scrupuleusement les exigences de sécurité du présent marché.

10.3 Pilotage et suivi des prestations

Le pilotage et le suivi des prestations est effectué conjointement par les équipes projets des deux parties, c'est-à-dire le titulaire et l'équipe projet « EPROJ » de la CNIL.

Le pilotage des réunions durant toute la durée du marché est assuré par l'équipe projet du titulaire.

Chacune des réunions présentées ci-dessous feront l'objet d'un compte rendu :

- Réunion de lancement avec présentation des équipes projet.
- Réunions d'avancement hebdomadaires pendant la mise en place des plateformes et des environnements, incluant la reprise de l'existant.
- Réunion de fin de marché pour la réversibilité.

Le suivi des prestations, sa recette ainsi que sa validation est assurée par l'équipe projet « EPROJ » de la CNIL dans les conditions définies à l'article 9 du CCAP.

ARTICLE 11 - CONFORMITE RGAA

Dans le cadre de l'exécution du marché, le titulaire s'engage à respecter les exigences du Référentiel Général d'Amélioration de l'Accessibilité (RGAA) version 4.1 en vigueur.

A ce titre, tous les livrables numériques des documents produits sous les logiciels Microsoft (Word, Excel, PowerPoint) ainsi que les documents Adobe PDF (Portable Document Format) dans le cadre de l'exécution des prestations du marché devront être accessibles aux personnes en situation de handicap, conformément aux obligations fixées par l'article 47 de la loi n°2005-102 du 11 février 2005.

À ce titre, les livrables doivent :

- Respecter au minimum le niveau de conformité AA du RGAA 4.1 applicable au moment de la remise ;
- Répondre aux critères applicables du référentiel, tels que :
 - Structure correcte des pages (titres, listes, tableaux, etc.).
 - Présence d'alternatives textuelles aux contenus non textuels (images, graphiques, icônes...)
 - Contrastes de couleurs suffisants.
 - Compatibilité avec les technologies d'assistance (lecteurs d'écran, navigation clavier, etc.)

Ce document comporte 3 annexes :

- ✓ Annexe 1 : « Liste des noms de domaines » ;
- ✓ Annexe 2 : « Politique de sécurité des systèmes d'information de l'Etat (PPSIE) » ;
- ✓ Annexe 3 : « Référentiel général de sécurité (RGS) » ;