



MARCHÉ PUBLIC DE PRESTATIONS DE SERVICES COURANTS

Objet du marché

EXTERNALISATION DE CERTAINES OPERATIONS LIEES AU TRAITEMENT DE PLAINTES

Consultation n°26_CNIL_03

Cahier des Clauses Techniques Particulières (CCTP)

TABLE DES MATIERES

ARTICLE 1. GLOSSAIRE	5
ARTICLE 2. OBJET DU MARCHÉ	7
ARTICLE 3. PRESENTATION DE LA CNIL ET DES PLAINTES.....	7
3.1 La CNIL	7
3.2 La direction de l'exercice des droits et des plaintes	8
3.2.1 Missions.....	8
3.2.1.1 Présentation générale	8
3.2.1.2 Présentation des plaintes.....	9
3.2.2 Organisation de la DEDP	11
3.2.2.1 Le greffe des plaintes.....	11
3.2.2.2 Les services instructeurs.....	11
ARTICLE 4. DESCRIPTION DU TRAITEMENT D'UNE PLAINTÉ PAR LA CNIL	11
4.1 Réception d'une plainte par la CNIL	11
4.2 Examen de la validité/recevabilité d'une plainte et le cas échéant, attribution aux services instructeurs.....	12
4.3 Envoi d'un accusé réception à l'auteur de la plainte	12
4.4 Qualification de la plainte par les services instructeurs	13
4.5 Instruction de la plainte	13
4.5.1 Objets de l'instruction	13
4.5.2 Action(s) éventuellement conduite(s) auprès de l'organisme incriminé au cours de l'instruction	14
4.5.2.1 A qui sont adressées les correspondances ?	14
4.5.2.2 Sous quel format sont adressées les correspondances ?	14
4.5.2.3 Quels sont la forme et le contenu des correspondances ?	14
4.5.3 Action(s) éventuellement conduites auprès de l'auteur de la plainte.....	15
4.5.4 Action(s) éventuellement conduite(s) auprès d'un tiers.....	15
4.6 Clôture de la plainte	16
4.6.1 Hypothèse 1. La situation signalée ne constitue pas un manquement au RGPD. S'il apparaît que la situation est régulière, l'agent attributaire adresse à l'auteur de la plainte un courrier de clôture afin de l'en informer.	16
4.6.2 Hypothèse 2. La situation signalée après instruction constitue un manquement.	16
ARTICLE 5. PRESENTATION ET MODALITES D'EXECUTION DES OPERATIONS EXTERNALISEES	17
5.1 Nature des opérations à effectuer.....	17
5.1.1 Description des opérations.....	17

5.1.2	Liste des courriers-types pouvant être générés par le prestataire	17
5.1.3	Identification des opérations à effectuer	17
5.2	Volumétrie des opérations.....	18
5.3	Délais de traitement	18
5.4	Application de la convention à des plaintes reçues par la CNIL avant l'entrée en vigueur du marché	18
ARTICLE 6. RESSOURCES MISES A DISPOSITION PAR LES PARTIES		18
6.1	Ressources mises à disposition par le titulaire.....	18
6.1.1	Ressources techniques.....	18
6.1.2	Ressources humaines.....	19
6.1.2.1	Désignation d'un responsable technique.....	19
6.1.2.2	Constitution d'une équipe opérationnelle en charge de l'exécution du marché	19
6.1.2.2.1	Compétences et qualités professionnelles requises	19
6.1.2.2.2	Modalités de sélection.....	20
6.1.2.2.3	Formations initiale et continue	20
6.1.2.2.4	Dimensionnement et stabilité de l'équipe opérationnelle pour l'exécution du marché.....	20
6.1.2.3	Possibilité d'exercer des fonctions au titre d'autres activités gérées par le prestataire	21
6.1.3	Ressources documentaires.....	21
6.2	Ressources mises à disposition par l'administration.....	21
6.2.1	Ressources techniques.....	21
6.2.2	Ressources humaines.....	22
6.2.2.1	Désignation des référents techniques.....	22
6.2.2.2	Formateurs/accompagnateurs.....	22
6.2.3	Ressources documentaires.....	22
ARTICLE 7. SUIVI DE L'EXECUTION DES OPERATIONS		22
7.1	Indicateurs de suivi	22
7.1.1	Tableau de bord.....	22
7.1.2	Suivi d'un échantillon de plaintes.....	23
7.2	Modalités de suivi.....	23
7.2.1	L'envoi d'une documentation par le titulaire	23
7.2.2	L'organisation de réunions d'exploitation et de réunions de pilotage	24
7.2.3	Organisation d'audits internes et externes	24
ARTICLE 8. SECURITE DES INFORMATIONS		24
8.1	Gestion des biens.....	24
8.2	Sécurité physique.....	25

8.3	Traitement des incidents	26
8.4	Sécurité du poste de travail	26
8.5	Sécurité des réseaux et de l'exploitation.....	26
8.6	Sécurité du compte Publik.....	28
8.7	Sécurité des documents et courrier au format papier	28
8.8	Environnement de travail sécurisé et traçabilité des actions	28
8.9	Non conservation des données à l'issue de la journée de travail	29
ARTICLE 9. ANNEXES		29
9.1	Schéma général du traitement d'une plainte	29
9.2	Exemples de scénarios de plaintes susceptibles d'être transmises au prestataire 29	
9.3	Modèles de courrier	29
9.3.1	Exemple de rappel à la loi (RAL).....	29
9.3.2	Exemple de courrier de clôture (CLA)	29

Article 1. Glossaire

Terme	Abréviation	Définition
Accusé réception	AR	Correspondance-type adressée par la CNIL à l’auteur d’une saisine pour lui indiquer qu’elle est recevable et a été transmise pour instruction au service compétent
Administration		Désigne le pouvoir adjudicateur : la CNIL
Agent attributaire		Agent en charge du traitement de la saisine
Commission nationale de l’informatique et des libertés	CNIL	Cf. 3.1
Courrier de clôture	CLA	Courrier adressé à l’usager pour l’informer de la clôture de sa plainte
Courrier au mis en cause	CM	Courrier adressé à l’organisme mis en cause pour l’interroger sur les faits objets de la plainte
Délégué à la protection des données personnelles	DPO	Le délégué à la protection des données est chargé de mettre en œuvre la conformité à la législation sur la protection des données au sein de l’organisme qui l’a désigné s’agissant de l’ensemble des traitements de données personnelles mis en œuvre par cet organisme
Demande		Requête adressée par un usager à la CNIL afin de solliciter son intervention
Demande de compléments	DC	Courrier adressé à l’usager pour l’inviter à fournir un justificatif et/ou des éléments complémentaires utiles à l’instruction de sa plainte
Direction de l’exercice des droits et des plaintes	DEDP	Cf. 3.2
Donnée personnelle (ou donnée à caractère personnel)		Toute information se rapportant à une personne physique identifiée ou identifiable
Information du plaignant	IPL	Courrier d’information de l’usager sur l’état d’avancement de son dossier
Lettre recommandée avec avis de réception	LRAR	
Loi informatique et libertés	LIL	
Mise en demeure	MED	
Organisme incriminé	OI	Organisme identifié par la CNIL comme mis en cause dans une plainte qui lui a été adressée
Personne concernée		Personne physique dont les données personnelles font l’objet d’un traitement
Plainte (ou réclamation)		Demande qui a pour objet de signaler un manquement à la réglementation sur la protection des données ou de contester la légalité d’une pratique et qui répond aux conditions requises (compétence et complétude) pour que la CNIL engage des actions nécessaires à son instruction

Priam		Applicatif métier de la CNIL utilisé notamment pour traiter les plaintes
Publik		Applicatif métier mis à disposition du titulaire : réceptionne les formulaires remplis par les usagers en front office, permet le traitement des demandes transmises au titulaire par la CNIL en back office
Rappel à la loi	RAL	Courrier adressé à l'organisme mis en cause pour lui signaler les faits objets de la plainte et lui rappeler les règles applicables
Réclamation		Cf. plainte
Règlement général sur la protection des données	RGPD	
Rejet	REJ	Courrier adressé à l'utilisateur pour l'informer du rejet de sa plainte
Résolution amiable		Courrier adressé à l'organisme mis en cause pour lui signaler les faits objets de la plainte et suggérer une résolution à l'amiable
Responsable de traitement		Personne physique ou morale, autorité publique, service ou autre organisme qui, seul ou conjointement avec d'autres, détermine les finalités et les moyens d'un traitement, c'est à dire l'objectif et la façon de le réaliser. En pratique et en général, il s'agit de la personne morale incarnée par son représentant légal
Service de l'exercice des droits et des plaintes	SEDP	Cf 3.4
Service des plaintes - affaires numériques et commerciales	SPANC	Cf 3.4
Service des plaintes - affaires publiques, sociales et financières	SPAPSF	Cf 3.4
Services instructeurs		SEDP, SPANC et SPAPSF
Sous-traitant	ST	Personne physique ou morale, autorité publique, service ou autre organisme qui traite des données pour le compte d'un autre organisme (« le responsable de traitement »)
Titulaire		Prestataire dont l'offre a été retenue à l'issue de la procédure d'appel d'offre du présent marché
Traitement de données personnelles		Opération, ou ensemble d'opérations, portant sur des données personnelles, quel que soit le procédé utilisé (collecte, enregistrement organisation, conservation, adaptation, modification, extraction, consultation, utilisation, communication par transmission ou diffusion ou toute autre forme de mise à disposition, rapprochement)

Traitement transfrontalier		Traitement de données à caractère personnel qui a lieu dans l'Union dans le cadre : - soit des activités d'établissements dans plusieurs États membres d'un responsable du traitement ou d'un sous-traitant lorsque le responsable du traitement ou le sous-traitant est établi dans plusieurs États membres - soit des activités d'un établissement unique d'un responsable du traitement ou d'un sous-traitant, mais qui affecte sensiblement ou est susceptible d'affecter sensiblement des personnes concernées dans plusieurs États membres
Vérifications préliminaires (<i>preliminary vetting</i>)		Courrier adressé à l'organisme mis en cause pour lui signaler les faits objets de la plainte et demander des éléments sur la nature transfrontalière du traitement en cause

Article 2. Objet du marché

Ce marché a pour objet l'externalisation de certaines opérations liées au traitement de plaintes.

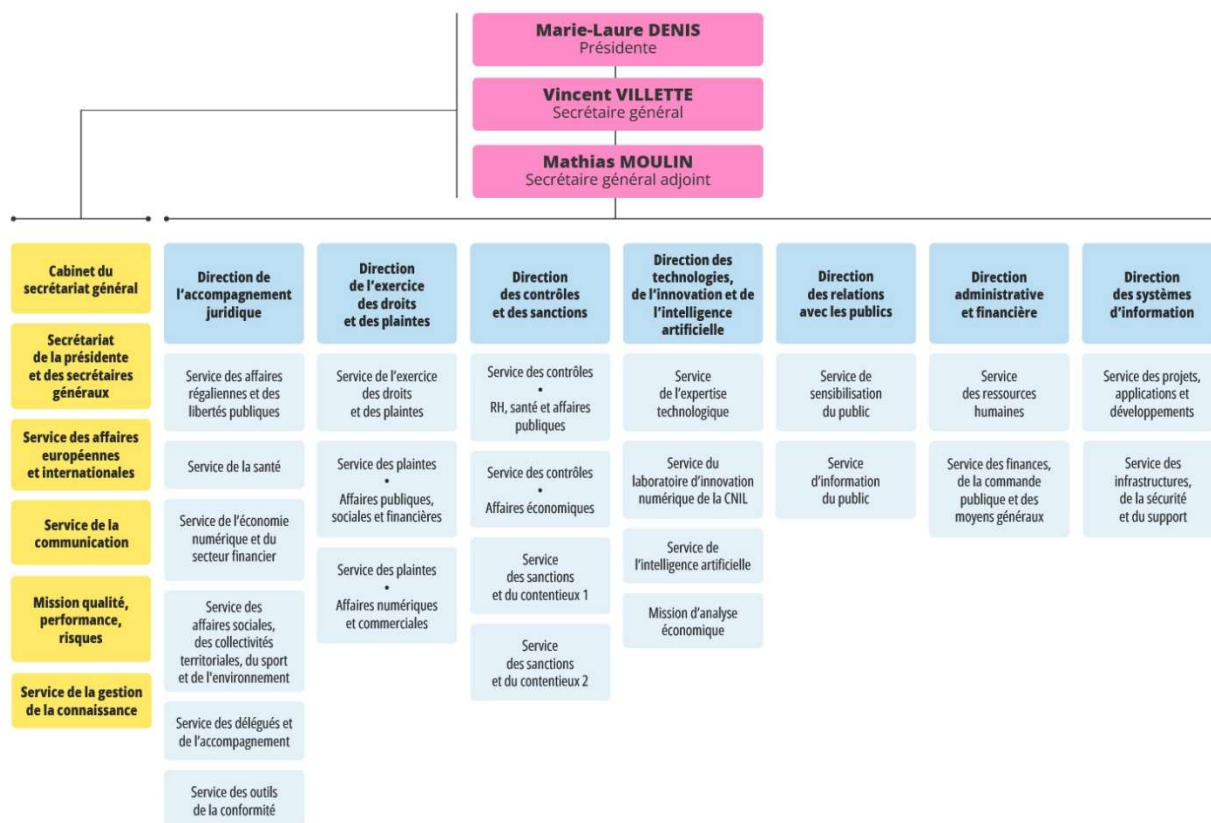
Article 3. Présentation de la CNIL et des plaintes

3.1 La CNIL

La Commission nationale de l'informatique et des libertés est une autorité administrative indépendante instituée et régie par la loi n° 78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés (LIL).

La CNIL est le régulateur des données personnelles et l'autorité de contrôle, au sens de l'article 51 du règlement européen (UE) 2016/679 du 27 avril 2016 (RGPD). Elle veille notamment à ce que les traitements de données à caractère personnel soient mis en œuvre conformément aux dispositions de la LIL et aux autres dispositions relatives à la protection des données personnelles prévues par les textes législatifs et réglementaires, le droit de l'Union européenne et les engagements internationaux de la France.

La CNIL exerce diverses missions, et notamment, répond aux demandes d'avis des pouvoirs publics, accompagne les professionnels dans leur mise en conformité, aide les particuliers à maîtriser leurs données personnelles et contrôle les traitements de données personnelles. Composée d'un collège de 18 membres, la CNIL s'organise autour de 7 directions :



Comme le prévoit le d) du 2° du I de l'article 8 de la LIL, la CNIL « traite les réclamations, pétitions et plaintes introduites par une personne concernée ou par un organisme, une organisation ou une association, examine ou enquête sur l'objet de la réclamation, dans la mesure nécessaire, et informe l'auteur de la réclamation de l'état d'avancement et de l'issue de l'enquête dans un délai raisonnable, notamment si un complément d'enquête ou une coordination avec une autre autorité de contrôle est nécessaire ».

Cette mission est dévolue à la direction de l'exercice des droits et des plaintes.

3.2 La direction de l'exercice des droits et des plaintes

3.2.1 Missions

3.2.1.1 Présentation générale

La direction de l'exercice des droits et des plaintes (DEDP) est chargée de traiter :

- les réclamations et plaintes introduites par une personne concernée ou par un organisme, une organisation ou une association (cf. [3.2.1.2](#)) ;
- les signalements émis par les lanceurs d'alerte concernant la protection des données à caractère personnel, en lien avec la direction des contrôles et des sanctions ;
- les demandes d'exercice indirect des droits portant sur les fichiers soumis à ce régime spécifique, en lien avec les commissaires, membres de la commission chargés de procéder, pour le compte des personnes, aux vérifications nécessaires.

Dans le cadre de ses missions, elle contribue à la mise en œuvre de la stratégie répressive de la commission en lien étroit avec la direction des contrôles et des sanctions, propose des dossiers à orienter vers la procédure de sanction simplifiée et concourt à l'élaboration de la doctrine de la commission en concertation avec les autres directions. Elle participe par ailleurs à la coopération européenne et représente la commission dans des sous-groupes du Comité européen de la protection des données.

3.2.1.2 Présentation des plaintes

Dans le cadre des plaintes, les usagers s'adressent à la CNIL afin de l'alerter sur l'illégalité d'une pratique au regard de la réglementation applicable en matière de protection des données personnelles.

La très grande majorité des plaintes reçues par la CNIL concerne une difficulté rencontrée par un individu lors de l'exercice de ses droits ou du traitement des données le concernant. De telles plaintes individuelles sont alors susceptibles d'avoir des répercussions pour l'ensemble des personnes concernées par le dispositif visé par cette saisine¹.

Ainsi, lorsqu'elle identifie plusieurs plaintes contre un même acteur, un même secteur et concernant une même pratique dénoncée, la CNIL peut les regrouper en une même instruction afin d'initier une instruction groupée, voire une procédure de contrôle (un tiers des contrôles ont ainsi pour origine des plaintes traitées par la DEDP ou des signalements). L'instruction ainsi menée d'une plainte unique ou de plusieurs plaintes peut aboutir à l'adoption de mesures correctrices (rappel aux obligations légales, mise en demeure, rappel à l'ordre, sanction financière, injonction, etc.). Les plaintes constituent alors un levier important dans la mise en conformité des organismes.

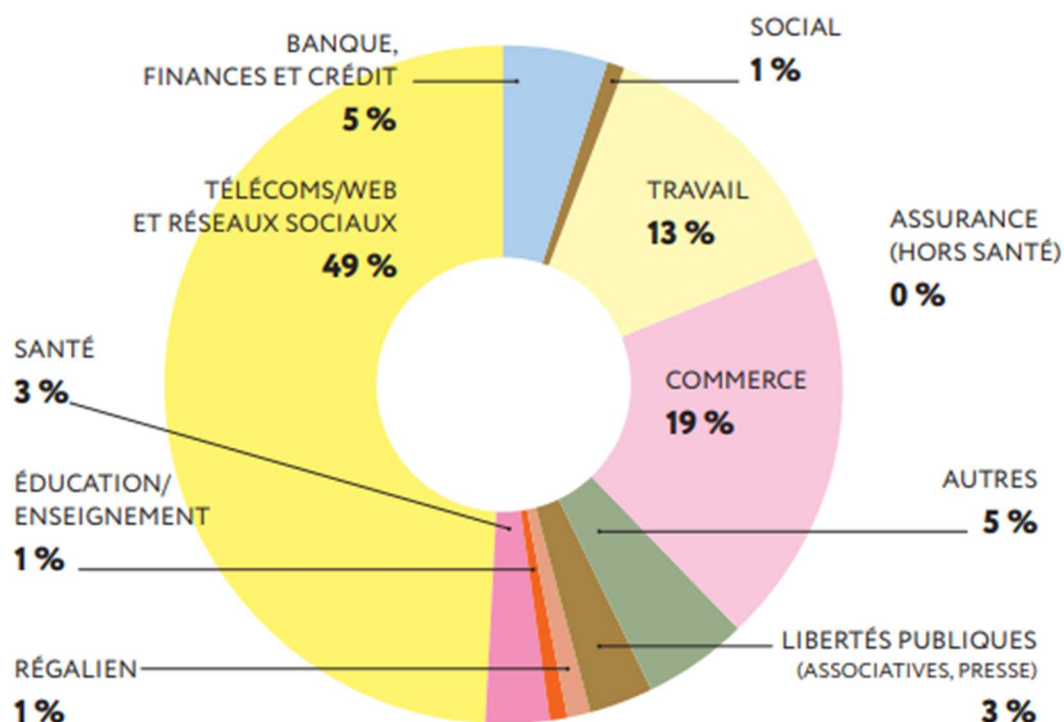
Le nombre de plaintes adressées à la CNIL a connu une croissance importante lors de l'entrée en application du RGPD. Il a ainsi franchi le seuil des 10 000 en 2018.

En 2025, ce chiffre a atteint 20 000. Parmi ces plaintes, 39 % ont été rejetées pour incompétence, désistement, irrecevabilité ou lorsque le grief soulevé ne constitue manifestement pas un manquement. Les dossiers restants ont fait l'objet d'une instruction en vue de la résolution de la problématique signalée et/ou poursuite des manquements relevés.

Les secteurs concernés sont nombreux, le plus grand nombre de plaintes reçues concernent cependant les secteurs de l'Internet ou des télécommunications.

¹ Par exemple, des caméras dans une salle de repos d'une entreprise concerneront tous les salariés et pas seulement le plaignant.

Répartition par secteur des plaintes reçues par la CNIL



Les circonstances à leur origine sont variables dans la mesure où les données personnelles et les traitements qui leur sont appliqués relèvent du quotidien des Français, comme l'illustre la situation en 2025 :

- exercice des droits d'accès ou d'effacement : constituant la majorité des plaintes reçues par la CNIL, les usagers y signalent les difficultés qu'ils rencontrent dans l'exercice de leurs droits. Dans de nombreux cas, ils font part d'une absence de réponse à leur demande ou encore du caractère incomplet / non conforme de la réponse qu'ils ont reçue.
Ces plaintes peuvent porter sur des données traitées par toutes sortes d'organismes (commerces, employeurs, etc.) ou encore des données diffusées sur internet.
- prospection commerciale, associative, politique : ces plaintes concernent la publicité par courrier électronique, SMS, voie postale et téléphone. Les personnes rencontrent le plus généralement des difficultés pour ne plus recevoir de prospection alors qu'elles ont exprimé leur opposition à ces envois ; elles rencontrent également des difficultés pour remonter la chaîne d'intermédiaires afin d'identifier qui a, au départ, transmis leurs coordonnées à des partenaires à des fins de prospection ;
- surveillance des employés : de nombreux usagers saisissent la CNIL pour signaler des situations de surveillance au travail. Ces plaintes mettent principalement en cause des dispositifs de vidéosurveillance au travail. Généralement ces plaintes visent des entreprises de taille réduite, qui ne disposent ni d'un service juridique ni du soutien d'un délégué à la protection des données. L'action de la CNIL vise donc à les informer de leurs obligations afin qu'elles se mettent en conformité. Lorsque cette action ne suffit pas, des contrôles sur place peuvent avoir lieu et/ou des mesures correctrices peuvent être adoptées.

3.2.2 Organisation de la DEDP

La DEDP est composée :

- d'agents en charge de l'examen de la recevabilité des plaintes et de leur pré instruction (greffe des plaintes), ainsi que d'agents en charge des cas transfrontaliers ;
- d'un service de l'exercice des droits indirect et des plaintes (SEDP) ;
- d'un service des plaintes - affaires numériques et commerciales (SPANC) ;
- d'un service des plaintes - affaires publiques, sociales et financières (SPAPSF).

3.2.2.1 Le greffe des plaintes

Au sein de la DEDP, un greffe est dédié à la prise en charge des plaintes dès leur enregistrement dans les applicatifs métier de la CNIL (Priam et Publik).

Le greffe des plaintes est chargé de veiller à la recevabilité et à la complétude des plaintes avant qu'elles ne soient prises en charge par les services de la DEDP.

3.2.2.2 Les services instructeurs

Les SEDP, SPANC et SPAPSF sont chargés de l'instruction de demandes adressées par des particuliers, lesquelles sont de deux ordres :

- les demandes d'exercice indirect des droits portant sur certains fichiers (fichiers de police, fichiers des services de renseignement...) soumis à ce régime spécifique (non concernées par le présent CCTP) ;
- les plaintes reçues par la CNIL.

Le SEDP, le SPANC et le SPAPSF seront désignés « services instructeurs » dans la suite de ce document.

Article 4. Description du traitement d'une plainte par la CNIL

Des usagers (personnes physiques ou morales) saisissent quotidiennement la CNIL afin 1/ de l'informer de manquements potentiels à la réglementation « informatique et libertés » et 2/ de solliciter son intervention afin que ces violations cessent.

Parmi ces plaintes, et conformément au d) du 2° du I de l'article 8 de la LIL, la CNIL est notamment compétente pour traiter les plaintes introduites par une personne concernée ou par un organisme, une organisation ou une association. Ainsi sollicitée, la CNIL « *examine ou enquête sur l'objet de la réclamation, dans la mesure nécessaire, et informe l'auteur de la réclamation de l'état d'avancement et de l'issue de l'enquête dans un délai raisonnable, notamment si un complément d'enquête [...] est nécessaire* ».

4.1 Réception d'une plainte par la CNIL

Les plaintes sont reçues par la CNIL via deux canaux :

- de manière dématérialisée, via un téléservice dédié composé de formulaires en ligne et accessible depuis le site web de la CNIL (<https://www.cnil.fr/fr/plaintes>) ;

- par courrier postal.

A titre indicatif et sans engagement contractuel en 2025 sur 20141 plaintes reçues :

- 18 610 plaintes ont été reçues par voie dématérialisée, soit un taux de 92,4% sur le volume total de plaintes reçues) ;
- 1531 plaintes par courrier postal, soit 7,6% sur le volume total des plaintes reçues.

4.2 Examen de la validité/recevabilité d'une plainte et le cas échéant, attribution aux services instructeurs

Le greffe des plaintes assure un premier niveau d'analyse et traite directement certaines demandes en les rejetant ou adressant une demande de compléments (par exemple, cas d'incompétence, absence d'exercice préalable des droits, etc.) ou les attribue à l'un des services de la direction en fonction des compétences de chacun des services instructeurs.

Dans ce cadre :

- il s'assure de la compétence de la CNIL (manquements aux dispositions du RGPD ou de la LIL en particulier) ;
- il s'assure que la plainte contient les éléments permettant à la CNIL d'intervenir au fond:
 - description du ou des manquements ;
 - mention d'un organisme/d'une personne mis(e) en cause ;
 - présence des justificatifs requis concernant l'auteur de la saisine (ex. : mandat) ;
 - présence des justificatifs du ou des manquements rapportés (ex. : copie de la demande préalablement adressée au responsable de traitement) ;
- à défaut de l'un de ces éléments, il peut demander à l'usager de compléter sa plainte dans un délai fixé, à défaut, sa plainte est classée.

A l'issue de l'analyse et des actions conduites, le greffe :

- rejette la plainte (incompétence, incomplétude en dépit des demandes de compléments ou de précisions, etc.) ;
- ou oriente la plainte vers un des services instructeurs de la DEDP.

4.3 Envoi d'un accusé réception à l'auteur de la plainte

Concernant les plaintes reçues par voie électronique, un accusé d'enregistrement électronique est émis à sa réception par la CNIL². Un accusé de réception est ensuite émis de manière automatique (par message électronique) lors de la transmission de la plainte aux services instructeurs de la DEDP.

Concernant les plaintes reçues par voie postale, un accusé de réception est imprimé automatiquement et transmis par courrier au moment de la transmission de la plainte aux services instructeurs.

² A condition que l'auteur de la saisine ait communiqué son adresse courriel dans le formulaire.

4.4 Qualification de la plainte par les services instructeurs

Au sein du service instructeur, l'agent attributaire prend connaissance de la plainte et en examine le contenu. Dans ce cadre, il conduit les actions suivantes qui sont retracées dans les applicatifs métiers :

- il prend connaissance des informations relatives à l'auteur de la plainte (identité, coordonnées) et de ses éventuelles autres démarches auprès de la CNIL ;
- il fait de même s'agissant de l'organisme incriminé (en prenant connaissance d'éventuelles autres plaintes déposées à son encontre, et y rattache, le cas échéant, un DPO).
Afin de fiabiliser les données relatives aux organismes, PRIAM est relié à l'API Entreprise.
Si l'organisme a désigné un DPO, celui-ci est également ajouté dans l'onglet « contacts ». Ce DPO est, sauf exception, l'interlocuteur des services instructeurs ;
- il recherche s'il existe d'autres plaintes liées à la nouvelle et, le cas échéant, les apparente. Les plaintes sont apparentées lorsqu'elles concernent un même organisme et un même manquement et sont formulées dans un délai proche ;
- il détermine le cadre légal dans lequel s'inscrit la plainte. A cet effet, il identifie :
 - o le(s) secteur(s), c'est-à-dire la catégorie d'activités ou d'entités concernée par la plainte ;
 - o le(s) motif(s), c'est-à-dire le droit ou l'obligation légale ou réglementaire que l'OI ne respecterait pas ;
 - o le(s) caractéristique(s), c'est-à-dire les éléments spécifiques à la plainte ayant un impact sur l'instruction (contexte soumis à une réglementation spécifique, etc.) ;Ces éléments sont automatiquement intégrés pour les plaintes reçues du téléservice (en fonction du scénario de plainte en ligne choisi par l'utilisateur), mais il faut en vérifier l'exactitude et les modifier au besoin ;
- si cela n'a pas été fait précédemment, il informe sa hiérarchie ou tout autre agent de la CNIL intéressé du caractère urgent ou sensible du dossier ;
- il identifie l'éventuel caractère transfrontalier de la plainte en cause qui n'aurait pas été identifié en amont ;
- le cas échéant, il identifie et ajoute le(s) autre(s) agent(s) susceptible(s) de contribuer à l'instruction de la plainte.

Ces vérifications sont en particulier conduites au regard des éléments disponibles dans la plainte. L'agent peut par ailleurs effectuer des recherches complémentaires. Il peut enfin solliciter de l'auteur de la plainte l'envoi de compléments nécessaires à l'instruction de sa demande. Il en est notamment ainsi si cette dernière est insuffisamment motivée ou si des pièces sont manquantes et que cela n'a pas été relevé lors de l'analyse de recevabilité. L'auteur de la plainte est alors invité à transmettre les éléments demandés dans un délai fixé, à défaut de quoi sa plainte est classée.

Dès qu'il a conduit ces actions, l'agent attributaire identifie celles à conduire dans le cadre de l'instruction.

4.5 Instruction de la plainte

4.5.1 Objets de l'instruction

Au cours de la phase d'instruction, l'agent attributaire conduit l'ensemble des actions nécessaires au rassemblement des éléments permettant à la CNIL de prendre une décision motivée et adaptée à la situation rapportée dans la plainte.

A cet effet, l'agent recourt à la documentation interne de la CNIL ou peut recueillir des éléments en source ouverte afin d'identifier notamment la réglementation applicable et les actions que la CNIL est susceptible d'engager pour obtenir la conformité de l'organisme.

Ces éléments peuvent suffire à l'agent attributaire pour prendre une décision. Dans ces circonstances, aucune action n'est conduite auprès de l'organisme, de l'auteur de la plainte ou de tiers dans le cadre de l'instruction, avant la prise de décision de l'agent attributaire sur l'issue de la plainte.

Si besoin, il peut au contraire solliciter des éléments complémentaires³ auprès de l'OI, de l'auteur de la plainte ou encore de tiers, avant que la décision soit prise sur l'issue de la plainte.

Par ailleurs, et s'agissant plus précisément des échanges adressés à l'auteur de la plainte, la CNIL est tenue de l'informer régulièrement de l'état de sa plainte.

4.5.2 Action(s) éventuellement conduite(s) auprès de l'organisme incriminé au cours de l'instruction

Ce n'est que dans la mesure où l'agent a besoin d'éléments complémentaires qu'il en sollicite auprès de l'OI.

4.5.2.1 A qui sont adressées les correspondances ?

Comme indiqué plus haut, si l'organisme a désigné un DPO auprès de la CNIL, celui-ci est en principe destinataire des correspondances adressées par l'agent attributaire dans le cadre de l'instruction d'une plainte. A défaut de DPO, l'interlocuteur est le représentant légal du responsable de traitement.

4.5.2.2 Sous quel format sont adressées les correspondances ?

Le traitement d'une plainte conduit à plusieurs actions, alternatives ou cumulatives selon les cas, auprès de l'OI. Ces actions passent par la rédaction de courriers, courriels ou éventuellement communications téléphoniques. Le traitement par courriel est privilégié, en utilisant, le cas échéant, les coordonnées non publiques du DPO disponibles dans Priam.

4.5.2.3 Quels sont la forme et le contenu des correspondances ?

Au stade de l'instruction, les correspondances adressées par l'agent attributaire à un OI visent en principe à obtenir des éléments nécessaires à l'instruction de la plainte.

- 1.** A cette fin, l'agent attributaire adresse un « courrier au mis en cause » (CM) ainsi composé :
 - présentation synthétique des circonstances à l'origine du courrier adressé par la CNIL :
 - o signification de la réception d'une plainte par la CNIL concernant un traitement mis en œuvre par l'organisme ;
 - o signification du ou des traitements concernés ;
 - o signification du ou des droits ou obligations dont le non-respect a été signalé à la CNIL ;
 - mention du ou des éléments sollicités par la CNIL ;
 - mention du délai de réponse accordé par la CNIL.

³ Cf [4.5.2](#)

Si l'organisme adresse en retour les éléments sollicités, ceux-ci sont traités par l'agent qui peut alors poursuivre l'instruction de la plainte.

2. En l'absence de réponse de l'organisme dans le délai annoncé, l'agent adresse à nouveau un courrier à l'organisme. Cette « relance » est adressée par voie postale en LRAR et comprend les éléments suivants :

- rappel de l'envoi d'un précédent courrier resté sans réponse, lequel est joint à la relance ;
- demande de communication des éléments sollicités dans un nouveau délai précisé. Le délai de réponse à la relance est en principe fixé à 1 mois mais il peut varier en fonction de la complexité ou de l'urgence de la demande ;
- indication des conséquences en cas de non réponse à la relance : engagement possible d'une procédure de sanction.

3. Dans le silence de l'organisme à l'issue de cette phase de relance, une mise en demeure (MED) de répondre, signée par la présidente de la CNIL, est adressée à l'organisme. Ce courrier est ainsi constitué :

- rappel des éléments chronologiques du dossier ;
- rappel du fait que l'absence de réponse ou l'envoi d'une réponse manifestement incomplète caractérise un manquement à l'obligation de coopération avec la CNIL prévue par l'article 18 de la LIL ;
- information sur les suites qui peuvent être données à cette mise en demeure.

4.5.3 Action(s) éventuellement conduites auprès de l'auteur de la plainte

L'instruction d'une plainte peut conduire un agent à engager plusieurs actions auprès de l'auteur de la plainte.

L'agent attributaire peut adresser deux catégories de correspondances à l'auteur de la plainte au stade de l'instruction :

- une demande de complément (DCT) : il s'agit des courriers adressés à l'auteur de la saisine afin d'obtenir des informations ou éléments complémentaires pour répondre à des interrogations survenues au cours de l'instruction ;
- une « information du plaignant » (IPL) : il s'agit de tous les courriers d'information de l'auteur de la plainte quant à l'état d'avancement de son dossier.

A ce propos, et comme déjà indiqué, un courrier doit être adressé par la CNIL afin d'informer l'auteur de la plainte de l'état d'avancement ou de l'issue de la plainte.

4.5.4 Action(s) éventuellement conduite(s) auprès d'un tiers

L'instruction d'une plainte peut conduire un agent à engager plusieurs actions à destination de tiers.

Dans la majorité des cas, il s'agit d'obtenir des compléments concernant l'identification d'un interlocuteur au sein d'un organisme. A titre d'exemple, si la CNIL est saisie au sujet de mauvaises pratiques constatées sur un site web dont elle ne réussit pas à contacter l'éditeur, elle peut solliciter l'hébergeur afin d'obtenir les coordonnées qui ont été transmises par son client, éditeur dudit site.

Ces demandes sont adressées dans des correspondances dites « consultation d'un tiers relatif à une plainte » (TC).

4.6 Clôture de la plainte

La phase d’instruction prend fin lorsque les éléments nécessaires à une prise de décision sont réunis – que ce soit ou non après avoir sollicité l’auteur de la plainte, l’OI ou un tiers.

Il existe diverses situations⁴. Il convient d’en distinguer deux.

4.6.1 Hypothèse 1. La situation signalée ne constitue pas un manquement au RGPD. S’il apparaît que la situation est régulière, l’agent attributaire adresse à l’auteur de la plainte un courrier de clôture afin de l’en informer.

En fonction de son degré de complexité ou de sensibilité, le courrier de clôture à l’attention de l’auteur de la plainte est signé par l’agent attributaire (type de courrier sortant « CLA »⁵) ou par l’un des encadrants des services instructeurs ou de la DEDP ou encore par la Présidente de la CNIL.

Le courrier de clôture doit mentionner les voies et délais de recours⁶.

L’envoi du courrier de clôture adressé à l’auteur de la plainte clôt la plainte dans Priam.

4.6.2 Hypothèse 2. La situation signalée après instruction constitue un manquement.

Si à l’issue de l’instruction, des manquements sont identifiés par l’agent attributaire, celui-ci doit engager des actions à destination de l’organisme puis à destination de l’auteur de la plainte.

A destination de l’organisme, l’agent peut en particulier adresser un courrier d’observation qui est désigné en interne sous le vocable « rappel à la loi » (RAL⁷) afin de rappeler à l’OI les règles applicables et lui indiquer ce qu’il doit faire pour respecter ses obligations et mettre fin aux manquements. Ce courrier n’appelle pas systématiquement de réponse de la part de l’OI. Cependant, une mention indique que la CNIL pourrait revenir vers lui si l’auteur de la plainte lui signale par la suite que sa situation n’a pas été régularisée ou si elle reçoit d’autres plaintes impliquant l’organisme pour des faits analogues.

A destination de l’auteur de la plainte, et dès que l’agent a adressé le RAL, l’agent adresse un courrier afin de l’informer des actions conduites par la CNIL (mention de l’envoi du courrier et du contenu de ce courrier) et afin de lui notifier la clôture de la plainte. L’auteur de la plainte est par ailleurs invité à revenir vers la CNIL si la situation initialement signalée n’était pas rectifiée par l’organisme à l’issue du délai qui lui a été accordé.

En cas de manquement(s) caractérisé(s) et présentant un certain degré de gravité, une mesure correctrice de type MED ou rappel aux obligations légales, voire l’ouverture d’une procédure de sanction, peut être proposée à la présidente de la CNIL.

L’ensemble de ces actions permet alors de clore la plainte.

⁴ L’ensemble des procédures mises en place au sein de la CNIL pour le traitement des saisines n’est pas traité dans le présent CCTP, compte tenu de l’objet du marché (ex : orientation en contrôle, proposition de mise en demeure ou de sanction...).

⁵ Cf. Annexe 9.3.1_modèle_CLA

⁶ « Sous réserve de l’intérêt pour agir des requérants, les décisions de la CNIL sont susceptibles de faire l’objet d’un recours devant le Conseil d’Etat dans un délai de deux mois à compter de leur notification »

⁷ Cf. Annexe 9.3.2_modèle_RAL

Article 5. Présentation et modalités d'exécution des opérations externalisées

5.1 Nature des opérations à effectuer

Après analyse de la plainte par les agents de la CNIL,, les plaintes répondant aux critères mentionnés *infra* au [5.1.3](#) sont transmises au prestataire *via* l'outil Publik.

5.1.1 Description des opérations

Les opérations suivantes doivent être effectuées par le prestataire conformément au scénario identifié par la CNIL pour chaque plainte transmise :

- a. prise de connaissance de la plainte, y compris les pièces jointes et du script dévolu, si identification d'une problématique n'entrant pas dans les critères du [5.1.3](#) : retransmission de la saisine à la CNIL par l'outil Publik ;
- b. vérification de la qualification de la saisine et, le cas échéant, correction/complétion de la qualification;
- c. vérification de l'organisme désigné et, le cas échéant, correction/complétion des éléments transmis par l'auteur de la plainte ;
- d. déroulement du process décrit dans le script identifié ;
 - envoi du courrier-type correspondant (via courriel envoyé par Publik ou courrier postal en lettre simple) à l'OI⁸ et ;
 - envoi du courrier-type correspondant (via Publik) à l'auteur de la plainte (courrier de clôture)⁹.

La CNIL est automatiquement informée de la réalisation des opérations, le statut de la plainte se mettant automatiquement à jour dans l'outil Publik.

Ces opérations sont intégralement retracées dans l'outil Publik mis à la disposition du prestataire.

En cas de questions, difficultés ou de doutes, le prestataire renvoie le dossier via l'outil dédié pour se voir confirmer les opérations à effectuer le cas échéant.

5.1.2 Liste des courriers-types pouvant être générés par le prestataire

Les courriers-types pouvant être générés dans Publik, au format PDF, par le prestataire dans le cadre du traitement générique des plaintes sont les suivants :

- à destination de l'auteur de la plainte : clôture (CLA) ;
- à destination de l'OI : rappel à la loi (RAL).

5.1.3 Identification des opérations à effectuer

Les opérations externalisées sont identifiées par la CNIL sous la forme de scénarios dont des exemples figurent en annexe 9.2. Ces scénarios sont susceptibles d'évoluer au cours du marché.

⁸ [Cf. 5.1.2](#)

⁹ [Cf. 5.1.2](#)

5.2Volumétrie des opérations

A titre indicatif et sans engagement contractuel, l'objectif de traitement annuel est fixé entre 3 500 et 4 000 unités. A titre d'illustration, au cours d'un précédent marché portant sur ces opérations, le nombre de plaintes pour lesquelles certaines opérations ont été externalisées s'établit comme suit :

- en 2023 : 3 100 ;
- en 2024 : 3 500 ;
- en 2025 : 3 700.

Ces chiffres étant sujet à fluctuation, il s'agit d'une simple estimation de volumétrie et non d'un engagement contractuel.

5.3Délais de traitement

Concernant le traitement des demandes, le prestataire s'engage, à compter de la date d'envoi de la plainte par la CNIL, à effectuer l'ensemble des opérations mentionnées au [5.1.1](#) dans un délai inférieur à 6 jours ouvrés pour 90% des plaintes et dans un délai inférieur à 12 jours ouvrés pour 100% des plaintes.

5.4Application de la convention à des plaintes reçues par la CNIL avant l'entrée en vigueur du marché

Les plaintes seront attribuées par la CNIL au titulaire au fil de leur réception à compter de l'entrée en vigueur du présent marché. Néanmoins, des plaintes reçues avant cette date pourront être attribuées en fonction des besoins de la CNIL et selon les critères définis *supra*.

Article 6. Ressources mises à disposition par les parties
--

6.1Ressources mises à disposition par le titulaire

6.1.1 Ressources techniques

Le titulaire fournira tous les moyens matériels et informatiques nécessaires à la prestation demandée (postes informatiques avec connexion internet haut débit, imprimantes, connexion informatique sécurisée pour se relier au réseau CNIL, affranchissement, papier, ...).

Les enveloppes seront fournies par la CNIL au Titulaire.

Le titulaire doit mettre en place une chaîne de traitement la plus optimale pour pouvoir :

- effectuer informatiquement les opérations confiées ;
- enregistrer les pièces dématérialisées dans l'outil Publik ;
- générer les documents et courriers ;
- imprimer les courriers générés ;
- adresser les courriers en France et à l'international.

Pour traiter les plaintes, le personnel du prestataire disposera de scripts, d'une base de connaissance et accédera à une ou plusieurs bases de données. Les scripts s'appuient sur les informations contenues dans des fiches de procédures¹⁰ et une ou plusieurs bases de données fournies par l'administration. Le titulaire développe l'ensemble des scripts et la base de connaissance sous l'autorité de l'administration.

6.1.2 Ressources humaines

Le titulaire du marché fournit un organigramme fonctionnel et nominatif à l'administration. De plus, le titulaire adresse à l'administration une liste de contacts (téléphonique et adresse électronique) en fonction des thématiques (formation, support, traitement des plaintes et relance, ...).

6.1.2.1 Désignation d'un responsable technique

Le titulaire désigne un responsable technique, qui est l'interlocuteur direct de l'administration, au niveau opérationnel. Il est présent sur le site de la CNIL sur convocation de l'administration et a un pouvoir de décision suffisant pour engager la responsabilité du titulaire.

Il doit être en mesure :

- d'organiser, de piloter et de coordonner son équipe dans l'exécution des prestations objet du présent marché ;
- de participer activement à l'exécution des prestations objet du présent marché ;
- de rédiger les comptes rendus, bilans et tableaux de bord ;
- d'informer l'administration ou ses représentants sur :
 - o les incidents ou anomalies constatés,
 - o les gênes occasionnées par un dysfonctionnement,
- de participer aux réunions avec les représentants de l'administration ;
- de répondre à toutes les questions posées par l'administration ou ses représentants relatives à l'exécution du présent marché ;
- de contrôler la qualité des prestations ;
- de garantir la discipline du personnel.

Il est précisé que le personnel du titulaire est sous le contrôle et la responsabilité de l'encadrement défini ci-dessus.

Si le responsable technique vient à changer, le titulaire doit impérativement informer l'administration et lui communiquer les coordonnées d'un nouvel interlocuteur et ce dans les 5 jours ouvrés suivant le changement opéré.

6.1.2.2 Constitution d'une équipe opérationnelle en charge de l'exécution du marché

6.1.2.2.1 Compétences et qualités professionnelles requises

Le personnel du titulaire amenés à effectuer les opérations du présent marché doit présenter les compétences et qualités suivantes :

- bonne maîtrise du français écrit ;
- capacités d'analyse ;

¹⁰ [Cf. 6.2.3](#)

- connaissances générales de la réglementation applicable à la protection des données personnelles (possibilité d'organiser une formation à cet effet) ;
- sens du service public et goût pour les sujets liés aux nouvelles technologies et à la protection de la vie privée ;
- grand sens de l'organisation et capacité à rendre compte.

6.1.2.2.2 *Modalités de sélection*

Le recrutement des employés affectés aux opérations décrites au présent marché est sous la responsabilité du titulaire. L'administration se réserve cependant un droit de regard sur le profil des employés recrutés. Ce droit de regard se traduit par la mise à disposition par le titulaire, sur demande de l'administration, des profils de ces employés, sous forme de curriculum vitae.

Concernant le responsable technique du titulaire mentionné au [6.1.2.1](#), le titulaire transmet à l'administration le curriculum vitae du responsable technique envisagé. L'administration se réserve la possibilité de recevoir le candidat en entretien et de refuser la candidature si celle-ci ne semble pas répondre aux critères mentionnés au [6.1.2.1](#).

6.1.2.2.3 *Formations initiale et continue*

Tous les employés du titulaire affectés aux opérations décrites au présent marché doivent avoir suivi une formation initiale. Cette formation aborde les thématiques suivantes :

- environnement CNIL ;
- gestion et traitement des plaintes;
- environnement informatique (sécurité des systèmes d'information et prise en main de l'outil métier Publik).

Les modalités de la formation initiale doivent être déterminées ou validées par l'administration qui peut par ailleurs animer, co-animer et/ou assister si elle le souhaite à toutes les sessions de formation initiale. Les employés du titulaire sont rémunérés par le titulaire pendant les formations. Ces sessions de formation doivent être mises en place à chaque fois que de nouveaux employés rejoindront l'équipe.

Le titulaire prend à sa charge les formations initiales en cas de renouvellement de l'équipe affectée au dispositif.

La formation continue est quant à elle pilotée par le titulaire. Le titulaire communiquera le nombre de journées de formation continue incluses par an dans le cadre du présent marché. L'objectif de la formation continue est d'apporter les connaissances et les compléments nécessaires à la gestion des opérations confiées. Il s'agit de faire monter en compétence les employés dédiés à l'activité CNIL. Les modalités de formation « continue » doivent être validées par l'administration qui peut par ailleurs animer, co-animer et/ou assister à toutes les sessions de formation continue.

6.1.2.2.4 *Dimensionnement et stabilité de l'équipe opérationnelle pour l'exécution du marché*

Le titulaire propose un dimensionnement des effectifs en fonction de l'estimation de volume indiquée au [5.3](#) et de la nature des opérations à effectuer mentionnées aux [5.1](#) et [5.2](#).

Le titulaire prend acte du caractère fluctuant du volume des demandes et s'engage à être réactif et à dimensionner les équipes en conséquence. L'administration s'engage à informer le titulaire, dans les

meilleurs délais, de toute évolution du nombre de plaintes à traiter afin de permettre un ajustement du dimensionnement de l'équipe dédiée dans les meilleures conditions possibles.

Compte tenu de la confidentialité des informations traitées et de la technicité de la matière qui implique de pouvoir valoriser la formation dispensée, le titulaire s'engage à garantir la stabilité de son équipe. Le titulaire précise les moyens mis en œuvre afin de fidéliser les employés affectés aux opérations décrites au présent marché.

Le candidat s'engage à communiquer les nom, prénom et adresse électronique des employés afin de permettre la création de leur compte individuel dans le back office Publik par la CNIL. Il s'engage également à notifier la CNIL de tout départ d'agent.

6.1.2.3 Possibilité d'exercer des fonctions au titre d'autres activités gérées par le prestataire

L'administration laisse au titulaire la possibilité d'affecter tout ou partie de l'équipe en charge des opérations décrites au présent marché à l'exécution d'autres contrats gérés par le titulaire. Cette mutualisation des activités ne doit cependant pas affecter la productivité et la qualité des actions de ces employés dans les opérations prévues au présent marché.

6.1.3 Ressources documentaires

Le titulaire s'engage à fournir à l'administration les documents suivants :

- documentation nécessaire au suivi de la réalisation des opérations¹¹;
- documentation permettant de garantir les diverses obligations du titulaire, notamment les exigences de sécurité, les procédures de recrutement, etc.

6.2 Ressources mises à disposition par l'administration

6.2.1 Ressources techniques

L'administration ne fournit pas au titulaire le matériel informatique nécessaire à l'exécution de la prestation. En revanche, elle fournit au titulaire une assistance technique afin d'installer l'accès au back office de l'outil Publik.

Le back office de Publik est accessible au moyen d'un navigateur internet. Les employés de l'équipe disposent de comptes individuels et nominatifs créés par la CNIL.

L'accès à l'outil Publik se fait *via* une connexion internet. Une liste limitative d'adresses IP du titulaire, correspondant aux postes informatiques des employés affectés aux opérations prévues au présent marché, se verra autoriser l'accès au back office de Publik. L'administration met à disposition son personnel technique pour l'installation et la sécurisation de la liaison. Un enregistrement des accès et opérations effectuées par le titulaire dans l'outil Publik sera opéré. Cette journalisation devra être transmise à l'administration sur demande.

L'outil Publik assure l'envoi et l'enregistrement des courriels depuis une adresse courriel de la CNIL. Il assure également la génération des documents et courriers en PDF et les met à disposition de l'agent traitant par le biais de la fonction « télécharger » du navigateur.

¹¹ [Cf article 7](#)

6.2.2 Ressources humaines

6.2.2.1 Désignation des référents techniques

L'administration s'engage à désigner en son sein des référents techniques qui seront les interlocuteurs du titulaire :

- un référent opérationnel au sein de la DEDP ;
- un référent support informatique, désigné au sein de la DSI.

L'administration fournira au titulaire les noms et coordonnées électroniques et téléphoniques de ces référents ainsi que celles de leur remplaçant en cas d'absence.

Si les référents techniques viennent à changer, l'administration s'engage à informer le titulaire et à lui communiquer les coordonnées d'un nouvel interlocuteur et ce dans les 5 jours ouvrés suivant le changement opéré.

6.2.2.2 Formateurs/accompagnateurs

L'administration établit, en collaboration avec le titulaire, le programme de la formation initiale¹². Le personnel du titulaire est formé par l'administration sur la base d'une session de formation initiale de 2 à 5 jours et de documents techniques.

En complément de cette formation initiale, des réunions pourront être organisées autant que de besoin afin d'accompagner le personnel du titulaire notamment en cas d'évolution des scénarios ou des scripts.

6.2.3 Ressources documentaires

L'administration met à la disposition du titulaire toute la documentation utile à l'exécution des prestations visées au présent marché et notamment :

- des fiches procédures, décrivant le traitement attendu d'une plainte en fonction du manquement identifié ;
- des courriers-types¹³ ;
- les bases de données nécessaires au traitement des plaintes (DPO, etc) et leurs mises à jour.

Article 7. Suivi de l'exécution des opérations

7.1 Indicateurs de suivi

Le titulaire mettra en place, en concertation avec l'administration, un ou plusieurs tableaux de bord de suivi des opérations réalisées par le prestataire.

7.1.1 Tableau de bord

¹² Cf. [6.1.2.2.3](#)

¹³ Cf. liste mentionnée au [5.1.2](#) et [5.2.2](#)

Le tableau de bord relatif au traitement des plaintes, présenté sous forme de tableau(x) et graphes présentera *a minima* les indicateurs suivants :

- nombre de plaintes reçues ;
- nombre de plaintes traitées ;
- nombre de plaintes réorientées vers la CNIL ;
- délai moyen de traitement ;
- nombre de courriers sortants à destination de l'auteur de la plainte émis ;
- nombre de courriers sortants à destination de l'organisme mis en cause.

Les indicateurs devront être accessibles par semaine / mois / an.

Cette liste d'indicateurs qui n'est pas exhaustive sera finalisée avec le titulaire dans le cadre de la mise en place du marché et pourra faire l'objet d'évolutions au cours du marché et ce, sans supplément de prix pour la CNIL.

7.1.2 Suivi d'un échantillon de plaintes

Le titulaire communique au plus tard 10 de chaque mois un ensemble d'informations concernant un échantillon de plaintes sur lesquels il a effectué les opérations listées au [5.2.1](#). Pour chaque plainte, ces informations sont les suivantes :

- référence (avec lien vers Publik) ;
- scénario appliqué ;
- les dates :
 - o de réception par le prestataire (a) ;
 - o d'envoi d'un courrier au plaignant par le prestataire (b) et délai entre (a) et (b) ;
 - o d'envoi d'un courrier à l'organisme mis en cause (c) et délai entre (a) et (c) ;
- qualification de la saisine – secteur(s), motif(s) et caractéristique(s) retenue(s) ;
- coordonnées de l'organisme tel quel désigné par l'utilisateur ;
- coordonnées de l'organisme mis en cause retenu par le titulaire, la modalité d'envoi (courriel ou courrier) et, en cas de courriel, le motif du choix de ce canal, ainsi que le cas échéant, désignation de la pièce jointe au courrier ;
- le cas échéant, coordonnées du DPO éventuellement identifié par le titulaire sur la base de la documentation fournie par l'administration.

Ces informations ainsi que la taille de l'échantillon seront finalisées avec le titulaire dans le cadre de la mise en place du marché et pourront faire l'objet d'évolutions au cours du marché et ce, sans supplément de prix pour la CNIL.

7.2 Modalités de suivi

7.2.1 L'envoi d'une documentation par le titulaire

Mensuellement le titulaire fournira à l'administration une analyse des opérations conduites pour le mois écoulé. Cette analyse se présentera sous forme de diagrammes commentés.

Le titulaire produira également un rapport semestriel relatif à l'exécution des prestations visées au présent marché.

Enfin le titulaire devra proposer un système d'information et d'alerte de l'administration en cas de pic d'activité, d'un problème sur l'outil Publik, d'une difficulté rencontrée dans le traitement d'une opération ou de constat d'un engorgement anormal.

7.2.2 L'organisation de réunions d'exploitation et de réunions de pilotage

L'administration se réserve la possibilité de convoquer des réunions d'exploitation (comité de production), avec le référent technique du titulaire le cas échéant, sur le site de la CNIL ou du titulaire, en fonction des besoins et au minimum une fois par mois. Au cours de ces réunions, le référent technique présente au référent opérationnel et pour la période courant depuis la précédente réunion d'exploitation les éléments issus du tableau de bord décrit au [7.1.1](#). Au cours de ces réunions, sont par ailleurs abordés les questionnements ou problèmes apparus dans l'exécution du marché, et tout autre élément pertinent concernant la mise en œuvre du marché. Ces réunions pourront être mutualisées avec les réunions d'accompagnement visées au [6.2.2.2](#).

En sus de ces réunions d'exploitation, l'administration se réserve la possibilité de convoquer des réunions de pilotage (comité de pilotage) en fonction des besoins et au minimum une fois par trimestre. Au cours de ces réunions, le titulaire présente à l'administration le tableau de bord pour la période précédant leur tenue. Au cours de ces réunions sont par ailleurs abordés les points transversaux dépassant le périmètre d'intervention du référent opérationnel. Ces réunions pourront être mutualisées avec les réunions d'accompagnement visées au [6.2.2.2](#).

La présence du titulaire est requise lors de ces réunions.

7.2.3 Organisation d'audits internes et externes

Afin de garantir la qualité d'exécution des prestations, l'administration se réserve la possibilité de solliciter auprès du titulaire la réalisation d'audit(s) interne(s). Le titulaire s'engage à tenir à la disposition de l'administration les conclusions de ce(s) audit(s).

A l'initiative de l'administration, un audit externe relatif à l'exécution des prestations visées au présent marché peut également être commandé. Le coût d'un tel audit sera pris en charge par l'administration

Article 8. Sécurité des informations

8.1 Gestion des biens

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

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.

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.

Échange de supports : le titulaire garantit que les supports échangés 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.

Supports de stockage hébergeant des données de l'administration : le titulaire conserve en lieu sûr les supports de stockage de données en fin de vie contenant des données de l'administration, en attendant de procéder à leur effacement ou à leur destruction avec des moyens adaptés visant à s'assurer qu'aucune donnée ne puisse être récupérée.

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

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 l'administration toutes les données relatives à la prestation. Le titulaire fournit systématiquement toute la documentation générée dans le cadre de la prestation à l'administration pour archive.

8.2 Sécurité physique

Changement de localisation géographique des services et des données : en cas de changement de localisation des données ou services, le titulaire en informe préalablement l'administration.

Hébergement de données : à la première demande de l'administration, le titulaire identifie tous les titulaires techniques hébergeant ou stockant les données et leurs copies, utilisées ou échangées en cours de marché ainsi que leur localisation.

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.

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.

Protection de l'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.

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.

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.).

8.3 Traitement des incidents

Remontée d'alerte : le service de supervision du titulaire met en place un système de remontée d'alerte à l'administration, afin de détecter tout comportement anormal sur un périmètre SI lié à la prestation (ex : montée en charge du réseau), vol ou perte d'informations appartenant à l'administration (documentation technique en particulier).

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.

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).

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.

8.4 Sécurité du poste de travail

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.

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, les serveurs, les espaces de travail, ou les supports amovibles.

8.5 Sécurité des réseaux et de l'exploitation

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

Sécurisation des flux d'administration : le titulaire chiffre tous les flux d'administration (système et fonctionnelle) par des procédés fiables 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.

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 aux bonnes pratiques et à l'état de l'art.

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 postes de travail et 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 l'administration.

Gestion des mises à jour : le titulaire gère les mises à jour et l'application des correctifs de sécurité et des mises à jour antivirales, pour assurer le maintien en condition opérationnelle de l'ensemble de ses équipements utilisés dans le cadre de la prestation.

Sauvegarde des données : le titulaire met 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 le chef de projet de l'administration dans le cadre de la prestation.

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

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 l'administration) dispose d'un compte individuel nominatif qui lui est personnel et qui ne sera utilisé uniquement par cette personne au cours de la vie du compte ;

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.

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.

Attaques en essai et erreurs sur 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 en essai et erreur sur les secrets d'authentification.

Journalisation des actions : le titulaire conserve de manière exploitable, sur une durée d'un an glissant (y compris après la fin de la prestation), la trace des actions réalisées dans son système pour permettre de conduire toute supervision ou investigation nécessaire à la sécurité des données.

Le titulaire collecte et stocke a minima les informations suivantes :

- connexions et déconnexions aux équipements et applications ;
- consultations d'informations liées à la prestation ;
- informations concernant les accès fructueux et infructueux (identifiant de l'utilisateur, date, heure) aux serveurs du titulaire.

Les traces enregistrées par le titulaire doivent être imputables à un individu ; elles sont par ailleurs horodatées selon une référence horaire commune à l'ensemble des équipements d'un même réseau.

Politique de mot de passe : le titulaire respecte les recommandations de sécurité de la CNIL relatives aux mots de passe pour l'ensemble des comptes d'accès utilisateurs aux postes de travail sous la responsabilité du titulaire.

Validité des licences : le titulaire s'assure de la bonne validité des licences des logiciels qu'il met à disposition de son personnel ou de l'administration dans le cadre de la prestation.

8.6 Sécurité du compte Publik

- L'identifiant de chaque compte utilisé pour accéder à Publik est obligatoirement l'adresse individuelle de messagerie professionnelle de l'employé. Chaque compte ne doit être utilisé que pour les opérations spécifiquement demandées par l'administration. L'utilisation de comptes génériques est proscrite.
- Les identifiants (dont l'adresse, le mot de passe et/ou tout autre facteur d'authentification) de ce compte sont strictement individuels et confidentiels.
- Le choix du mot de passe doit être opéré dans le respect des recommandations de la CNIL (<https://www.cnil.fr/fr/les-conseils-de-la-cnil-pour-un-bon-mot-de-passe>) et celui-ci doit être uniquement utilisé pour ce compte.
- L'enregistrement du mot de passe du compte dans le navigateur est interdit. Le stockage du mot de passe peut être réalisé dans un gestionnaire de type KeePass.
- Les données personnelles techniquement accessibles dans le back-office, en particulier celles relatives aux usagers et à leurs dossiers, ne doivent faire l'objet d'aucune consultation, modification ou suppression qui ne serait pas strictement nécessaire aux opérations externalisées.
- En cas de départ ou de changement de mission de l'employé du titulaire du compte, le titulaire du marché en informe sans délai la CNIL et le compte de l'employé est immédiatement supprimé.

8.7 Sécurité des documents et courrier au format papier

La gestion de documents au format papier est réalisée, sous la responsabilité du titulaire, de façon à en garantir la confidentialité et l'intégrité. En particulier, s'ils doivent l'être, les documents édités au format papier sont détruits d'une façon sécurisée.

8.8 Environnement de travail sécurisé et traçabilité des actions

À des fins de sécurité des données, le titulaire met en œuvre, après information de ses employés et des représentants du personnel le cas échéant, un environnement de travail sécurisé, dédié au traitement des plaintes dans l'outil Publik. L'environnement de travail devra être configuré pour permettre de retracer les actions effectuées individuellement lors du traitement des plaintes dans l'outil Publik sur une durée équivalente à celle de la journalisation des actions de l'article 8.5, et devra garantir un niveau d'étanchéité propre à limiter la capacité à extraire des données de Publik et à garantir leur traitement au sein de l'Union européenne. Cet environnement de travail sécurisé pourra consister en une machine virtuelle équipée d'un système de traçabilité avancé au travers de laquelle les employés pourront accéder à Publik, en un système de traçabilité avancé appliqué au navigateur utilisé pour l'accès à Publik, ou à toute autre solution technique apportant un même niveau de sécurité des données dans le respect des principes de protection des données à caractère personnel.

8.9 Non conservation des données à l'issue de la journée de travail

Le titulaire s'assure de la suppression quotidienne et sécurisée de l'ensemble des données et pièces relatives au traitement des saisines susceptibles d'être enregistrées, pour les stricts besoins définis au marché, sur le poste informatique de ses personnels habilités ou dans son système d'information, à l'exception des journaux d'événements.

Article 9. Annexes

9.1 Schéma général du traitement d'une plainte

9.2 Exemples de scénarios de plaintes susceptibles d'être transmises au prestataire

9.3 Modèles de courrier

9.3.1 Exemple de rappel à la loi (RAL)

9.3.2 Exemple de courrier de clôture (CLA)