Délibération n° 2024-168 du 11 septembre 2024

de la Commission de Contrôle des Informations Nominatives portant avis favorable à la mise en œuvre du traitement automatisé d'informations nominatives ayant pour finalité

« *Gestion des demandes d'exercice des droits adressées à la Délégation Interministérielle chargée de la Transition Numérique* »

exploité par la Délégation Interministérielle chargée de la Transition Numérique

présenté par le Ministre d'Etat

Vu la Constitution du 17 décembre 1962 ;

Vu la Convention Européenne de Sauvegarde des Droits de l'Homme et des Libertés Fondamentales du Conseil de l'Europe du 4 novembre 1950 ;

Vu la Convention n° 108 du Conseil de l'Europe du 28 janvier 1981 pour la protection des personnes à l'égard du traitement automatisé des données à caractère personnel et son Protocole additionnel ;

Vu la Loi n° 1.165 du 23 décembre 1993 relative à la protection des informations nominatives, modifiée ;

Vu l'Ordonnance Souveraine n° 2.230 du 19 juin 2009 fixant les modalités d'application de la Loi n° 1.165 du 23 décembre 1993, modifiée, susvisée ;

Vu l'Ordonnance Souveraine n° 5.840 du 13 mai 2016 portant création du Secrétariat Général du Gouvernement ;

Vu la délibération n° 2011-82 du 21 octobre 2011 de la Commission de Contrôle des Informations Nominatives portant recommandation sur les principes européens applicables aux traitements automatisés ou non automatisés d'informations nominatives ;

Vu la demande d'avis déposée par le Ministre d'Etat, le 13 mai 2024 concernant la mise en œuvre de la modification du traitement automatisé ayant pour finalité « *Gestion des demandes d'exercice des droits adressées à la Délégation Interministérielle chargée de la Transition Numérique* », exploité par le Secrétariat Général du Gouvernement et par la Délégation Interministérielle chargée de la Transition Numérique (DITN) ;

Vu la prorogation du délai d'examen de la présente demande d'autorisation notifiée au responsable de traitement le 11 juillet 2024, conformément à l'article 19 de l'Ordonnance Souveraine n° 2.230 du 19 juin 2009 susvisée ;

Vu le rapport de la Commission de Contrôle des Informations Nominatives en date du 11 septembre 2024 portant examen du traitement automatisé susvisé.

La Commission de Contrôle des Informations Nominatives,

Préambule

Dans le cadre des traitements mis en œuvre par la Délégation Interministérielle chargée de la Transition Numérique (DITN) pour le programme de transition numérique du Gouvernement Princier ou par l'une de ses Directions (Direction des Services Numériques, Direction des Systèmes d'Information, Direction des Plateformes et Ressources Numériques), cette dernière doit se conformer aux obligations qui lui incombent au titre de la protection des informations nominatives.

Afin de répondre à ses obligations, la DITN souhaite proposer aux personnes concernées de pouvoir exercer des demandes concernant leurs droits relatifs à la protection des informations nominatives par le biais d'un formulaire en ligne, par courrier électronique, ou par voie postale.

Ainsi, ce traitement est soumis à l'avis de la Commission, conformément à l'article 7 de la Loi n° 1.165 du 23 décembre 1993.

I. Sur la finalité et les fonctionnalités du traitement

Le traitement a pour finalité « *Gestion des demandes d'exercice des droits adressées à la Délégation Interministérielle chargée de la Transition Numérique* ».

Les personnes concernées sont tout demandeur, les personnels de l'Administration intervenant dans le processus ainsi que le personnel des prestataires en charge de l'intégration et de l'infogérance du site Internet.

Les fonctionnalités du traitement sont :

- permettre aux demandeurs d'exercer leurs droits relatifs à la protection des données personnelles (droit d'accès, droit de rectification, droit d'opposition) auprès des Services de la DITN par le biais du formulaire adressé à la boite email « *mesdonnees@gouv.mc* », par courrier électronique ou par courrier (voie postale) ;
- permettre aux demandeurs de contacter la DITN afin de se renseigner sur le traitement de leurs données personnelles par cette dernière ;
- permettre à la Cellule juridique de la DITN de réceptionner les demandes des personnes relatives à la protection des données (droit d'accès, droit d'opposition, etc…) ;
- permettre la conservation par la DITN des éléments à des fins de démonstration du respect de la réglementation tenant compte des délais de prescriptions légales ;
- permettre la tenue du registre de suivi des demandes de droit d'accès par la DITN.

La Commission constate que la finalité du traitement est déterminée et explicite, conformément aux dispositions de l'article 10-1 de la Loi n° 1.165 du 23 décembre 1993.

II. Sur la licéité et la justification du traitement

La Commission relève que conformément à l'article 15 de la Loi n° 1.165 du 23 décembre 1993 relative à la protection des informations nominatives « *Toute personne justifiant de son identité peut obtenir auprès du responsable du traitement ou de son représentant :*

1° des renseignements portant au moins sur la finalité du traitement, les catégories d'informations sur lesquelles il porte et les destinataires ou catégories de destinataires auxquels les informations sont communiquées ;

2° confirmation que des informations la concernant sont, ou non, traitées ;

3° communication de ces informations sous une forme écrite, non codée et conforme au contenu des enregistrements ; les informations concernant la santé ne peuvent être communiquées par le responsable du traitement ou son représentant qu'aux personnes auxquelles elles peuvent l'être en application des dispositions de la législation relative au consentement et à l'information en matière médicale et selon les modalités qu'elles prévoient ;

4° des informations sur les raisonnements automatisés ayant abouti à la décision visée à l'article 14-1. »

Par ailleurs, la Commission relève que le second alinéa du même texte dispose que :

« *Sauf dispositions législatives particulières, il doit être procédé à la communication dans le mois suivant la réception de la demande. Toutefois, le président de la commission de contrôle des informations nominatives peut, après avis favorable de celle-ci, accorder des délais de réponse ou dispenser de l'obligation de répondre à des demandes abusives par leur nombre, leur caractère répétitif ou systématique, la personne concernée dûment avisée.* »

A cet égard la Commission relève qu'il est indiqué dans le dossier que le délai de réponse est d'1 mois, ou de 3 mois en cas de cas complexe.

Aussi elle rappelle qu'en application de l'article 15, susvisé, le délai légal de réponse à une demande de droit d'accès est d'1 mois, sauf dispositions législatives particulières, et que des délais de réponse supplémentaires ne peuvent être accordés que par le Président de la CCIN, après avis favorable de la Commission.

Sous cette réserve la Commission considère que ce traitement est licite et justifié, conformément aux dispositions des articles 10-1 et 10-2 de la Loi n° 1.165 du 23 décembre 1993.

III. Sur les informations traitées

Les informations nominatives traitées sont :

- identité :
    - pour la demande et la tenue du registre : nom, prénom ;
    - dans le cadre de l'authentification pour accéder au back office (contributeur – personnel de l'Administration) : nom, prénom ;

- coordonnées : adresse email de l'usager qui fait la demande ;

- données d'identification électronique :
    - dans le cadre de l'authentification pour accéder au backoffice (contributeur – personnel de l'Administration) : adresse email, ID d'authentification, adresse IP, mot de passe chiffré ;
    - dans le cadre du formulaire : numéro d'identifiant de la demande ;
    - dans le cadre du registre : référence de la demande ;

- informations temporelles :
    - compte contributeur en backoffice : date et heure de création d'un compte, date et heure de modification d'un compte ;
    - système : logs système ;
    - dans le cadre de la traçabilité des connexions au backoffice (contributeur – personnel de l'Administration) : données d'horodatage ;
    - dans le cadre de la traçabilité des modifications de contenus via le backoffice (contributeur – personnel de l'Administration : logs (nom, prénom, données d'horodatage) ;
    - dans le cadre du formulaire : date et heure d'envoi du formulaire ;

- demande d'exercice de droits : type de la demande (types de droits concernés), message, pièce d'identité en noir et blanc (facultative, en cas de doute raisonnable sur l'identité de la personne concernée) ;

- registre des demandes de droits des personnes : référence de la demande, date d'anonymisation, identité du demandeur, catégorie du demandeur, coordonnées du demandeur, localisation du demandeur, vérification de l'identité, première demande (O / N), date de la demande, date de réception de la demande, type de droit exercé, objet de la demande, date limite de réponse, date d'envoi de la réponse ;

- données issues du widget FriendlyCaptcha : données relatives à l'en-tête de la requête http (notamment le navigateur de l'utilisateur, l'origine et le site internet référent), date / heure de la requête, version du widget utilisé, ID du compte de l'Administration du site web de l'Administration, valeur de hachage (cryptage à sens unique) de l'adresse IP entrante (l'adresse IP n'est pas prise en compte, seule la valeur de hachage est enregistrée), nombres de demandes provenant de l'adresse IP (hachée par période, réponse au problème arithmétique résolu sur l'ordinateur du visiteur.

S'agissant de la collecte de la pièce d'identité, le responsable de traitement précise qu'une copie de celle-ci est demandée en noir et blanc uniquement en cas de doute raisonnable sur l'identité du demandeur. La Commission en prend acte et rappelle néanmoins que les modalités de collecte d'une copie d'un document d'identité doivent faire l'objet de mesures de protection particulières, comme rappelé dans sa délibération n° 2015-113 du 18 novembre 2015 portant recommandation sur la collecte et la conservation de la copie de documents d'identité officiels.

Le responsable de traitement indique que les informations objet du présent traitement proviennent de la personne concernée à l'exception des :

- informations temporelles qui sont générées par le système ;
- informations traitées dans le cadre de l'authentification pour accéder au backoffice (personnel de l'Administration) qui ont pour origine le traitement légalement mis en œuvre ayant pour finalité *« Gestion centralisée des accès aux applications du SI »* ; et

- informations contenues dans le registre des demandes de droits qui proviennent du personnel habilité à recevoir la demande.

La Commission considère que les informations traitées sont *« adéquates, pertinentes et non excessives »* au regard de la finalité du traitement, conformément aux dispositions de l'article 10-1 de la Loi n° 1.165, modifiée.

IV. Sur les droits des personnes concernées

➢ *Sur l'information préalable des personnes concernées*

Le responsable de traitement indique que l'information préalable des personnes concernées est assurée au moyen d'une mention particulière intégrée en bas de tous les formulaires de contact du Gouvernement.

A la lecture de la mention jointe, la Commission constate qu'elle est conforme aux exigences légales.

Par ailleurs, elle relève que le responsable de traitement a également mis en place une procédure de gestion des exercices des droits qui a été portée à la connaissance des membres de la DITN par l'envoi d'un email.

➢ *Sur l'exercice du droit d'accès des personnes concernées*

Le responsable de traitement ne prévoit pas des mesures relatives au droit d'accès dans le dossier en indiquant que le présent traitement concerne la gestion de l'exercice du droit d'accès pour les traitements qu'il met en œuvre. La Commission rappelle toutefois que le droit d'accès s'applique aux informations objet du présent traitement.

V. Sur les destinataires et les personnes ayant accès au traitement

Les accès sont définis comme suit :

- personnel de la DITN habilité à recevoir les demandes d'exercice de droits : tous les droits dans le cadre de leurs missions liées au traitement de la demande (accès à la boite email, aux demandes reçues via le formulaire en ligne, aux demandes par voie papier, au registre de suivi des demandes. Il ne dispose pas d'un accès au back-office de la solution ;
- la Direction des Services Numériques (DSN) dans le cadre du formulaire en ligne : tous les droits dans le cadre des missions de maintenance, développement des applicatifs nécessaires au fonctionnement des sites et de sécurité des sites et système d'information et en consultation, exploitation, validation et traitement des données pour les webmasters ;
- la Direction des Systèmes d'Information (DSI) : tous les droits et accès aux données techniques nécessaires à l'exécution de ses missions liées à la maintenance de l'infrastructure ;
- le personnel de l'éditeur : tous les droits pour la TMA ;
- le personnel de l'infogérant : tous les droits pour l'infogérance de l'infrastructure.

La Commission considère que ces accès sont justifiés au regard du traitement.

Cependant elle rappelle, en ce qui concerne les prestataires que conformément aux dispositions de l'article 17 de la Loi n° 1.165 du 23 décembre 1993, les droits d'accès de ces

derniers doivent être limités à ce qui est strictement nécessaire à l'exécution de leurs contrats de prestation de service. De plus, lesdits prestataires sont soumis aux mêmes obligations de sécurité et de confidentialité que celles imposées au responsable de traitement, en application de ce même article.

VI. Sur les interconnexions et rapprochements avec d'autres traitements

Le responsable de traitement indique que le présent traitement est interconnecté avec les traitements suivants, légalement mis en œuvre :

- « *Gestion des habilitations et des accès au Système d'Information* » afin de disposer des éléments permettant de créer un compte aux utilisateurs pour qu'ils puissent se connecter au réseau afin d'exécuter leurs missions selon leur profil ;
- « *Gestion et analyse des évènements du système d'information* » afin de veiller à la traçabilité et à la sécurité des actions effectuées sur le réseau ;
- « *Gestion centralisée des accès aux applications du SI* » afin de permettre aux contributeurs et webmasters de gérer les sites grâce à un accès backoffice de la plateforme ;
- « *Gestion des accès dédiés au système d'information* », afin de sécuriser les accès prestataire en cas de montées de version, maintenance ou correction d'anomalies.

Il précise en outre que le traitement est rapproché avec les traitements, légalement mis en œuvre suivants :

- « *Gestion de la messagerie professionnelle* » afin de permettre aux acteurs du traitement (techniciens, utilisateurs…) de pouvoir échanger dans le cadre de leurs fonctions ;
- « *Assistance aux utilisateurs par le Centre de Service de la DSI* » afin de permettre de remonter un incident sur un des sites ou sur le backoffice ;
- *« Gestion des sites internet du Gouvernement Princier ».*

Il appert en outre, à la lecture du dossier que le présent traitement fait l'objet d'un rapprochement avec le traitement légalement mis en œuvre ayant pour finalité *« Gestion d'un outil de partage et de conservation sécurisés de documents »*.

Enfin, le responsable de traitement indique que le présent traitement est rapproché avec tout traitement mis en œuvre par la DITN (SGG) ou par l'une des Directions de la DITN (DSI, DSN, DPRN), afin de permettre d'effectuer les recherches et extraction nécessaires pour apporter une réponse au demandeur.

La Commission en prend acte et rappelle que tout rapprochement ou interconnexion ne peut avoir lieu qu'entre des traitement légalement mis en œuvre.

Sous cette condition, la Commission considère que ces interconnexions et ces rapprochements sont conformes aux exigences légales.

VII. Sur la sécurité du traitement et des informations

Les mesures prises pour assurer la sécurité et la confidentialité du traitement et des informations qu'il contient n'appellent pas d'observation particulière.

Il convient toutefois de rappeler que les communications d'information doivent être sécurisées en tenant compte de la nature des informations transmises.

La Commission rappelle par ailleurs que les éléments de réponses constitués dans le cadre de ce traitement doivent être conservés dans un espace sécurisé accessible aux seules personnes habilitées.

En outre, la Commission rappelle que les ports non utilisés doivent être désactivés et que les serveurs, périphériques, équipements de raccordements (switchs, routeurs, pare-feux) ainsi que chaque compte utilisateur et administrateur doivent être protégés individuellement par un identifiant et par un mot de passe réputé fort, régulièrement renouvelé.

Elle rappelle enfin que, conformément à l'article 17 de la Loi n° 1.165 du 23 décembre 1993, les mesures techniques et organisationnelles mises en place afin d'assurer la sécurité et la confidentialité du traitement au regard des risques présentés par celui-ci et de la nature des données à protéger devront être maintenues et mises à jour en tenant compte de l'état de l'art, afin de permettre de conserver le haut niveau de fiabilité attendu tout au long de la période d'exploitation du présent traitement.

VIII. Sur la durée de conservation

Le responsable de traitement précise que les données d'identité et les données d'identification électronique des contributeurs dans le backoffice, personnels de l'Administration, sont conservées *« tant que le compte de l'utilisateur est activé sur le backoffice concerné »*.

Il indique en outre que les informations temporelles dans le cadre de la traçabilité des connexions au backoffice et des modifications de contenus via le backoffice sont conservées 12 mois glissants.

Les logs systèmes sont conservés 1 mois.

Par ailleurs, le responsable de traitement précise s'agissant des données issues du widget Friendly Captcha, que « *les adresses IP ne sont stockées que sous forme hachée. Les données d'utilisation personnelles sont supprimées dans un délai de 30 jours. Le widget n'installe pas de cookies sur l'ordinateur du visiteur* ». De plus « *les données des utilisateurs de l'Administration sont stockées dans la base de données sous forme chiffrée. Les adresses IP entrantes des utilisateurs de l'Administration sont uniquement sauvegardées par Friendly Captcha sous forme hachée en utilisant un chiffrage à sens unique* ».

Le responsable de traitement indique de plus que *« la copie de la pièce d'identité est supprimée immédiatement après la clôture de la demande »*. La Commission en prend acte.

En outre, il indique que les informations collectées dans le cadre du formulaire sont conservées pendant 2 ans à compter de la réception de la demande d'exercice de droits *« sur l'interconnexion avec le traitement ayant pour finalité « Gestion des sites internet du Gouvernement Princier » »*.

Il précise que *« parallèlement les données collectées sont également conservées 5 ans à compter de la réception de la demande d'exercice de droits sur la boîte mail dédiée, accessible uniquement par la personne en charge des données personnelles à la DITN et la responsable juridique »*.

De plus, le responsable de traitement indique que les données présentes sur le registre sont conservées *« 5 ans sur un espace sécurisé puis anonymisation »*.

A cet égard, la Commission relève que l'article 13 du Code de procédure pénale dispose que l'action publique résultant d'un délit est prescrite après trois années révolues. Ainsi, elle considère que la durée de 5 ans est trop longue et la fixe en conséquence à 3 ans à compter de la réception de la demande.

Sous cette condition, la Commission considère que ces durées de conservation sont conformes aux exigences légales.

Après en avoir délibéré, la Commission :

Rappelle que :

- les modalités de collecte d'une copie d'un document d'identité doivent faire l'objet de mesures de protection particulières, comme rappelé dans sa délibération n° 2015-113 du 18 novembre 2015 portant recommandation sur la collecte et la conservation de la copie de documents d'identité officiels ;

- en application de l'article 15 de la Loi n° 1.165 le délai légal de réponse à une demande de droit d'accès est d'1 mois, sauf dispositions législatives particulières, et que des délais de réponse supplémentaires ne peuvent être accordés que par le Président de la CCIN, après avis favorable de la Commission ;

- le droit d'accès s'applique aux informations objet du présent traitement ;

- tout rapprochement ou interconnexion ne peut avoir lieu qu'entre des traitement légalement mis en œuvre ;

- les communications d'information doivent être sécurisées en tenant compte de la nature des informations transmises ;

- les éléments de réponses constitués dans le cadre de ce traitement doivent être conservés dans un espace sécurisé accessible aux seules personnes habilitées ;

- les ports non utilisés doivent être désactivés et que les serveurs, périphériques, équipements de raccordements (switchs, routeurs, pare-feux) ainsi que chaque compte utilisateur et administrateur doivent être protégés individuellement par un identifiant et par un mot de passe réputé fort, régulièrement renouvelé.

Fixe la durée de conservation :

- de l'ensemble des informations collectées dans le cadre de l'exercice d'un droit d'accès, à l'exception des documents d'identité, à 3 ans à compter de la réception de la demande ;

- du registre à 3 ans.

Sous le bénéfice de la prise en compte de ce qui précède,

la Commission de Contrôle des Informations Nominatives **émet un avis favorable à la mise en œuvre, par le Ministre d'Etat, du traitement automatisé d'informations nominatives ayant pour finalité *« Gestion des demandes d'exercice des droits adressées à la Délégation Interministérielle chargée de la Transition Numérique ».***

Le Président,

Robert CHANAS