Délibération n° 2024-132 du 12 juin 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

« *Sensibilisation à la sécurité numérique et tests de faux phishing* »

exploité par le Secrétariat Général du Gouvernement et 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 la Loi n° 1.435 du 8 novembre 2016 relative à la lutte contre la criminalité technologique ;

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 l'Arrêté ministériel n° 2022-331 du 13 juin 2022 portant application de l'article 23 de la Loi n° 1.435 du 8 novembre 2016 relative à la lutte contre la criminalité technologique, fixant les mesures de sécurité des systèmes d'information de l'Etat ;

Vu la délibération n° 2011-82 du 21 octobre 2011 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 28 mars 2024 concernant la mise en œuvre de la modification du traitement automatisé ayant pour finalité « *Sensibilisation à la sécurité numérique et tests de faux phishing* », exploité par le Secrétariat Général du

Gouvernement et par la Délégation Interministérielle chargée de la Transition Numérique (DITN) ;

Vu le rapport de la Commission de Contrôle des Informations Nominatives en date du 12 juin 2024 portant examen du traitement automatisé susvisé.

## La Commission de Contrôle des Informations Nominatives,

### Préambule

Afin de protéger l'Administration contre les courriels frauduleux, ce qui implique de sensibiliser les utilisateurs du Système d'Information de l'Etat, le Gouvernement Princier souhaite se doter d'une solution permettant de réaliser des campagnes de faux phishing et la mise à disposition pour les personnes concernées de modules de formation sur des thématiques relatives à la sécurité numérique.

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 « *Sensibilisation à la sécurité numérique et tests de faux phishing* ».

Les personnes concernées sont les utilisateurs de la messagerie des Services exécutifs de l'Etat (fonctionnaires, agents de l'Etat), les prestataires ainsi que les utilisateurs de la plateforme d'administration.

Les fonctionnalités du traitement sont :

- réaliser des campagnes de faux phishing ;
- proposer des modules de sensibilisation (e-learning) aux utilisateurs du Gouvernement ;
- consulter le suivi des modules du e-learning ;
- permettre aux utilisateurs du Gouvernement de remonter les faux phishings réceptionnés via le bouton d'alerte phishing ;
- importer des utilisateurs du Gouvernement depuis le back-office ;
- générer des rapports nominatifs et anonymisés depuis le back-office ;
- établir des statistiques nominatives et anonymisées depuis le back-office.

Il résulte de l'analyse du dossier que les statistiques nominatives permettent de savoir quel utilisateur a cliqué ou non sur les liens frauduleux, et le taux d'avancement dans le e-learning de sensibilisation. A cet égard, la Commission rappelle que la finalité du traitement est de sensibiliser et former les personnels à la sécurité numérique et que l'analyse des statistiques des utilisateurs ne doit pas conduire à des prises de décision ayant des conséquences juridiques les concernant.

La Commission considère que le présent traitement ne concerne que la sensibilisation des utilisateurs à la sécurité numérique et aux tentatives de phishing par le biais de tests.

A cet égard, le responsable de traitement indique que le bouton alerte phishing permet de faire remonter également des potentielles réelles tentatives de phishing, susceptibles d'être réceptionnées par les utilisateurs. Dans ce cas, l'alerte sera remontée à l'équipe DSI chargée

de sa qualification dans le cadre du traitement, légalement mis en œuvre ayant pour finalité *« Assistance aux utilisateurs par le Centre de Service de la DSI »*.

Cela avait conduit le responsable de traitement à indiquer au sein du présent traitement un accès DSI, une interconnexion GLPI et des données de tickets. La Commission estime que ces informations permettent d'apprécier le cheminement complet des emails une fois le bouton alerte activé. Elle considère cependant que ces éléments ne font pas partie du traitement.

Enfin, elle prend acte que ce bouton d'alerte sera intégré de manière permanente et les modalités d'utilisation portées dans la documentation interne à destination des utilisateurs.

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

Le responsable de traitement indique que le présent traitement est justifié par le respect d'une obligation légale ainsi que par un motif d'intérêt public.

A cet égard, il indique que conformément à l'article 23 de la Loi n° 1.435 du 8 novembre 2016 relative à la lutte contre la criminalité *technologique « le Ministre d'Etat veille à ce que toutes mesures soient prises aux fins d'assurer, dans la Principauté, la sécurité des systèmes d'information »*.

Le responsable de traitement précise que le Gouvernement est investi d'une mission de sécurité au regard de l'ensemble des systèmes d'information de l'Etat. Le Responsable de la Sécurité des Systèmes d'Information (RSSI) est chargé, conformément à l'article 4 de l'Arrêté Ministériel n° 2022-331 du 13 juin 2022 portant application de la Loi susvisée, de la mise en œuvre et du suivi de la Politique de Sécurité des Systèmes d'Information de l'Etat sur les systèmes d'information. Ainsi, il a notamment pour mission « *de conduire des actions de sensibilisation et formation à la sécurité des systèmes d'information auprès des fonctionnaires et agents publics ou préposés des services publics* ».

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 : nom et prénom de l'utilisateur du SI de l'Etat ;
- coordonnées : adresse email de l'utilisateur ;
- vie professionnelle : groupe (Direction), Service (Interne / Externe) ;
- données d'identification électronique :
    - utilisation bouton phishing (données à usage statistiques transmises au prestataire) : email signaleur ;
    - adresse IP (e-learning) des PC du Gouvernement ;
    - user agent, engine version, OS name, OS version, device CPU ;
- données techniques : log des utilisateurs du back-office ;

- logs de connexion : login utilisateur, nom du poste, adresse MAC, type d'action effectuée/refusée sur la ressource loguée, action effectuée sur le poste de travail, données d'horodatage (date, heure précise), durée de l'action, applications exécutées, les événements ;
- données de paramétrage de l'envoi des emails : langue de l'utilisateur, fuseau horaire de l'utilisateur.

La Commission relève que la préparation des campagnes et l'envoi des emails de faux phishing ont vocation à cibler l'utilisateur et ainsi l'induire à cliquer sur le lien ou sur la pièce jointe. Ainsi, elle considère que ces envois ne doivent pas conduire le responsable de traitement à obtenir des informations supplémentaires de la part des utilisateurs tels que des identifiants, mots de passe ou encore des informations sensibles, notamment des données de santé ou encore des données bancaires.

Les informations relatives à l'identité, à la vie professionnelle ainsi que l'adresse et les données de paramétrage de l'envoi des emails ont pour origine l'Administrateur de la solution. Les autres données proviennent du système.

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*

A titre liminaire, le responsable de traitement indique que pendant la phase d'audit aucune information préalable ne peut être fournie aux personnes concernées afin de ne pas fausser les résultats.

Toutefois, le responsable de traitement précise qu'une mention d'information apparaîtra sur l'écran des utilisateurs après réception d'un email de faux phishing. A cet égard, il indique que la mention d'information s'affiche uniquement dans les hypothèses où « *les utilisateurs cliquent sur le lien ou la pièce jointe présente dans l'email de faux phishing »* ou qu'ils signalent l'email à l'aide du Bouton Alerte Phishing. Le responsable de traitement précise qu' « *un message apparaît informant l'agent de la nature de l'email* ».

En outre, la Commission relève que cette information n'intervient qu'après un clic de l'utilisateur sur le lien inséré dans l'email ou sur la pièce jointe. Ainsi, elle considère que certains utilisateurs, notamment ceux « *passifs* » ne cliquant pas et ne signalant pas l'email, ne disposeront pas d'une information pendant la phase d'audit.

Cependant, le responsable de traitement précise que ces personnes bénéficieront d'une information « *lors de la publication des résultats généraux de l'audit* » qui sera assurée par le biais d'une notice disponible sur l'Intranet.

A la lecture desdites mentions, jointes au dossier la Commission considère que l'information est conforme à l'article 14 de la Loi n° 1.165. Toutefois, ladite mention d'information indique une liste de personnes ayant accès qui ne correspond pas à celle mentionnée au dossier, qui comprend le prestataire. Aussi, si les personnes ayant accès ne sont pas spécifiquement visées par l'article 14 de la Loi susvisée, la Commission estime que si le responsable de traitement souhaite les indiquer cela doit être conforme à la réalité desdits accès.

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

Le responsable de traitement indique que le droit d'accès s'exerce par voie postale auprès de la Délégation Interministérielle de la Transition Numérique (DITN).

Par ailleurs, il ressort à l'étude du dossier que le droit d'accès peut également être exercé au moyen d'un formulaire permettant de contacter le service de protection des données personnelles de la DITN.

A cet égard, la Commission rappelle que la réponse au droit d'accès doit s'exercer dans le mois suivant la réception de la demande.

Sous cette condition, la Commission considère que les modalités d'exercice des droits des personnes concernées sont conformes aux dispositions des articles 13, 15 et 16 de la Loi n° 1.165 du 23 décembre 1993, modifiée.

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

Les accès sont définis comme suit :

- le Responsable de la Sécurité des Systèmes d'Information (RSSI) et son adjoint : en inscription, modification et consultation (accès au back office de la solution) ;
- le prestataire (éditeur de la solution) :
  - administrateurs développeurs : accès à l'intégralité du code en production, validation des modifications apportées au code, accès à l'intégralité des données client : en consultation et maintenance ;
  - développeurs : accès au code uniquement en environnement de test, proposent les modifications à apporter au code : pas d'accès aux données nominatives.

La Commission rappelle, en ce qui concerne le prestataire que conformément aux dispositions de l'article 17 de la Loi n° 1.165 du 23 décembre 1993, les droits d'accès de ce dernier doivent être limités à ce qui est strictement nécessaire à l'exécution de son contrat de prestation de service. De plus, ledit prestataire est soumis aux mêmes obligations de sécurité et de confidentialité que celles imposées au responsable de traitement, en application de ce même article.

La Commission considère que ces accès sont justifiés.

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

Le responsable de traitement indique que le présent traitement est rapproché avec le traitement suivant, 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 et d'insérer les coordonnées des agents de l'Etat par l'implémentation d'un fichier CSV dans la solution du prestataire.

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

- « *Gestion de la messagerie professionnelle* » afin de pouvoir échanger sur toutes informations concernant le traitement (communication, formation, etc.) et envoyer les

emails de faux phishing aux personnes concernées dans le cadre de la sensibilisation à la sécurité numérique et tests de faux phishing ;

- « *Gestion et analyse des événements du Système d'Information* » afin de veiller à la traçabilité et à la sécurité des actions effectuées sur le réseau.

La Commission considère que ces interconnexions et ce rapprochement 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.

Cependant, 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 par ailleurs que la copie ou l'extraction d'informations issues de ce traitement devra être chiffrée sur son support de réception.

La Commission 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 indique que les informations relatives à l'identité, à la vie professionnelle ainsi que les coordonnées et les données de paramétrage de l'envoi des emails sont conservés « *tant que l'utilisateur est actif* » et seront supprimées au bout de *« 120 jours à compter de la fin de la relation contractuelle avec l'éditeur de la solution »*. Il précise qu'en cas de départ de l'utilisateur avant la fin de la relation contractuelle avec l'éditeur de la solution, son profil *« est archivé et est anonymisé 180 jours après l'archivage* ».

Par ailleurs, il indique que les données d'identification électronique relatives à l'utilisation du bouton phishing (données à usage statistique transmises au prestataire) sont supprimées au bout de *« 120 jours à compter de la fin de la relation contractuelle avec l'éditeur de la solution »*.

Il indique en outre, que les logs des utilisateurs du back office sont conservées 6 mois glissants.

Enfin, le responsable de traitement indique que les logs de connexion sont conservés 3 mois en base active puis ils sont gardés 1 an en archivage long terme. Il justifie cette durée en faisant référence au traitement ayant pour finalité *« Gestion et analyse des évènements du système d'information »*.

A cet égard, la Commission rappelle que conformément à sa délibération n° 2020-126 du 16 septembre 2020 portant avis favorable à la mise en œuvre du traitement ayant pour finalité *« Gestion et analyse des évènements du système d'information »* les logs de connexion

sont conservés pendant 12 mois glissants. Ainsi, la Commission fixe la durée de conservation des logs de connexion à 12 mois glissants.

**Après en avoir délibéré, la Commission :**

**Considère** que les envois d'emails de faux phishing ne doivent pas conduire à obtenir des informations supplémentaires de la part des utilisateurs tels que des identifiants, des mots de passe ou encore des informations sensibles, notamment des données de santé ou encore des données bancaires.

**Rappelle que :**

- la finalité du traitement est de sensibiliser et former les personnels à la sécurité numérique et que l'analyse des statistiques des utilisateurs ne doit pas conduire à des prises de décision ayant des conséquences juridiques les concernant ;

- la réponse au droit d'accès doit s'exercer dans le mois suivant la réception de la demande ;

- 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 ;

- la copie ou l'extraction d'informations issues de ce traitement devra être chiffrée sur son support de réception.

**Fixe** la durée de conservation des logs de connexion à 12 mois glissants.

**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 modification, par le Ministre d'Etat, du traitement automatisé d'informations nominatives ayant pour finalité *« Sensibilisation à la sécurité numérique et tests de faux phishing ».***

Le Président

Guy MAGNAN