Délibération n° 2021-171 du 21 juillet 2021

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

« *Gestion des accès dédiés au Système d'information* »,

exploité par la Direction des Systèmes d'Information

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 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 délibération n° 2019-136 du 18 juillet 2019 portant avis favorable à la mise en œuvre du traitement du traitement automatisé ayant pour finalité « *Gestion des accès à distance au système d'information du Gouvernement* » ;

Vu la demande d'avis déposée par le Ministre d'Etat, le 20 avril 2021, concernant la modification d'un traitement automatisé ayant pour finalité la « *Gestion des accès à distance au Système d'information du Gouvernement* » ;

Vu la prorogation du délai d'examen de la présente demande d'avis notifiée au responsable de traitement le 17 juin 2021, 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 21 juillet 2021 portant examen du traitement automatisé susvisé.

La Commission de Contrôle des Informations Nominatives,

Préambule

Par délibération n° 2019-136 du 18 juillet 2019, la Commission avait émis un avis favorable à la mise en œuvre d'un traitement automatisé ayant pour finalité la « *Gestion des accès à distance au Système d'information du Gouvernement* », qui avait pour objectif d'« *assurer la sécurité des accès à distance au Système d'information du Gouvernement par le biais d'une solution adaptée en évitant le recours à des logiciels de prise en main à distance non sécurisés et non maîtrisés* ».

Le Gouvernement souhaite désormais en élargir les fonctionnalités.

Ainsi, cette modification est soumise à l'avis de la Commission, conformément aux dispositions des articles 7 et 9 de la Loi n° 1.165 du 23 décembre 1993.

I. Sur la finalité et les fonctionnalités du traitement

Le responsable de traitement souhaite modifier la finalité comme suit : « *Gestion des accès dédiés au Système d'information* ».

Il concerne toujours les fonctionnaires et agents de l'Etat, ainsi que les prestataires avec accès à distance.

Les fonctionnalités du traitement sont désormais :

- Permettre un accès à certains environnements du système d'information du Gouvernement de manière sécurisée ;
- Disposer d'informations permettant d'examiner les demandes, d'implémenter la procédure et son fonctionnement ;
- Assurer l'implémentation de la solution, son activation, sa désactivation et sa suppression ;
- Assurer la gestion d'un annuaire spécifique et gérer les comptes associés ;
- Analyser les besoins de maintenance de la solution et communiquer avec les personnes intéressées en cas d'intervention sur le Bastion (ex. maintenance) ;
- Permettre la traçabilité des sessions et l'imputabilité des actions ;
- Vérifier, a posteriori, si nécessaire, les actions réalisées par les utilisateurs de la solution et disposer, le cas échéant, de preuves ou de débuts de preuves si de besoin ;
- Conserver des éléments retraçant la réalisation des opérations réalisées par les agents à des fins, le cas échéant, de vérification et de compréhension d'une situation donnée ;
- Assurer les opérations de suivi et de maintenance des équipements et ressources de l'environnement ;
- Etablir des statistiques, rapports d'évaluation et d'analyse.

Il est rappelé que les accès aux applications, environnements, logiciels, etc., sont gérés par les logs dédiés desdits environnements, applications, logiciels, etc. La Commission relève que le traitement sert désormais à tracer des accès à des environnements du système d'information nécessitant une plus grande traçabilité, même si l'accès n'est pas effectué à distance, notamment pour des tâches d'administration.

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 le fondement juridique du traitement demeure inchangé.

III. Sur les informations traitées

Pour rappel, les informations nominatives traitées sont :

En ce qui concerne les référents du service demandeur :

- identité : nom, prénom ;
- coordonnées professionnelles : téléphone, email ;
- vie professionnelle : fonction, service ;
- informations relatives à la demande : projet, raison de l'accès, date de début, date de fin, date de validation, commentaires ;
- statut de la demande : production/en attente/clôturée/refusée avec raison.

En ce qui concerne le prestataire signataire de la convention :

- identité du signataire : nom, prénom ;
- vie professionnelle : fonction, signature, société;
- statut : date de la convention.

En ce qui concerne la personne désignée pour accéder à distance :

- identité : nom, prénom ;
- vie professionnelle : société ou entité, fonction ;
- coordonnées professionnelles : email, téléphone, adresse postale, email autre pour des informations sur les opérations de maintenance ;
- données d'identification électronique : login, mot de passe ;
- données de connexion : serveur, lieu et adresse IP publique depuis laquelle le/les prestataires devront ouvrir la connexion (IP de l'entreprise ou du domicile) ;
- connaissance de la solution : oui/non (explication orale si réponse négative) ;
- objet de la demande : horaire de connexion, date (début-fin), raison de l'accès, intitulé du projet/logiciel/mission concerné ;
- logs de connexion sur le réseau (pare-feu/environnement/équipement interne réseau/serveur cible interne) : données d'horodatage de la dernière connexion (date et heure), DN de l'utilisation (sur serveur cible, prénom, nm, login, adresse IP de connexion (pare-feu) ;
- éléments de la solution Wallix : DN de l'utilisation ; enregistrement des sessions (vidéo des actions réalisées par la personne) ;
- profil utilisateur/plateforme Wallix : nom, prénom.

En ce qui concerne le contact/référent chez le prestataire (si autre au précédente) :

- identité : nom, prénom ;
- coordonnées professionnelles : email.

En ce qui concerne les Agents de la DRSI en charge du projet (référent interne) :

- identité : nom, prénom ;
- coordonnées professionnelles : téléphone, email ;
- vie professionnelle : fonction, service.

IV. Sur les droits des personnes concernées

➢ ***Sur l'information préalable des personnes concernées***

L'information préalable des personnes concernées est réalisée par une mention sur le document de collecte ou une mention dans la convention.

Toutefois ces documents ne sont pas joints à la demande d'avis.

Aussi la Commission rappelle que l'information des personnes concernées doit être effectuée conformément à l'article 14 de la Loi n° 1.165.

➢ ***Sur l'exercice du droit d'accès, de modification et de mise à jour***

Le droit d'accès est exercé par voie postale auprès de la Direction des Systèmes d'Information.

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

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

La Commission constate que les informations objets du traitement sont susceptibles d'être communiquées aux Autorités compétentes en cas de litige.

Les accès sont en outre définis comme suit :

- RSSI : tout accès dans le cadre de ses missions de validation et de contrôle ;

- RSO (Responsable de la Sécurité Opérationnelle) : en lecture pour dans le cadre de la vérification du respect des procédures ;

- Administrateurs de la cellule sécurité de la DRSI : tout accès pour ses missions de Création de compte et de Gestion des vidéos ;

- Administrateurs des divisions infra et réseaux : communication des données permettant le paramétrage des serveurs *via* les tickets d'intervention GLPI et assurer la MCO (Maintient Continuité Opérationnel) du système en production ;

- Agents du Centre de Service chargés de la gestion des comptes AD : Communication des données permettant de valider la procédure de création d'un compte AD (tout accès).

La Commission constate qu'il est fait recours à des prestataires. Elle rappelle 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.

La Commission considère que ces accès sont justifiés.

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

Le responsable de traitement indique que le traitement est rapproché aux traitements légalement mis en œuvre suivants :

- « *Assistance aux utilisateurs par le Centre de Service de la DSI* », pour effectuer toute demande support en lien avec le traitement ;

- « *Gestion de la messagerie professionnelle* », pour permettre l'échange de messages entre intervenants ;

- « *Gestion des habilitations et des accès au Système d'information* », pour des raisons de corrélations d'informations ;

Il est également interconnecté avec le traitement légalement mis en œuvre suivant :

- « *Gestion et analyse des évènements du système d'information* », afin de collecter les logs des ressources support du traitement pour exploitation comme décrit dans le traitement concerné.

La Commission considère que ces rapprochements et interconnexions 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.

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

En outre, les ports non utilisés doivent être désactivés et 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 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

Par délibération n° 2019-136, la Commission avait considéré les durées de conservation conformes aux exigences légales, excepté les durées relatives à l'identité des référents du service demandeur. Elle avait ainsi fixé ces durées de conservation à un an à compter de la collecte, ou en cas de demande ayant fait l'objet d'un refus, à 6 mois à compter dudit refus.

Le responsable de traitement indique dans la présente demande d'avis modificative avoir intégré la durée de conservation de 6 mois à compter du refus, mais souhaite garder les informations relatives au référent tant qu'il en a le rôle, car c'est « *la personne qui au sien de l'Administration suit un projet nécessitant la mise en place de la procédure. Aussi, ce référent est « le relais » de la Division Sécurité, par exemple, afin de déterminer si ce type d'accès doit être créé, modifié, ou supprimé* ».

La Commission prend acte de ces précisions et considère la durée demandée comme conforme aux dispositions légales. Elle relève également que le responsable de traitement précise que « *si le référent venait à changer, alors l'identité de son prédécesseur est supprimée et remplacée par le nouveau référent* ».

Après en avoir délibéré, la Commission :

Rappelle que :

- l'information des personnes concernées doit être effectuée conformément à l'article 14 de la Loi n° 1.165 ;

- les ports non utilisés doivent être désactivés et 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 doit être chiffrée sur son support de réception.

Considère que les informations relatives à l'identité des référents du service demandeur peuvent être conservées tant que ces derniers conservent ce rôle.

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 *« Gestion des accès dédiés au Système d'information ».***

Le Président

Guy MAGNAN