

Décision n° HOM-2021-001 du 28 juillet 2021 portant homologation de sécurité du portail usager et des téléservices associés mis en œuvre par la Commission nationale de l'informatique et des libertés

La Présidente de la Commission nationale de l'informatique et des libertés,

Vu le règlement 2016/679 du Parlement européen et du Conseil du 27 avril 2016 relatif à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données, et abrogeant la directive 95/46/CE (règlement général sur la protection des données) ;

Vu la loi n° 78-17 du 6 janvier 1978 modifiée relative à l'informatique, aux fichiers et aux libertés ;

Vu l'ordonnance n° 2005-1516 du 8 décembre 2005 relative aux échanges électroniques entre les usagers et les autorités administratives et entre les autorités administratives ;

Vu le décret n° 2010-112 du 2 février 2010 pris pour l'application des articles 9, 10 et 12 de l'ordonnance n° 2005-1516 du 8 décembre 2005 relative aux échanges électroniques entre les usagers et les autorités administratives et entre les autorités administratives ;

Vu l'arrêté du 13 juin 2014 portant approbation du référentiel général de sécurité et précisant les modalités de mise en œuvre de la procédure de validation des certificats électroniques ;

Vu les pièces composant le dossier d'homologation de sécurité ;

Observe :

I. SUR LE PORTAIL USAGER ET LES TELESERVICES ASSOCIES

Le portail usager mis en œuvre par la CNIL permet à ses publics d'accomplir des démarches auprès de la Commission, via différents téléservices, de façon sécurisée. Il peut s'appuyer sur un compte usager facilitant les échanges et permettant le suivi des demandes.

II. SUR LE REFERENTIEL GENERAL DE SECURITE

Le référentiel général de sécurité, prévu par l'article 9 de l'ordonnance du 8 décembre 2005, a été approuvé, dans sa version 2.0, par l'arrêté du 13 juin 2014. Il définit un ensemble de règles et de recommandations applicables aux téléservices des administrations. Il a pour objet le renforcement de la confiance des usagers dans les services électroniques mis à disposition par les autorités administratives.

III. SUR LA PROTECTION DES DONNEES A CARACTERE PERSONNEL

Le règlement général sur la protection des données (RGPD) et la loi du 6 janvier 1978 modifiée imposent notamment au responsable d'un traitement de données à caractère personnel de mettre en œuvre les mesures techniques et organisationnelles appropriées afin de garantir un niveau de sécurité adapté au risque.

IV. SUR L'EVALUATION ET LA REDUCTION DES RISQUES

L'analyse conduite a permis de définir les mesures de sécurité adaptées aux risques identifiés. Les exigences du référentiel général de sécurité sont mises en œuvre.

Cette démarche a également permis d'évaluer les garanties définies en matière de protection des données à caractère personnel.

Un plan d'action visant à réduire les risques identifiés a été élaboré en concertation avec les services de la Commission chargés de la mise en œuvre du portail usager et des téléservices associés.

Considérant l'ensemble de ces éléments, décide :

- la mise en œuvre des mesures définies dans le plan d'action présenté dans le cadre du dossier d'homologation, et leur suivi par le responsable de la sécurité des systèmes d'information de la CNIL ;
- l'homologation de sécurité du portail usager et des téléservices associés, au vu de l'étude des risques réalisée et du plan d'action associé, jusqu'au 28 juillet 2024.

La Présidente

Marie-Laure DENIS