

DECLARATION

28/05/2020

RU 48
« FranceConnect »

« FRANCECONNECT »

(Déclaration N° 48)

Suite à l'entrée en application du RGPD, l'engagement de conformité à certains actes réglementaires uniques n'a plus de valeur juridique à compter du 25 mai 2018. Dans l'attente de la production de référentiels RGPD, la CNIL a décidé de les maintenir accessibles afin de permettre aux responsables d'orienter leurs premières actions de mise en conformité.

L'acte réglementaire unique n° RU-048 définit le cadre général de mise en œuvre des fonctionnalités offertes par le dispositif « FranceConnect ». Il permet aux autorités administratives de proposer à leurs administrés des mécanismes de simplification des identités numériques, d'échange de données et d'informations entre les administrations et d'identification électronique des administrés auprès d'autres services publics européens.

Ce dispositif, mis en œuvre par le SGMAP, consiste principalement en une solution de fédération d'identités numériques. Il permet à l'administré d'utiliser des téléservices publics différents sans avoir à s'identifier à nouveau auprès de chacun d'eux ou à créer un compte d'accès dédié pour chacun de ces services publics dématérialisés.

Il permet également, avec le consentement de l'utilisateur, aux administrations d'échanger directement entre elles les données nécessaires à la démarche entreprise, dispensant ainsi l'utilisateur de fournir les données et pièces justificatives déjà enregistrées auprès d'un service public.

Le RU-048 concerne chaque fournisseur de service, partenaire de « FranceConnect ». Il leur permet de mettre en œuvre facilement, par simple engagement de conformité à cet arrêté, toutes ou partie des fonctionnalités « FranceConnect ».

Voir aussi :

[Délibération n° 2015-254 du 16 juillet 2015 portant avis sur un projet d'arrêté portant création d'un traitement de données à caractère personnel par la direction interministérielle des systèmes d'information et de communication d'un téléservice dénommé « FranceConnect »](#)

TEXTE OFFICIEL

[Arrêté du 24 juillet 2015 portant création d'un traitement de données à caractère personnel par la direction interministérielle des systèmes d'information et de communication d'un téléservice dénommé « FranceConnect »](#)

SECTEURS D'ACTIVITE EXCLUS DU CHAMP DE LA NORME

Services et établissements publics à caractère industriels et commerciaux

RESPONSABLES DE TRAITEMENT CONCERNES

Toute autorité administrative qui, en vertu d'un texte législatif ou réglementaire, est habilitée à traiter la démarche ou formalité entreprise par l'administré (désigné dans ce type d'écosystème « fournisseur de service »).

Concrètement, est concernée toute administration qui souhaite simplifier les démarches entreprises par les usagers par voie dématérialisée. Il peut s'agir de l'État, d'une collectivité, de toute autre autorité administrative ou leur groupement.

Chaque fournisseur de service souhaitant proposer une fonctionnalité « FranceConnect » doit :

- adresser à la CNIL un engagement de conformité à l'[arrêté du 24 juillet 2015](#) (RU-048) ;
- s'inscrire à « FranceConnect » via le formulaire d'enregistrement mis à sa disposition sur le portail « FranceConnect ». Afin de valider son enregistrement, le fournisseur de services doit valider les conditions générales d'utilisation (CGU) du service « FranceConnect » ;
- publier un acte réglementaire autorisant la mise en œuvre d'un ou de plusieurs téléservices publics.

Comme le rappelle [l'article 5 de cet arrêté](#), l'engagement de conformité à l'acte réglementaire unique RU-048 ne concerne pas les « traitements métiers » utilisés pour instruire les démarches administratives. Ces traitements de données doivent faire l'objet de formalité spécifique, tout comme les téléservices qui s'appuient sur les fonctionnalités d'authentification « FranceConnect » (à titre d'illustration, le [RU-030 pour les « téléservices publics locaux »](#) ou le [RU-052 pour les « téléservices de l'État et des ÉPA »](#)).

La Direction interministérielle du numérique et du système d'information et de communication de l'État (DINSIC) est responsable de la mise en œuvre du dispositif « FranceConnect ».

OBJECTIF(S) POURSUIVI(S) PAR LE TRAITEMENT (FINALITES)

Le dispositif « FranceConnect » vise à simplifier les démarches administratives entreprises par voie électronique par les usagers en leur proposant

- des fonctionnalités de fédération d'identités numériques
- un mécanisme d'échanges sécurisés de données entre administrations, prévus aux articles [L.113-12](#), [L.114-8](#) et [L.114-9](#) du code des relations entre le public et l'administration (CRPA).

Les usagers peuvent ainsi, à leur initiative, fédérer leurs identités électroniques en s'appuyant sur des comptes utilisateurs déjà créés auprès de services publics. Ils peuvent en outre consentir à bénéficier d'échange de données directement entre administrations.

UTILISATION(S) EXCLUE(S) DU CHAMP DE LA NORME

L'identification d'un administré est requise exclusivement pour accomplir une démarche administrative individuelle. Aucun traitement de données à caractère personnel ne peut être imposé à l'internaute pour accéder à une information générale.

Les données personnelles traitées dans le cadre de « FranceConnect » ne doivent pas être utilisées pour alimenter d'autres fichiers ou pour constituer un « fichier de population ».

DONNEES PERSONNELLES CONCERNEES

[L'article 3 du RU-048](#) énumère les catégories de données à caractère personnel qui sont traitées dans le cadre de « FranceConnect ».

En ce qui concerne les fournisseurs de service, les données relatives à la gestion de l'identification des administrés par l'intermédiaire de « FranceConnect » sont les suivantes :

1. Sont obligatoirement traitées pour construire une « identité pivot » :

- le sexe,
- le nom de famille,
- le(s) prénom(s),
- la date et le lieu de naissance complets,
- le cas échéant, le numéro d'inscription de l'établissement au répertoire des entreprises et de leurs établissements (SIRET) vérifié et utilisé dans les conditions fixées par les articles R. 123-220 et suivants du code du commerce,
- les clés de fédération ou « alias » générés par le système à la connexion de l'utilisateur.

1. Peuvent être traitées de façon facultative :

- le nom d'usage,
- le numéro de téléphone fixe,
- le numéro de téléphone portable,
- l'adresse de courrier électronique,
- l'adresse postale.

1. Sont également concernées les données relatives à la gestion de la traçabilité des accès :

- l'adresse *IP* de l'utilisateur ;
- les dates et heures de connexion des utilisateurs au téléservice ;
- les jetons issus du mécanisme d'échange de données permettant de vérifier la bonne information de l'utilisateur et, le cas échéant, le recueil de son consentement.

Le téléservice proposant de recourir à « FranceConnect », traite également par définition un ensemble de données personnelles nécessaires à l'instruction de la démarche entreprise par l'utilisateur. Comme le rappelle [l'article 5 de cet arrêté](#), ces « traitements métiers » doivent faire l'objet de formalités spécifiques.

DONNEES EXCLUES DU CHAMP DE LA NORME

Aucun partenaire de « FranceConnect », qu'il soit fournisseur de services, de données ou d'identités, ne peut traiter directement l'alias technique unique propre à « FranceConnect » qui est obtenu par le hachage irréversible de tout ou partie des données composant « l'identité pivot ». Comme le rappelle [l'article 3 de l'arrêté du 24 juillet 2015 \(RU-048\)](#), seule la DINSIC est habilitée à traiter cet alias technique unique à la seule fin d'assurer la prestation de service dont elle a charge.

DUREE DE CONSERVATION DES DONNEES

Pour respecter le principe de pertinence des données à caractère personnel, chaque responsable de traitement doit s'interroger sur l'utilité de traiter l'ensemble des données transmises par « FranceConnect ». Si toutes ces données, notamment celles composant « l'identité pivot », ne sont pas nécessaires à l'instruction de la démarche, il convient de ne pas les conserver.

La durée de conservation des données relatives à la gestion de l'identification ne peut excéder la durée de la session de l'utilisateur.

Pour les données visant à assurer la sécurité du mécanisme, la durée de conservation correspond aux besoins propres à chaque « traitement métier » mis en œuvre pour instruire les démarches entreprises par les administrés à partir d'un téléservice ou d'un autre vecteur de saisine.

Conservés par la DINSIC, les clés de fédération et l'alias technique unique propre au système « FranceConnect » doivent être supprimés en l'absence de connexion de l'utilisateur pendant une durée de 36 mois.

DESTINATAIRES DES DONNEES

Seuls les agents habilités à mettre en œuvre le téléservice recourant à « FranceConnect » et à instruire les saisines transmises par ce vecteur peuvent accéder aux données, en raison de leurs fonctions ou pour les besoins du service et dans la limite de leur besoin d'en connaître.

Il peut être procédé à la transmission de certaines données aux applications informatiques régulièrement mises en œuvre par les services compétents pour instruire les démarches entreprises.

La mise en œuvre de « FranceConnect » induit également les destinataires suivants :

- le service « FranceConnect » de la DINSIC, pour assurer la liaison technique entre chaque fournisseur de service et chaque fournisseur d'identités ou de données choisis par l'administré ;
- le fournisseur d'identités ou de données, partenaire de « FranceConnect », pour fournir des données adaptées aux besoins exprimés par le fournisseur de service, responsable de traitement s'engageant à être conforme au RU-048 ;
- l'INSEE, pour vérifier les données transmises systématiquement par le fournisseur d'identités à la DINSIC et traitées de façon obligatoire pour la gestion de l'identification (« identité pivot »), en consultant le Répertoire national d'identification des personnes physiques (RNIPP) en vue d'une certification, dans le cas où le responsable de traitement n'est pas en mesure de la réaliser lui-même.

INFORMATION DES PERSONNES ET RESPECT DES DROITS "INFORMATIQUE ET LIBERTES"

Les internautes sont informés de la mise en œuvre de « FranceConnect » par la publication de l'acte réglementaire portant création d'un ou plusieurs téléservices proposant notamment de recourir à tout ou partie des fonctionnalités « FranceConnect ». Les éléments d'information mentionnés à [l'article 32 de la loi « Informatique et Libertés »](#) ainsi que les modalités d'utilisation des téléservices (CGU) doivent également leur être délivrés.

Ces modalités d'information doivent être organisées de façon à matérialiser tout particulièrement la volonté de l'utilisateur qui agit, si ce n'est jusqu'à garantir le recueil de son consentement quant à recourir aux fonctionnalités « FranceConnect ».

Le dispositif « FranceConnect » étant en effet facultatif, il nécessite également de maintenir une voie alternative pour accéder au même service public.

De plus, les administrés disposent d'un droit d'opposition pour motif légitime, sauf si l'acte réglementaire portant création du téléservice proposant de recourir à « FranceConnect » en dispose expressément autrement.

Les personnes concernées bénéficient enfin de droits d'accès, de rectification et de suppression qui s'exercent auprès de différents services désignés dans l'arrêté du 24 juillet 2015 et les actes réglementaires à intervenir.

- S'agissant de données traitées pour instruire la démarche, les personnes concernées exercent leurs droits « Informatique et Libertés » directement auprès du responsable de traitement, fournisseur de service.
- S'agissant de données traitées pour la mise en œuvre de « FranceConnect », ces droits s'exercent auprès de la DINSIC, par voie postale ou électronique, comme le précise [l'article 7 de cet arrêté](#).
- S'agissant de données fournies par l'intermédiaire de « FranceConnect » à la demande de l'utilisateur pour simplifier certaines démarches entreprises, ces droits s'exercent auprès du fournisseur de données d'identités.

Lorsque le téléservice le permet, l'utilisateur peut exercer ses droits par voie électronique, voire accéder directement aux données le concernant.

SECURITE ET CONFIDENTIALITE

Chaque téléservice public doit être conforme à l'exigence de sécurité prévue par l'article 34 de la loi « Informatique et Libertés » ainsi qu'au référentiel général de sécurité (RGS). Le référentiel général d'interopérabilité (RGI) et le référentiel général d'accessibilité de l'administration (RGAA) doivent également être respectés dans la mesure où ils garantissent l'efficacité des échanges de données entre différentes autorités administratives.

À ce titre, les consultations, créations, modifications ou suppressions de données doivent notamment faire l'objet d'un enregistrement comprenant l'identifiant de leur auteur, ainsi que la date, l'heure et l'objet de l'opération. Ces traces doivent être conservées, par le fournisseur de service, pendant un délai adapté à la sécurisation des différents types de démarches entreprises avec l'appui de « FranceConnect ».

Plus particulièrement, les données relatives à la gestion de la traçabilité des accès des administrés doivent être supprimées en l'absence de connexion de l'administré pendant une durée de 6 mois.

La Commission recommande de mener une « analyse d'impact relative à la protection des données » (AIPD). [Trois guides pratiques sont publiés par la CNIL](#) pour aider le responsable de traitement à définir les mesures de gouvernance nécessaires à la protection des données personnelles traitées. Développé à partir de la même méthode dite « eBIOS », une telle étude peut être effectuée à l'occasion de l'analyse de risques « SSI » (sécurité du système d'information) exigée dans le cadre de la procédure d'homologation RGS.