

La protection des données personnelles

Depuis le 25 mai 2018, les bénéficiaires de financements européens tels qu'Horizon 2020 doivent se conformer au Règlement Général de Protection des Données (RGPD).

Qu'est-ce qu'une donnée personnelle ?

Une **donnée à caractère personnel** concerne toute information, quelle que soit sa nature, relative à une personne physique identifiée ou qui peut être identifiée, directement ou indirectement, par référence à un numéro d'identification ou à un ou plusieurs éléments qui lui sont propres.

Une donnée personnelle est dite **sensible** lorsqu'elle réfère à une origine raciale ou ethnique, des opinions politiques, des croyances religieuses, appartenance à un syndicat, relative à la santé, vie sexuelle, génétique, biométrique et criminelle.

Qu'est-ce que le traitement de données personnelles ?

Le **traitement de données à caractère personnel** concerne toute opération ou tout ensemble d'opérations portant sur de telles données, quel que soit le procédé utilisé, et notamment la collecte, l'enregistrement, l'organisation, la conservation, l'adaptation ou la modification, l'extraction, la consultation, l'utilisation, la communication par transmission, diffusion ou toute autre forme de mise à disposition, le rapprochement ou l'interconnexion, ainsi que le verrouillage, l'effacement ou la destruction.

Les données personnelles doivent être traitées dans les projets selon certains principes et conditions visant à garantir la qualité et la confidentialité.

Implications pour les bénéficiaires de projets H2020

Le bénéficiaire doit notifier à ses agents le recueil et la transmission de données à caractère personnel à la Commission européenne ou à l'une de ses agences dans le cadre de la mise en œuvre d'un projet H2020. Leur accès doit être limité aux seuls agents nécessaires au traitement de ces données, conformément au principe de confidentialité.

Le traitement des données à des fins de recherche doit être réalisé sous réserve de garanties appropriées. Elles garantissent que les aspects techniques et mesures organisationnelles sont en place afin de garantir le respect des principes de minimisation des données, anonymisation, précision, intégrité, équité et transparence de la gestion des données.

- **Minimisation** : L'utilisation des données doit être limitée à l'objectif de la recherche. Cela signifie s'assurer que les données sont adaptées aux fins de la recherche, restreindre l'accès aux données personnelles ou déterminer si des données anonymisées, agrégées ou pseudonymisées seraient suffisantes. Ce principe vise par exemple à empêcher la collecte de données personnelles inutiles.
- **Anonymisation** : processus afin de s'assurer que le risque de quelqu'un soit identifié par les données est négligeable. Les données anonymisées ne sont plus personnelles.
- **Précision** : les données inexactes doivent être effacées ou rectifiées sans délai.
- **Intégrité** : mesures techniques et organisationnelles appropriées pour protéger les données personnelles contre le traitement non autorisé ou illégal et contre la perte accidentelle, la destruction ou l'endommagement. Les mesures de sécurité doivent garantir que (a) seules les personnes autorisées peuvent accéder, modifier, divulguer ou détruire les données personnelles; b) ces personnes n'agissent que dans le cadre de leur autorité; et (c) si des données personnelles sont accidentellement perdues ou détruites, elles peuvent être récupérées pour éviter tout dommage aux personnes concernées.
- **Équité** : exige de prendre en compte la manière dont l'utilisation des données personnelles affecte les intérêts des individus.
- **Transparence** : fournir aux participants les informations nécessaires. Celles-ci doivent être concises et rédigées dans un langage clair et simple. Par exemple l'identité et les coordonnées du responsable du traitement, comment les informations personnelles sont collectées, la finalité du traitement de ces données, la durée de conservation...

Le traitement des données personnelles fait également partie des obligations éthiques à titre de la convention de subvention (article 34).

Il est recommandé de solliciter l'avis du *Data protection officer* (DPO), de son institution, nommé en français « délégué à la protection des données », sur la manière de respecter les obligations. Si le projet soulève des problèmes complexes en raison de la sensibilité des données, il est possible de désigner un responsable de la protection des données du projet.

Où trouver de l'aide ?

- Guide de la Commission européenne « [Ethics and data protection](#) »
- Section Ethique du manuel H2020 en ligne : https://ec.europa.eu/research/participants/docs/h2020-funding-guide/cross-cutting-issues/ethics_en.htm
- [Outils de conformité de la CNIL](#)
- [15 recommandations aux chercheurs](#)

Textes de référence

- [Règlement général de protection des données à caractère personnel](#) (Règlement UE 2016/679)
- [Modèle général de convention de subvention Horizon 2020](#), article 39.2 et 34
- [Version annotée du modèle général de convention de subvention](#), article 39.2, 34 et annotations

Ministère de l'Enseignement supérieur, de la Recherche et de l'Innovation (MESRI)
1, rue Descartes - 75231 Paris cedex 05

www.horizon-europe.gouv.fr

Fiche préparée par les membres du P.C.N. juridique et financier : MESRI, ANRT, CNRS, INSERM, CPU et AP-HP.
Février 2021 (document non contraignant).