



HAL
open science

Gestion et utilisation des données personnelles dans le cadre des projets de sciences participatives

Nathalie Gandon, Iñaki Garcia de Cortazar Aauri

► **To cite this version:**

Nathalie Gandon, Iñaki Garcia de Cortazar Aauri. Gestion et utilisation des données personnelles dans le cadre des projets de sciences participatives. NOV'AE, 2021, Sciences et Recherches Participatives à INRAE, Numéro Spécial 01, pp.55-61. 10.17180/novae-2022-NS01-art05 . hal-04624869

HAL Id: hal-04624869

<https://hal.science/hal-04624869v1>

Submitted on 25 Jun 2024

HAL is a multi-disciplinary open access archive for the deposit and dissemination of scientific research documents, whether they are published or not. The documents may come from teaching and research institutions in France or abroad, or from public or private research centers.

L'archive ouverte pluridisciplinaire **HAL**, est destinée au dépôt et à la diffusion de documents scientifiques de niveau recherche, publiés ou non, émanant des établissements d'enseignement et de recherche français ou étrangers, des laboratoires publics ou privés.



Distributed under a Creative Commons Attribution - ShareAlike 4.0 International License

Gestion et utilisation des données personnelles dans le cadre des projets de sciences participatives

Nathalie GANDON,

INRAE - Déléguée Informatiques et Libertés

Iñaki GARCIA DE CORTAZAR ATAURI

INRAE - US AgroClim

Les données recueillies par la société civile dans le cadre des projets de crowdsourcing peuvent être de natures très diverses. On pense généralement aux données générées pour le projet. Mais il ne faudrait pas oublier que l'on recueille, également, des données à caractère personnel, parfois même involontairement. Voici quelques clefs pour gérer et utiliser ces données en conformité avec le cadre du RGPD.

Les données qui sont recueillies dans le cadre de certains projets de sciences participatives peuvent être de natures très diverses. Ceci est notamment vrai dans le cadre de projets de crowdsourcing (en français, production participative ou externalisation ouverte), dont l'objectif est de faire participer la société civile à l'acquisition d'observations de façon massive et distribuée, le plus souvent via des outils et/ou des applications mobiles. L'objet et le type de données recueillies peuvent avoir des formats très divers : dates de développement (phénologie) d'une espèce (migration, floraison) ; le signalement de la présence ou absence d'une espèce dans un lieu donné ; les comptages d'individus d'une espèce dans un lieu donné ; la prise de photo (numérique) d'un objet ou espèce vivante pour son identification ; l'enregistrement sonore d'un bruit, musique, chant... ; ou l'échantillonnage d'un objet physique ou biologique (terres, tiques, fleurs...)¹.

Toutes ces informations sont souvent initialement gérées et utilisées par les scientifiques qui veulent explorer une question de recherche et dont le périmètre d'observation initiale serait trop restreint s'ils s'appuyaient exclusivement sur les dispositifs expérimentaux existants. L'avantage de ce type de projet réside donc dans la possibilité d'accéder à des informations qui sont réparties sur un plus large territoire, et sur des périodes temporelles parfois plus importantes que

celles définies dans les projets de recherche ou dans les réseaux d'expérimentation. Néanmoins, le fait d'impliquer des citoyens (ou collectifs) volontaires, en dehors du cadre d'une activité professionnelle, génère un contexte d'utilisation de ces informations qui doit être compris et précisé dès le départ.

Dans une telle situation, nous pouvons d'ores et déjà faire une différenciation entre les divers types d'informations qui sont ainsi récupérées (acquises), de façon volontaire², dont la nature et la gestion peuvent s'avérer très différentes. Nous ferons ainsi la différence **entre les données à caractère personnel**, notamment celles associées au compte utilisateur créé pour la participation au projet, qui seront l'objet d'analyse de cet article, et les données générées par le projet participatif, qui peuvent être de natures très différentes comme nous l'avons vu plus haut (voir encadré 2).

Le Règlement Général sur la Protection des Données - RGPD

Pour traiter les questions relatives à ces données, il existe le Règlement Général sur la Protection des Données (RGPD) qui encadre le traitement des données personnelles sur le territoire de l'Union européenne. Le RGPD est un règlement

¹ Ici, nous nous intéressons uniquement aux données acquises dans les projets de sciences participatives sur l'environnement. Les recherches impliquant la personne humaine (par exemple données comportementales) ne sont pas concernées, et nécessiteraient d'ailleurs un papier à part entière pour traiter du respect du RGPD.

² « De façon volontaire » : la plupart des fois, mais pas toujours ! Par exemple, des informations Exif sont associées aux photos et renseignent sur l'appareil, le modèle, la date de prise de vue, les coordonnées, etc. Ce sont des données collectées involontairement. C'est également le cas pour les adresses IP des participants, pour donner un autre exemple.

européen, ce qui signifie que, contrairement à une directive, il est directement applicable dans l'ensemble de l'Union sans nécessiter de transposition dans les différentes législations des États membres. Il laisse, cependant, des marges de manœuvre aux États sur certains sujets. Ce règlement, entré en vigueur le 25 mai 2018, s'applique dès lors que le responsable de traitement (par exemple le directeur d'une unité sous tutelle d'INRAE) est établi sur le territoire de l'Union européenne ou qu'il met en œuvre des traitements visant à fournir des biens et des services aux résidents européens. Ce règlement a trois objectifs principaux :

- Renforcer les droits des personnes
- Responsabiliser les acteurs traitant des données (responsables de traitement et sous-traitants)
- Crédibiliser la régulation grâce à des sanctions renforcées et une coopération renforcée entre les autorités de protection des données, qui pourront notamment adopter des décisions communes lorsque les traitements de données seront transnationaux.

Ce règlement est à articuler avec la loi de la République Numérique qui encadre la diffusion des documents administratifs (incluant les données), produits ou reçus par des administrations, et donc les données produites par les établissements d'enseignement supérieur et de la recherche. Il faut ainsi noter que l'obligation d'ouverture ne vaut pas lorsque des données de recherche contiennent des données à caractère personnel, afin de protéger la vie privée des individus concernés. En revanche, le décret 2018-1117 liste le type de documents administratifs pouvant faire l'objet d'une diffusion sans anonymisation préalable.

Par données personnelles, on entend toute information permettant d'identifier une personne physique, directement ou indirectement. Contrairement à une idée reçue, il ne s'agit donc pas uniquement de données relatives à la vie privée des individus, mais bien toute information ayant un pouvoir d'identification. Ainsi, par exemple, le nom ou prénom d'un individu permettent de l'identifier directement, alors que le numéro d'identité ou son adresse IP permettent de l'identifier indirectement. Parmi les données qui permettent d'identifier un individu on peut citer :

- tous les identifiants d'une personne : adresse physique ou IP, adresse mail, numéro de téléphone, ...
- ses caractéristiques physiques : taille, poids, couleur des yeux, ADN, empreintes digitales ou rétinienne, ...
- ses opinions et comportements : idées politiques, appartenances associatives, orientation sexuelle, goûts, ...

- d'autres informations liées à l'utilisation des services numériques, telles que la géolocalisation, l'image, les contenus postés, ...

Par ailleurs, il faut aussi prendre en compte que certains jeux de données qui ne contiennent pas d'informations directes d'une personne (par exemple le prénom ou le nom) peuvent permettre quand même son identification s'ils sont combinés ou croisés avec d'autres jeux de données. C'est pour cette raison que la notion de donnée indirectement identifiante est très importante.

Une autre notion essentielle est celle de « responsable de traitement » qui est celui qui définit les finalités du traitement et les moyens (notamment informatiques) nécessaires à sa mise en œuvre. Dans le cadre d'INRAE³, le DU est responsable de traitement pour les Unités de Recherche (mixtes ou propres), Service et Expérimentales, et le PDG est responsable du traitement pour la plupart des traitements liés à l'appui à la recherche. Néanmoins, pour ces derniers, c'est bien le directeur du service d'appui qui a « délégation » pour la mise en œuvre du traitement.

Enfin, il existe quelques particularités concernant certaines données. C'est le cas des données considérées comme **particulières ou sensibles** dont font partie, par exemple, les **données de santé**. Ce type de données fait référence aux informations « concernant l'origine raciale ou ethnique, les opinions politiques, philosophiques ou religieuses, l'appartenance syndicale, les données génétiques, les données biométriques aux fins d'identification unique de la personne, les données concernant la santé ou la vie sexuelle des personnes. L'utilisation de ces données peut nécessiter la réalisation d'une analyse d'impact sur la protection de données, voire d'une autorisation ou avis de la CNIL, avant leur traitement. Les données de santé peuvent décrire la santé physique ou mentale, passée, présente ou future d'une personne physique (y compris les soins de santé associés). Ces données font l'objet d'une protection renforcée et particulière dans différents textes (RGPD, Loi Informatique et Libertés, Code de la Santé Publique notamment).

Ainsi, dans le cas des projets du type crowdsourcing, mais pas seulement, il est très courant d'acquérir des données personnelles (nom, prénom, pseudonyme, localisation, photo...) associées aux données qui sont générées par le projet lui-même. Nous allons par la suite explorer plusieurs questions qui devraient permettre aux scientifiques d'avoir les bons réflexes dans le cadre de l'animation d'un projet de Sciences et Recherches (idéalement avant de le lancer, au pire s'il est déjà en cours).

3 Cf. la Note de Service 2019-28.

ENCADRÉ 1

Quelques précisions concernant l'open data et la propriété intellectuelle

Les données à caractère personnel ne sont pas, en tant que telles, éligibles à la mise à disposition en open data. Il est nécessaire d'avoir, au préalable, obtenu le consentement (sur la finalité et les modalités de la communication des données) de la personne concernée ou d'avoir anonymisé les données ou de pouvoir diffuser grâce à un texte législatif ou réglementaire (exemple du décret 2019-1024).

Pour rappel, l'anonymisation (voir plus bas) consiste à supprimer tout caractère identifiant à un ensemble de données. Concrètement, cela signifie que toutes les informations permettant une ré-identification des personnes sont supprimées.

Dans le cadre des projets qui font appel à l'acquisition d'images, il est très important de clarifier dès le début le type de licence qui sera apposé aux images et le cadre de diffusion qui sera mis en place. Ainsi, afin d'éviter de gérer la propriété intellectuelle, il est conseillé d'utiliser des licences du type Creative Commons, et notamment celles qui obligent à citer l'origine des informations/données/images (licences compatibles CC-BY 4.0).

Gestion des comptes des participants au projet

La plupart de projets de Crowdsourcing demandent la création d'un compte utilisateur, via un outil ou plateforme informatique, pour pouvoir participer au projet. L'intérêt de la création d'un tel compte est multiple : identifier les utilisateurs uniques ; assurer une certaine traçabilité des données acquises ; contacter l'utilisateur si besoin d'un complément d'information ; contacter l'utilisateur pour lui donner des informations du projet ; et bien d'autres raisons qui peuvent apparaître comme importantes ou nécessaires aux yeux du scientifique (organisateur). De nombreuses plateformes permettent de gérer les données personnelles permettant d'identifier directement (nom, prénom, adresse courriel) ou indirectement (n° de téléphone, adresse IP, etc.) les utilisateurs de ce service. Dans tous les cas, la règle de base est de **ne pas utiliser les données pour une autre finalité** que celle liée à la gestion des participants au projet. Attention donc aux démarches de profilage, évaluation ou *scoring*⁴ des utilisateurs. Par ailleurs, si vous avez recours à un prestataire, notamment, pour l'hébergement du site web du projet, il faut choisir un prestataire qui présente des garanties RGPD (hébergeur européen de préférence) et faire attention aux Conditions Générales d'Utilisation ou de Vente de ce prestataire.

Il est donc très important de mener une réflexion au préalable concernant l'identification des données personnelles qui seront véritablement nécessaires à la gestion et animation du projet. Cela permettra de limiter le nombre d'informations et leur nature, et donc de complexifier le système de gestion. C'est ce que l'on appelle **le principe de minimisation** qui impose que les données à caractère

personnel recueillies doivent être « adéquates, pertinentes et limitées à ce qui est nécessaire au regard des finalités pour lesquelles elles sont traitées ». **Attention donc à la boulimie de données !**

À ce niveau il est important de rappeler que l'acquisition de ces données au moment de la création d'un compte doit impérativement faire l'objet d'une information claire et transparente sur la finalité de la collecte et l'utilisation de ces données. Il est recommandé également d'indiquer quelles données sont obligatoires et lesquelles sont facultatives. De plus, les responsables du traitement doivent être en mesure de respecter les droits **d'accès, de rectification, d'opposition et d'effacement des données**. Ils sont, par ailleurs, tenus de répondre à ces demandes dans le délai d'un mois. La gestion et application de ces droits nécessitent de prévoir, notamment dans le cadre de projets faisant appel à des outils/applications informatiques, la mise en place d'une architecture logiciel et/ou d'un modèle relationnel de base de données qui permettent des requêtes et effacement sur ces données de compte.

Plusieurs situations peuvent se présenter à nous concernant la gestion de ces données :

- Le projet a été mis en place avant l'application du RGPD et il a été arrêté depuis. Ce cas nécessite de définir s'il y a un intérêt de garder les données personnelles pour faire un lien avec les données générées (ou un autre objectif). Si la réponse est positive, dans ce cas, il est nécessaire de mettre en conformité le jeu des données en réinformant les anciens participants. Dans le cas contraire, les informations personnelles devront être supprimées. Néanmoins, il faut savoir que cette action n'élimine pas

⁴ Le scoring est une technique qui permet d'affecter un score à un client ou prospect. Il mesure donc l'appétence pour une offre potentielle.

la propriété intellectuelle. Par exemple, dans le cas d'un programme où la donnée est une photo et celle-ci a une licence associée (par exemple une CC-BY qui permet une utilisation libre, mais oblige à citer l'auteur), nous pouvons éliminer les données personnelles des comptes des participants, mais l'utilisation de la photo doit toujours s'accompagner de la citation de son auteur.

- Le projet a été mis en place avant l'application du RGPD et il est toujours actif. Dans cette situation, nous devons le mettre en conformité et communiquer, auprès de tous les participants, sur la mise à jour des conditions d'utilisation de leurs données personnelles. Cela peut se présenter de différentes manières : par exemple, un courriel qui décrit les nouvelles conditions d'utilisation avec un lien permettant de les accepter ou un message et une obligation d'acceptation de ces conditions à la prochaine connexion sur l'application ou le site web.
- Le projet a été mis en place après la mise en place du RGPD. Ce dernier cas est en théorie le plus simple, car il permet d'anticiper les différentes étapes et procédures nécessaires (indiquées plus haut) à la gestion des données.

D'une manière générale les principales informations et un exemple peuvent être trouvés dans la fiche référentiel concernant la « Gestion des données personnelles des utilisateurs d'un service » accessible sur : <https://intranet.inrae.fr/donnees-personnelles/Les-demarches-de-mise-en-conformite/Les-formalites-obligatoires/Fiches-Referentiel>

En cas de doute, vous pouvez contacter la Déléguée Informatique et Libertés (DIL) d'INRAE via l'adresse cil-dpo@inrae.fr.

Comment gérer les coordonnées géographiques

Outre les données personnelles des participants, liées à leur compte, un autre type de donnée personnelle peut être manipulé : les coordonnées GPS. Ce type d'information est typiquement recueilli dans les projets de crowdsourcing qui ont comme objectif de décrire la distribution spatiale et temporelle de certaines informations (phénologie dans le cadre de l'Observatoire des Saisons, présence/absence d'une espèce dans le cadre d'Agir ou de PlantNet ; présence et piqûres dans le cadre du programme CiTique, etc.). Tous ces projets utilisent cette information spatiale, car elle va permettre aux scientifiques de mieux comprendre et caractériser l'effet de l'environnement (par exemple, le climat) sur les écosystèmes/biomes étudiés. Néanmoins, cette

information spatiale (décrite via la latitude, la longitude et, parfois, l'altitude du point d'observation) est une information qui peut être considérée comme personnelle dans le cas où elle se rapporte à une propriété privée.

D'une manière générale, la coordonnée elle-même ne pose pas de problème en ce qui concerne son utilisation, mais c'est la nature des données associées à cette coordonnée qui peut être considérée comme personnelle, car elle peut révéler un comportement ou pratique. Afin de comprendre les différences entre les types de données, voici quelques exemples :

- Les données concernant le type de sol, la floraison d'une plante, la présence d'une tique, le chant d'un oiseau... NE SONT PAS considérées comme personnelles, même associées à des coordonnées d'un lieu privé (par exemple un jardin), car elles ne décrivent pas un comportement ou une pratique du propriétaire.
- Les données d'un acte technique, traitement phytosanitaire, type de production... PEUVENT ÊTRE considérées comme personnelles, si elles sont associées à des coordonnées d'un lieu privé, car elles peuvent informer sur le comportement ou pratiques du propriétaire. Néanmoins, cette contrainte n'est plus retenue si ces données sont relatives à des émissions de substances dans l'environnement⁵. Mais, ce type d'analyse peut se prêter à interprétation, donc il ne faut pas hésiter à solliciter les personnes compétentes de la Direction des Affaires Juridiques et/ou la DIL.

Dans certains cas, et afin d'éviter tout problème concernant l'utilisation de ces données, il est possible de dégrader les informations géographiques, afin de ne plus pointer sur le lieu d'observation précis. Une solution classiquement utilisée dans les bases de données, qui diffusent ou affichent les données spatialisées, consiste à déplacer le point des coordonnées géographiques de l'observation (qui peut être dans un lieu public ou privé) vers les coordonnées géographiques de la Mairie de la commune où les observations ont été réalisées. Néanmoins, ce type de démarche doit pouvoir se justifier vis-à-vis de la précision du travail de recherche réalisé.

Dans tous les cas, il est important de bien se poser la question, au début du projet, concernant le besoin de cette localisation précise.

5 Cf. article L124-5 du code de l'environnement.

ENCADRÉ 2

A qui appartiennent les données collectées via les applications smartphones ou renseignées sur le site du projet ?

Le site web ou application smartphone doit disposer de conditions générales d'utilisation (appelées CGU) qui définissent les droits et devoirs des utilisateurs du site ainsi que les éléments de propriété du contenu et des licences de réutilisation. Les juristes en droit numérique, informatique et libertés de la Direction des affaires juridiques (DAJ) d'INRAE peuvent vous conseiller sur les informations à fournir dans les CGU de votre site web. Le participant au projet doit pouvoir valider les CGU avant de verser du contenu sur le site web.

Les données sont transmises à INRAE via le site web ou l'application. INRAE en acquiert généralement les droits d'exploitation, afin qu'elles puissent être réutilisées (sous réserve qu'un cadre juridique général en limite la divulgation). Dans certains cas, l'institut peut envisager d'en demander la co-propriété si cela sert la finalité du projet. Dans certains projets, il peut y avoir des participations sous contributions financières ou avec des accords de droit plus restreints pour INRAE. Une fois défini le cadre juridique de propriété et d'exploitation, dans le cadre du contrat de partenariat du projet par exemple, il sera à mentionner dans les CGU.

Lorsque les données sont complexes et relèvent de la propriété intellectuelle, il est recommandé d'envisager, en amont, des formes de reconnaissance; ceci est à discuter avec les contributeurs.

D'après des informations recueillies auprès de Stéphanie Rennes (Direction des Affaires Juridiques, INRAE)

Quid des données personnelles professionnelles (en dehors de celles des comptes des participants au projet) ?

D'une manière générale, la plupart des salariés et agents de la fonction publique (dont ceux d'INRAE) sont identifiés dans différents annuaires ou listings qui permettent d'avoir accès à différentes informations : unité et centre de rattachement, adresse courriel et téléphone professionnels, fonctions... Ces informations tout en étant professionnelles sont aussi soumises à un certain nombre de règles. Ainsi, ces données publiées n'interdisent pas le fait que tout agent peut demander la modification ou la suppression des coordonnées publiées directement sur le site d'origine. Par ailleurs, toute réutilisation de données publiées qui auraient la nature de données personnelles (numéro de téléphone, adresse de courrier électronique, etc.) suppose préalablement, de la part du réutilisateur, la vérification du complet respect de ses obligations prévues par le RGPD (information, modification, etc.)⁶. Il ne faut donc pas confondre le fait que les données soient librement accessibles avec le fait qu'elles soient librement réutilisables.

D'un point de vue pratique, il y a plusieurs points d'attention qui doivent être pris en compte pour qu'une liste de contacts liée à votre projet de sciences participatives⁷ soit respectueuse du RGPD. Plusieurs situations peuvent se présenter à nous :

- Les contacts sont des collègues INRAE : l'utilisation des adresses mèl professionnelles à des fins professionnelles est autorisée. Vous n'avez pas de démarches particulières à faire. Cependant, dans le cas de l'utilisation de listes de contact telles qu'une liste d'échange sur un sujet particulier ou pour l'envoi d'une newsletter, il est recommandé d'avoir obtenu l'accord des collègues au préalable ou qu'ils se soient abonnés eux-mêmes. Dans tous les cas, un désabonnement facile doit être proposé.
- Les contacts sont des professionnels non INRAE : l'utilisation des adresses professionnelles à des fins professionnelles (information sur des projets, demandes d'intervention, etc.), ponctuelles et dans le champ d'intérêt de la personne est possible sans information préalable de celle-ci. Mais celle-ci doit pouvoir à tout moment s'opposer et ne plus recevoir de sollicitation. Cela est valable pour la diffusion de lettres d'information sur un sujet

⁶ Voir à ce propos l'avertissement 2 sur la réutilisation des coordonnées des DPO d'entreprise mises en open data : <https://www.data.gouv.fr/fr/datasets/organismes-ayant-designe-un-e-delegue-e-a-la-protection-des-donnees-dpd-dpo/>.

⁷ Il est important ici de rappeler que nous nous plaçons dans le cadre d'un projet de sciences participatives. Ces points d'attention ne pourraient être repris tels quels dans d'autres contextes pour lesquels les consignes peuvent être différentes (par exemple mèl syndicaux ou démarchage).

d'intérêt de la personne⁸. Par ailleurs, la base légale pour réaliser ce type de diffusion est l'exécution d'une mission d'intérêt public au regard des statuts INRAE qui comprennent la diffusion de la connaissance scientifique. En revanche, pour inscrire un collègue non INRAE sur une liste d'échange sur un sujet particulier, il faut au préalable obtenir son consentement. Dans le cas particulier où vous n'utilisez pas simplement un listing d'adresses professionnelles, mais que vous avez créé une vraie base de données incluant d'autres renseignements sur les personnes que leur seule adresse mèl, alors vous devrez les informer de cela et leur laisser la faculté de s'opposer à être intégrées dans cette base. Cette base de données devra par ailleurs être déclarée⁹.

En termes de bonnes pratiques, vous ne devez jamais envoyer de message en mettant toute la liste d'abonnés destinataires en copie-visible.

Anonymiser les données personnelles ?

L'anonymisation d'un jeu de données peut être une tâche assez ardue. En effet, le croisement de différentes informations, a priori anonymes, peut permettre de retrouver des individus. Des informations utiles sont produites par la CNIL et disponibles sur la page : <https://www.cnil.fr/fr/lanonymisation-de-donnees-personnelles>. Deux types de techniques d'anonymisation y sont présentés : la randomisation (modification d'attributs) et la généralisation (modification d'échelle).

Trois critères permettent d'évaluer l'efficacité d'une solution d'anonymisation :

- **L'individualisation** : est-il toujours possible d'isoler un individu ?
- **La corrélation** : est-il possible de relier entre eux des ensembles de données distincts concernant un même individu ?
- **L'inférence** : peut-on déduire de l'information sur un individu ?

Des initiatives à l'échelle européenne ont été initiées avec l'objectif de produire des outils fiables pour réaliser cette étape d'anonymisation. C'est notamment le cas de l'outil libre Amnesia¹⁰, développé dans le cadre du projet H2020 OpenAIRE.

Rappel des quelques bonnes pratiques

Enfin, nous rappelons, ci-dessous, quelques notions qui nous semblent importantes à retenir, avant de lancer un projet dans lequel nous allons recueillir et manipuler des données personnelles :

- La première notion est celle de **l'Information/non-opposition** pour recueillir les données personnelles. Sans cette première étape, nous n'avons le droit de récupérer aucune donnée permettant d'identifier les utilisateurs ou participants à un projet.
- La deuxième notion qu'il est important de rappeler est celle de la **Transparence** concernant l'utilisation et la gestion des données personnelles recueillies.
- La troisième notion est celle de la **Sobriété** vis-à-vis des données à demander. Plus de données nous recueillons, plus de responsabilités et de contraintes à leur utilisation peuvent émerger. Rappelons-nous que l'identification peut se faire de manière directe ou indirecte et, donc, il est important de prévoir tous les cas de figures.
- La quatrième notion est celle de la **Prévision et Réactivité** vis-à-vis des demandes de l'utilisateur. Nous rappelons que le participant doit être informé du projet et, à tout moment, pouvoir exercer ses droits **d'accès, de rectification, d'opposition et d'effacement de ses données**. Et cela dans un délai d'un mois (ce qui demande d'être prêt).
- La cinquième, mais très importante aussi, est la notion de **Responsabilité engagée** dans le cadre du manquement de l'une ou plusieurs dispositions décrites ci-dessus. Il est important de rappeler que la mauvaise gestion et utilisation de ces données peut être passible de sanctions.

Toutes ces notions et informations (ainsi que d'autres concernant la propriété intellectuelle et la gestion des données générées par le projet) doivent être décrites dans les conditions générales de participation au projet. ■

⁸ <https://intranet.inrae.fr/donnees-personnelles/Les-demarches-de-mise-en-conformite/Les-formalites-obligatoires/Fiches-Referentie.L>

⁹ Cf. <https://intranet.inrae.fr/donnees-personnelles/Les-demarches-de-mise-en-conformite/Les-formalites-obligatoires>.

¹⁰ <https://amnesia.openaire.eu/>.

POUR ALLER PLUS LOIN

Site INRAE sur les données personnelles contenant toutes les informations nécessaires :
<https://intranet.inrae.fr/donnees-personnelles>

Petite présentation de la loi Informatique et Libertés via l'AMUE :
<https://www.youtube.com/watch?v=XuoLsvJSmps&feature=youtu.be>



Open data et données personnelles :
<https://www.cnil.fr/fr/open-data-la-cnil-et-la-cada-publient-un-guide-pratique-de-la-publication-en-ligne-et-de-la>