Foire Aux Questions RGPD

À destination des masterant·es et doctorant·es de l'EUR Sciences sociales du genre et de la sexualité

EUR Sciences sociales du genre et de la sexualité – Océane Legrand – Février 2022

Avant de vous reporter à cette FAQ, nous vous conseillons d'avoir lu :
- Le guide RGPD (C. Avril)
- Le formulaire DPO annoté (O. Legrand et C. Avril)

Sommaire

Définitions

Le RGPD s'applique-t-il dans le cadre d'une enquête hors Union européenne ?

Le RGPD est extraterritorial : peu importe le lieu où se déroule l'enquête, le RGPD s'applique.

Que signifie « archiver les données » ?

L'archivage signifie que les données ne sont plus « en base active », c'est-à-dire que l'accès aux données est restreint. Par exemple, les données des doctorant·es doivent être versées aux archives de l'établissement et effacées de leur ordinateur. Pour les masterant·es, le versement des données aux archives de l'établissement n'est pas prévu : cela revient donc à les stocker dans un disque dur externe, et non plus sur l'ordinateur ou les clouds utilisés couramment.

Qu'est-ce que la « portabilité des données » ?

Il est extrêmement peu probable qu'un·e enquêté·e vous contacte pour la portabilité des données. Cela correspond au fait de transférer des données d'un service vers un autre service, par exemple des playlists Spotify vers Deezer, votre numéro de téléphone de votre opérateur téléphonique vers un autre, etc.

Qu'est-ce que le « principe de minimisation » ?

Il s'agit de minimiser les données personnelles recueillies en évaluant quelles sont les données réellement nécessaires pour l'enquête et l'analyse.

Les « données sensibles » font-elles partie des données personnelles ?

Oui, les données sensibles sont des données personnelles qui sont sensibles au sens de la loi. En théorie, ces données ne doivent pas être traitées, mais la recherche fait partie des domaines bénéficiant d'une exception. Ces données nécessitent un traitement particulier, c'est-à-dire une vigilance accrue.

Que sont les « données économiques » ?

Les revenus, les salaires, le patrimoine sont par exemple des données économiques et bancaires. Les données économiques ne sont pas des données sensibles telles que définies par le RGPD.

Est-ce que les personnes âgées sont considérées comme des « personnes vulnérables » ?

L'avancée en âge n'est pas un critère déterminant la vulnérabilité des personnes. Tout dépend de leur état de santé, notamment mental, ou du fait qu'ils ou elles entrent dans une autre catégorie définissant les populations vulnérables.

Quelle est la différence entre pseudonymisation et anonymisation ? Quels sont les critères d'une bonne anonymisation ?

Au sens du RGPD, la pseudonymisation consiste à remplacer les données identifiantes par d'autres données fictives : un prénom par un autre prénom, le nom d'une ville par un nom fictif, etc. Mais les sciences sociales utilisent la notion d'« anonymisation » pour désigner cette pratique.

Anonymisation/Pseudonymisation

Comment gérer des données personnelles déjà rendues publiques ?

Même si un·e chercheur·se s'expose à moins de risque concernant ces données, l'anonymisation/la pseudonymisation des données dépend toujours de la situation des personnes concernées et de l'impact que cela peut avoir sur elles, notamment car les personnes n'ont pas nécessairement anticipé le croisement de ces données rendues publiques en divers lieux, moments et contextes.

De même, si vous récupérez des données, des citations d'une personne dans un article de presse et que vous menez ensuite un entretien, une observation avec cette même personne sur votre terrain, il convient d'anticiper le croisement des données et donc de réfléchir à la pseudonymisation totale des données, y compris celles issues d'un article de presse, ou à les présenter séparément dans la rédaction du mémoire pour ne pas rendre caduque la pseudonymisation de l'entretien.

Lors de la pseudonymisation/anonymisation des données, doit-on aussi modifier les pseudonymes des internautes ?

Les pseudonymes récupérés sur internet sont aussi des données personnelles puisqu'ils ont été choisis par l'internaute et permettent de le retrouver, de l'identifier, via une adresse IP par exemple, il faut donc aussi les modifier.

Dans quelle mesure faut-il anonymiser/pseudonymiser les organismes au sein desquels l'enquête est réalisée s'il y a déjà eu anonymisation/pseudonymisation de la personne concernée ?

Par précaution, **nous vous conseillons fortement de systématiquement anonymiser/pseudonymiser les lieux, en plus des personnes**.

Il convient de toujours réfléchir de façon contextualisée : une même donnée peut être identifiante pour une personne et pas pour une autre, en fonction de la spécificité de la recherche menée. Plus un groupe enquêté est réduit/spécifique, plus son identification est facile. Par exemple, préciser qu'il s'agit du boulanger d'un village de moins 500 habitant·es dans le département Y ne permet pas d'identifier la personne s'il y a plusieurs villages de moins de 500 habitant·es avec une boulangerie dans ce département. En revanche, s'il s'agit d'un département avec seulement 3 villages de moins de 500 habitant·es, dont un seul a encore une boulangerie, il est évident qu'il sera possible de savoir qui est l'enquêté·e.

Comment gérer les captures d'écran de profils personnels, citations de commentaires, tweets, ou autres, récupérés sur internet et rendus publics par les internautes elleux-mêmes ?

Si vous citez un commentaire en entier récupéré sur internet, il faut aussi pseudonymiser/anonymiser le groupe, le site…dans lequel il a été posté. Une autre solution est de retranscrire les commentaires en modifiant des mots, qui permettent de garder l'idée transmise par le commentaire, mais d'empêcher de le retrouver.

Si vous annexez des captures d'écran à votre mémoire, idem : il faut les anonymiser/pseudonymiser.

Que faire si les données sont anonymisées et réutilisées plus tard, mais que l'enquêté·e se reconnaît ?

Les données anonymisées n'entrent plus dans le cadre du RGPD. Si l'anonymisation a été faite correctement, la personne concernée n'est pas censée se reconnaître.

Consentement des enquêté·es

Nous rappelons que deux bases de licéité sont possibles vis-à-vis du RGPD :

1. la mission de service public pour les masterant·es et les doctorant·es en thèse « classique » ;
2. le consentement des enquêté·es pour les doctorant·es en thèse Cifre ou autre financement privé (fondation, etc.).

L'obtention du consentement est donc obligatoire pour les doctorant·es financé·es sur fonds privé et fortement recommandée, pour des questions d'éthique de la recherche, pour les masterant·es et les doctorant·es hors thèses Cifre.

Doit-on demander un consentement spécifique pour prendre une photo et/ou filmer l'enquêté·e ?

Oui, le consentement doit être spécifique.

Comment gérer un consentement oral ?

Il faut procéder en deux étapes :

1) demander le consentement de l'enquêté·e avant l'enregistrement,
2) démarrer l'enregistrement, préciser l'objet de l'entretien et le nom de la personne concernée et redemander le consentement de l'enquêté·e pour que celui-ci soit enregistré et conservé.

Que faire si je n'ai que le consentement oral de mes enquêté·es ?

Si vous avez déjà obtenu un consentement oral et transmis votre contact à vos enquêté·es, il n'est pas nécessaire d'envoyer un formulaire de consentement plusieurs mois après l'entretien/l'observation.

Que faire si je n'ai pas informé les enquêté·es du devenir des données ou laissé mon contact ?

Si la personne n'a pas de moyen de vous contacter ou si vous ne les avez pas informé·es des conditions de leur participation à l'enquête, il vaut mieux les recontacter pour les prévenir et les informer de la possibilité de se retirer de l'enquête.

Transmettre les informations sur les conditions de participation à l'enquête, c'est-à-dire le détail des différentes utilisations qui seront faites des données, est une obligation. Votre contact doit également être transmis au cas où les personnes changeraient d'avis.

Si les enquêté·es ne sont pas francophones, dans quelle langue faire signer le consentement ?

Le protocole doit être adapté en fonction des populations concernées, donc le consentement doit être obtenu dans la langue de la personne enquêtée.

Le consentement des parents est-il toujours obligatoire pour les mineur·es ?

De façon générale, le consentement des parents est obligatoire pour les mineur·es de moins de 15 ans. Toutefois, si le fait d'informer les parents de l'objet de l'enquête peut mettre le ou la mineur·e concerné·e en danger, il est alors possible de s'affranchir du consentement des parents.

Que faire si un·e enquêté·e retire son consentement ?

Si la personne retire son consentement, il faut retirer tout ce qui a été obtenu d'elle d'un point de vue éthique puisqu'il est ici question de participation libre à la recherche.

Est-il nécessaire de demander le consentement des enquêté·es pour toutes les activités présentées sur le modèle de consentement à la recherche proposée par la DPO (cf. ENT de l'EHESS) ?

Non, les demandes de consentement doivent être adaptées à ce que vous faites concrètement dans votre enquête.

Comment gérer le consentement des personnes dans le cadre d'une observation/d'une ethnographie ?

Le consentement des personnes n'est pas nécessaire si les données collectées ne permettent pas d'identifier précisément les personnes. Si les données personnelles sont collectées, il est possible de passer par voie d'affichage (sur les lieux de l'enquête par exemple) en donnant vos coordonnées pour les personnes qui ne souhaiteraient pas participer à l'enquête (consentement par la négative).

Que faire si les personnes enquêté·es sont des personnalités publiques qui acceptent d'être citées dans le mémoire, mais dont les entretiens portent aussi sur des questions relatives à leur vie privée ?

Les personnalités publiques sont considérées comme des populations vulnérables, il faut donc redoubler de vigilance en traitant leurs données personnelles. Il est par exemple possible d'utiliser la pseudonymisation/anonymisation pour les éléments les plus personnels, demander le consentement des personnes pour chaque partie de l'entretien pour identifier ce qui devra être pseudonymisé/anonymisé ou non. Il est aussi possible de traiter les données « très personnelles » via des comptages plutôt que par citations d'entretiens, pour anonymiser. En disant par exemple qu'une majorité des enquêté·es ou bien les deux tiers déclarent avoir eu le sentiment d'être victime de discrimination dans leur entreprise, etc. Plutôt que, dans ce cas précis, citer un·e enquêté·e en particulier.

Que faire si une personne enquêtée, que je n'ai pas rencontrée, revendique le non-anonymat sur internet et souhaite être sourcée/nommée lorsque quiconque reprend ses citations ?

Si une personne revendique d'être citée, les risques vis-à-vis du RGPD sont plus limités. Toutefois, des éléments peuvent entrer en compte d'un point de vue éthique de la recherche : la situation de la personne a pu évoluer entre le moment de la publication de la citation qui fait l'objet de l'analyse et

est reprise dans votre travail, et le moment de la publication de la recherche et, si la citation était tombée dans l'oubli, sa republication peut avoir un effet sur la personne concernée.

Dans quels cas doit-on envoyer la retranscription des entretiens aux enquêté·es ?

Si un·e enquêté·e demande l'accès à ses données personnelles dans le cadre du RGPD, il est obligatoire de les fournir. En dehors de ce cadre, il n'y a aucune obligation à envoyer les retranscriptions d'entretien.

Est-il possible de réutiliser l'enregistrement d'un entretien dans un podcast (ou tout autre diffusion non prévue initialement) ?

Il convient d'obtenir le consentement des personnes concernées pour cette utilisation précise de l'entretien, par exemple en envoyant le podcast monté à la personne concernée en précisant via quelle plateforme le podcast va être diffusé pour vérifier que la personne n'a pas d'objection à l'utilisation de l'enregistrement de son entretien dans le contexte du podcast. Il est aussi possible de proposer d'utiliser un pseudonyme pour parler de la personne concernée en introduisant l'enregistrement dans le podcast, plutôt que son vrai nom.

Déclaration à la DPO EHESS

Quand contacter la DPO ?

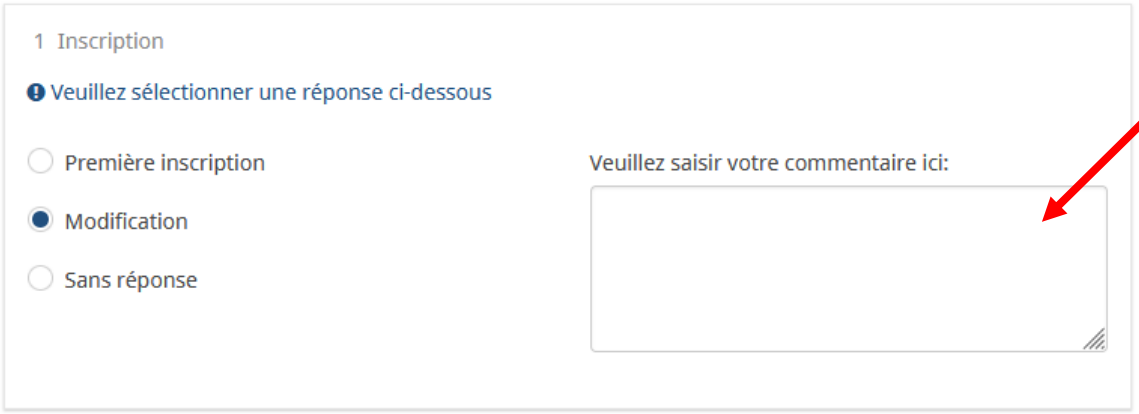
Dès que vous avez une idée assez précise de la population enquêtée, du terrain de recherche et des données personnelles qui seront récoltées.

Comment prouver que l'on a encore besoin des données identifiantes ?

Par exemple en expliquant que vous avez le projet de poursuivre en doctorat, que vous devez les conserver jusqu'à la soutenance de votre mémoire pour vérifier/prouver que la méthodologie de recherche a été respectée, etc.

Que faire vis-à-vis de la déclaration du projet auprès de la DPO si on change de méthodologie en cours d'enquête ?

Il est possible de réutiliser le même formulaire en ligne pour les modifications au projet, en cochant « Modification » lors de la première question du formulaire et en précisant dans la zone de commentaire quelle partie de la déclaration est modifiée :



Stocker et partager les données de manière sécurisée

Qu'est-ce que « transférer des données hors de l'Union Européenne » ?

Vous transférez des données hors de l'UE dès lors que vous envoyez des données à des chercheur·ses basées hors de l'UE et, surtout, si vous utilisez un outil de stockage à distance (cloud) hébergé hors UE, comme par exemple Dropbox, Google Drive, Trello, Padlet, etc. Il est fortement déconseillé d'envoyer des données personnelles identifiantes par e-mail (les services d'envoi de mail ne proposent généralement pas un niveau de sécurité suffisant, il faut *a minima* crypter les documents, par exemple avec VeraCrypt, avant de les envoyer).

Comment gérer l'enregistrement d'entretiens réalisés en visioconférence, par exemple Zoom, ou par téléphone ou encore par les messageries de réseaux sociaux ?

Les outils de visioconférence sont considérés comme non-sécurisés, en particulier Zoom. Si vous devez réaliser un entretien en visioconférence, nous vous recommandons fortement d'utiliser l'outil BBB (https://services-numeriques.ehess.fr/services/visioconference/) proposé par l'EHESS et accessible avec votre compte étudiant. Concernant les réseaux sociaux, si tous les échanges se font via leurs services de messagerie, les conversations sont conservées, analysées, et peuvent être revendues par l'entreprise. Il n'est pas interdit de les utiliser, mais il faut toujours évaluer les risques pris par votre enquêté·e.

Comment gérer l'effacement des messages sur les messageries de réseaux sociaux alors que ceux-ci conservent quoiqu'il en soit les messages ?

Effacer les messages sur vos comptes personnels demeure malgré tout une mesure de sécurité puisque cela rend plus difficile l'accès aux données, par exemple il y a moins de risques que les données personnelles soient transférées à autrui en cas de vol de téléphone.

Comment faire si un enregistrement automatique de données sur le *cloud* est activé sur mon téléphone ou mon ordinateur ?

Si le cloud en question est hébergé hors de l'Union européenne, il convient de désactiver le téléchargement automatique. Nous vous conseillons d'utiliser l'outil de stockage mis à disposition à tous·tes les étudiant·es et enseignant·es par l'EHESS : https://mesdocuments.aria.ehess.fr/.

Dès lors que les données sont pseudonymisées/anonymisées sans possibilité de réidentifier les personnes (par exemple, la table de correspondance n'est pas envoyée/transférée/stockée au même endroit), il est possible de les envoyer/transférer/stocker sur des clouds hébergés hors UE.

Qu'est-ce qu'une table de correspondance ?

Il s'agit d'un tableau explicitant quel·le enquêté·e, quelle organisation, quelle ville correspond à quel pseudonyme.

Comment évaluer la durée de conservation des données personnelles ?

L'idée est de ne pas conserver indéfiniment les données personnelles, mais la durée est définie par le ou la chercheur·se concerné·e selon ses besoins. Si vous évaluez par exemple qu'il vous faudra un an pour retranscrire les entretiens, puis les pseudonymiser, cette durée est acceptable.

La durée de conservation dépend de la nécessité de réutiliser les données et, pour la déterminer, quelques questions sont à vous poser : est-ce indispensable de conserver les données identifiantes ? est-ce que vous prévoyez de recontacter les personnes ? et si oui, les avez-vous prévenues de cette possibilité ?

Que faire s'il y a violation des données personnelles identifiantes alors que je n'ai pas accès à mes outils (par exemple, si mon ordinateur est volé alors que je suis en congés loin de chez moi et que je ne le sais pas encore) ?

Le délai est de 72h pour déclarer les violations de données court *à partir de la découverte de l'incident,* et non pas à partir de la date de l'incident.

Que faire si un·e enquêté·e me transmet des archives personnelles, par exemple leur correspondance avec des tiers non informé·es de l'enquête ?

Les correspondances sont en théorie protégées par le secret de la correspondance, donc les données concernant les tiers qui ne sont pas informé·es de l'enquête doivent être anonymisées si certaines informations sont réutilisées et il n'est pas possible de diffuser les lettres (donc de les annexer au mémoire ou à la thèse).

Que faire si j'ai commencé à utiliser un outil en ligne avant de me rendre compte que celui-ci est hébergé hors UE ?

Ce qui est important est d'être de « bonne foi », c'est-à-dire d'avoir cessé d'utiliser l'outil en question dès lors que vous avez été informé de sa non-conformité avec le RGPD.

Quel antivirus gratuit utiliser sur son ordinateur ?

Il est recommandé d'éviter les antivirus gratuits de manière générale. La plupart des PC récents ont un antivirus intégré à présent (vérifier qu'il est activé et à jour).