PANELFIT

PARTICIPATORY APPROACHES TO A NEW ETHICAL AND LEGAL FRAMEWORK FOR ICT

Code de conduite sur la protection des données pour une recherche et une innovation responsables

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 788039.. It reflects only the author's view and the Agency is not responsible for any use that may be made of the information it contains.

Partenaires du projet impliqués dans le document

N°	Nom de l'organisation participante	Acronyme
1	Institut de Ciències del Mar (Consejo Superior de Investigaciones Científicas)	ICM-CSIC
2	Université du Pays basque / Euskal Herriko Unibertsitatea	UPV/EHU
3	Réseau européen des comités d'éthique de la recherche	EUREC
4	Centre régional de protection des données (Unabhängiges Landeszentrum für Datenschutz) AöR	ULD
5	Oesterreichische Akademie der Wissenschaften (Académie des sciences d'Autriche)	OEAW
6	Fonden Teknologiradet	DBT

Historique du document

Statut	Version	Date	Auteur(s)	Révisé par
Prov.	v0.5	30/10/2020	Pranesh Prakash (ICM-CSIC)	Karen Soacha (ICM-CSIC), Jaume Piera (ICM-CSIC)
Prov.	v1.0	03/11/2020	Pranesh Prakash (ICM-CSIC)	Julia Maria Mönig (EUREC), Johann Cas (OEAW), Bud Bruegger (ULD), Harald Zwingelberg (ULD), Bjørn Bested (DBT)
Prov.	v2.0	06/12/2020	Pranesh Prakash (ICM-CSIC)	Iñigo de Miguel Beriain (UPV/EHU), Karen Soacha (ICM-CSIC)
Prov.	v3.0	23/01/2021	Pranesh Prakash (ICM-CSIC)	Karen Soacha (ICM-CSIC)
Final	v4.0	02/08/2021	Pranesh Prakash (ICM-CSIC)	Karen Soacha (ICM-CSIC), Iñigo de Miguel Beriain (UPV/EHU)

Table of Content

1 Préambule

Ce code de conduite sur la protection des données pour une recherche et une innovation responsables (CCDP) est une contribution du projet PANELFIT à la communauté des chercheurs.

PANELFIT *(Participatory Approaches to a New Ethical and Legal Framework for ICT)* est un projet financé par Horizon 2020 qui a produit des normes opérationnelles et des lignes directrices pratiques pour répondre à certains des problèmes éthiques et juridiques posés par les technologies TIC. Le projet PANELFIT vise ainsi à fournir des éclaircissements et des orientations concernant les questions à l'intersection entre la recherche et l'innovation responsables,[1] l'éthique et la protection des données.

Le CCDP vise à fournir un ensemble de règles de conduite faciles à comprendre qui couvrent les grands principes prévus par le règlement général sur la protection des données (RGPD) de l'UE, ainsi qu'un ensemble de pratiques souhaitables, spécifiquement adaptées à la communauté des chercheurs.[2] Il existe de multiples codes de conduite relatifs à la recherche et à l'innovation responsables. Cependant, ces codes de conduite existants ne cherchent pas à fournir des conseils sur les principes de protection des données, ce qui est une lacune que le CCDP cherche à combler. Le CCDP se veut un texte d'introduction aux principes de protection des données, et ne cherche pas à couvrir tous les aspects du RGPD qui peuvent concerner les chercheurs. Ainsi, par exemple, le CCDP ne cherche pas à couvrir toutes les obligations qu'un chercheur peut avoir en vertu des lois sur la protection des données, ni tous les droits des personnes dont les données à caractère personnel sont utilisées par les chercheurs, ni les exigences légales concernant le partage des données à caractère personnel avec des collègues chercheurs en dehors de l'UE, ni les lois nationales sur la protection des données, etc. Le projet PANELFIT a également créé des "Lignes directrices sur les questions éthiques et juridiques de la protection des données dans la recherche et l'innovation en matière de TIC", qui visent à être beaucoup plus complètes à cet égard.

[1] La recherche et l'innovation responsables (RRI) est une composante importante du programme "Science avec et pour la société" du programme Horizon 2020 (H2020) de l'UE. "La RRI est le processus continu d'alignement de la recherche et de l'innovation sur les valeurs, les besoins et les attentes de la société." ("Déclaration de Rome sur la recherche et l'innovation responsables en Europe"). La Commission européenne note que "la RRI est une approche inclusive de la recherche et de l'innovation (R&I), afin de s'assurer que les acteurs sociétaux travaillent ensemble tout au long du processus de recherche et d'innovation... D'une manière générale, la RRI inclut l'anticipation et l'évaluation des implications potentielles et des attentes sociétales en matière de recherche et d'innovation." (Commission européenne, "La science avec et pour la société")

[2] Bien qu'il n'existe pas de définition unique et universellement acceptée de la recherche, il est utile de garder à l'esprit les mots du Contrôleur européen de la protection des données dans un récent rapport : "Les définitions réputées de la recherche tendent à mettre l'accent sur une activité systématique, y compris la collecte et l'analyse de données, qui accroît le stock de compréhension et de connaissances et leur application. La Commission européenne a défini les objectifs de la recherche et des politiques de l'UE comme étant "l'ouverture du processus d'innovation à des personnes ayant une expérience dans des domaines autres qu'universitaires et scientifiques", "la diffusion des connaissances dès qu'elles sont disponibles grâce aux technologies numériques et collaboratives" et "la promotion de la coopération internationale dans la communauté des chercheurs"." (Contrôleur européen de la protection des données, "Un avis préliminaire sur la protection des données et la recherche scientifique", 9-10).

1.1 RRI et protection des données

L'activité de recherche, qu'il s'agisse de l'engagement de la recherche ou de la diffusion de la recherche, implique souvent des données à caractère personnel d'autres personnes. 3
Ainsi, l'éthique des données est une composante nécessaire d'une recherche et d'une innovation responsables, et cela inclut la protection des données à caractère personnel. Dans l'UE, la protection des données à caractère personnel est un droit fondamental en vertu de la Charte des droits fondamentaux de l'Union européenne, et le règlement général sur la protection des données fournit des orientations réglementaires concrètes sur ce droit.
Lorsque les chercheurs traitent des données à caractère personnel, ils sont tenus de respecter la législation sur la protection des données et doivent s'efforcer de suivre les bonnes pratiques en la matière.
Le CCDP vise à aider les chercheurs à comprendre les principes fondamentaux qui sous-tendent la législation sur la protection des données en Europe et à les doter des connaissances nécessaires pour appliquer concrètement ces principes dans le cadre d'une recherche et d'une innovation responsables. La notion de recherche au sens du RGPD est large, elle couvre les activités visant à fournir des connaissances susceptibles "d'améliorer la qualité de vie d'un certain nombre de personnes et d'améliorer l'efficacité des services sociaux", et comprend "le développement technologique, la recherche fondamentale et appliquée et les recherches et études financées par le secteur privé et menées dans l'intérêt public dans le domaine de la santé publique". 4

2 Principes de protection des données

La protection des données à caractère personnel en vertu du RGPD s'articule autour d'un certain nombre de principes :
• Légalité, équité, transparence [5]
• Limitation de la finalité [6]
• Minimisation des données [7]
• Précision [8]
• Limitation du stockage [9]
• Intégrité et confidentialité [10]
• Responsabilité [11]

[3] Les données à caractère personnel sont toutes les informations relatives à une personne physique identifiée ou identifiable. Il s'agit d'une catégorie très large, qui comprend le nom d'une personne, un numéro d'identification, des données de localisation, un identifiant en ligne ou des facteurs spécifiques à l'identité physique, physiologique, génétique, mentale, économique, culturelle ou sociale de cette personne.
[4] Règlement général sur la protection des données, Règlement UE 2016/679, considérant 159.

[5] Règlement général sur la protection des données, Règlement UE 2016/679, art. 5(1)(a).
[6] Règlement général sur la protection des données, Règlement UE 2016/679, art. 5(1)(b).
[7] Règlement général sur la protection des données, Règlement UE 2016/679, art. 5(1)(c).
[8] Règlement général sur la protection des données, Règlement UE 2016/679, art. 5(1)(d).
[9] Règlement général sur la protection des données, Règlement UE 2016/679, art. 5(1)(e).
[10] Règlement général sur la protection des données, Règlement UE 2016/679, art. 5(1)(f).
[11] Règlement général sur la protection des données, Règlement UE 2016/679, art. 5(2).

2.1 Légalité, équité et transparence

Afin de se conformer aux exigences du principe de légalité, de transparence et d'équité, les chercheurs doivent :
• Déterminer les finalités de la collecte et de l'utilisation des données à caractère personnel.
• S'assurer qu'ils identifient un motif valable (au moins un des six motifs ("bases légales") prévus par le RGPD) pour collecter et utiliser les données.
• S'assurer que tout ce qu'ils font avec les données est légitime et conforme à toutes les lois et directives éthiques applicables, y compris celles relatives aux essais cliniques, à la propriété intellectuelle, aux droits de l'Homme, aux contrats, etc.
• Déterminer les attentes des individus quant à la manière dont les chercheurs pourraient utiliser leurs données et ce qu'ils considéreraient comme raisonnable.
• Déterminer les préjudices potentiels pour les personnes dont les données sont utilisées.
• Collecter et utiliser les données d'une manière ouverte et transparente.
• Informer les personnes, dans un langage clair, de l'identité de la personne qui collecte ou obtient les données, du fondement juridique de la collecte ou de l'obtention, des raisons de la collecte ou de l'obtention, de la durée de conservation des données, de la manière dont elles seront utilisées et par qui, et des droits dont elles disposent.
• Utiliser les données d'une manière équitable, conforme aux attentes des personnes, et d'une manière qui n'entraîne pas de préjudice injustifié ou injuste pour elles.
• Vérifier si les données qui doivent être collectées concernent des "catégories particulières de données à caractère personnel" (données sensibles, définies dans le RGPD), auquel cas l'une des bases légitimes spécifiques énumérées à l'art. 9(2) du RGPD doit être satisfaite, comme avoir le consentement explicite de la personne concernée, ou être sur la base d'une loi qui permet cette collecte à des "fins d'archivage dans l'intérêt public, à des fins de recherche scientifique ou historique ou à des fins statistiques."
• Vérifier si les données qui doivent être collectées concernent des "condamnations pénales et des infractions", auquel cas des lois spéciales s'appliquent.

Contexte

En vertu du droit européen, tout traitement de données à caractère personnel doit être effectué dans un but légal et avec un objectif légitime. Alors que les autres principes prévoient des limitations sur la manière dont les données à caractère personnel peuvent être traitées, ce principe impose des limitations sur les finalités pour lesquelles les données à caractère personnel peuvent être traitées.

Base légale

Le RGPD prévoit six bases juridiques[12] pour lesquelles les données à caractère personnel peuvent être traitées légalement. Ainsi, la finalité du traitement des données à caractère personnel doit relever d'au moins une des six catégories :
• Consentement de l'individu
• Exécution d'un contrat
• Respect d'une obligation légale, tel qu'autorisé par la loi
• Nécessaire à la protection des intérêts vitaux d'une personne
• Nécessaire pour une tâche officielle ou d'intérêt public légalement autorisée, conformément à la loi
• Intérêts légitimes

[12] Règlement général sur la protection des données, Règlement UE 2016/679, art. 6.

Il convient de noter que, contrairement aux institutions privées, les autorités publiques ne sont pas autorisées à utiliser l'"intérêt légitime" comme finalité, sauf si le traitement ne relève pas des missions de l'autorité publique. En outre, la "nécessité" et l'"intérêt public" impliquent un "besoin social impérieux", par opposition à des avantages largement privés ou commerciaux. [13]

Si le "consentement" est utilisé comme base, il est important que la finalité soit spécifiée de manière claire et explicite et qu'elle révèle, explique ou exprime sous une forme aisément compréhensible pourquoi les données sont collectées et traitées. Le consentement lui-même doit être librement donné, spécifique, éclairé et sans ambiguïté, et la personne a le droit de le retirer à tout moment.

Le RGPD reconnaît qu'"il n'est souvent pas possible d'identifier pleinement la finalité du traitement des données à caractère personnel à des fins de recherche scientifique au moment de la collecte des données. Par conséquent, les personnes concernées devraient être autorisées à donner leur consentement à certains domaines de la recherche scientifique lorsque cela est conforme aux normes éthiques reconnues en matière de recherche scientifique. Les personnes concernées devraient avoir la possibilité de ne donner leur consentement qu'à certains domaines de la recherche ou à certaines parties des projets de recherche, dans la mesure où la finalité prévue le permet."[14]

Le Contrôleur européen de la protection des données (CEPD) note que "le consentement spécifique normalement requis en vertu du RGPD peut donc devenir moins approprié dans le cas de données collectées et déduites et en particulier dans le cas de catégories spéciales de données sur lesquelles repose une grande partie de la recherche scientifique", et donc, "lorsque les finalités de la recherche ne peuvent pas être entièrement spécifiées, on attendrait d'un responsable du traitement qu'il prenne plus de mesures pour garantir l'essence des droits de la personne concernée à un consentement valide, y compris par une transparence aussi grande que possible et d'autres garanties." [15]

Équité

En outre, la manière dont le traitement est effectué doit être équitable et transparente. Même si le traitement entrepris a une base légale, il peut être injuste, et donc en violation de ce principe. L'équité est un concept large : elle exige que les chercheurs ne traitent les données à caractère personnel que d'une manière à laquelle les gens s'attendent raisonnablement, et qu'ils ne fassent rien qui puisse nuire aux personnes concernées.

Transparence

La transparence exige que les personnes soient informées des finalités prévues pour la collecte et l'utilisation des données à caractère personnel, des motifs juridiques du traitement, etc. Cette information est nécessaire, qu'il s'agisse de la collecte directe de données à caractère personnel auprès des personnes concernées (qu'elles aient été fournies consciemment par la personne ou qu'elles aient été recueillies par observation de la personne), ou de l'obtention de données à caractère personnel auprès d'une autre source (comme un tiers à qui les données ont été confiées, des sources publiques, des courtiers en

[13] Contrôleur européen de la protection des données, "Un avis préliminaire sur la protection des données et la recherche scientifique", 23.

[14] Règlement général sur la protection des données, Règlement UE 2016/679, considérant 33.

[15] 15 Contrôleur européen de la protection des données, "Un avis préliminaire sur la protection des données et la recherche scientifique", 19.

données ou d'autres personnes).[16] Les informations qui doivent être fournies comprennent au minimum les éléments suivants : [17]
• qui est votre entreprise/organisation (vos coordonnées et celles de votre DPD, le cas échéant) ;
• la raison pour laquelle votre entreprise/organisation utilisera leurs données à caractère personnel (finalités) ;
• les catégories de données à caractère personnel concernées ;
• la justification légale du traitement de leurs données ;
• la durée de la conservation des données ;
• les éventuels autres destinataires ;
• le transfert éventuel de leurs données à caractère personnel à un destinataire situé en dehors de l'UE ;
• leur droit d'obtenir une copie des données (droit d'accès aux données à caractère personnel) et d'autres droits fondamentaux dans le domaine de la protection des données (voir la liste complète des droits) ;
• leur droit de déposer une plainte auprès d'une autorité de protection des données (APD) ;
• leur droit de retirer leur consentement à tout moment ;
• le cas échéant, l'existence d'une prise de décision automatisée et la logique qu'elle implique, y compris ses conséquences.

Si vous avez obtenu des données à caractère personnel d'une source autre que les personnes concernées, vous devez les informer dans un délai raisonnable, et au maximum dans un mois à compter de la date à laquelle vous avez eu accès à leurs données à caractère personnel.
Les obligations de transparence ne s'appliquent pas lorsque et dans la mesure où la personne concernée dispose déjà de l'information.[18] Pour les données à caractère personnel collectées auprès d'un tiers, il existe trois situations supplémentaires dans lesquelles les obligations de transparence ne s'appliquent pas : [19]
• Lorsque cela s'avère impossible (notamment à des fins d'archivage, de recherche scientifique/ historique ou de statistiques) ;
• Lorsque cela impliquerait un effort disproportionné (notamment à des fins d'archivage, de recherche scientifique/historique ou de statistiques) ; ou
• Lorsque la fourniture des informations requises en vertu de l'article 14.1 rendrait impossible ou compromettrait gravement la réalisation des objectifs du traitement.

Catégories spéciales de données à caractère personnel / Données sensibles
Les catégories spéciales de données à caractère personnel, ou données sensibles,[20] sont des données qui révèlent :
• l'origine raciale ou ethnique,
• les opinions politiques,
• les croyances religieuses ou philosophiques,
• l'adhésion à un syndicat,

ou sont :
• des données génétiques,

[16] Règlement général sur la protection des données, Règlement UE 2016/679, art. 12(1), (5), (7), art. 13, art. 14, considérants 39, 58-62.
[17] Commission européenne, "Quelles informations doivent être fournies aux personnes dont les données sont collectées ?".
[18] Règlement général sur la protection des données, Règlement UE 2016/679, art. 13(4), art. 14(5)(a).
[19] Règlement général sur la protection des données, Règlement UE 2016/679, art. 14(5)(b).
[20] Règlement général sur la protection des données, Règlement UE 2016/679, art. 9(1), considérants 51-56.

• des données biométriques dans le but d'identifier de manière unique une personne physique,
• des données concernant la santé, ou
• des données concernant la vie sexuelle ou l'orientation sexuelle d'une personne physique.
Ces données sensibles ne peuvent être collectées que si la collecte relève de l'un des dix motifs légitimes prévus par le RGPD,[21] ce qui inclut le consentement explicite, ainsi que lorsque cela est nécessaire pour la recherche archivistique, scientifique ou historique, et les statistiques avec les garanties appropriées qui sont légalement requises par le RGPD et sont prévues par une loi appropriée.[22] Étant donné les différences nationales dans les lois régissant les données sensibles, et en particulier les données génétiques, biométriques ou concernant la santé,[23] les chercheurs devraient consulter le délégué à la protection des données de leur institution, ou l'autorité locale de protection des données pour en savoir plus sur ce qui est autorisé et ce qui ne l'est pas.
En outre, bien que les données relatives aux condamnations pénales et aux infractions ne soient pas considérées comme "sensibles" au sens du RGPD, le règlement exige que toute utilisation de ces données par les chercheurs soit autorisée par une loi européenne ou nationale et respecte les garanties prévues par cette loi. [24]

2.2 Limitation de la finalité

Pour se conformer au principe de limitation de la finalité, les chercheurs doivent :
• Documenter en termes clairs et spécifiques les finalités qui sous-tendent la collecte et l'utilisation des données à caractère personnel.
• Fournir aux personnes des informations sur les finalités de la collecte et de l'utilisation de leurs données.
• Limiter le traitement des données à caractère personnel aux finalités spécifiées ou à des finalités compatibles avec ces dernières.
• Veiller à informer la personne concernée dans les cas où le motif initial d'utilisation des données à caractère personnel était autre que le consentement ou une exigence légale, et où ces données font maintenant l'objet d'une nouvelle utilisation compatible. Cette notification doit être effectuée raisonnablement avant que la nouvelle utilisation des données à caractère personnel ait lieu, afin de permettre à la personne de s'opposer au traitement.
• Veiller à demander un nouveau consentement dans les cas où le motif initial d'utilisation des données à caractère personnel était le consentement, et où ces données sont maintenant utilisées à d'autres fins (indépendamment du fait que la nouvelle utilisation soit "compatible").
• S'assurer qu'ils ont soit le consentement, soit une obligation/fonction claire prévue dans l'intérêt public dans une loi s'ils souhaitent utiliser les données à caractère personnel à des finalités autres que celles spécifiées ou compatibles.
• Veiller à ce que la nouvelle utilisation soit équitable, légale et transparente.

Contexte

La finalité doit être "spécifiée, explicite et légitime".[25] Le groupe de travail "Article 29" note qu'"une finalité vague ou générale, comme par exemple ... "des recherches futures", ne répondra généralement pas - sans plus de détails - aux critères de "spécificité". Cela dit, le degré de détail dans lequel une finalité doit être spécifiée dépend du contexte particulier

[21] Règlement général sur la protection des données, Règlement UE 2016/679, art. 9(2)(a).
[22] Règlement général sur la protection des données, Règlement UE 2016/679, art. 89.
[23] Règlement général sur la protection des données, Règlement UE 2016/679, art. 9(4).
[24] Règlement général sur la protection des données, Règlement UE 2016/679, art. 10.
[25] Règlement général sur la protection des données, Règlement UE 2016/679, art. 5(1)(b).

dans lequel les données sont collectées et des données à caractère personnel concernées. Dans certains cas clairs, un langage simple sera suffisant pour fournir une spécification appropriée, alors que dans d'autres cas, plus de détails peuvent être nécessaires."[26]
L'autorisation de traiter est limitée à :
• les finalités légitimes qui ont été explicitement spécifiées lors de la collecte des données, ou
• d'autres finalités compatibles avec les objectifs initiaux.

La compatibilité peut être jugée à l'aide des critères suivants :
a) le lien entre les finalités initiales et les finalités supplémentaires envisagées ;
b) le contexte dans lequel les données à caractère personnel ont été collectées, notamment en ce qui concerne la relation entre les personnes concernées et le responsable du traitement ;
c) la nature des données à caractère personnel, en particulier si elles comprennent des catégories spéciales de données à caractère personnel (c'est-à-dire des données sensibles) ou si des données à caractère personnel relatives à des condamnations pénales et à des infractions sont traitées ;
d) les conséquences possibles du traitement ultérieur envisagé pour les personnes concernées ;
e) l'existence de garanties appropriées, qui peuvent inclure la pseudonymisation.

Certaines finalités sont présumées compatibles, si les garanties appropriées et prescrites par la loi sont respectées :
• l'archivage dans l'intérêt public,
• la recherche scientifique ou historique, et
• les statistiques

Cependant, comme le CEPD le note, "la présomption n'est pas une autorisation générale de traiter ultérieurement des données dans tous les cas à des fins historiques, statistiques ou scientifiques. Chaque cas doit être examiné selon ses propres mérites et circonstances. Mais en principe, les données à caractère personnel collectées dans le contexte commercial ou des soins de santé, par exemple, peuvent être utilisées ultérieurement à des fins de recherche scientifique, par le responsable initial ou un nouveau responsable du traitement, si des garanties appropriées sont en place... afin de garantir le respect des droits de la personne concernée, le test de compatibilité prévu à l'article 6, paragraphe 4, devrait toujours être envisagé avant la réutilisation des données à des fins de recherche scientifique, en particulier lorsque les données ont été initialement collectées à des fins très différentes ou en dehors du domaine de la recherche scientifique." [27]

2.3 Minimisation des données

Pour être en accord avec le principe de minimisation des données, les chercheurs doivent :
• S'assurer qu'ils ne collectent des données à caractère personnel que si elles sont adéquates, pertinentes et nécessaires à la finalité qu'ils ont spécifiée.
• S'abstenir de collecter des quantités de données à caractère personnel plus importantes que nécessaire.
• S'abstenir de collecter des types de données à caractère personnel plus détaillées ou granulaires que nécessaire.

[26] Groupe de travail Article 29 sur la protection des données, "Avis 03/2013 sur la limitation de la finalité", 15-16.
[27] Contrôleur européen de la protection des données, "Un avis préliminaire sur la protection des données et la recherche scientifique", 22-23.

• S'assurer qu'ils ne conservent pas les données à caractère personnel plus longtemps que nécessaire.
• Examiner périodiquement les données à caractère personnel qu'ils stockent pour vérifier s'ils continuent à être en conformité avec ce qui précède, et supprimer toutes les données à caractère personnel qui ne remplissent pas les conditions requises.

Contexte

L'adéquation, la pertinence et la nécessité sont trois exigences pour le traitement des données à caractère personnel en vertu du RGPD. Ainsi, les données inadéquates, c'est-à-dire impropres à la finalité spécifiée, ne peuvent être collectées ou traitées ; les données doivent également être pertinentes, c'est-à-dire qu'elles doivent servir la finalité spécifiée. Et la limitation de la nécessité comporte trois aspects :
• quantité de données ;
• la granularité des données, et
• la durée du stockage (traitée plus en détail dans le principe de "limitation du stockage" ci-dessous)

Ainsi, en termes simples, les chercheurs devraient s'efforcer de collecter, de stocker et de traiter le moins de données à caractère personnel possible, pendant une période aussi courte que possible pour atteindre la finalité spécifiée. Comme pour les autres principes, cet objectif est atteint par des mesures techniques et organisationnelles.
La minimisation des données est mentionnée comme une préoccupation particulière dans le RGPD pour ceux qui traitent des données à caractère personnel à des fins d'archivage dans l'intérêt public, à des fins de recherche scientifique ou historique, ou à des fins statistiques, puisque ces derniers fonctionnent sous un régime légèrement plus souple en ce qui concerne le principe de limitation de la finalité. Les mesures qui peuvent être prises pour minimiser les données incluent la pseudonymisation, si cela est possible.

2.4 Précision

Pour respecter le principe d'exactitude, les chercheurs doivent :
• S'assurer que les données à caractère personnel qu'ils détiennent sont factuellement correctes.
• S'assurer que les données à caractère personnel qu'ils détiennent sont à jour.
• Mettre en place des processus pour vérifier l'exactitude des données, avec des délais de vérification de l'actualité.
• Corriger toute donnée factuellement incorrecte ou trompeuse dès qu'elle est découverte.
• Enregistrer toutes les erreurs qui doivent être préservées en tant qu'erreurs, ainsi que la raison de leur préservation.
• Donner suite à toute demande de rectification émanant de personnes.

Contexte

Le principe d'exactitude comporte deux aspects : l'exactitude factuelle et la mise à jour. Il est interdit d'utiliser des données à caractère personnel inexactes, car elles pourraient être impropres à la finalité pour laquelle elles sont recherchées. En outre, des données inexactes pourraient nuire aux personnes concernées et violer ainsi le principe d'équité. Les chercheurs ont donc l'obligation d'effacer ou de corriger les données à caractère personnel inexactes.
Afin de garantir l'exactitude de leurs données à caractère personnel, les personnes concernées se sont vu accorder le droit de demander la rectification des données.

2.5 Limitation du stockage

Pour garantir le respect du principe de limitation du stockage, les chercheurs doivent :
• S'assurer qu'ils ne conservent pas les données à caractère personnel plus longtemps que nécessaire pour la finalité pour laquelle elles ont été collectées.
• S'assurer qu'ils suppriment ou rendent anonymes les données à caractère personnel qui ne sont plus nécessaires.
• Documenter la finalité pour laquelle les données à caractère personnel ont été collectées, et la durée de conservation des données nécessaire pour atteindre cette finalité.
• Documenter la justification de la période de conservation.
• Vérifier la nécessité de la conservation lorsque la période de conservation prédéterminée prend fin.
• Identifier et documenter l'archivage d'intérêt public, la recherche scientifique ou historique, ou la finalité statistique pour laquelle les données sont conservées pendant une période plus longue que celle strictement nécessaire, dans le cas où les données sont conservées en vertu de l'exception pour une telle recherche, ainsi que le respect des garanties adéquates, comme le prescrit légalement l'art. 89.

Contexte

Les chercheurs ne doivent pas conserver les données à caractère personnel plus longtemps que nécessaire aux finalités spécifiées pour lesquelles les données ont été collectées. Les données devraient être détruites dès qu'elles ne sont plus nécessaires aux finalités spécifiées. L'un des moyens d'y parvenir est de procéder à l'anonymisation des données chaque fois que cela est possible, convertissant ainsi les données à caractère personnel en données qui ne permettent plus l'identification directe ou indirecte des personnes concernées par ces données.
Les chercheurs sont autorisés à conserver les données à caractère personnel plus longtemps que ce qui est strictement nécessaire si les données à caractère personnel sont utilisées uniquement à des fins d'archivage dans l'intérêt public, à des fins de recherche scientifique ou historique ou à des fins statistiques, et si elles remplissent en outre les conditions énoncées à l'article 89 du RGPD, à savoir disposer de garanties adéquates sous la forme de mesures techniques et organisationnelles appropriées pour sauvegarder les droits des personnes. En outre, les chercheurs devraient s'assurer qu'ils n'utilisent pas ces données à caractère personnel comme base pour toute mesure ou décision concernant une personne en particulier[28]

2.6 Intégrité et confidentialité

Pour respecter le principe d'intégrité et de confidentialité, les chercheurs doivent :
• Veiller à ce que les données à caractère personnel soient conservées en toute sécurité, en les protégeant contre tout traitement non autorisé ou illégal, ainsi que contre toute perte, destruction ou dommage accidentels, en utilisant des mesures techniques et organisationnelles.
• Documenter les mesures techniques et organisationnelles mises en place pour assurer la sécurité.

Contexte

Les chercheurs sont tenus de veiller à ce que les données à caractère personnel soient conservées en toute sécurité, ce qui signifie qu'ils assurent la confidentialité, l'intégrité et la disponibilité des données, et les protègent ainsi contre tout traitement non autorisé ou illégal

[28] Groupe de travail Article 29 sur la protection des données, "Avis 03/2013 sur la limitation de la finalité", 28.

et contre toute perte, destruction ou dommage accidentels, en utilisant des moyens techniques et organisationnels.
La sécurité des données est donc un élément essentiel de la protection des données à caractère personnel. Pour déterminer si la confidentialité et l'intégrité ont été respectées, il est important de se placer du point de vue des personnes concernées, et non du point de vue des chercheurs. En d'autres termes, même si les chercheurs n'ont subi aucun dommage en raison d'un traitement non autorisé, on ne peut pas dire que le traitement non autorisé n'a causé aucun préjudice.
Cela signifie que les chercheurs doivent avoir défini des rôles et des responsabilités clairement définis afin de savoir qui est autorisé à accéder aux données à caractère personnel dans le cadre d'un projet de recherche particulier.

2.7 Responsabilité

Pour le respect du principe de responsabilité, les chercheurs doivent :
• Veiller à ce qu'ils se conforment de manière proactive et organisée à la législation sur la protection des données.
• Découvrir les obligations qui leur incombent et les droits dont disposent les particuliers en vertu de la loi.
• Mettre en place des politiques, des processus et des mesures techniques clairs qui garantissent le respect des principes ci-dessus et de la loi.
• Veiller à ce que l'approche "privacy by design and by default" soit suivie.
• Veiller à ce que votre organisation dispose d'un responsable à la protection des données si elle est une autorité ou un organisme public, si elle effectue un suivi régulier et systématique des personnes à grande échelle ou si elle traite un grand nombre de catégories spéciales de données, telles que des données sensibles.
• Réaliser une analyse d'impact sur la protection des données si le type de traitement des données qu'ils souhaitent entreprendre est susceptible d'entraîner un risque élevé, et en particulier s'ils prévoient d'utiliser un profilage systématique et étendu ayant des effets significatifs, de traiter à grande échelle des données relatives à des catégories spéciales ou à des infractions pénales, ou de surveiller systématiquement à grande échelle des lieux accessibles au public.
• Notifier les personnes, généralement par l'intermédiaire du délégué à la protection des données de votre institution, d'une violation de données au plus tard 72 heures si la violation est susceptible de présenter un risque pour les droits et libertés des personnes dont les données à caractère personnel ont été violées.
• Répondre immédiatement à tout exercice par les personnes de leurs droits sur leurs données.
• Documenter leur conformité à tous les principes ci-dessus et à la loi.

Contexte

Les personnes qui collectent et utilisent des données à caractère personnel, comme les chercheurs, sont responsables du respect des principes énumérés ci-dessus. Il est important qu'ils soient en mesure de démontrer qu'ils s'y conforment.
Le respect de ces principes doit donc être planifié et documenté. Par exemple, les chercheurs devraient être en mesure de justifier pourquoi ils ont besoin de certaines données à caractère personnel, à la granularité à laquelle ils les collectent, et la durée de conservation des données. De nombreux aspects de la responsabilité bénéficieraient de la mise en place de mesures techniques automatisées.

3 Bonnes pratiques relatives aux principes de protection des données

Les bonnes pratiques pour les principes de protection des données couvrent les pratiques qui vont au-delà du minimum requis par le RGPD et les lois nationales. Bien qu'elles ne soient pas légalement obligatoires, elles aideront les chercheurs à se conformer aux principes de protection des données déjà abordés dans ce document.

3.1 Anonymisation, pseudonymisation et cryptage

Les diverses exigences du RGPD ne s'appliquent pas si les chercheurs ne manipulent pas de données à caractère personnel. Par conséquent, dans la mesure du possible, vérifiez si les données nécessaires à la recherche nécessitent de pouvoir identifier une personne. Mais notez que le RGPD fait une distinction entre les données pseudonymisées et les données anonymisées. Le simple fait de supprimer tous les identifiants personnels ne rend pas automatiquement les données "anonymes".

Les données à caractère personnel pseudonymisées sont des données à caractère personnel qui ne peuvent plus être attribuées à une personne spécifique sans l'utilisation d'informations supplémentaires ; mais avec des informations supplémentaires, la personne concernée peut être découverte.

Pour les données anonymisées, non seulement il ne faut pas être en mesure d'identifier une personne en particulier sur la base des données que l'on a collectées et traitées, mais il faut également prendre en compte tous les moyens que d'autres personnes pourraient trouver "raisonnablement susceptibles d'être utilisés, tels que la singularisation (...) pour identifier la personne physique directement ou indirectement." Pour voir quels moyens sont "raisonnablement susceptibles d'être utilisés pour identifier la personne physique", le RGPD nous informe qu'il convient de "tenir compte de tous les facteurs objectifs, tels que les coûts et le temps nécessaires à l'identification, en prenant en considération la technologie disponible au moment du traitement et les évolutions technologiques."[29] Ainsi, s'il est pratiquement possible de désanonymiser les données, alors cela ne peut pas être considéré comme des données anonymes - il s'agirait alors de données pseudonymisées, qui comptent toujours comme des données à caractère personnel.

Le RGPD suggère la pseudonymisation et le cryptage comme deux moyens d'assurer une meilleure sécurité des données à caractère personnel. Ces deux techniques permettraient de répondre aux exigences du principe d'intégrité et de confidentialité. La pseudonymisation permettrait également de respecter le principe de minimisation des données. Dans le cas de certains types de traitement de données à des fins de recherche scientifique, pour lesquels le principe de limitation de la finalité est légèrement assoupli, le RGPD exige que les chercheurs cherchent à minimiser les données, et qu'ils le fassent en utilisant la pseudonymisation chaque fois que cela est possible ou en rendant les données anonymes si cela est réalisable. [30]

3.2 Données agrégées et grossières

Dans la mesure du possible, préférez les données agrégées aux données au niveau individuel, et préférez les données grossières aux données granulaires. Par exemple, si des données sur l'âge sont nécessaires, choisissez de les collecter sous la forme d'un nombre plutôt que d'une date de naissance. Mieux encore, si une fourchette d'âge suffit, choisissez

[29] Règlement général sur la protection des données, règlement UE 2016/679, considérant 26.

[30] Règlement général sur la protection des données, Règlement UE 2016/679, art. 89(1).

de la collecter plutôt qu'un âge précis. Enfin, si la date de plusieurs personnes peut être agrégée et les données individuelles détruites, choisissez de le faire.

3.3 Transparence

Si les données à caractère personnel sont collectées dans un contexte en ligne, fournissez un lien bien visible vers la déclaration ou l'avis de confidentialité, ou assurez-vous que les informations sont disponibles sur la même page que celle sur laquelle les données à caractère personnel sont collectées.[31] Si des changements interviennent dans la manière dont vous traitez les données à caractère personnel, toutes les informations doivent être fournies à nouveau à la personne concernée, tout en veillant à ce qu'il soit facile de savoir quelles sont les informations nouvelles.[32]

3.4 Motifs multiples de traitement

Le RGPD semble permettre la possibilité d'utiliser plusieurs motifs légaux pour le traitement des mêmes données à caractère personnel. Toutefois, cela pourrait conduire à une situation où deux motifs (tels que le consentement et l'intérêt légitime) sont utilisés, mais où l'un des motifs est supprimé (par exemple, une personne qui révoque son consentement). Dans ce cas, ce que la loi exige n'est pas clair et il n'y a pas d'avis unanime clair parmi les autorités juridiques. Il est préférable de résoudre cette incertitude par une compréhension conservatrice de la loi, et de cesser de traiter les données lorsque l'un des motifs disparaît. Pour éviter cette situation, il peut être préférable de ne pas combiner le consentement avec d'autres motifs. Dans ce cas, il peut être préférable de choisir de ne traiter les données qu'en vertu du motif le plus approprié.

3.5 Le consentement dans la protection des données et dans l'éthique

Le consentement en tant que motif légal de traitement des données en vertu de la législation sur la protection des données est différent du "consentement éclairé" en tant que principe d'éthique pour la recherche sur des sujets humains.[33] Il est donc toujours préférable de fournir des formulaires de consentement distincts et d'obtenir chaque type de consentement séparément. Même si l'institution obtient les deux types de consentement à l'aide d'un seul formulaire, il convient de conserver une trace claire de ce à quoi chaque participant a consenti en ce qui concerne la recherche. Même dans les cas où le consentement n'est pas utilisé comme motif en vertu du RGPD, "le consentement éclairé en tant que participant à une recherche sur l'Homme pourrait toujours servir de "garantie appropriée" des droits de la personne concernée."[34]

3.6 Approbations de légitimité, d'équité et d'éthique

La légitimité de la collecte de données sera parfois déterminée par des lois qui prescrivent des exigences éthiques (comme pour les essais cliniques). Mais même lorsque les

[31] Groupe de travail Article 29 sur la protection des données, "Lignes directrices sur la transparence en vertu du règlement 2016/679", 8.
[32] Groupe de travail Article 29 sur la protection des données, 27-28.
[33] Contrôleur européen de la protection des données, "Un avis préliminaire sur la protection des données et la recherche scientifique", 19-20.
[34] Contrôleur européen de la protection des données, 20.

recherches spécifiques ne sont pas couvertes par des exigences légales d'autorisation éthique, il est préférable de partir du principe qu'une collecte ou une utilisation de données non éthique sera également considérée comme une finalité illégitime au sens du RGPD, et ne respectera pas le principe d'équité. Ainsi, par exemple, les chercheurs devraient s'abstenir de s'engager dans tout traitement de données qu'un comité d'examen éthique désapprouve.

3.7 3Autorités chargées de la protection des données et comités d'éthique

Compte tenu de l'interaction croissante entre les questions éthiques et les questions de protection de la vie privée et des données, il serait profitable que les comités d'éthique s'engagent davantage avec les responsables et les autorités chargés de la protection des données.[35] Il existe de nombreux cas (tels que les données génétiques) dans lesquels l'utilisation des données à caractère personnel d'un individu dans la recherche affecterait non seulement cet individu, mais aussi d'autres personnes. Le cadre de la protection des données, à lui seul, peut ne pas être suffisant pour prendre en compte ces préoccupations comme le ferait un cadre combiné d'éthique de la recherche et de protection des données. Cela nécessite une plus grande collaboration entre ceux qui travaillent sur les questions d'éthique et ceux qui travaillent sur les questions de protection des données.

3.8 Lignes directrices en matière de protection des données et DPD

De nombreuses institutions de recherche ont publié des lignes directrices sur la protection des données, en plus des lignes directrices sur l'éthique. Les chercheurs doivent se familiariser avec les directives de leur institution. Souvent, les bailleurs de fonds ont également des exigences particulières en matière de protection des données. Tous les projets financés par Horizon 2020, par exemple, exigent la participation d'un délégué à la protection des données (DPD) s'il a été désigné, et même dans les cas où un DPD n'est pas légalement requis,36 une politique de protection des données doit être élaborée.

Il y a certaines questions sur lesquelles les lois des États membres s'appliquent, plutôt que le seul RGPD. Fait important pour les chercheurs, le régime spécial de protection des données pour le traitement à des fins d'archivage dans l'intérêt public, de recherche scientifique ou historique, ou à des fins statistiques, peut comporter des assouplissements des droits de l'individu et des obligations qui en découlent pour le chercheur, si les lois nationales le permettent. Des garanties appropriées sont requises pour le traitement des données à caractère personnel à l'une de ces fins. Les chercheurs doivent respecter les principes évoqués ci-dessus et accorder une attention particulière aux mesures techniques et organisationnelles visant à garantir la minimisation des données.[37] Étant donné que les spécificités des obligations des chercheurs en vertu de la loi ne sont donc pas uniformes, les chercheurs devraient consulter le délégué à la protection des données et les directives de protection des données de leur institution si possible, car ils seraient en mesure de guider les chercheurs sur les normes légales et extra-légales applicables.

[35] Contrôleur européen de la protection des données, 25.

[36] Règlement général sur la protection des données, Règlement UE 2016/679, art. 38.

[37] Règlement général sur la protection des données, Règlement UE 2016/679, art. 89.

3.9 Analyse d'impact sur la protection des données

Si un projet traite d'une grande quantité de données à caractère personnel, ou de données à caractère personnel de personnes vulnérables, il serait alors bénéfique de discuter de ce projet avec le DPD et de mettre en place une analyse d'impact sur la protection des données (DPIA), même si ce n'est pas légalement obligatoire. Le CEPD note qu'une "DPIA est obligatoire pour les opérations de traitement de données présentant des risques élevés pour les personnes concernées, par exemple lorsque deux des critères suivants s'appliquent" :381. Évaluation/profilage systématique 2. Prise de décision automatisée 3. Surveillance systématique 4. Traitement de données sensibles 5. Traitement à grande échelle 6. Appariement/combinaison d'ensembles de données à des fins différentes 7. Personnes concernées vulnérables 8. Nouvelles technologies 9. Empêcher les personnes d'exercer leurs droits ou de conclure un service/contrat

4 Annexes

4.1 Annexe 1 : Ressources clés

Le projet PANELFIT a élaboré un ensemble détaillé de lignes directrices sur la protection des données, les questions éthiques et juridiques dans la recherche et l'innovation en matière de TIC, ainsi qu'une analyse critique du cadre réglementaire de la protection des données en matière de TIC. Le CCDP est largement basé sur ces deux documents. Pour en savoir plus sur les questions soulevées dans le CCDP ou mieux comprendre les aspects de la protection des données qui n'ont pas été abordés dans le CCDP, consulter les lignes directrices, qui sont beaucoup plus détaillées. Elles seront toutes deux disponibles sur https://www.panelfit.eu/deliverables/.

Voici d'autres ressources importantes pour les chercheurs qui souhaitent en savoir plus sur la protection des données et la recherche et l'innovation responsables.

• Contrôleur européen de la protection des données. "Un avis préliminaire sur la protection des données et la recherche scientifique", janvier 2020. https://edps.europa.eu/sites/edp/files/publication/20-01-06_opinion_research_en.pdf.

• Groupe de travail Article 29 sur la protection des données. "Avis 03/2013 sur la limitation de la finalité", 2 avril 2013. https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2013/wp203_en.pdf.

• Groupe de travail Article 29 sur la protection des données. "Avis 05/2014 sur les techniques d'anonymisation", 10 avril 2014. https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2014/wp216_en.pdf*.

• Groupe de travail Article 29 sur la protection des données. "Lignes directrices sur la transparence en vertu du règlement 2016/679", 29 novembre 2017. https://ec.europa.eu/newsroom/article29/items/622227.

• Conseil européen de la protection des données. "Lignes directrices 03/2020 sur le traitement des données concernant la santé à des fins de recherche scientifique dans le contexte de l'épidémie de COVID-19." Lignes directrices, 30 avril 2020.

[38] Contrôleur européen de la protection des données, "Décision du contrôleur européen de la protection des données du 16 juillet 2019 sur les listes DPIA émises en vertu de l'article 39, paragraphes 4 et 5, du règlement (UE) 2018/1725", annexe 1.

https://edpb.europa.eu/sites/edpb/files/files/file1/edpb_guidelines_202003_healthdatascientificresearchcovid19_en.pdf.

• Conseil européen de la protection des données. "Lignes directrices 4/2019 sur l'article 25 Protection des données par conception et par défaut". Lignes directrices, 13 novembre 2019. https://edpb.europa.eu/sites/edpb/files/consultation/edpb_guidelines_201904_dataprotection_by_design_and_by_default.pdf.

• Conseil européen de la protection des données. "Lignes directrices 04/2019 sur l'article 25 : La protection des données dès la conception et par défaut. " Lignes directrices, 20 octobre 2020. https://edpb.europa.eu/sites/edpb/files/files/file1/edpb_guidelines_201904_dataprotection_by_design_and_by_default_v2.0_en.pdf.
• Contrôleur européen de la protection des données. "Lignes directrices du CEPD sur l'évaluation de la proportionnalité des mesures qui limitent les droits fondamentaux à la vie privée et à la protection des données à caractère personnel", 19 décembre 2019. https://edps.europa.eu/sites/edp/files/publication/19-12-19_edps_proportionality_guidelines2_en.pdf.

• Contrôleur européen de la protection des données. "Organigrammes et listes de contrôle sur la protection des données". 2020. https://doi.org/10.2804/823679.

• Commission européenne (direction générale de la recherche et de l'innovation). "Éthique et protection des données", novembre 2018. https://ec.europa.eu/research/participants/data/ref/h2020/grants_manual/hi/ethics/h2020_hi_ethics-data-protection_en.pdf.

• ALLEA. *Le code de conduite européen pour l'intégrité de la recherche*. 2e éd., 2017. https://ec.europa.eu/research/participants/data/ref/h2020/other/hi/h2020-ethics_code-of-conduct_en.pdf.

• Projet RESPECT. "Code de pratique de RESPECT pour la recherche socio-économique". Institute for Employment Studies, 2004. http://www.respectproject.org/code/respect_code.pdf

• EFAMRO et ESOMAR. "Note d'orientation pour le secteur de la recherche : Utilisation appropriée des différentes bases juridiques dans le cadre du RGPD." Juin 2017. https://www.esomar.org/uploads/public/government-affairs/position-papers/EFAMRO-ESOMAR_GDPR-Guidance-Note_Legal-Choice.pdf.

• Wilford, Sara, Malcolm Fisk, et Bernd Stahl. "Lignes directrices pour une recherche et une innovation responsables". Projet GREAT, 2016. https://www.great-project.eu/Deliverables10.

• Le Conseil européen de la protection des données a déclaré qu'il "a l'intention de publier des orientations sur les conditions "horizontales et complexes" d'applicabilité de la "présomption de compatibilité" du traitement ultérieur à des fins d'archivage dans l'intérêt public, de recherche scientifique, historique ou statistique, comme le prévoit l'article 5, paragraphe 1, point b), du RGPD".[39] Il sera utile pour les chercheurs lorsqu'il sera publié.

[39] Conseil européen de la protection des données, "Avis du Conseil (art. 70.I.b)".

4.2 Annexe 2 : Bibliographie

Groupe de travail Article 29 sur la protection des données. "Lignes directrices sur la transparence en vertu du règlement 2016/679", 29 novembre 2017. https://ec.europa.eu/newsroom/article29/items/622227.

———. " Avis 03/2013 sur la limitation de la finalité ", 2 avril 2013. https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2013/wp203_en.pdf.

Commission européenne. "La science avec et pour la société". Horizon 2020, 11 novembre 2013. https://ec.europa.eu/programmes/horizon2020/en/h2020-section/science-and-society.

———. Quelles informations doivent être fournies aux personnes dont les données sont collectées ? Texte. Principe du RGPD - Quelles informations doivent être données aux personnes dont les données sont collectées ?, 8 janvier 2018. https://ec.europa.eu/info/law/law-topic/data-protection/reform/rules-business-and-organisations/principles-gdpr/what-information-must-be-given-individuals-whose-data-collected_en.

Conseil européen de la protection des données. "Avis du Conseil (art. 70.I.b)". Avis, 23 janvier 2019. https://edpb.europa.eu/sites/edpb/files/files/file1/edpb_opinionctrq_a_final_en.pdf.

Contrôleur européen de la protection des données. Un avis préliminaire sur la protection des données et la recherche scientifique, janvier 2020. https://edps.europa.eu/sites/edp/files/publication/20-01-06_opinion_research_en.pdf.

———. "Décision du contrôleur européen de la protection des données du 16 juillet 2019 concernant les listes d'évaluation des risques avant expédition émises en vertu de l'article 39, paragraphes 4 et 5, du règlement (UE) 2018/1725", 16 juillet 2019. https://edps.europa.eu/sites/default/files/publication/19-07-16_edps_dpia_list_en.pdf.

Règlement général sur la protection des données, règlement UE 2016/679 (2016). https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A02016R0679-20160504.

"Déclaration de Rome sur la recherche et l'innovation responsables en Europe", 21 novembre 2014. https://ec.europa.eu/research/swafs/pdf/rome_declaration_RRI_final_21_November.pdf.

4.3 Annexe 3 : Processus de création du code de conduite sur la protection des données pour une recherche et une innovation responsables

Nous avons cherché à impliquer de multiples parties prenantes dans l'examen du CCDP et à obtenir le plus de commentaires possible. Le processus de consultation est décrit ci-dessous.

La première version du PDCC a été diffusée en octobre 2020 et la version finale a été consolidée en août 2021. Cinq versions ont été générées à différentes étapes du processus, intégrant les commentaires à chaque étape. Les sections suivantes résument le processus de retour d'information du PDCC, reprennent les commentaires les plus importants reçus et les mesures prises pour y répondre dans chaque cas.

La portée de chacune des étapes de rétroaction est décrite ci-dessous :

- Consultation d'experts internes (PANELFIT) : la première version du PDCC générée en octobre 2020 a été examinée par le consortium du projet PANELFIT qui comprend des experts en cyber-sécurité, gouvernance, vie privée, protection des données, entre autres.

- Consultation d'experts externes (parties prenantes) : cette consultation a été réalisée par le biais de la rencontre d'apprentissage mutuel pour les parties prenantes organisée par le projet. Lors de cet événement en ligne qui s'est tenu le 20 avril 2021, 13 personnes des organisations suivantes se sont rencontrées : ALLEA, Groupe européen d'éthique (GEE) auprès de la Commission européenne, Université de Vilnius, NEC Laboratories Europe, Tech Uni Cluj-Napoca, Museum for Naturkunde, COCIR, Université Babes-Bolyai, Centre de recherche pour la science des données et maître de conférences, École d'informatique, d'électronique et de mathématiques à l'Université de Coventry, Uni Babes Bolyai, Commission européenne, Open Science (DG RTD), Université de Tilburg, École d'informatique, d'électronique et de mathématiques à l'Université de Coventry, Université de Copenhague.

- Consultation de chercheurs externes : des chercheurs de diverses disciplines ont participé à la rencontre d'apprentissage mutuel pour les chercheurs organisée par le projet. L'événement en ligne a eu lieu le 24 juin 2021.

- Consultation publique : le CCDP a été publié sur le site Web de PANELFIT avec un formulaire disponible pour recevoir les réactions de toute personne intéressée. La participation aux commentaires a été encouragée par le biais des réseaux sociaux et des listes de diffusion. Le document a été disponible de mars à août 2021 sur : https://www.panelfit.eu/a-code-of-conduct-on-data-protection-for-responsible-research-and-innovation-ccdp/.

- Enquête auprès des chercheurs : l'enquête faisait partie du processus de clôture du retour d'informations du CCDP. Elle a été diffusée avant, pendant et après la rencontre d'apprentissage mutuel pour les chercheurs. Le retour d'informations a contribué à l'amélioration de la section sur les bonnes pratiques.