


**CONFIDENTIALITÉ, ÉTHIQUE ET  
PROTECTION DES DONNÉES**  
NOTE D'ORIENTATION DU GNUD  
CONCERNANT LES MÉGADONNÉES  
À L'APPUI DE LA RÉALISATION  
DU PROGRAMME 2030



---

**GROUPE DES  
NATIONS UNIES  
POUR LE  
DÉVELOPPEMENT**

---



DLA NOTE D'ORIENTATION SUR LA CONFIDENTIALITÉ, L'ÉTHIQUE ET LA PROTECTION DES MÉGADONNÉES POUR LA RÉALISATION DE L'AGENDA 2030 a été rédigée par le Groupe de travail du GNUM sur les données et la transparence dirigée par l'Initiative Global Pulse.

© GNUM 2017

Cette publication peut être téléchargée gratuitement à partir du site <http://undg.org>

Le Groupe des Nations Unies pour le développement (GNUM) regroupe les 32 fonds, programmes, institutions spécialisées, départements et bureaux du système des Nations unies qui jouent un rôle dans le développement. Le Bureau de la coordination des activités de développement des Nations Unies (DOCO) est le secrétariat du GNUM, et regroupe les organismes du système des Nations Unies pour le développement, afin de promouvoir le changement et l'innovation qui permettront d'assurer ensemble le développement durable.

Conception: AHOY Studios

Ce document a été approuvé par l'intermédiaire du Groupe des Nations Unies pour le Développement et s'applique à l'ensemble des organisations membres du GNUM et à ses mécanismes de fonctionnement. L'approbation de ce document s'appuie sur le consensus au sein des membres du GNUM et les dispositions du présent document s'appliquent à toutes les entités du GNUM : FAO, FIDA, OIT, OIM, UIT, HCDH, ONUSIDA, EPNU, DAES, PNUD, CEA, CEE, CEPALC, PNUE, CESAP, UNESCO, CESAO, UNICEF, ONUDI, FNUAP, ONU-HABITAT, HCR, OHRLLS, UNOPS, OSAA, SRSG/CAAC, ONU Femmes, OMT, PAM, OMS et OMM. En leur qualité d'observateurs auprès du GNUM, le BCAH, le Bureau de la VSG, le Bureau du porte-parole du Secrétaire général, le DAM, l'OMPH, le DAP, le DOMP, la FNUPI, l'UNISDR, le PBSO peuvent également appliquer les dispositions du présent document, le cas échéant.

Un grand merci à Caroline Alewaerts, anciennement avocate au barreau de Bruxelles et actuellement juriste spécialisée en protection des données personnelles et vie privée, pour son travail de supervision de la traduction de cette note d'orientation de l'anglais vers le français.



# TABLE DES MATIÈRES

<b>OBJET DE LA PRÉSENTE NOTE D'ORIENTATION</b>	<b>2</b>
<b>PRINCIPES</b>	<b>4</b>
1. UTILISATION LICITE, LÉGITIME ET LOYALE	4
2. SPECIFICATION DE LA FINALITE, LIMITATION DE L'UTILISATION ET COMPATIBILITÉ AVEC LA FINALITE	4
3. ATTÉNUATION DES RISQUES ET ÉVALUATION DES RISQUES, DES PRÉJUDICES ET DES AVANTAGES	4
4. DONNÉES SENSIBLES ET CONTEXTES SENSIBLES	5
5. SÉCURITÉ DES DONNÉES	5
6. CONSERVATION ET MINIMISATION DES DONNÉES	6
7. QUALITÉ DES DONNÉES	6
8. DONNÉES OUVERTES, TRANSPARENCE ET RESPONSABILITÉ	7
9. VÉRIFICATIONS PRÉALABLES CONCERNANT LES COLLABORATEURS TIERS	7
<b>DÉFINITIONS ET NOTES</b>	<b>8</b>
<b>NOTE ADDITIVE A</b>	<b>12</b>
<b>COMMENT L'ANALYSE DES DONNÉES PEUT AIDER À PROMOUVOIR LES ODD</b>	<b>12</b>
<b>BIBLIOGRAPHIE</b>	<b>14</b>



# OBJET DE LA PRÉSENTE NOTE D'ORIENTATION

Ce document présente des orientations générales sur la confidentialité, l'éthique et la protection des données pour le Groupe des Nations Unies pour le développement (GNUD). Elles concernent plus spécifiquement l'utilisation des mégadonnées (big data) collectées en temps réel par des organismes privés dans le cadre de leurs prestations de services et de leurs produits<sup>1</sup>, et qui sont transmises aux membres du GNUD à des fins de renforcement de la mise en œuvre opérationnelle de leurs programmes en vue de la réalisation du Programme 2030<sup>2</sup>. Cette note d'orientation vise à :

- Établir des principes communs applicables à l'ensemble du GNUD pour régir l'utilisation opérationnelle des mégadonnées à l'appui de la réalisation des objectifs de développement durable (ODD) ;
- Servir d'outil de gestion des risques tenant compte des droits humains fondamentaux ; et
- Définir des principes pour l'obtention, la conservation, l'utilisation et le contrôle de la qualité des données fournies par des acteurs privés.

Il est établi que la révolution des données constitue un moteur des objectifs de développement durable, non seulement pour suivre l'avancement des travaux, mais aussi pour mobiliser toutes les parties prenantes à tous les niveaux dans la promotion de politiques et de programmes fondés sur des éléments factuels et atteindre les plus vulnérables<sup>3</sup>.

1 Cette note d'orientation porte essentiellement sur l'utilisation des mégadonnées collectées par des parties hors ONU. Un bon nombre des principes directeurs qu'elle énonce peuvent cependant s'appliquer dans les cas où des membres du GNUD collectent des mégadonnées aux fins de l'accomplissement de leur mandat, par exemple sous la forme de photographies ou de vidéos recueillies par des véhicules aériens sans pilote.

2 La présente note d'orientation vient appuyer la mise en œuvre des recommandations de l'Examen quadriennal complet des activités opérationnelles de développement du système des Nations Unies (A/C.2/71/L.37), en particulier l'appel lancé aux fonds, programmes et institutions spécialisées des Nations Unies de renforcer leur soutien pour « recueillir, analyser et accroître sensiblement la disponibilité en temps opportun de données ventilées de haute qualité et fiables ... en utilisant à cet effet les capacités nationales dans toute la mesure possible dans le cadre des activités opérationnelles de développement des Nations Unies ».

3 On retrouvera à la Note additive A des exemples de la façon dont des mégadonnées pourraient être utilisées pour promouvoir les Objectifs de développement durable.

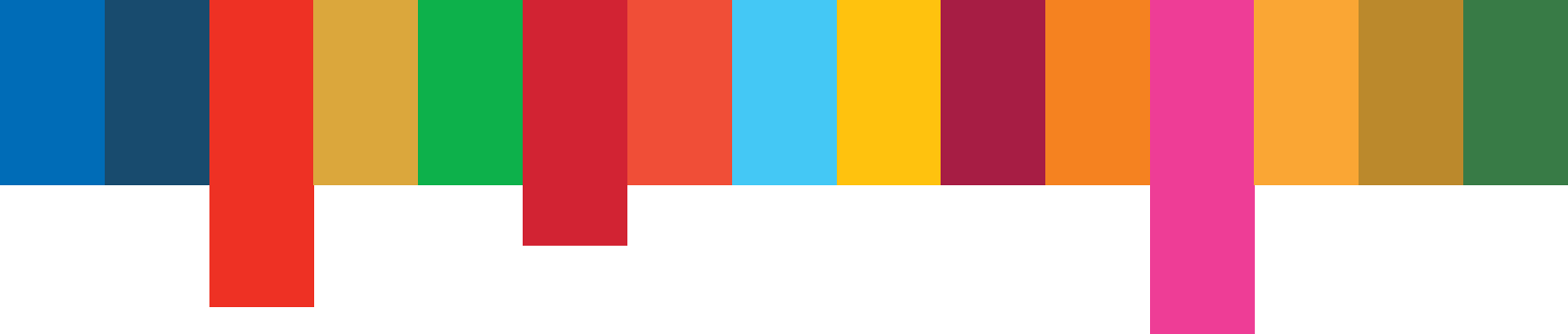
Le Programme 2030 indique qu'« il faudra disposer en temps utile de données ventilées de qualité, qui soient facilement accessibles et fiables, pour mesurer les progrès accomplis (ODD) et garantir qu'il n'y aura pas de laissés-pour-compte du développement durable. Ces données sont essentielles pour la prise de décisions ».<sup>4</sup>

Cela dit, des inquiétudes légitimes subsistent quant aux risques associés à la manipulation et au traitement des mégadonnées, en particulier au regard du contexte réglementaire actuel fragmenté et en l'absence d'un ensemble commun de principes régissant la confidentialité, l'éthique et la protection des données. Ces préoccupations continuent de compliquer les efforts déployés pour mettre en place des mécanismes standardisés et modulables de gestion des risques et d'accès aux données. Une approche coordonnée est nécessaire pour assurer l'émergence de cadres garantissant une utilisation sûre et responsable des mégadonnées à l'appui de la réalisation du Programme 2030.

Les orientations fournies dans le présent document tiennent compte et s'inspirent des Principes directeurs des Nations Unies pour la réglementation des fichiers personnels informatisés, adoptés par l'Assemblée générale des Nations Unies dans la résolution 45/95. Elles prennent également en compte aussi bien les instruments internationaux existants que les réglementations, les règles et les politiques pertinentes des organismes membres du GNUD concernant la confidentialité et la protection des données.

4 Pour plus de détails, voir Transformer notre monde : le Programme de développement durable à l'horizon 2030 (A/RES/70/1, p. 13), disponible à l'adresse : <https://sustainable-development.un.org/post2015/transformingourworld>.

5 Le droit à la vie privée est consacré par la Déclaration universelle des droits de l'homme, en son article 12 (résolution 217 A (III) de l'Assemblée générale des Nations Unies, Paris, France, 10 décembre 1948) ; le Pacte international relatif aux droits civils et politiques, en son article 17 (résolution 2200 A (XXI) de l'Assemblée générale, New York, 19 décembre 1966, série des traités de l'ONU, vol. 999, n° 14668, p. 171 et vol. 1057, p. 4019), la Convention relative aux droits de l'enfant (article 16), la Convention internationale sur la protection des droits de tous les travailleurs migrants et membres de leur famille (article 14) ; la Convention européenne des droits de l'homme (article 8) ; la Convention américaine relative aux droits de l'homme (article 11).



Cette note d'orientation se fonde sur des normes qui ont résisté à l'épreuve du temps, ce qui témoigne de la solidité des valeurs fondamentales qu'elles incarnent.

Cette note d'orientation est destinée à aider les membres et les partenaires du GNUD à développer une collaboration efficace et cohérente en matière de données.

Réaffirmant que le droit à la vie privée est un droit de l'homme fondamental<sup>5</sup> et reconnaissant la valeur sociale des données, y compris la valeur des indicateurs ventilés des ODD<sup>6</sup> en ce qui concerne la mise en œuvre du Programme 2030, ce document vise à établir un cadre général harmonisé pour des méthodes de traitement des données qui appellent à rendre des comptes et se veulent suffisamment transparentes et responsables à travers l'ensemble du GNUD et pour les partenaires.

Cette note d'orientation n'est pas un document juridique. Elle se contente d'établir une base minimale d'autoréglementation, et peut donc être développée et complétée par les organismes d'exécution.

Reconnaissant les risques et préjudices potentiels ainsi que les avantages qui peuvent découler de l'utilisation des mégadonnées<sup>7</sup>, ce document va au-delà de la vie privée des personnes et tient compte des effets possibles sur un ou plusieurs groupes d'individus. En outre, il prend en compte les normes de conduite morale et éthique, et reconnaît l'importance du contexte lorsque des mégadonnées sont utilisées.

6 L'Objectif de développement durable n° 17 consiste à « renforcer les moyens de mettre en œuvre le partenariat mondial pour le développement durable et le revitaliser ». La cible 17.18 indique la nécessité de disposer de données ventilées par niveau de revenu, sexe, âge, race, appartenance ethnique, statut migratoire, handicap, emplacement géographique et selon d'autres caractéristiques propres à chaque pays (A/70/L.1).

7 Pour de plus amples informations, voir « Report of the Special Rapporteur on the right to privacy », Annex II. A more in-depth look at Open Data and Big Data (A/HRC/31/64, p. 24), Joseph A. Cannataci (annexe II consacrée à un examen plus approfondi des données ouvertes et des mégadonnées du rapport du Rapporteur spécial Joseph A. Cannataci sur le droit à la vie privée).

Il est conseillé d'appliquer les recommandations de la présente note d'orientation à travers des lignes directrices opérationnelles plus détaillées qui prennent en compte l'accomplissement des mandats des organismes membres du GNUD ainsi que l'application de leurs règlements, règles et politiques existants concernant la confidentialité, la protection, l'éthique et la sécurité des données. Il est en outre recommandé de consulter, le cas échéant, des experts désignés en droit, éthique, protection de la vie privée, et en sécurité au sujet de la mise en œuvre et du respect des recommandations de cette note. Les organismes d'exécution sont encouragés à mettre en place un mécanisme de suivi de l'observance et de l'application des recommandations de cette note.

Comme les technologies et les données ne cessent d'enregistrer des progrès, le paysage international relatif à la confidentialité et à la protection des données (notamment grâce au travail de l'ONU en ce domaine) peut également évoluer. En conséquence, cette note se veut un document vivant qui peut aussi évoluer au fil du temps.

**Le GNUD tient à exprimer sa reconnaissance à UN Global Pulse pour l'élaboration de cette note d'orientation et remercie le Groupe consultatif sur la confidentialité des données de Global Pulse (Global Pulse Privacy Advisory Group) ainsi que d'autres experts publics et privés pour leurs précieuses contributions. Toute question, tout commentaire ou toute recommandation concernant cette note d'orientation sont à adresser à [kit.doco@undg.org](mailto:kit.doco@undg.org).**

# PRINCIPES

## 1. UTILISATION LICITE, LÉGITIME ET LOYALE

L'accès aux données, leur analyse et toute autre utilisation qui peut en être faite doivent être conformes à la Charte des Nations Unies et viser à promouvoir la réalisation des objectifs de développement durable.

Que ce soit directement ou par le biais d'un contrat passé avec un fournisseur de données tiers, les données devraient être obtenues, collectées, analysées ou utilisées de toute autre manière par des moyens licites, légitimes et loyaux. Plus précisément, l'accès aux données (ou leur collecte, le cas échéant), leur analyse et toute autre utilisation qui leur est réservée devraient être conformes aux lois applicables, en ce compris les lois sur la confidentialité et la protection des données, ainsi qu'aux normes de confidentialité et de conduite morale et éthique les plus rigoureuses.

L'accès aux données, leur analyse et toute autre utilisation qui leur est réservée devraient toujours tenir compte des intérêts légitimes des personnes dont les données sont utilisées. Plus précisément, pour garantir une utilisation loyale des données, ces dernières ne devraient pas être utilisées d'une manière qui porte atteinte aux droits de l'homme ou de toute autre manière susceptible d'avoir des effets injustifiés ou néfastes sur un ou plusieurs individus ou groupes d'individus. Il est recommandé de toujours évaluer la légitimité et la loyauté de l'utilisation des données en prenant en compte les risques, les préjudices et les avantages examinés à la section 6.

Les mégadonnées contiennent souvent des données à caractère personnel et des données sensibles. L'utilisation des données à caractère personnel devrait reposer sur l'une ou plusieurs des bases légitimes et loyales suivantes, sous réserve de l'application des règlements, règles et politiques des organismes membres du GNUD (y compris les politiques relatives à la confidentialité et à la protection des données) : i) le consentement adéquat de l'individu dont les données sont utilisées, ii) le respect de la loi, iii) la poursuite de missions institutionnelles internationales, iv) d'autres nécessités légitimes de protection de l'intérêt vital ou supérieur d'un ou plusieurs individus ou groupes d'individus.

## 2. SPECIFICATION DE LA FINALITE, LIMITATION DE L'UTILISATION ET COMPATIBILITÉ AVEC LA FINALITE

Toute utilisation de données doit être compatible ou autrement pertinente et non excessive par rapport aux finalités pour lesquelles les données ont été obtenues. La finalité du traitement des données ne peut être changée à moins que ce ne soit sur une base légitime, comme indiqué à la section 1. La finalité devrait être légitime et formulée d'une manière aussi concise et précise que possible. Toute demande ou proposition d'accès à des données devrait correspondre à une finalité précise.

Tout changement de finalité incompatible avec la finalité pour laquelle des données ont été collectées doit pouvoir reposer sur une base légitime et loyale. Pour autant, le simple changement de finalité ne rend pas nécessairement la nouvelle finalité incompatible. Pour déterminer la compatibilité de la finalité, les critères suivants, par exemple, pourraient être pris en considération : la manière dont le détournement de la finalité initiale pourrait affecter un ou plusieurs individus ou groupes d'individus ; le type de données utilisées (par exemple, données publiques, sensibles ou non sensibles) ; les mesures prises pour préserver l'identité des individus dont les données sont utilisées (par exemple, la pseudonymisation, le masquage, le cryptage).

La finalité de l'accès aux données (ou de leur collecte, le cas échéant) devrait être indiquée au plus tard lors de l'accès aux données (ou de leur collecte, le cas échéant).

## 3. ATTÉNUATION DES RISQUES ET ÉVALUATION DES RISQUES, DES PRÉJUDICES ET DES AVANTAGES


Une évaluation des risques, des préjudices et des avantages qui tient compte de la protection, de la confidentialité et de l'éthique des données devrait être effectuée avant toute nouvelle utilisation de données ou tout changement substantiel de leur utilisation (notamment la finalité). Des mesures adéquates d'atténuation des risques devraient être prises. Les individus et groupes d'individus ne devraient pas être exposés à un préjudice ou à un traitement indigne ou discriminatoire par suite de l'utilisation de données par les organismes membres du GNUD.

Toute évaluation des risques, des préjudices et des avantages devrait prendre en considération le contexte de l'utilisation des données, et notamment les facteurs sociaux, géographiques, politiques et religieux. Une telle évaluation devrait tenir compte des préjudices physiques, émotionnels ou économiques éventuels, ainsi que de tout préjudice qui pourrait être causé par suite d'une atteinte aux droits de l'individu ou des individus concernés.

Toute évaluation des risques, des préjudices et des avantages devrait prendre en compte l'incidence de l'utilisation des données sur un ou plusieurs individus et/ou groupes d'individus, qu'ils soient légalement visibles ou non et qu'ils soient connus ou inconnus au moment de l'utilisation des données.

Une évaluation des préjudices devrait prendre en considération des facteurs clés tels que : i) la probabilité de la survenance de préjudices, ii) l'ampleur potentielle de ces préjudices et iii) leur gravité potentielle.

Qui plus est, l'évaluation devrait tenir compte de la maîtrise du numérique tant par les utilisateurs potentiels des données que par les personnes dont les données sont utilisées.



Dans la mesure du possible, l'évaluation devrait être effectuée par une équipe diversifiée d'experts (experts en droit, en éthique et en sécurité, ainsi qu'experts dans le domaine concerné) et, lorsque cela est raisonnablement possible, un représentant du ou des groupes d'individus qui pourraient éventuellement être affectés.

Le risque de préjudice est beaucoup plus élevé lorsque des données sensibles sont concernées, et des mesures de protection plus strictes devraient être prises lorsque ces données constituent explicitement des données à caractère personnel ou lorsqu'elles sont raisonnablement susceptibles de permettre l'identification d'un ou plusieurs individus ou groupes d'individus.

Les décisions concernant l'utilisation de données sensibles devraient, si possible, être prises à la suite d'une consultation des groupes concernés (ou de leur représentant) afin d'atténuer les risques associés.

En outre, il est important de tenir compte des risques liés aux violations de données et à la vulnérabilité de certains systèmes de sécurité des données, comme indiqué dans la section 3.

L'utilisation des données devrait être fondée sur le principe de proportionnalité. Plus particulièrement, les risques et préjudices potentiels ne devraient pas être excessifs par rapport aux effets positifs (avantages) de l'utilisation des données. Par ailleurs, il est recommandé, dans la mesure du possible, d'évaluer l'effet des données sur les droits individuels conjugués les uns avec les autres plutôt que de considérer ces droits les uns en opposition aux autres.

L'évaluation des risques, des préjudices et des avantages peut constituer un outil permettant d'aider à déterminer si l'utilisation des données est légitime, appropriée et loyale.

## 4. DONNÉES SENSIBLES ET CONTEXTES SENSIBLES

---

Des normes plus strictes de protection des données devraient être appliquées dans le cadre de l'obtention, l'accès, la collecte, l'analyse ou autre utilisation de données concernant les populations vulnérables et les personnes à risque, les enfants et les jeunes, ou toutes autres données sensibles.

Il est important d'envisager la possibilité que le contexte puisse transformer des données non sensibles en données sensibles. Le contexte dans lequel les données sont utilisées (par exemple, les circonstances culturelles, géographiques, religieuses, politiques, etc.) peut avoir une incidence sur l'effet de l'analyse de ces données sur un ou plusieurs individus ou groupes d'individus, même si ces données ne revêtent pas un caractère explicitement personnel ou sensible

## 5. SÉCURITÉ DES DONNÉES

---

La sécurité des données est essentielle pour garantir leur confidentialité et leur protection. Tenant compte des technologies disponibles et du coût de la mise en œuvre, des mesures et des procédures techniques et organisationnelles rigoureuses de protection (y compris un suivi efficace de l'accès aux données et des procédures de notification des violations des données) devraient être mises en place pour garantir une gestion adéquate des données tout au long de leur cycle de vie et empêcher toute utilisation ou divulgation non autorisée ou toute violation de données à caractère personnel.


Il est vivement recommandé d'intégrer, de façon proactive, les principes fondamentaux du respect de la vie privée dès la conception (Privacy by Design) et de recourir à des technologies renforçant la protection de la vie privée à tous les stades du cycle de vie des données pour garantir une protection efficace des données, ceci afin de prévenir les risques de violation de la vie privée et les préjudices qui découleraient de leur matérialisation.

Les données à caractère personnel devraient être anonymisées, le cas échéant, au moyen de méthodes telles que l'agrégation, la pseudonymisation ou le masquage, afin de réduire les risques potentiels de violation de la vie privée, et en tenant compte du risque de préjudice associé à l'utilisation et à la non-utilisation des données. Le cas échéant, les organismes membres du GNUD devraient envisager de travailler avec des données qui auront été anonymisées par des fournisseurs de données tiers avant même que celles-ci ne soient communiquées aux organismes membres du GNUD.

Les données sensibles et à caractère personnel devraient être cryptées lorsqu'elles sont transférées vers ou depuis tout serveur connecté à un réseau. Aucune ré-identification de données anonymisées ne devrait être opérée sciemment et à dessein, à moins qu'il n'y ait une base légitime, licite et loyale pour ce faire, comme indiqué dans la section 1. Pour limiter toute possibilité d'une ré-identification, il est recommandé d'éviter que les données anonymisées ne soient analysées ni utilisées de quelque manière par les mêmes personnes qui ont procédé initialement à leur anonymisation.

Il est important de veiller à ce que les mesures prises pour protéger la vie privée et assurer la sécurité des données ne compromettent pas de manière disproportionnée l'utilité des données par rapport à la finalité visée.

Ces mesures devraient être appliquées de manière à optimiser l'impact positif attendu de l'utilisation des données et à atteindre les finalités dans lesquelles elles ont été obtenues.



L'accès aux données devrait être limité au personnel autorisé, en application du principe du « besoin d'en connaître ». Le personnel concerné devrait suivre régulièrement et systématiquement des formations sur le respect de la confidentialité et de la sécurité des données. Avant toute utilisation de données, les vulnérabilités du système de sécurité (concernant notamment le stockage des données, les moyens de transfert, etc.) devraient être évaluées.

Les mesures de sécurisation des données devraient être évaluées à la lumière des risques, des préjudices et des avantages découlant de leur utilisation, y compris suivant les modalités énoncées dans la section 3.

Lors de l'examen des risques associés à la vulnérabilité des systèmes de sécurité des données, il est important de prendre en considération des facteurs tels que la fuite ou la violation non autorisée des données, qu'elle soit intentionnelle ou non intentionnelle, : i) du fait de membres du personnel autorisés, ii) du fait de tiers connus qui ont demandé l'accès ou pourraient l'obtenir, ou qui pourraient chercher à obtenir l'accès pour détourner des données et des informations, iii) du fait de tiers inconnus (par exemple, à la suite de la publication d'ensembles de données ou des résultats d'une analyse).

Il conviendrait de faire particulièrement attention à l'utilisation de services de cloud, surtout en ce qui concerne le dispositif de sécurité des données et les emplacements physiques où les données sont stockées. L'utilisation d'un système de stockage hors cloud devrait être envisagée pour les données sensibles. Lorsqu'il est fait recours à des fournisseurs tiers de services de stockage de données sur le cloud, les risques et préjudices potentiels associés à l'utilisation de ce mode de stockage, tel que présenté de manière détaillée dans la section 3, devraient être pris en compte.

## 6. CONSERVATION ET MINIMISATION DES DONNÉES

---

L'accès aux données, leur analyse et toute autre utilisation qui leur est réservée devraient être limités au minimum nécessaire pour atteindre la finalité pour laquelle les données sont traitées, comme indiqué à la section 2.

8 Les orientations concernant la conservation des données s'appliquent principalement aux cas où le GNUD est en possession d'un ensemble de données par opposition aux cas où l'accès lui a été accordé pour un ensemble de données qui reste en la possession d'un tiers.

9 Il est important de souligner que les mégadonnées générées par l'utilisation des médias sociaux, des téléphones mobiles, des cartes de crédit, etc. appartiennent généralement soit à l'auteur initial soit au fournisseur de services numériques (par exemple, une plateforme de médias sociaux, une société de téléphonie mobile ou une banque).

La quantité de données, y compris leur niveau de détail, devrait être limitée au minimum nécessaire. L'utilisation des données devrait être contrôlée pour s'assurer qu'elle n'excède pas les besoins légitimes de leur utilisation.

Toute conservation de données<sup>8</sup> devrait reposer sur une base légitime et loyale, y compris au-delà des finalités pour lesquelles l'accès aux données a été initialement accordé, comme précisé à la section 1, afin de s'assurer qu'aucun ensemble de données supplémentaire ou de données stockées « juste au cas où » ne soit conservé. Toute conservation de données devrait également être envisagée en tenant compte des risques, des préjudices et des avantages potentiels examinés à la section 3. Les données devraient être supprimées définitivement au terme de la période requise pour atteindre la finalité pour laquelle les données sont traitées, à moins que la prolongation de leur conservation ne soit justifiée, comme indiqué ci-dessus dans la présente section. Toute suppression de données devrait être effectuée de manière appropriée en tenant compte de leur caractère plus ou moins sensible et des moyens technologiques disponibles.

## 7. QUALITÉ DES DONNÉES

---


Toutes les activités liées aux données devraient être conçues, réalisées, rapportées et consignées avec un niveau de qualité et de transparence adéquat. Plus précisément, dans la mesure du possible, les données devraient être validées du point de vue de leur exactitude, leur pertinence, leur suffisance, leur intégrité, leur exhaustivité, leur facilité d'utilisation, leur validité et leur cohérence, et devraient être tenues à jour.

La qualité des données devrait être soigneusement étudiée compte tenu des risques que l'utilisation de données de qualité insuffisante en appui à la prise de décisions peut engendrer pour un ou plusieurs individus ou groupes d'individus.

La qualité des données doit, dans la mesure du possible, être analysée pour déterminer l'existence de données biaisées afin d'éviter tout effet néfaste, y compris la possibilité de donner lieu à une discrimination illégale et arbitraire.

10 En général, il sera possible d'obtenir le consentement si l'organisme est l'entité qui a collecté les données à l'origine. Toutefois, dans les cas où des données sont obtenues auprès d'un fournisseur de données tiers, il est recommandé, lors du processus de vérification préalable, de vérifier si un fournisseur de données tiers a obtenu le consentement adéquat (par exemple, directement ou indirectement à travers les conditions d'utilisation en ligne) ou s'est fondé sur une autre base légitime pour collecter et partager les données.





Le traitement automatique des données, notamment par des algorithmes, sans intervention humaine ni expertise dans le domaine, devrait être évité lorsque les données sont analysées pour la prise de décisions susceptibles d'avoir un impact sur un ou plusieurs individus ou groupes d'individus afin d'éviter les préjudices éventuels qui résulteraient de la mauvaise qualité des données.

Une évaluation périodique de la qualité des données est recommandée pendant le cycle de vie de ces dernières. Il est par ailleurs important de mettre en place un système interne de mise à jour régulière des données et de suppression des données obsolètes, le cas échéant, et lorsque cela est possible sur le plan pratique.

## 8. DONNÉES OUVERTES, TRANSPARENCE ET RESPONSABILITÉ

---

Des mécanismes appropriés de gouvernance et de responsabilisation devraient être mis en place pour contrôler le respect des dispositions légales pertinentes, y compris celles concernant la protection de la vie privée ainsi que les normes de confidentialité et de conduite morale et éthique les plus strictes en matière d'utilisation des données (dont la présente note d'orientation fait partie).

La transparence est un élément essentiel de l'éthique de responsabilité. Il est généralement recommandé de faire preuve de transparence dans l'utilisation des données (par exemple, la publication d'ensembles de données ou la publication par une organisation de ses pratiques en matière d'utilisation de données ou de l'utilisation d'algorithmes) lorsque les avantages de la transparence sont plus importants que les risques et les préjudices éventuels.

À l'exception des cas où il existe une raison légitime pour ne pas le faire, l'existence, la nature, la durée de conservation prévue et la finalité de l'utilisation des données, ainsi que les algorithmes utilisés pour les traiter devraient au minimum être rendus publics et décrits dans un langage clair et non technique, adapté au grand public.

Les données ouvertes (open data) constituent un moteur important de l'innovation, de la transparence et de l'éthique de responsabilité. Par conséquent, chaque fois que cela est possible, les données devraient être ouvertes, à moins que les risques liés au fait de les rendre ouvertes ne l'emportent sur les avantages, ou qu'il y ait d'autres raisons légitimes de ne pas le faire. La divulgation d'informations à caractère personnel, même si celles-ci proviennent de données appartenant au domaine public, doit être évitée ou évaluée de manière prudente pour déterminer les risques et préjudices potentiels décrits à la section 3.

Une évaluation des risques, des préjudices et des avantages (mentionnée à la section 3) devrait constituer l'un des principaux mécanismes de

responsabilisation à l'égard de chaque utilisation de données et devrait aider à déterminer les autres mécanismes de gouvernance qui pourraient être nécessaires pour contrôler le respect des règles et principes. Plus particulièrement, rendre les données ouvertes ou faire preuve de transparence quant aux utilisations qui en sont faites devrait être considéré comme une étape distincte du cycle de vie des données, et il est par conséquent recommandé de procéder à une évaluation, mentionnée à la section 3, distincte pour prendre en compte les risques, les préjudices et les avantages liés à cette étape. L'évaluation devrait aider à déterminer le degré d'ouverture et de transparence.

## 9. VÉRIFICATIONS PRÉALABLES CONCERNANT LES COLLABORATEURS TIERS

---

Les collaborateurs tiers qui participent à l'utilisation des données devraient agir dans le respect des lois applicables, y compris les lois relatives à la protection de la vie privée, ainsi que des normes les plus strictes en matière de confidentialité et de conduite morale et éthique. Leurs agissements devraient être conformes au mandat global des Nations Unies ainsi qu'aux règlements, règles et politiques de l'ONU. En outre, les agissements des collaborateurs tiers devraient être conformes aux recommandations de la présente note d'orientation, y compris celle qui préconise d'avoir une base légitime et loyale pour partager des données avec les organismes membres du GNUD<sup>9</sup>.

Il est recommandé qu'un processus de vérification préalable soit mené pour évaluer les pratiques en matière de données des éventuels collaborateurs tiers<sup>10</sup>.

Des accords juridiquement contraignants décrivant les paramètres d'accès aux données et de leur traitement (par exemple, la sécurité, les formats, la transmission, la fusion, l'analyse, la validation, le stockage, la conservation, la réutilisation, l'exploitation sous licence des données, etc.) devraient être conclus pour garantir un accès fiable et sécurisé aux données fournies par des collaborateurs tiers.

# DÉFINITIONS ET NOTES



## AGRÉGATION DE DONNÉES

Aux fins du présent document, l'agrégation de données désigne un processus par lequel des ensembles de données au niveau individuel sont combinés dans un format tel qu'il n'est pas possible de remonter ni de relier ces données à un individu. Généralement, les données agrégées sont utilisées à des fins analytiques ou statistiques pour présenter une synthèse ou obtenir des résultats/chiffres moyens concernant l'âge, le sexe, les préférences communautaires, etc.

En outre, la Section des archives et de des records de l'Organisation des Nations Unies, dans son glossaire de termes concernant la conservation des records (Glossary of Recordkeeping Terms) définit les « records agrégés » comme des « records accumulés ou acquis qui sont organisés en groupes ou en séries ». L'Organisation internationale des migrations (OIM), dans son manuel sur la protection des données définit également les « données agrégées » comme des informations, généralement des synthèses statistiques, pouvant être compilées à partir de données à caractère personnel, mais qui sont regroupées de manière à empêcher l'identification de cas individuels.



## CONSENTEMENT ADÉQUAT

Le consentement est dit adéquat lorsqu'il est libre, explicite, éclairé et donné par écrit. Un consentement adéquat devrait être obtenu avant de collecter les données ou lorsque la finalité de la réutilisation des données sort du cadre de la finalité pour laquelle le consentement a été obtenu à l'origine.

Pour s'assurer que le consentement est éclairé, il est recommandé d'inclure dans la demande de consentement autant d'informations que possible concernant la finalité de l'utilisation des données (par exemple, les risques, les préjudices et les effets positifs et négatifs éventuels). Il est important de relever que, dans de nombreux cas, le consentement peut ne pas être éclairé de manière adéquate. Il est donc important d'envisager une évaluation la proportionnalité des risques, des préjudices et des avantages liés à l'utilisation des données, même si le consentement a été obtenu.

Le consentement devrait être obtenu avant que les données ne soient collectées ou autrement utilisées, et les individus devraient avoir la possibilité de retirer leur consentement ou de faire objection à l'utilisation de leurs données. Il est recommandé de vérifier si un fournisseur de données tiers a obtenu le consentement adéquat (par exemple, directement ou indirectement à travers les conditions d'utilisation en ligne) ou dispose d'une autre base légitime pour collecter et partager les données.

Bien qu'il puisse y avoir une possibilité d'obtenir un consentement au moment de la collecte des données, la réutilisation des données présente souvent des difficultés lorsqu'il s'agit d'obtenir le consentement (par exemple, dans les situations de crise où le contact avec les personnes concernées peut être perdu). Dans les situations où il n'est pas possible ou raisonnablement pratique d'obtenir un consentement éclairé, en dernier recours, des experts en données peuvent toujours envisager d'utiliser ces données

dans l'intérêt vital ou supérieur d'un ou plusieurs individus ou groupes d'individus (par exemple, sauver leur vie, réunir des familles, etc.). Dans ces cas, toute décision d'utiliser les données sans le consentement doit être fondée sur une évaluation détaillée supplémentaire des risques, des préjudices et des avantages pour justifier une telle démarche, qui doit être jugée loyale, licite, légitime et conforme au principe de proportionnalité (par exemple, les risques et préjudices potentiels ne devraient pas être excessifs par rapport aux avantages attendus de l'utilisation des données).



## MÉGADONNÉES

Il existe de nombreuses définitions du terme « mégadonnées » (big data). UN Global Pulse, dans son rapport intitulé *Big data for development: Challenges and opportunities*, adopte une approche traditionnelle, définissant les mégadonnées comme « un volume massif de données à la fois structurées et non structurées d'une telle quantité qu'il est difficile de les traiter à l'aide des techniques de bases de données et logicielles traditionnelles. Les caractéristiques qui distinguent globalement les mégadonnées sont parfois appelées les « 3 V » : plus de volume, plus de variété et plus de vitesse ». Le rapport fournit des exemples de données de ce type, notamment les données provenant des capteurs utilisés pour recueillir des informations sur le climat, les publications sur les sites de réseaux sociaux, les images et vidéos numériques publiées en ligne, les dossiers de transaction d'achats en ligne et les signaux GPS de téléphones cellulaires.

Il existe de nombreux types de mégadonnées présentant une utilité potentielle pour le développement. Les recommandations de ce document s'appliquent spécifiquement aux données collectées en temps réel par des entités du secteur privé pouvant être utilisées par le GNUD pour observer les comportements humains, et influencer ainsi sur le processus de prise de décisions concernant un ou plusieurs individus ou groupes d'individus. Généralement, ces données sont la propriété d'un auteur originaire (par exemple, un utilisateur des médias sociaux) ou d'un fournisseur de services numériques (par exemple, une plateforme de médias sociaux, une société de téléphonie mobile, une banque, etc.).

Dans sa recommandation sur les « Exigences et capacités pour les mégadonnées basées sur l'informatique en nuage », l'Union internationale des télécommunications (UIT) définit les mégadonnées

comme « un paradigme qui permet la collecte, le stockage, la gestion, l'analyse et la visualisation, éventuellement dans les contraintes d'exploitation en temps réel, d'ensemble de données de grande quantité présentant des caractéristiques hétérogènes ».



## DÉPERSONNALISATION (ANONYMISATION) DES DONNÉES

Aux fins du présent document, la dépersonnalisation s'entend d'une procédure qui consiste à utiliser tous les moyens raisonnables pour convertir des données à caractère personnel en données anonymes, de sorte qu'il ne soit pas possible de remonter ou de relier ces données à un ou plusieurs individus ou groupes d'individus. Il existe de nombreuses méthodes de dépersonnalisation des données, comme l'agrégation, le masquage, la pseudonymisation et le k-anonymat.

Des données dépersonnalisées peuvent être dépouillées de tous leurs identifiants personnels tels que le nom, la date de naissance, la situation géographique exacte, etc.). Cependant, comme le document intitulé *UN Global Pulse Data Innovation Risk Assessment Tool Guidance* (orientations de UN Global Pulse relatives à l'outil d'évaluation des risques liés à l'innovation en matière de données) l'indique, ces données, bien que n'identifiant ni ne distinguant pas directement ou explicitement un ou plusieurs individus ou groupes d'individus, peuvent toujours être reliées à un ou plusieurs individus ou groupes d'individus en utilisant les moyens technologiques, les compétences et les intentions adéquats, et peuvent ainsi requérir le même niveau de protection que les données explicitement à caractère personnel.



## MAÎTRISE DU NUMÉRIQUE

Aux fins du présent document, la maîtrise du numérique désigne la façon dont les personnes comprennent les données avec lesquelles elles travaillent ou qu'elles partagent, y compris la mesure dans laquelle elles ont conscience des impacts positifs et négatifs de l'utilisation et du partage des données. La maîtrise du numérique concerne aussi bien les acteurs qui utilisent les données que ceux dont les données sont utilisées.



## CRYPTAGE

Dans le glossaire de la Section des archives et des records de l'Organisation des Nations Unies, le cryptage (ou « chiffrement ») est défini comme une « procédure de sécurité qui traduit des données informatiques de texte brut en un code chiffré au moyen d'un code ou d'un système cryptographique afin de les rendre incompréhensibles sans l'aide du code ou du système cryptographique initial ».



## GROUPE OU GROUPES D'INDIVIDUS

Aux fins du présent document, la référence à un ou plusieurs groupes d'individus englobe également un groupe ou plusieurs groupes « légaux » invisibles (connus ou inconnus) d'individus, tel qu'adapté de l'approche à l'égard des données fondée sur les droits de l'homme du Haut-Commissariat des Nations Unies aux droits de l'homme (HCDH).



## MASQUAGE

Aux fins du présent document, le masquage désigne une technique de dépersonnalisation par laquelle des informations à caractère personnel de base collectées à travers les médias sociaux, tels que les commentaires, les photos et les vidéos, sont modifiées de sorte qu'il ne soit pas possible de les remonter ni de les relier à un ou plusieurs individus ou groupes d'individus.



## DONNÉES À CARACTÈRE PERSONNEL

Aux fins du présent document, les données à caractère personnel s'entendent des données, présentées sous quelque forme ou support, se rapportant à un individu identifié ou identifiable, directement ou indirectement, par des moyens raisonnablement susceptibles d'être utilisés, y compris lorsque l'individu peut être identifié en reliant les données à d'autres informations raisonnablement disponibles. Les données à caractère personnel sont définies par de nombreux instruments régionaux et nationaux et peuvent également être appelées informations personnelles ou renseignements personnels.

Les données à caractère personnel peuvent être rendues privées par leur propriétaire en en restreignant l'accès ou rendues publiques par lui (par exemple, en les partageant publiquement sur les réseaux sociaux). Bien que le partage (et le partage excessif) de renseignements à caractère personnel sur sa propre personne et sur les autres sur les réseaux sociaux soit devenu courant, ces informations accessibles au public demeurent personnelles et peuvent présenter des risques pour les individus représentés dans les données.



## RESPECT DE LA VIE PRIVÉE

Un rapport du Rapporteur spécial au Conseil des droits de l'homme (A/HRC/23/40) définit le respect de la vie privée comme « la présomption selon laquelle les individus devraient disposer d'un domaine de développement autonome, d'échanges et de liberté, une « sphère privée » avec ou sans interaction avec autrui, libre de toute intervention de l'État et d'ingérence excessive non sollicitée d'autres individus ». Bien que la majorité de la littérature et des textes législatifs se focalise sur « le droit à la vie privée », dans un autre rapport de ce type (A/HRC/31/64), il a été noté qu'il n'existe actuellement aucune définition du respect de la vie privée qui soit acceptée à l'échelle internationale.



## RESPECT DE LA VIE PRIVÉE DÈS LA CONCEPTION<sup>11</sup>

Le respect de la vie privée dès la conception (Privacy by Design) consiste en une démarche qui promeut la prise en compte du respect de vie privée dans la conception et la fabrication de technologies dès le départ. Ce concept englobe sept principes directeurs concernant le respect de la vie privée et la sécurité.



## PSEUDONYMISATION

Aux fins du présent document, la pseudonymisation désigne la modification de données à caractère personnel en supprimant tous les éléments d'identification directs (par exemple, dans de nombreux cas, le nom, l'adresse, la date de naissance, etc.) ou en les remplaçant par d'autres identifiants uniques (par exemple, dans de nombreux cas, des algorithmes de hachage, des numéros d'identité, etc.) de telle sorte qu'il reste possible de distinguer un individu unique dans un ensemble de données. Le masquage est une forme de pseudonymisation.



## RÉ-IDENTIFICATION

Aux fins du présent document, la ré-identification désigne un processus par lequel des données dépersonnalisées (anonymisées) deviennent à nouveau personnalisables de sorte qu'il est possible de remonter à un ou plusieurs individus ou groupes d'individus. Comme le document intitulé UN Global Pulse Data Innovation Risk Assessment Tool Guidance l'indique, pour déterminer si un ou plusieurs individus ou groupes d'individus sont identifiables, il faut envisager tous les moyens raisonnablement susceptibles d'être utilisés pour isoler un ou plusieurs individus ou groupes d'individus. Parmi les facteurs à prendre en considération pour déterminer s'il est raisonnablement probable qu'un ou plusieurs individus ou groupes d'individus puissent être ré-identifiés, on citera l'expertise requise, les coûts et le temps requis pour la ré-identification et les moyens technologiques raisonnablement et commercialement disponibles.



## DONNÉES SENSIBLES

Aux fins du présent document, le terme « données sensibles » renvoie aux données relatives aux aspects suivants : i) l'origine raciale ou ethnique, ii) les opinions politiques, iii) l'association syndicale, iv) les croyances religieuses ou d'autres croyances de nature similaire, v) la santé ou l'état physique ou mental(e) (ou toute donnée génétique), vi) l'orientation sexuelle et d'autres activités connexes, vii) la commission ou la commission présumée de toute infraction, viii) toute information concernant les procédures judiciaires, ix) les données financières, x) les enfants et xi) un ou plusieurs individus ou groupes d'individus exposés à des risques de préjudice (par exemple, physique, émotionnel, économique).

<sup>11</sup> La démarche a été élaborée par Ann Cavoukian. Un résumé est proposé à l'adresse : <https://www.ipc.on.ca/wp-content/uploads/Resources/7foundationalprinciples.pdf>

# NOTE ADDITIVE A

COMMENT L'ANALYSE DES DONNÉES PEUT AIDER  
À PROMOUVOIR LES ODD



Comment la science et  
l'analyse des données  
peuvent contribuer au  
développement durable



[www.unglobalpulse.org](http://www.unglobalpulse.org)

@UNGlobalPulse 2017

### 1 PAS DE PAUVRETÉ

Les habitudes de dépense pour les services de téléphonie mobile peuvent fournir des indicateurs indirects du niveau de revenu

### 2 FAIM « ZÉRO »

Le crowdsourcing ou le suivi des prix alimentaires répertoriés en ligne peut aider à surveiller la sécurité alimentaire en temps quasi réel

### 3 BONNE SANTÉ ET BIEN-ÊTRE

La cartographie des mouvements des utilisateurs de téléphones mobiles peut aider à prédire la propagation des maladies infectieuses

### 4 ÉDUCATION DE QUALITÉ

Les déclarations des citoyens peuvent aider à interpréter les taux d'abandon scolaire

### 5 ÉGALITÉ DES SEXES

L'analyse des transactions financières peut révéler les habitudes de dépense et les différents effets des chocs économiques sur les hommes et les femmes

### 6 EAU PROPRE ET ASSAINISSEMENT

Les capteurs connectés à des pompes à eau contribuent au suivi de l'accès à l'eau propre

### 7 ÉNERGIE PROPRE ET D'UN COÛT ABORDABLE

L'utilisation de compteurs intelligents permet aux entreprises de services publics d'augmenter ou de limiter la consommation d'électricité, de gaz ou d'eau afin de lutter contre le gaspillage et d'assurer un approvisionnement suffisant pendant les périodes de pointe

### 8 TRAVAIL DÉCENT ET CROISSANCE ÉCONOMIQUE

Les tendances du trafic postal mondial peuvent fournir des indicateurs tels que la croissance économique, les transferts de fonds, le commerce et le PIB

### 9 INDUSTRIE, INNOVATION ET INFRASTRUCTURE

Les données provenant d'appareils GPS peuvent être utilisées pour contrôler la circulation et améliorer les transports publics

### 10 INÉGALITÉS RÉDUITES

Les analyses axées sur la conversion de la voix en texte des contenus des programmes de radios locales peuvent révéler des problèmes de discrimination et étayer la formulation de mesures pour y remédier

### 11 VILLES ET COMMUNAUTÉS DURABLES

La télédétection par satellite peut permettre de détecter des cas d'empiètement sur des terrains ou espaces publics tels que les parcs et les forêts

### 12 CONSOMMATION ET PRODUCTION RESPONSABLES

Les habitudes de recherche en ligne ou les transactions de commerce électronique peuvent révéler le rythme de la transition vers des produits à haut rendement énergétique

### 13 MESURES RELATIVES À LA LUTTE CONTRE LES CHANGEMENTS CLIMATIQUES

La combinaison de l'imagerie satellitaire, de témoignages provenant de la population et de données ouvertes peut aider à surveiller le déboisement

### 14 VIE AQUATIQUE

Les données de suivi des navires peuvent révéler des activités de pêche illégales, non réglementées et non déclarées

### 15 VIE TERRESTRE

Le suivi des médias sociaux peut aider à gérer des catastrophes grâce à des informations recueillies en temps réel sur la localisation des victimes, les effets et l'intensité des feux de forêt ou de la brume

### 16 PAIX, JUSTICE ET INSTITUTIONS EFFICACES

L'analyse des sentiments sur les médias sociaux peut révéler l'opinion que se fait le public concernant l'efficacité de la gouvernance, la prestation de services publics ou les droits de l'homme

### 17 PARTENARIATS POUR LA RÉALISATION DES OBJECTIFS

Les partenariats permettant de combiner des statistiques, des données mobiles et des données d'Internet peuvent aider à mieux comprendre en temps réel le monde hyperconnecté d'aujourd'hui



# BIBLIOGRAPHIE

Asia-Pacific Economic Cooperation (2005). APEC Privacy Framework. Décembre. Singapour : Secrétariat de l'APEC.

Cavoukian, Ann (2011). Privacy by Design: The 7 Foundational Principles. Janvier. Ontario, Canada : Commissaire à l'information et à la protection de la vie privée de l'Ontario.

Conseil de l'Europe (1981). Convention pour la protection des personnes à l'égard du traitement automatisé des données à caractère personnel. 28 janvier. Série des traités européens - n° 108. Strasbourg, Autriche.

(1953). Convention de sauvegarde des droits de l'homme et des libertés fondamentales, telle qu'amendée par les Protocoles n° 11 et 14. 4 novembre. Série des traités européens - n° 5. (Article 8).

Communauté économique des États de l'Afrique de l'Ouest (2010). Acte additionnel A/SA.1/01.10 relatif à la protection des données à caractère. 16 février.

Union européenne (2016). Règlement (UE) 2016/679 du Parlement européen et du Conseil du 27 avril 2016 relatif à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données, et abrogeant la directive 95/46/CE (règlement général sur la protection des données) (Texte présentant de l'intérêt pour l'EEE).

Comité international de la croix rouge (2015). ICRC Code of Conduct on Data Protection. Novembre. Genève, Suisse : CICR.

Comité international de la croix rouge (2016). ICRC Rules on Personal Data Protection. Janvier. Genève, Suisse : CICR.

Conférence internationale des commissaires à la protection des données et de la vie privée, Résolution sur la protection des données et les organisations internationales.

Organisation internationale des migrations (2010). IOM Data Protection Manual. Genève, Suisse : OIM.

Organisation internationale de normalisation. Online Collection: Information Security Management Systems. Genève, Suisse : ISO.

Union internationale des télécommunications (2015). Recommandation Y.3600. Exigences et capacités pour les mégadonnées basées sur l'informatique en nuage. 6 novembre.

Organisation de coopération et de développement économiques (1980). Lignes directrices régissant la protection de la vie privée et les flux transfrontières de données de caractère personnel. 23 septembre.

Paris : OCDE.

Organisation des États américains (1969). Convention américaine relative aux droits de l'homme, « Pacte de San Jose », Costa Rica. 22 novembre. Washington : OEA. (Article 11).

Nations Unies (1989). Convention internationale relative aux droits de l'enfant. Série de traités - n° 1577 (1989) : 3 (article 16).

Section des archives et de la gestion des dossiers de l'Organisation des Nations Unies. Glossary of Recordkeeping Terms.

Fonds des Nations Unies pour l'enfance (2007). Les principes de Paris : Principes directeurs relatifs aux enfants associés aux forces armées ou aux groupes armés. Février. New York : UNICEF.

Groupe consultatif d'experts indépendants sur la révolution des données pour le développement durable (2014). A World that Counts: Mobilising the data revolution for sustainable development. Groupe consultatif d'experts indépendants sur la révolution des données pour le développement durable du Secrétaire général des Nations Unies. Novembre.


Programme des Nations Unies pour le développement et United Nations Global Pulse (2016). A Guide to Data Innovation for Development – From ideas to proof-of-concept. New York : ONU.

Commission économique des Nations Unies pour l'Europe (2014). The Role of Big Data in the Modernisation of Statistical Production. Genève, Suisse : CENUE)

Assemblée générale des Nations Unies (2016). Examen quadriennal complet des activités opérationnelles de développement du système des Nations Unies. 28 octobre. A/C.2/71/L.37.

A/70/L.1 (2015). Transformer notre monde : le Programme de développement durable à l'horizon 2030. 18 septembre.





A/RES/68/261 du 29 janvier 2014 (2014).

Principes fondamentaux de la statistique officielle. 3 mars.

A/RES/45/158 (1990). Convention internationale sur la protection des droits de tous les travailleurs migrants et membres de leur famille (article 14). 18 décembre.

A/RES/45/95 (1990). Principes directeurs pour la réglementation des fichiers informatisés contenant des données à caractère personnel. 14 décembre.

2200/A (XXI) (1966). Pacte international relatif aux droits civils et politiques. 19 décembre. Série de traités de l'ONU, vol. 999, n° 14668, p. 171 (de la version anglaise) et vol. 1057, p. 4019 (de la version anglaise) (art. 17).

217 A (III) (1948). La Déclaration universelle des droits de l'homme. 10 décembre. Paris, France. (Article 12).

United Nations Global Pulse (mai 2012). Big data for development: Challenges and opportunities, p. 13.

Principles. Data Privacy and Data Protection Principles.

Privacy Tools. Risks, Harms, Benefits Assessment.

Haut-Commissariat des Nations Unies aux droits de l'Homme (2016). A Human Rights-Based Approach to Data: Leaving No One Behind in the 2030 Development Agenda, Guidance Note to Data Collection and Disaggregation. 19 février. Genève, Suisse, HCR.

(2015). Policy on the Protection of Personal Data of Persons of Concern to UNHCR. Mai. Genève, Suisse : HCR.

Comité des droits de l'homme des Nations Unies (1988). CCPR General Comment No 16: Article 17 (Right to Privacy), The Right to Respect of Privacy, Family, Home and Correspondence, and Protection of Honour and Reputation. 8 avril.

United Nations Information Security Special Interest Group (juin 2013). Use of Cloud Computing in the UN System, Recommendations for Risk Mitigation

Commission internationale du droit des Nations Unies (2006). Report on the work of the fifty-eight session (2006). Annex IV. Protection of Personal Data in Transborder Flow of Information.

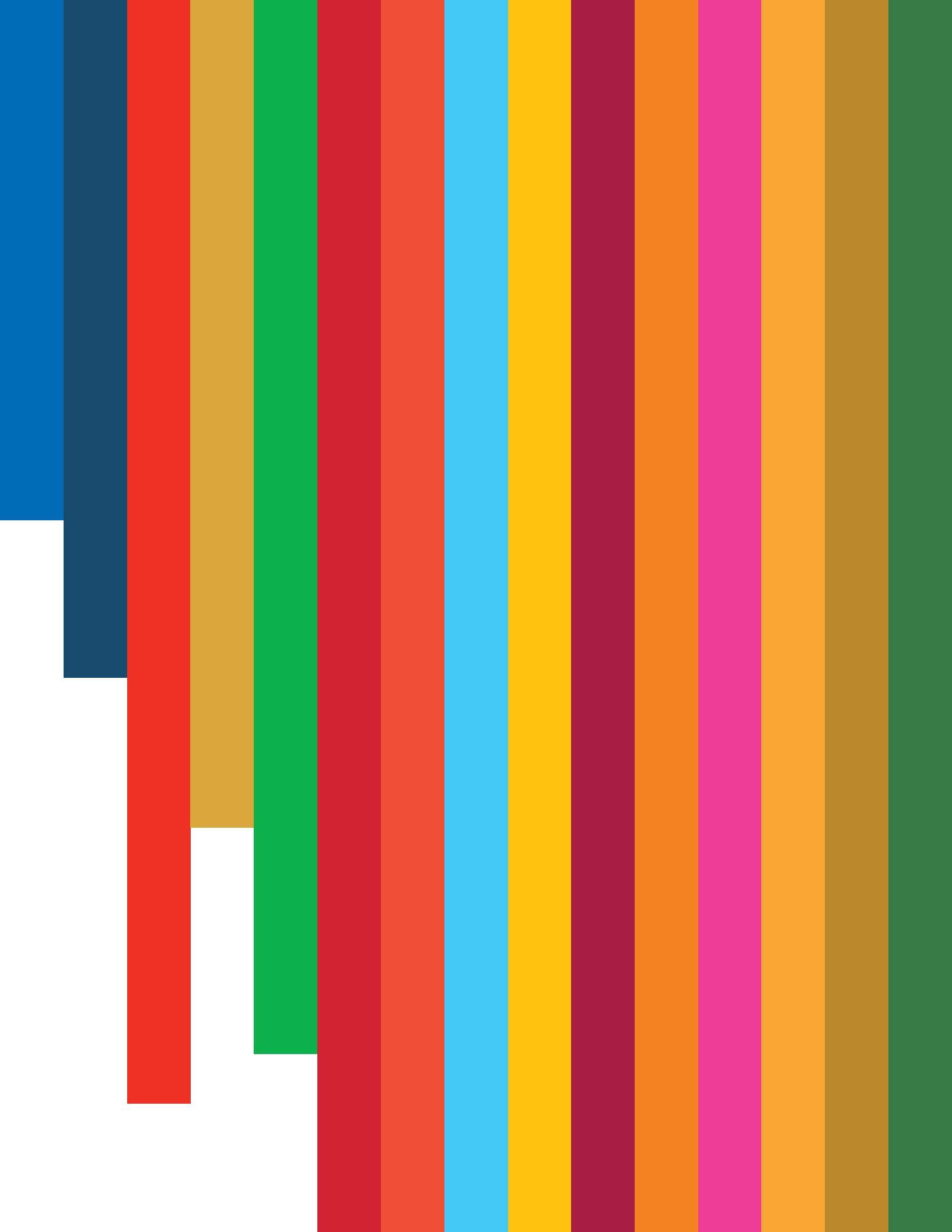
Commission de statistique des Nations Unies (2015). Report of the Global Working Group on Big Data for Official Statistics. 17 décembre. E/CN.3/2016/6

Conseil des droits de l'homme des Nations Unies (2016). Report of the Special Rapporteur on the right to privacy, Joseph A. Cannataci. 8 mars. A/HRC/31/64, pp. 6, 10. Annex II. A more in-depth look at Open Data & Big Data.

(2013). Report of the Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression, Frank La Rue. 17 avril. A/HRC/23/40, p. 6

Programme alimentaire mondial (2017). WFP Guide to Personal Data Protection and Privacy. 22 février. Rome : PAM.

Organisation mondiale de la Santé (2016). Guidance on Good Data and Record Management Practices. Série de Rapports techniques de l'OMS n° 996. Annexe 5.





---

**GROUPE DES  
NATIONS UNIES  
POUR LE  
DÉVELOPPEMENT**

---

Le Groupe des Nations Unies pour le développement (GNUD) regroupe les 32 fonds, programmes, institutions spécialisées, départements et bureaux du système des Nations unies qui jouent un rôle dans le développement. Depuis 2008, le GNUD est l'un des trois piliers du Conseil des chefs de secrétariat des organismes des Nations Unies pour la coordination, l'instance de coordination de plus niveau du système des Nations Unies.

Au niveau régional, six équipes régionales du GNUD jouent un rôle essentiel pour mener à bien les priorités du GNUD, grâce au soutien apporté aux équipes de pays des Nations Unies dans l'établissement de priorités stratégiques, l'analyse et les conseils.

Au niveau national, 131 équipes de pays des Nations Unies dans 165 pays et territoires œuvrent ensemble pour accroître les synergies et l'impact commun du système des Nations Unies.

Le Bureau de la coordination des activités de développement des Nations Unies (DOCO) est le secrétariat du GNUD, et regroupe les organismes du système des Nations Unies pour le développement, afin de promouvoir le changement et l'innovation qui permettront d'assurer ensemble le développement durable.