F

联合国粮食及农业组织 | Food and Agriculture Organization of the United Nations | Organisation des Nations Unies pour l'alimentation et l'agriculture | Продовольственная и сельскохозяйственная организация Объединенных Наций | Organización de las Naciones Unidas para la Alimentación y la Agricultura | منظمة الأغذية والزراعة للأمم المتحدة

COMITÉ DES QUESTIONS CONSTITUTIONNELLES ET JURIDIQUES

Cent quinzième session

Rome, 21-23 mars 2022

Informations actualisées sur les politiques de la FAO relatives à la protection des données et aux droits de propriété intellectuelle

I. Contexte

1. À sa cent soixante-cinquième session, le Conseil de la FAO a demandé que les cadres de l'Organisation relatifs à la protection des données et aux droits de propriété intellectuelle soient renforcés, notamment dans le contexte de l'Initiative Main dans la main[1], de la nouvelle Stratégie de la FAO relative à la mobilisation du secteur privé[2], du nouveau Cadre stratégique et de l'action menée par la FAO pour faire face à la pandémie de covid-19[3]. À sa cent soixante-sixième session, le Conseil a rappelé qu'il convenait «*de mettre au point une politique de données transversale pour garantir la gouvernance, l'intégrité et la confidentialité des données, ainsi que les droits de propriété intellectuelle, et de respecter les normes et protocoles internationaux*[4]».

2. Par la suite, à sa cent soixante-huitième session, le Conseil a approuvé «*les constatations et conclusions du [Comité des questions constitutionnelles et juridiques] sur les grands principes concernant la protection des données et la propriété intellectuelle qui façonneront l'élaboration du cadre de la FAO sur la protection des données et les droits de propriété intellectuelle et, constatant l'intérêt et l'engagement des Membres de la FAO sur cette question*[5]», a souligné *«qu'il était important de consulter les Membres pour l'élaboration des politiques et a recommandé à la Direction de la FAO d'organiser de nouvelles consultations inclusives avec les Membres en vue de clarifier le document-cadre et d'y mettre la dernière main, y compris par l'intermédiaire des organes directeurs, le cas échéant*[6]».

3. En juillet 2021, la Direction a demandé aux Membres, via le Portail des Membres, leurs avis concernant les éléments sur lesquels devrait porter le cadre relatif à la protection des données. Des contributions précieuses ont été reçues et, au vu de certaines observations et demandes soumises, une

[1] CL 165/REP, paragraphe 14, alinéa i).
[2] CL 165/REP, paragraphe 11, alinéa j).
[3] CL 165/REP, paragraphe 13, alinéa c).
[4] CL 166/REP, paragraphe 24, alinéa k).
[5] CL 168/REP, paragraphe 30, alinéa d).
[6] *Ibid.*

Les documents peuvent être consultés à l'adresse www.fao.org.

NI334/f

réunion d'information informelle sur la protection des données et la propriété intellectuelle s'adressant à tous les Membres a été tenue en octobre 2021. En novembre 2021, la Direction a invité à nouveau les Membres à soumettre des contributions écrites.

4. À la lumière des recommandations des organes directeurs, la Direction a organisé une autre réunion d'information informelle le 7 mars 2022 pour informer les Membres des progrès réalisés et recueillir leurs observations. Une réunion informelle conjointe du Comité des questions constitutionnelles et juridiques et du Comité du Programme sera organisée le 18 mars 2022 pour aborder expressément la question de la gouvernance des activités statistiques et de l'alignement sur les politiques relatives à la protection des données et aux droits de propriété intellectuelle.

II. Politique de protection des données

5. Le projet de politique interne sur la protection des données, joint en annexe au présent document, énonce les principes directeurs en matière de protection des données («principes FIRST relatifs à la protection des données») et présente la classification des données, ainsi que les responsabilités et le mécanisme de contrôle au sein de l'Organisation. La politique s'appliquera à toutes les activités et opérations de la FAO requérant le traitement par cette dernière de données personnelles et non personnelles. Le projet a été élaboré à la lumière des orientations que le Comité des questions constitutionnelles et juridiques a formulées à sa cent treizième session, ainsi que des informations et des vues reçues des Membres dans le cadre des processus de consultation décrits ci-dessus. Il a également été tenu compte des normes internationales et des instruments équivalents élaborés par les organismes du système des Nations Unies ou en coordination avec le système des Nations Unies.

6. La politique vise à donner des orientations suffisantes pour permettre au personnel d'appliquer directement les principes dans leurs activités officielles; elle sera complétée par des directives et des procédures opérationnelles détaillées portant sur certains types d'activités ou de données. On examine actuellement les procédures détaillées existantes – et on continuera de le faire – pour assurer leur cohérence avec la politique[7].

III. Politique sur la propriété intellectuelle

7. Tandis que le projet de politique de protection des données concerne les données personnelles et non personnelles et couvre par conséquent certains aspects des droits de propriété intellectuelle, un instrument distinct portant sur la gestion des droits de propriété intellectuelle par l'Organisation est en cours d'élaboration. Il intégrera les principes directeurs relatifs aux droits de propriété intellectuelle examinés par le Comité des questions constitutionnelles et juridiques, les informations et les vues communiquées par les Membres, ainsi que des pratiques et normes internationales ou propres au système des Nations Unies.

IV. Suite que le Comité est invité à donner

8. Le Comité est invité à prendre note des progrès accomplis dans l'élaboration du cadre de la FAO relatif à la protection des données et aux droits de propriété intellectuelle. Il souhaitera peut-être en particulier prendre note du projet de politique de protection des données et formuler des observations à son sujet.

[7] Par exemple, les sections suivantes du Manuel administratif de la FAO: 702 *Cash Transfers* (Transferts monétaires), 340 *Confidential Personnel Files* (Fichiers confidentiels du personnel), 502 *Procurement of Goods, Work and Services* (Achat de biens, exécution de travaux et prestation de services), 505 *Information Technology* (Technologies de l'information) et 601 *Records and Archive Management* (Gestion des dossiers et des archives).

ANNEXE I

PROJET DE POLITIQUE DE PROTECTION DES DONNÉES

circulaire administrative

Nº 2022/XX
Date: XX mars 2022

POLITIQUE DE PROTECTION DES DONNÉES

I. INTRODUCTION

1. L'article premier de l'Acte constitutif de la FAO dispose que l'une des fonctions de l'Organisation est de «*réuni[r], analyse[r], interpr[éter] et diffuse[r] tous renseignements relatifs à la nutrition, l'alimentation et l'agriculture*[8]». En outre, le Cadre stratégique 2022-2031 indique que l'une des fonctions essentielles de la FAO consiste à «*rassembler, analyser et contrôler les données et les informations dans les domaines relevant du mandat de la FAO, et en améliorer l'accès*» et à «*mener des activités de promotion et de communication aux niveaux national, régional et mondial, notamment auprès des consommateurs, en s'appuyant sur les connaissances et les données de la FAO, sa position en tant qu'organisme spécialisé des Nations Unies et son rôle d'intermédiaire neutre et de confiance*[9]».

2. Les données constituent une ressource stratégique pour l'exécution du mandat de la FAO, et l'Organisation devrait être en mesure de les utiliser sans les compromettre. Une politique de protection des données est essentielle pour assurer la protection des données traitées par la FAO et faire en sorte que ces données conservent leur valeur et leur intégrité et qu'elles puissent être exploitées.

3. Toute donnée[10] utilisée, traitée ou transférée à une tierce partie par la FAO doit faire l'objet d'un traitement adéquat et uniforme tout au long de son cycle de vie, qui va de la collecte à la suppression, en passant par le stockage.

4. La divulgation non autorisée, l'usage abusif et le traitement inapproprié de données, ainsi que le traitement de données de mauvaise qualité, exposent l'Organisation à des risques juridiques, financiers et opérationnels et sont susceptibles de nuire à sa réputation. Une politique de protection des données, lorsqu'elle est correctement mise en œuvre, contribue à renforcer la confiance dans l'Organisation et dans le travail qu'elle accomplit. Il est impératif que toute donnée que la FAO détient ou confie à une tierce partie soit protégée de manière appropriée.

5. La présente politique, qui vise à atténuer les risques et à renforcer la protection, établit les principes FIRST de la FAO relatifs à la protection des données. Présentés en détail dans la section III

[8] Acte constitutif, article premier, paragraphe 1.
[9] Cadre stratégique 2022-2031 de la FAO, paragraphe 43.
[10] Voir le paragraphe 9 ci-dessous et la section «Définitions» à l'annexe I.

du présent document, ces principes généraux sont conformes aux normes et contrôles internationaux en matière de protection des données, y compris ceux du système des Nations Unies[11]. Ils s'appliquent tout au long du cycle de traitement des données et portent notamment sur la manière de collecter, de conserver et de traiter les données, ainsi que sur la manière de les supprimer et le moment auquel les supprimer.

6. Comme il est décrit plus avant dans la section III, les principes FIRST relatifs à la protection des données sont les suivants:

- ✓ **F**inalité légitime
- ✓ **I**ntégrité
- ✓ **R**esponsabilité
- ✓ **S**écurité
- ✓ **T**ransparence

7. Les principes FIRST, de même que les obligations qui en découlent, sont de haut niveau et neutres du point de vue de la technologie. Leur application quotidienne peut donc se faire de manière souple. Le personnel doit mettre en pratique ces principes en les intégrant dans des mesures et des outils qui répondent aux besoins de ses activités, tout en assurant un niveau de protection approprié des données traitées. Des orientations opérationnelles supplémentaires concernant certains types d'activités requérant un traitement de données seront publiées dans le cadre de la présente politique.

II. CHAMP D'APPLICATION ET MISE EN ŒUVRE

8. Compte tenu du statut juridique de la FAO, en sa qualité d'institution spécialisée des Nations Unies, ainsi que de ses privilèges et immunités, et étant donné que les lois nationales et régionales ne s'appliquent pas à ses activités, la présente politique établit les principes généraux et les règles qui gouvernent le traitement et la protection des données par la FAO[12].

9. La présente politique ne s'applique pas aux données publiques, telles qu'elles sont décrites au paragraphe 14, ni aux données anonymisées, telles qu'elles sont définies à l'**annexe I**. Elle s'applique à toutes les autres données, quel que soit leur format[13], y compris les données non personnelles et les données personnelles, communiquées par une personne physique ou morale à la FAO ou provenant de la FAO[14].

10. Cette politique s'applique à toutes les activités et opérations requérant le traitement de données par la FAO ou par des tierces parties dans le cadre de leurs relations avec la FAO. L'ensemble du personnel doit traiter les données conformément à la présente politique. Toutes les

[11] Voir, par exemple, la *Stratégie du Secrétaire général pour l'exploitation des données par tout le monde, partout: perspectives, impact et intégrité* et les *Principes des Nations Unies pour la protection des données personnelles et le respect de la vie privée*.

[12] Cette politique doit être appliquée compte dûment tenu des attributs fondamentaux de la FAO, notamment son statut intergouvernemental, sa neutralité et le pouvoir d'offrir une plateforme neutre pour le dialogue et l'échange de connaissances entre les pays, ainsi que l'autorité de demander à tout Membre de soumettre des informations ayant trait au but de l'Organisation. Voir les textes fondamentaux de la FAO, notamment l'article premier et l'article VI de l'Acte constitutif, et le Cadre stratégique 2022-2031 de la FAO.

[13] Format papier ou numérique.

[14] Cette politique s'applique indépendamment du fait que les données traitées soient ou non fournies par la personne qu'elles concernent ou par une autre entité (par exemple lorsqu'un Membre fournit des informations concernant des personnes relevant de sa juridiction).

autres règles et politiques internes concernant des aspects particuliers de la protection des données doivent être mises en œuvre et interprétées conformément à la présente politique. En cas d'incompatibilité, la présente politique prévaudra.

11. La présente politique établit les normes minimales concernant la protection des données générées par la FAO ou confiées à cette dernière par une personne physique ou morale (autrement dit, un fournisseur de données). Elle établit également les mécanismes institutionnels internes qui permettront de contrôler la mise en œuvre des principes FIRST relatifs à la protection des données et de vérifier que la politique reste adaptée à l'objectif poursuivi. Les définitions des termes employés dans la présente politique sont données dans l'**annexe I**, tandis que l'**annexe II** présente des exemples de l'application des principes FIRST.

III. LES CINQ PRINCIPES FIRST RELATIFS À LA PROTECTION DES DONNÉES

1. FINALITÉ LÉGITIME

«Nous traitons les données sur une base légitime et uniquement à une fin précise. Nous collectons et conservons le minimum de données nécessaires.»

1.1 Points essentiels

La finalité légitime fait référence au fait que la FAO traite les données d'une façon qui est conforme à ce que le fournisseur de données peut raisonnablement attendre. À cet effet, il est nécessaire de déterminer le fondement légitime du traitement et de définir une finalité précise. La FAO ne doit collecter que le minimum d'éléments de données nécessaires à l'atteinte de cette finalité. Une fois celle-ci atteinte, les données ne doivent pas être conservées.

1.2 Responsabilités

1.2.1 Fondement légitime

Le personnel ne peut traiter les données que dans le cadre des activités menées par la FAO en vertu de son mandat et conformément à son cadre juridique. En plus de devoir s'assurer que la condition ci-dessus est remplie, le personnel doit justifier de l'un des fondements légitimes suivants pour pouvoir traiter les données: *i*) le consentement éclairé préalable du fournisseur de données[15]; *ii*) les intérêts vitaux d'une personne dans le cas où le consentement éclairé préalable ne peut être obtenu[16]; ou *iii*) la nécessité d'appliquer un accord juridique conclu préalablement au traitement (par exemple, un contrat de travail).

1.2.2 Détermination de la finalité

La finalité du traitement des données doit être déterminée avant la collecte des données.

[15] Un fournisseur de données peut retirer son consentement. Des orientations relatives au retrait de consentement sont fournies au paragraphe 33, alinéa c). Voir également le paragraphe 24, portant sur le traitement des données sensibles.

[16] Dans des cas exceptionnels où il n'est pas possible d'obtenir un consentement éclairé – par exemple lorsque le traitement est nécessaire pour préserver la vie, l'intégrité ou la santé de la personne, ou la sécurité de cette même personne ou d'une autre –, les données peuvent être traitées au titre de l'intérêt vital. Les raisons pour lesquelles le consentement éclairé n'est pas obtenu doivent être dûment consignées et régulièrement examinées pour vérifier que les circonstances qui empêchent le consentement n'ont pas changé. Les circonstances exceptionnelles de ce type ne dispensent pas le personnel de se conformer à tous les autres éléments de cette politique.

1.2.3 Autre traitement	Des données ne peuvent être traitées pour de nouvelles finalités que si leur traitement remplit l'une au moins des conditions suivantes: *i*) est compatible avec la finalité initiale; *ii)* a son propre fondement légitime; *iii*) se fonde sur une nouvelle expression de consentement, si le consentement constituait le fondement légitime initial; *iv*) est lié à des activités relatives à la statistique ou à la recherche menées dans le cadre du mandat technique de la FAO; *v*) est effectué à des fins d'archivage conformément à la section 601 du Manuel administratif de la FAO, consacrée à la gestion des dossiers et des archives.
1.2.4 Nécessité	Autant que faire se peut, seul le minimum de données nécessaires pour atteindre la finalité poursuivie doit être collecté et traité. Aucune donnée non nécessaire, non pertinente ou superflue par rapport à cette finalité ne doit être collectée ou traitée.
1.2.5 Conservation	Les données ne doivent être conservées que le temps nécessaire pour parvenir à la finalité pour laquelle elles ont été collectées. Une fois la finalité atteinte, à moins qu'elles ne soient utilisées à des fins de statistiques, de recherche ou d'archivage, les données doivent être supprimées ou anonymisées, selon qu'il convient, dans un délai raisonnable. Elles peuvent être stockées pendant une période plus longue que celle nécessaire à la finalité pour laquelle elles ont été collectées à condition qu'un motif légitime justifie leur conservation (par exemple, le respect des durées de conservation imposées par les règles de la FAO ou des accords passés avec les pays bénéficiaires et les partenaires fournisseurs de ressources).
1.2.6 Processus de conservation et de suppression	Le personnel est tenu de mettre en œuvre les normes, processus et dispositifs appropriés pour assurer la conservation des données sur une durée limitée, puis leur suppression.
1.2.7 Conservation par une tierce partie	Lorsque des données doivent être transférées à une tierce partie, le personnel doit s'assurer que cette dernière à l'obligation contractuelle de détruire ou de retourner à la FAO toutes les données transférées une fois que la finalité du transfert a été atteinte ou à la résiliation ou à l'expiration de l'accord en vertu duquel les données ont été transférées, à moins que la tierce partie ait reçu le consentement explicite du fournisseur de données, l'autorisant à poursuivre le traitement des données.

2. INTÉGRITÉ

«*Nous vérifions l'exactitude des données. Nous supprimons ou corrigeons toute donnée incorrecte ou peu fiable.»*

2.1 Points essentiels	L'intégrité fait référence à la mise en œuvre de processus et de contrôles destinés à garantir l'exactitude générale des données. Elle est nécessaire pour assurer l'utilisation et l'interprétation correctes des données. Avant la collecte et tout au long du cycle de vie des données, le personnel doit adopter des mesures raisonnables pour garantir l'exactitude et la fiabilité des données traitées. Si, pour quelque raison que ce soit et à tout moment, il

est établi que des données sont inexactes ou trompeuses, des mesures immédiates doivent être prises en vue de leur rectification ou suppression.

2.2 Responsabilités

2.2.1 Obligation générale — Il incombe à chaque membre du personnel de veiller à l'exactitude des données qu'il traite. Ainsi, le personnel est tenu de prendre toutes les mesures rationnelles pour s'assurer de l'exactitude des données.

2.2.2 Enregistrement et suppression — Toutes les mesures rationnelles doivent être prises pour: *i*) garantir que seules des données exactes sont enregistrées et traitées, et *ii*) s'assurer que toute donnée inexacte est rapidement supprimée ou corrigée.

2.2.3 Examen — Des processus doivent être mis en place pour vérifier régulièrement l'exactitude des données, afin d'empêcher et de réduire le plus possible les erreurs et les incohérences.

3. RESPONSABILITÉ

«*Nous nous conformons de manière proactive aux principes FIRST relatifs à la protection des données et sommes en mesure de le démonter*.»

3.1 Points essentiels — Tous les membres du personnel sont tenus de se conformer aux principes FIRST relatifs à la protection des données et doivent pouvoir démontrer avoir pris des mesures rationnelles pour garantir le respect de la présente politique, ainsi que des directives et des procédures établies par l'Organisation.

3.2 Responsabilités

3.2.1 Obligation générale — Il convient d'adopter des mesures appropriées et proportionnées pour s'assurer et démontrer que le traitement des données est effectué conformément à la présente politique. Avant de traiter les données, il convient de prendre les mesures nécessaires pour prévenir ou limiter les risques que comporte le processus de traitement pour le fournisseur de données et l'Organisation. Ces mesures doivent aussi garantir que seules les données nécessaires à l'atteinte de la finalité poursuivie seront collectées. Elles doivent être régulièrement révisées et mises à jour selon qu'il convient.

3.2.2 Preuves du respect de la politique — Les mesures suivantes peuvent servir à démontrer le respect de la présente politique:

- la tenue à jour d'un registre des activités de traitement devant inclure, au minimum, des informations sur la finalité du traitement, les données traitées, le niveau de confidentialité et, le cas échéant, les destinataires des données (internes et externes), les durées de conservation envisagées et les mesures de sécurité mises en place;
- la réalisation, avant le traitement des données, d'une évaluation («évaluation de l'impact de la protection des données») destinée à recenser, prendre en compte et atténuer les risques, dans le cas d'une opération de

traitement des données susceptible de comporter un risque élevé pour le fournisseur de données ou l'Organisation. Pour établir si le traitement présente un risque élevé, le personnel doit déterminer la probabilité et la gravité de tout préjudice que le fournisseur de données ou l'Organisation est susceptible de subir. Lorsqu'on établit qu'une opération de traitement présentera probablement un risque élevé pour le fournisseur de données ou l'Organisation, il convient de consulter l'Unité de protection des données[17] pour obtenir des conseils et des orientations concernant de possibles mesures d'atténuation et leur mise en œuvre;

- la conception d'un mode de traitement permettant de prévenir, d'éviter ou de réduire le plus possible les risques recensés;
- l'établissement de processus et de procédures pour traiter les demandes des fournisseurs de données et y répondre;
- la mise en œuvre de processus, de méthodes et de techniques destinés à garantir un niveau de sécurité proportionnel au niveau de confidentialité, déterminé conformément à la section IV ci-après. Ces mesures peuvent comprendre l'anonymisation, la pseudonymisation ou le chiffrement (voir l'**annexe I**).

4. SÉCURITÉ

«*Nous protégeons les données en adoptant des mesures raisonnables contre les menaces externes et internes.*»

4.1 Points essentiels

La FAO est responsable des données qu'elle traite, et le personnel doit adopter des mesures de sécurité raisonnables pour les protéger. Ces mesures doivent garantir la confidentialité des données en empêchant leur divulgation ou utilisation non autorisée, et assurer le maintien de l'intégrité des données en empêchant toute modification non autorisée et en ne permettant qu'un accès autorisé. Il incombe à chaque membre du personnel d'évaluer les risques liés à une opération de traitement et de veiller à ce que des mesures de sécurité raisonnables soient en place.

4.2 Responsabilités

4.2.1 Obligation générale

Le personnel est tenu de protéger les données qu'il traite conformément aux sections pertinentes du Manuel administratif de la FAO et aux dispositions administratives applicables.

4.2.2 Mesures de sécurité appropriées

Sur la base du niveau de confidentialité des données, il convient de mettre en place des mesures, procédures et contrôles de sécurité organisationnels, physiques et techniques appropriés pour protéger les données. Ces mesures, procédures et contrôles de sécurité doivent à tout moment être proportionnés et adaptés aux risques recensés par le personnel lors de l'évaluation effectuée en application du paragraphe 3.2.2.

[17] Voir le paragraphe 44 ci-après.

4.2.3 Examen	Le personnel doit examiner périodiquement et, le cas échéant, mettre à jour les mesures de sécurité mises en œuvre conformément au paragraphe 4.2.2.
4.2.4 Utilisation des ressources des technologies de l'information et de la communication	Tous les systèmes de technologies de l'information et de la communication, y compris les systèmes d'information de gestion, utilisés pour le traitement et le stockage de données visées par la présente politique doivent être gérés conformément à la section 505 et à toute autre disposition pertinente du Manuel administratif.
4.2.5 Stockage	Suivant leur niveau de confidentialité, les données doivent être stockées dans des lieux appropriés et de sorte à être protégées contre le traitement accidentel ou non autorisé, la perte ou la corruption. Si les données doivent être traitées ou stockées par un fournisseur de services d'informatique dématérialisée, la stratégie de la FAO relative au passage à l'informatique en nuage, les lignes directrices relatives à l'informatique en nuage et le processus d'évaluation des risques s'appliquent.
4.2.6 Accès aux données	Suivant le niveau de confidentialité attribué aux données, l'accès à celles-ci ne doit être autorisé et accordé qu'aux personnes qui ont besoin de savoir pour permettre la réalisation de la finalité du traitement des données. Il convient de tenir un registre dans lequel sont consignés les noms des personnes autorisées et les droits d'accès qui leur ont été octroyés. Avant de transférer des données à des tierces parties en vue de leur traitement, le personnel doit s'assurer que les mesures de sécurité de ces tierces parties sont au moins équivalentes à celles requises pour des données ayant le même niveau de confidentialité à la FAO.

5. TRANSPARENCE

«Nous faisons preuve de clarté et de franchise au sujet des données que nous traitons, des raisons pour lesquelles nous les traitons et de la manière dont nous les utilisons. Nous pouvons donner à cet égard une explication claire au fournisseur de données.»

5.1 Points essentiels	Le principe de transparence fait référence à la clarté et à la franchise envers les fournisseurs de données au moment de la collecte, c'est-à-dire en ce qui concerne les questions de savoir *quelles* données la FAO entend traiter, *pourquoi* le traitement est nécessaire et *comment* les données seront traitées. Le niveau d'information à fournir variera suivant la nature des données et le contexte opérationnel.
5.2 Responsabilités	
5.2.1 Obligation générale	Il incombe au personnel de communiquer au fournisseur de données, le cas échéant, des informations suffisantes, pertinentes et à jour concernant le traitement de ses données, y compris de l'informer des différentes demandes qu'il peut soumettre concernant ses données, comme indiqué au paragraphe 33 ci-après.

5.2.3 Moyens favorisant la transparence	Il convient de recourir à des moyens appropriés, comme des bulletins d'information, pour informer le fournisseur de données du traitement de ces dernières tout au long de leur cycle de vie. Ces moyens doivent être régulièrement revus pour s'assurer que les informations communiquées au fournisseur de données sont toujours pertinentes et à jour.
5.2.5 Exceptions	Si aucune information n'est communiquée, il convient de consulter l'Unité de protection des données. Les raisons pour lesquelles aucune information n'est communiquée doivent être dûment consignées et régulièrement examinées pour vérifier que les circonstances qui justifient la décision de ne pas fournir d'informations n'ont pas changé[18].

IV. CLASSIFICATION DES DONNÉES ET NIVEAUX DE CONFIDENTIALITÉ

12. Le personnel est chargé de classer les données en fonction de leur teneur, de leur caractère plus ou moins sensible et des risques liés à leur divulgation inappropriée.

13. Il existe quatre niveaux de confidentialité indiquant le degré de sensibilité des données et les risques associés que pourrait comporter l'utilisation ou la divulgation non autorisée des données traitées par le personnel.

14. Les données doivent être classées dans l'un des quatre niveaux de confidentialité suivants:

Niveau de confidentialité	Description et risques potentiels	Exemples
Données publiques	Données qui ne sont pas sensibles et dont la FAO a approuvé la mise à la disposition du public[19]. Risque: **NUL** L'accès non autorisé aux données ou leur divulgation inappropriée ne devrait vraisemblablement pas porter préjudice à la FAO ou au fournisseur de données.	• Rapports publiés, statistiques ou communiqués de presse.

[18] Par exemple, dans des situations d'urgence, il peut être impossible en raison de contraintes de sécurité et de logistique de communiquer immédiatement des informations aux fournisseurs de données au moment de la collecte.

[19] Les données publiques peuvent être mises à la libre disposition du public conformément à la Politique de libre accès (en anglais) de la FAO et à d'autres dispositions concernant les données en accès libre relatives aux bases de données statistiques.

Niveau de confidentialité	Description et risques potentiels	Exemples
Données internes	Données qui, parce qu'elles sont en cours d'élaboration ou incomplètes, ou parce qu'elles doivent être approuvées en interne, ne doivent pas être divulguées hors de la FAO. Risque: **MOYEN** L'accès non autorisé aux données ou leur divulgation inappropriée pourrait vraisemblablement porter préjudice au fournisseur de données ou à la FAO (par exemple en compromettant l'indépendance des processus décisionnels de la FAO).	• Communications internes. • Descriptifs de projet, rapports détaillés de projet et rapports financiers pouvant requérir le consentement du fournisseur de données à la communication de ces informations. • Projets de documents techniques en cours d'élaboration, devant encore être validés et approuvés avant d'être mis à la disposition du public.
Données confidentielles	Données à caractère sensible. Risque: **ÉLEVÉ** L'accès non autorisé aux données ou leur divulgation inappropriée porterait grandement préjudice au fournisseur de données ou à la FAO. Le préjudice causé à la FAO pourrait être d'ordre financier, juridique, stratégique ou opérationnel, ou concerner sa réputation.	• Informations sur l'assistance technique fournie à des pays et accords relatifs à des contributions conclus avec les Membres. • Microdonnées dont le fournisseur indique spécifiquement qu'elles ne doivent pas être divulguées. • Listes de participants à des formations organisées par la FAO et autres documents contenant des données personnelles, comme les noms, adresses électroniques, titres de poste et numéros de téléphone. • Vérifications préalables et évaluations des risques. • Processus de sélection du personnel.

Niveau de confidentialité	Description et risques potentiels	Exemples
Données sensibles	Données de nature très sensible. Il peut également s'agir de données qui, du fait de leur teneur ou du contexte dans lequel elles sont créées ou communiquées, deviennent sensibles et doivent être classées comme telles. Risque: **TRÈS ÉLEVÉ** L'accès non autorisée aux données ou la divulgation inappropriée des données causerait un préjudice extrêmement grave au fournisseur de données ou à la FAO. Le préjudice subi par la FAO pourrait consister en des dommages de nature financière, juridique, stratégique ou opérationnelle ou en une atteinte à la réputation, dont les conséquences seraient majeures et irréversibles.	• Données personnelles révélant, entre autres, l'origine raciale ou ethnique, la confession, l'état de santé ou des caractéristiques génétiques ou biométriques d'une personne physique. • Documents relatifs à des procédures d'enquête, à des procédures disciplinaires ou à des procédures d'appel. • Documents transmis à la FAO par des Membres ou des tierces parties sous réserve du respect de leur confidentialité. • Documents relatifs à des achats dont le fournisseur a signalé la nature commercialement sensible.

15. La communication de données à une partie externe ou au public doit obligatoirement s'effectuer selon les procédures d'autorisation ou de publication établies.

16. Au moment de mettre en œuvre les mesures de sécurité et les contrôles qui s'imposent, le personnel doit déterminer, au cas par cas, le niveau de protection à appliquer aux données dont il effectue le traitement, et ce en tenant compte des risques recensés pour le traitement en question. Le personnel doit adopter des mesures de sécurité qui sont proportionnées et adaptées au niveau de confidentialité déterminé.

17. Si un fournisseur de données transmet des données à la FAO auxquelles il a préalablement attribué tel ou tel niveau de confidentialité, le personnel de la FAO est tenu de traiter ces données conformément au niveau de confidentialité attribué. Dans le cas d'un fournisseur de données qui n'aurait pas défini de niveau de confidentialité, les données transmises sont toutefois classées comme confidentielles, à moins qu'il en ait été convenu autrement entre la FAO et le fournisseur de données.

18. Afin de garantir un niveau de protection proportionné et adapté au niveau de confidentialité, le personnel doit régulièrement réexaminer le classement des données en sa possession et le modifier s'il y a lieu. Dans l'éventualité où ni le personnel de la FAO ni le fournisseur de données n'auraient attribué de niveau de confidentialité aux données, ces dernières seront classées comme confidentielles.

19. En cas de doute concernant le niveau de confidentialité à attribuer, les membres du personnel consulteront leur chef de bureau, le Représentant de la FAO, le Sous-Directeur général/Représentant régional de la FAO ou l'Unité de protection des données, selon le cas.

V. DEVOIR DE CONFIDENTIALITÉ

20. Les données doivent être traitées avec la plus grande discrétion tout au long de leur cycle de vie. Le personnel est responsable du traitement des données, y compris lorsque celles-ci sont transférées à une tierce partie. Il est tenu par le devoir de confidentialité, qui est défini en vertu du paragraphe 301.1.5 du Statut du personnel, du paragraphe 39 des Normes de conduite de la fonction publique internationale et du paragraphe 5.12 du Code de conduite éthique de la FAO. Le devoir de confidentialité s'applique à tous les membres du personnel et ceux-ci s'exposent à des mesures administratives, y compris disciplinaires, s'ils ne respectent pas les dispositions susmentionnées lorsqu'ils sont amenés à traiter des données internes, confidentielles ou sensibles dont ils ont eu connaissance du fait des fonctions officielles qu'ils exercent.

21. Le personnel doit veiller à garantir la confidentialité des données qu'il recueille, qu'il consulte ou qu'il traite. Les données ne doivent être consultées ou transférées qu'aux fins prévues et ne doivent être communiquées à aucune autre personne, y compris à des tierces parties ou à d'autres membres du personnel de la FAO, à moins que le destinataire ait été expressément autorisé à les recevoir ou à y accéder sous réserve de l'application de mesures de sécurité adéquates au regard du niveau de confidentialité des données.

VI. APPLICATION CONCRÈTE DES PRINCIPES FIRST RELATIFS À LA PROTECTION DES DONNÉES

Communication d'informations aux fournisseurs de données

22. Avant de recueillir des données, ou dans un délai raisonnable après les avoir recueillies, il convient de communiquer un certain nombre de renseignements au fournisseur de données, en lui indiquant au minimum: *i)* quelles données seront traitées; *ii*) à quelles fins les données seront traitées; *iii*) si les données seront transférées à une tierce partie; *iv*) comment soumettre une demande d'accès à ses données, une demande de vérification, de rectification ou de suppression de ses données ou une demande d'opposition à l'utilisation de ses données; *iv*) comment déposer une plainte [auprès de l'Unité de protection des données] concernant ses données, par exemple s'il n'est pas satisfait de la suite donnée à une demande qu'il a soumise; *v*) l'identité et les coordonnées d'un point de contact de la FAO auquel s'adresser pour toute question ou demande relative aux données.

23. Dans le cas du traitement de données personnelles, les renseignements communiqués à un fournisseur de données doivent être formulés de manière claire et intelligible, et présentés sous une forme adaptée à l'âge, au niveau d'alphabétisation et au degré de vulnérabilité du fournisseur de données.

Traitement de données sensibles

24. **Adoption de mesures appropriées**. Il convient de mettre en place des mesures et des mécanismes de contrôle destinés à garantir une utilisation et une protection adéquates des données sensibles, en tenant compte du contexte dans lequel les données seront traitées et utilisées ainsi que des principes FIRST relatifs à la protection des données.

25. **Évaluation de la nécessité**. Avant de recueillir des données sensibles, il incombe au personnel de chercher à savoir s'il serait possible d'atteindre les fins visées par le traitement des données sans avoir à traiter de données sensibles.

26. **Fondement légitime**. Le traitement de données doit s'effectuer dans le cadre des activités de la FAO conformément au mandat et au cadre juridique de l'Organisation. En outre, le personnel n'est autorisé à procéder au traitement de données sensibles que si une telle opération repose sur l'un des fondements légitimes suivants, en fonction des circonstances propres à chaque cas:

i)) le consentement explicite du fournisseur de données; ou *ii*) la protection des intérêts vitaux du fournisseur de données.

27. **Conseils**. Dans le cas du traitement de données sensibles qui sont susceptibles d'exposer les fournisseurs de données et la FAO à des risques importants, il convient de solliciter les conseils de l'Unité de protection des données quant aux mesures à prendre.

Transferts de données

28. **Données reçues par la FAO**. Le personnel doit s'assurer que les données reçues par la FAO lui sont transférées de manière légitime, par exemple à la suite de l'obtention du consentement du fournisseur de données.

29. **Données transférées par la FAO à une tierce partie**. Le personnel n'est autorisé à communiquer des données à une tierce partie qu'à la condition que celle-ci assure un niveau de protection des données égal ou comparable à celui procuré par la FAO conformément à ses propres règles et politiques, y compris la présente politique.

30. **Évaluation du niveau de protection procuré par une tierce partie**. En fonction du niveau de confidentialité attribué aux données, le personnel doit, préalablement à tout transfert, évaluer le niveau de protection qui est fourni par la tierce partie. Cela suppose d'évaluer les mécanismes de sécurité mis en place par la tierce partie aux niveaux technique et organisationnel, les risques et les avantages découlant du transfert, ainsi que tout autre élément d'intérêt en vue du transfert. S'il est établi que la tierce partie ne peut procurer un niveau de protection identique ou comparable aux mesures qui seraient appliquées par la FAO aux données, il convient, en consultation avec l'Unité de protection des données, s'il y a lieu, de définir des mesures de nature à atténuer les risques potentiels, faute de quoi les données ne pourront être transférées.

31. **Arrangements contractuels**. Le transfert de données doit se faire dans le cadre d'un arrangement contractuel écrit ou, le cas échéant, moyennant l'intégration de mécanismes de protection adéquats dans les arrangements contractuels conclus conformément aux règles et lignes directrices applicables à chaque type d'arrangement, par exemple les sections 501, 507 et 701 du Manuel administratif et la Stratégie de la FAO en matière de partenariats avec le secteur privé (liste non exhaustive). Il est possible, dans de rares cas, de déroger à l'obligation d'établir des instruments contractuels, mais toute dérogation doit être raisonnable compte tenu des circonstances, et les motifs la justifiant, y compris les mesures de protection prises, doivent être consignés.

32. **Méthodes de transfert**. Le transfert de données n'est autorisé que par des méthodes qui garantissent la protection adéquate des données. Les méthodes de transfert doivent être déterminées en fonction du niveau de confidentialité des données. Conformément aux dispositions énoncées à la section 1.2.7, le personnel doit, en consultation avec l'Unité de protection des données, s'il y a lieu, veiller à ce que la tierce partie détruise toutes les données transférées ou les renvoie à la FAO une fois que la finalité du transfert a été atteinte.

Demandes soumises par les fournisseurs de données

33. **Types de demandes.** Un fournisseur de données doit pouvoir demander l'accès à ses données qui font l'objet d'un traitement par la FAO, ainsi que leur rectification et leur suppression; il doit également avoir la possibilité de s'opposer au traitement de ses données par la FAO.

a) Accès. Un fournisseur de données peut demander la confirmation que ses données sont actuellement traitées par la FAO et, le cas échéant, demander à y avoir accès.

b) Correction. Un fournisseur de données peut demander que ses données soient corrigées ou mises à jour.

c) Suppression. Un fournisseur de données peut demander que ses données soient supprimées dans l'un des cas suivants: i) les données ne sont plus nécessaires au regard des finalités pour lesquelles elles étaient traitées; ou ii) il retire son consentement au traitement des données et il n'existe aucun autre motif légitime justifiant le traitement.

d) Opposition. Un fournisseur de données peut s'opposer, au moment de la collecte, à ce que ses données fassent l'objet d'un traitement. Le personnel de la FAO est tenu de l'informer des conséquences éventuelles de cette décision, selon qu'il convient[20].

34. **Mise en œuvre.** Le personnel veille à réceptionner les demandes d'accès, de correction, de suppression et d'opposition, à les consigner, les valider et les traiter et à y répondre dans les meilleurs délais et de manière efficace. S'il existe des motifs légitimes d'accéder à une demande, le personnel doit prendre les mesures nécessaires pour y donner suite en totalité ou en partie.

35. **Restrictions**. Après consultation de l'Unité de protection des données, le personnel peut rejeter les demandes des fournisseurs de données ou y appliquer des restrictions compte tenu de *i*) la sécurité des membres du personnel, des tierces parties ou des fournisseurs de données; *ii*) des règles et des directives connexes en matière de confidentialité et de communication d'informations, notamment de la présente politique; ou *iii*) du caractère peu clair ou peu raisonnable de la demande.

36. **Dispositions spéciales**. La présente politique ne limite pas le droit dont dispose le Bureau de l'Inspecteur général, au titre de sa Charte, d'accéder à toutes les données détenues par l'Organisation. Elle ne crée pas non plus de nouveaux droits d'accès aux données gérées et traitées par le Bureau de l'Inspecteur général, le Bureau de la déontologie et le médiateur.

Violations de données

37. Dès qu'il prend connaissance d'une violation de données, le personnel chargé du traitement des données doit consulter son chef de bureau, le Représentant de la FAO ou le Sous-Directeur général/Représentant régional de la FAO, selon qu'il convient. Il faut déterminer si la violation de données expose le fournisseur de données ou la FAO à un quelconque risque. Le cas échéant, on procédera à une évaluation du risque et on établira un compte rendu sommaire de l'analyse, que l'on transmettra à l'Unité de protection des données pour qu'elle donne des indications sur les mesures à mettre en place pour atténuer le risque.

38. Si la violation de données entraîne un risque pour le fournisseur de données, ce dernier sera informé de l'incident et des mesures mises en œuvre pour atténuer le risque, à moins que l'Unité de protection des données estime que la communication de ces informations ne serait pas nécessaire ou souhaitable.

VII. RESPONSABILITÉS ET CONTRÔLE

Comité de contrôle de la protection des données

39. Le Comité de contrôle de la protection des données supervise les activités de protection des données dans l'ensemble de l'Organisation et surveille la mise en œuvre de la présente politique. Il est responsable devant le Directeur général, auquel il fait rapport et donne des indications sur les questions intéressant la protection des données.

[20] À titre d'exemple, si un bénéficiaire de la FAO s'oppose au traitement de ses données dans le cadre d'activités de transferts monétaires, la FAO doit renoncer à traiter les données en question. Si, sans ces données, elle n'est plus en mesure de fournir l'assistance prévue, elle devra en informer le bénéficiaire.

40. Le Comité de contrôle de la protection des données se compose comme suit:

a) président: fonction assurée par un Directeur général adjoint désigné par le Directeur général;

b) membres: Directeur de la Division de la transformation numérique et de l'informatique (CSI), Conseillère juridique (Bureau juridique), [Fonctionnaire chargée des questions de déontologie (Bureau de la déontologie), Directeur de la Division des services logistiques (CSL), Directrice de la Division des ressources humaines (CSH), Directrice de la Division d'appui aux projets (PSS)] et deux membres des bureaux décentralisés désignés par le Directeur général.

41. Le Comité de contrôle de la protection des données fournit des orientations à l'échelle de l'Organisation concernant les activités de protection des données. En particulier, le Comité:

a) surveille la mise en œuvre opérationnelle et l'application de la présente politique et recommande, s'il le juge utile, la mise au point d'instruments complémentaires;

b) reçoit des rapports sur la mise en œuvre et, s'il y a lieu, recommande des modifications qu'il conviendrait d'apporter à la présente politique;

c) procède à l'examen de la présente politique au moins tous les trois ans, en tenant compte des enseignements tirés de sa mise en œuvre et des éventuels changements opérés dans les structures organisationnelles, des politiques complémentaires et de toute autre évolution au sein de la FAO ou du systèmes des Nations Unies susceptible d'influer sur sa mise en œuvre;

d) rend régulièrement compte au Directeur général, de façon à le tenir informé du fonctionnement de la politique et des instruments connexes, ainsi que de la pertinence des mesures en place.

42. Le Comité se réunit au moins deux fois par an, par visioconférence ou en présentiel. Sous réserve du consentement de ses membres, le Comité peut prendre ses décisions par correspondance.

43. Les questions qui sont soulevées au sein du Groupe de coordination sur les données, présidé par l'Économiste en chef, et qui intéressent la protection des données sont portées devant le Comité de contrôle de la protection des données pour qu'il formule des indications.

Unité de protection des données

44. L'Unité de protection des données:

a) fournit des services de secrétariat au Comité de contrôle de la protection des données;

b) veille au respect de la présente politique et fait régulièrement rapport au Comité de contrôle de la protection des données sur le respect et l'application de la présente politique, ainsi que sur toute autre question ayant trait à la protection des données;

c) gère et évalue les demandes des fournisseurs de données;

d) conseille les chefs de bureau, les sous-directeurs généraux/représentants régionaux et les membres du personnel sur les mesures à prendre pour garantir le respect de la présente politique, notamment en ce qui concerne: la marche à suivre pour réaliser une évaluation de l'impact de la protection des données; le traitement de données sensibles susceptibles d'engendrer un risque élevé; l'évaluation de la validité des demandes adressées par les fournisseurs de données; et les violations de données;

e) reçoit des rapports annuels des chefs de bureau et des sous-directeurs généraux/représentants régionaux, selon qu'il convient, sur la mise en œuvre de la présente politique au sein de leur unité.

Chefs de bureau et sous-directeurs généraux/représentants régionaux

45. Les chefs de bureau et les sous-directeurs généraux/représentants régionaux assument les responsabilités suivantes:

a) superviser le traitement des données relevant de leur compétence;

b) agir à titre de point de contact pour les questions de protection de données relevant de leur compétence;

c) solliciter, au besoin, l'avis du Comité de contrôle de la protection des données en cas de questions concernant l'application et l'interprétation de la présente politique;

d) établir des procédures internes pour s'assurer que les données traitées au sein de leur unité le sont conformément à la présente politique;

e) surveiller les activités de traitement des données au sein de leur unité, afin de s'assurer que la présente politique est bien appliquée, et détecter de possibles risques en veillant à déterminer les mesures qui permettraient de les atténuer;

f) attribuer aux différents intervenants au sein de leur unité des responsabilités particulières pour le traitement des données, en tenant compte de la nécessité d'assurer une séparation adéquate des fonctions à toutes les étapes du cycle de vie des données;

g) présenter chaque année à l'Unité de protection des données un rapport sur la mise en œuvre de la présente politique et des instruments connexes.

Personnel

46. Tous les membres du personnel sont individuellement responsables du respect de la présente politique et des instruments connexes. À ce titre, il leur incombe notamment de:

a) déterminer, conformément à la présente politique, pour quelles finalités et par quels moyens les données sont traitées;

b) mettre en œuvre les mesures voulues sur les plans technique et organisationnel, ce qui peut comprendre la conclusion d'instruments contractuels, pour s'assurer que le traitement des données s'effectue conformément à la présente politique, et procéder à intervalles réguliers à l'examen de ces mesures et, au besoin, à leur actualisation;

c) tenir des registres pour les opérations de traitement des données, les accords de partage de données, les demandes et plaintes déposées par les fournisseurs de données, les évaluations de l'impact de la protection des données, les avis de violation de données et autres éléments connexes;

d) prévenir immédiatement leurs supérieurs hiérarchiques en cas de violation de données et coopérer à toute enquête au sujet d'une violation présumée de données;

e) solliciter l'avis de l'Unité de protection des données concernant l'application et l'interprétation de la présente politique.

VIII. EXAMEN ET MODIFICATION

47. Le Comité de contrôle de la protection des données examinera la présente politique 12 mois après sa publication officielle et y apportera les modifications qu'il jugera utiles. Par la suite, il procédera à un examen au moins tous les deux ans, afin de s'assurer que la politique demeure adaptée à sa finalité.

48. Toute modification apportée à la présente politique entre en vigueur à la date de sa publication.

IX. DATE D'ENTRÉE EN VIGUEUR

49. La présente circulaire administrative prend effet immédiatement et annule et remplace la circulaire administrative nº 2013/23 relative à la politique de confidentialité et la circulaire administrative nº 2021/01 relative aux principes en matière de protection des données personnelles.

Annexe I

Définitions

Chiffrement: processus consistant à convertir des données pour les rendre illisibles par toute personne n'ayant pas connaissance d'une information spéciale, telle qu'une «clé de chiffrement» ou un mot de passe.

Consentement: indication par laquelle un fournisseur de données manifeste de façon libre, spécifique, éclairée et univoque son accord au traitement de ses données, cet accord pouvant être implicite, sauf dans le cas de données sensibles, où il doit être explicite.

Cycle de vie des données: toutes les étapes de la vie des données, de la planification jusqu'à la destruction, en passant par la collecte, le stockage et le transfert.

Donnée: toute information provenant de la FAO ou communiquée à la FAO par un fournisseur de données et susceptible de se prêter à un traitement. Au sens de la présente politique, le terme «données» renvoie aux données ayant ou non un caractère personnel, quelle que soit leur forme.

Données anonymisées: informations ne concernant pas une personne physique identifiée ou identifiable ou données personnelles rendues anonymes de telle manière que le fournisseur de données concerné ne soit pas identifiable.

Données non personnelles: toute information de nature financière, technique ou opérationnelle qui ne se rapporte pas à une personne identifiée ou identifiable. Il peut notamment s'agir de rapports financiers, de données commercialement sensibles communiquées par un fournisseur ou de données sensibles sur le plan de la sécurité communiquées par des Membres.

Données personnelles: toute information concernant une personne identifiée ou identifiable. Il peut notamment s'agir de noms, de coordonnées professionnelles et personnelles, y compris électroniques, d'une date de naissance ou de titres de poste.

Données sensibles: données classées par le personnel comme étant sensibles compte tenu de la probabilité que des risques potentiels se matérialisent à la suite de leur divulgation inappropriée, ainsi que des conséquences qui pourraient en découler. Cela comprend notamment les données personnelles révélant l'origine raciale ou ethnique, les opinions politiques ou les croyances religieuses, ainsi que les données génétiques ou biométriques et les données relatives à l'état de santé d'une personne, lesquelles sont considérées par défaut comme des données particulièrement sensibles. Cela comprend également les données non personnelles qui sont sensibles sur le plan commercial ou économique, qui ont trait à la sécurité nationale ou d'autres informations présentant également un caractère sensible qui sont fournies par des Membres de la FAO ou d'autres personnes morales.

Fournisseur de données: personne morale ou physique qui communique des données à la FAO. En vertu de la présente politique, des personnes morales – y compris des Membres de la FAO, des organismes du système des Nations Unies, des organisations intergouvernementales, des organisations non gouvernementales et des entités du secteur privé – peuvent communiquer à la FAO des données non personnelles les concernant ou des données personnelles concernant une personne physique.

Personnel: au sens de la présente politique, désigne les fonctionnaires et le personnel non fonctionnaire engagé par l'Organisation, y compris les consultants, les titulaires d'accords de services personnels, le personnel national affecté à des projets, les volontaires, les stagiaires, ainsi que toutes les autres personnes qui fournissent des services à l'Organisation dans le cadre d'un arrangement contractuel.

Pseudonymisation: traitement appliqué aux données, de sorte qu'on ne puisse plus les attribuer à un fournisseur de données en particulier sans avoir recours à des informations supplémentaires. Ces informations supplémentaires doivent être conservées séparément et font l'objet de mesures techniques visant à garantir que les données personnelles ne peuvent être attribuées à une personne précise.

Tierce partie: toute entité, autre que la FAO et le fournisseur de données, à laquelle des données sont transférées.

Traitement: toute opération ou série d'opérations, automatisées ou non, qui sont exécutées sur des données, notamment la collecte, l'enregistrement, l'organisation, la structuration, le stockage, l'adaptation ou la modification, l'extraction, la consultation, l'utilisation, le transfert (sous forme informatisée, orale ou écrite), la diffusion ou toute autre forme de mise à disposition, la correction ou la destruction.

Violation de données: perte, destruction, altération ou acquisition de données ou accès à des données, y compris sensibles, de manière accidentelle ou non autorisée, ou toute autre utilisation à des fins non autorisées, qui compromet la confidentialité, la sécurité, la disponibilité ou l'intégrité des données.

Annexe II

Exemples d'application des principes FIRST relatifs à la protection des données

Principe	Exemple
Finalité légitime	Dans le cadre d'un projet d'octroi d'aides financières aux bénéficiaires, la FAO compte utiliser les données personnelles provenant des demandes d'aide financière pour envoyer des invitations à participer à une enquête. Conformément au principe relatif à la finalité légitime, il serait souhaitable d'obtenir au préalable le consentement éclairé des personnes concernées pour l'utilisation de leurs données personnelles à cette fin. À la suite d'une catastrophe naturelle, il demeure très difficile de communiquer avec un État Membre ou de se rendre sur son territoire. Devant l'impossibilité de déterminer le type d'assistance à fournir immédiatement ou à plus long terme, la FAO entreprend un vaste exercice de collecte de données dans le but d'évaluer les besoins des personnes touchées. Une fois l'urgence passée, la FAO supprime les données qui ne sont pas nécessaires pour assurer l'assistance technique requise. Lorsqu'elle élabore une proposition de financement à l'intention d'un donateur multilatéral, la FAO collecte toute une série de données, certaines d'entre elles provenant de partenaires du projet. En vertu du principe relatif à la finalité légitime, le bureau de pays ne conserve les données, suivant la classification, que pendant une période déterminée. Lorsqu'il est impossible de déterminer pendant combien de temps il faut conserver les données, le bureau établit une période de conservation initiale, qui sera réévaluée de manière périodique. S'il a communiqué les données à une tierce partie, le bureau prend des mesures raisonnables pour s'assurer que celle-ci supprimera les données.
Intégrité	La FAO prévoit de mettre en œuvre un projet de transferts monétaires en s'appuyant sur les données collectées un an auparavant lors de l'inscription des bénéficiaires. Afin de s'assurer que les données sont toujours exactes, l'Organisation doit vérifier, avant le début de la mise en œuvre du projet, si l'emplacement et la composition des ménages bénéficiaires ont changé durant cette période. Il conviendra de réaliser des contrôles de l'exactitude des données à intervalles réguliers jusqu'à la fin du projet.
Responsabilité	Un bureau régional traite des données pour diverses activités, telles que l'exécution de projets, le recrutement, l'établissement de contrats avec des fournisseurs et l'organisation d'ateliers. Afin de démontrer qu'il se conforme à la politique, il tient à jour des registres pour chaque opération de traitement, dans lesquels sont consignés la finalité, le type de données utilisées, le destinataire des données, le cas échéant, la période de conservation des données et les mesures de sécurité mises en place.
Sécurité	Dans le cadre du Programme de gestion durable de la faune sauvage, la FAO a mis au point un protocole pour les activités de recherche.

	Conformément au principe de sécurité, le protocole prévoit l'obligation d'attribuer un identifiant unique aux personnes, appelé *SubjectID*, ce qui garantit la séparation des données – en n'autorisant l'accès aux données qu'aux enquêteurs principaux – et assure le chiffrement et la protection par mot de passe des fichiers contenant des données personnelles. La FAO a octroyé un contrat à un prestataire de services, qui est chargé d'envoyer aux membres du personnel des alertes sur leurs téléphones personnels pour les prévenir ou les tenir informés de situations potentiellement dangereuses. L'utilisation de ces données personnelles à des fins commerciales par le prestataire de services ou le partage de ces données avec des tierces parties est expressément interdit. En outre, avant que les données ne soient transmises au prestataire, il convient d'évaluer le niveau de protection que celui-ci est en mesure de fournir.
Transparence	Un bureau de pays de la FAO engage des discussions avec le pays hôte dans le but de permettre aux membres du personnel et aux personnes à leur charge remplissant les conditions requises de se faire vacciner contre la covid-19. En application du principe de transparence et au moyen d'un questionnaire prévu à cet effet, le bureau informe les membres du personnel que des données personnelles utiles aux fins de l'administration du vaccin contre la covid-19 seront communiquées aux autorités sanitaires nationales et leur demande leur consentement à cet égard. La FAO reçoit des données de recherche de la part d'un partenaire d'un consortium de recherche. L'Organisation doit indiquer à son partenaire quelles données seront traitées, comment elles seront traitées, à qui elle seront communiquées et quelle devrait être la durée des opérations de traitement. Si le partenaire adresse une demande d'accès aux données, le personnel de la FAO doit s'assurer d'avoir obtenu une preuve satisfaisante de l'identité du demandeur et veiller à ne révéler aucune donnée concernant des tierces parties.