

Commission de statistique  
Trente-huitième session  
27 Février - 2 Mars 2007  
Point 3(j) de l'ordre du jour provisoire  
**Points sur lesquels la Commission de statistique  
devra se prononcer après examen : questions  
de gestion des bureaux nationaux de statistique :  
accès aux microdonnées**

Document de référence  
Original : anglais

**Principes et lignes directrices concernant  
la gestion de la confidentialité et de l'accès  
aux microdonnées**

Note : Ce document s'appuie sur le rapport sur l'Accès aux microdonnées soumis par le comité de réflexion de la CENUE. Il a cependant été rédigé afin de prendre en compte les circonstances touchant d'autres régions du monde.

# Sommaire

<b>I. INTRODUCTION.....</b>	<b>3</b>
<b>II. POURQUOI LES OFFICES NATIONAUX DE STATISTIQUE DEVRAIENT-ILS APPORTER LEUR APPUI A LA COMMUNAUTE DES CHERCHEURS ?.....</b>	<b>4</b>
<b>III. LES PRINCIPES DE BASE.....</b>	<b>6</b>
<b>IV. FONDEMENTS JURIDIQUES ET RESPONSABILITE DE L'ONS EN TANT QUE GARDIEN DE LA CONFIDENTIALITE .....</b>	<b>7</b>
<b>V. MÉTHODES D'APPUI À LA COMMUNAUTÉ DES CHERCHEURS .....</b>	<b>9</b>
<b>VI. GESTION DES DIFFÉRENCES DE POINTS DE VUE ENTRE LES OFFICES NATIONAUX DE STATISTIQUE ET LES CHERCHEURS .....</b>	<b>15</b>
<b>VII. PROBLÈMES DE GESTION ASSOCIÉS À LA PUBLICATION DES MICRODONNÉES .....</b>	<b>19</b>
<b>VIII. QUELQUES QUESTIONS PARTICULIÈRES.....</b>	<b>20</b>
<b>ANNEXE.....</b>	<b>25</b>

# I. INTRODUCTION

1. Historiquement, la question de la protection de la confidentialité s'est essentiellement posée en termes nationaux. Pourtant, compte tenu de la diffusion croissante des données via l'Internet, du vif intérêt suscité pour les comparaisons internationales, et de la collaboration internationale assez intensive qui s'est établie dans ce domaine, au sein de la communauté des chercheurs, cette question revêt également, aujourd'hui, une dimension internationale. Par voie de conséquence, la demande en microdonnées adressée aux pays s'est accrue. L'accès à de telles données n'intéresse pas seulement les chercheurs, mais aussi les organisations internationales, qui souhaitent exploiter les microdonnées dans le cadre de leurs études, en particulier pour effectuer des comparaisons entre pays. De telles études se révèlent généralement importantes pour les pays concernés ; pourtant l'accès aux microdonnées nationales est souvent limité par la crainte que la protection de la confidentialité ne puisse être garantie.

2. Ce rapport s'interroge essentiellement sur la possibilité d'arrêter, à l'échelle internationale, certains principes communs aux fins de la diffusion des microdonnées. Cette question a été régulièrement soulevée par la Conférence des statisticiens européens (CSE) depuis sa session de 2003 et la création d'un comité de réflexion chargé de proposer un premier ensemble de principes et de lignes directrices associées qui soient suffisamment généraux pour être facilement adaptés aux pays participant à la CSE. Le rapport original est disponible sur le site Internet de la CSE.

3. Ce rapport s'appuie largement sur le travail du comité de réflexion, toutefois révisé afin de prendre en compte le contexte des offices nationaux de statistique (ONS) dans d'autres régions du monde.<sup>2</sup> Ce rapport reconnaît que soutenir la recherche est une fonction importante des ONS, et que, en règle générale, les ONS pourraient en faire davantage pour satisfaire les besoins d'accès aux microdonnées des utilisateurs. Il recense les moyens au travers desquels les microdonnées sont actuellement mises à dispositions des utilisateurs nationaux et internationaux, et esquisse des procédures de protection de la confidentialité des personnes interrogées. Ce rapport met l'accent sur la gestion du risque, et retient trois objectifs essentiels :

- a) Faciliter l'accès de la communauté des chercheurs aux microdonnées lorsque les objectifs poursuivis en valent la peine ;
- b) Permettre aux pays d'améliorer leurs dispositifs en matière d'accès aux microdonnées ; et
- c) Encourager une plus grande uniformité des démarches suivies par les pays.

4. Même s'il y a lieu d'espérer que les principes proposés permettront une démarche davantage uniforme, certains pays peuvent ne pas avoir à disposition les systèmes ou les ressources permettant de maintenir les nécessaires dispositions de confidentialité. En effet, les modalités précises d'accès aux microdonnées varient d'un pays à l'autre, en fonction de paramètres tels que le contexte historique, le niveau de développement de l'appareil statistique, la législation, l'attitude du public ou encore la capacité à apporter son soutien à la communauté des chercheurs. Des études de cas se rapportant aux différentes options décrites dans ce rapport sont présentées en annexe (en anglais). Plusieurs pays en développement songent actuellement à revoir leur législation en matière de statistiques. Dans ce contexte de possibles promulgations ou modifications des législations gouvernant la confidentialité et l'accès aux microdonnées, les études de cas annexés à ce rapport peuvent être utiles au choix des modifications appropriées.

---

<sup>2</sup> Certaines parties ont été abrégées, certains paragraphes révisés, et une section sur les autres formes d'accès aux données, spécifiques à certains pays en développement hors d'Europe, a été ajoutée.

## Utilisation de mots clés

5. Offices nationaux de statistique (ONS) : Bien que référence soit faite, dans ce rapport, aux ONS, nombre de pays, en particulier ceux disposant de systèmes décentralisés, comptent plusieurs producteurs de statistiques. C'est pourquoi la référence faite aux ONS dans ce document englobe l'ensemble des producteurs de statistiques officielles.
6. La communauté des chercheurs : Elle comprend ceux qui travaillent dans les institutions académiques, mais aussi les chercheurs travaillant dans les organisations non gouvernementales (ONG) ainsi que dans les organisations internationales. Par ailleurs, certains des chercheurs désireux d'avoir accès aux microdonnées travaillent au sein d'agences financées par le gouvernement, ou au sein d'institutions. L'ensemble de ces chercheurs est considéré comme la « communauté des chercheurs », même si la pertinence des sujets abordés peut varier quelque peu d'un élément à l'autre de la communauté.
7. Le terme microdonnées utilisé dans ce rapport fait référence à des données concernant un individu, un ménage, une entreprise ou toute autre entité. Ces données peuvent être directement recueillies par l'ONS, ou obtenues auprès d'autres sources, notamment de sources administratives.
8. Anonymisé : Ce terme signifie non seulement que les noms et adresses sont supprimés des enregistrements individuels dans l'ensemble de microdonnées considéré, mais aussi que d'autres dispositions sont prises (par exemple, soustraction d'informations telles que des renseignements géographiques, l'âge, le lieu de naissance et la profession) afin d'assurer que l'identification des individus est hautement improbable.

## II. POURQUOI LES OFFICES NATIONAUX DE STATISTIQUE DEVRAIENT-ILS APPORTER LEUR APPUI A LA COMMUNAUTE DES CHERCHEURS ?

9. Dans la plupart des pays, les statistiques officielles sont collectées non seulement à l'usage des pouvoirs publics, mais aussi au profit de la collectivité. La communauté des chercheurs joue un rôle particulièrement important dans le cadre des efforts qui visent à stimuler l'analyse des politiques et encourager le débat sur ces politiques. C'est important, en particulier dans le cas des démocraties pour lesquelles les statistiques officielles peuvent servir à évaluer l'efficacité des politiques et programmes du gouvernement. Elles constituent un reflet de la société, et il est par conséquent dans l'intérêt du public que les données soient analysées et présentées selon différentes perspectives. En outre, une plus large exploitation en ce sens des données d'enquêtes peut offrir un niveau de protection supplémentaire contre les réductions de budget qui touchent ces programmes statistiques.
10. Par ailleurs, assurer aux chercheurs un accès aux microdonnées peut constituer un moyen de mieux rentabiliser l'onéreuse collecte des statistiques officielles, d'en étendre les résultats, de bénéficier d'un précieux regard sur la qualité des données, et sur la manière dont on pourrait améliorer les enquêtes statistiques. Inversement, les chercheurs qui ne peuvent accéder aux données statistiques officielles risquent de recueillir leurs propres données, vraisemblablement à travers des échantillons de taille plus réduite et de qualité inférieure à ceux des enquêtes officielles. Ces collectes engendrent un coût additionnel, à la fois pour les collecteurs de données et pour les répondants, ce qui augmente d'autant le fardeau de réponse imposé à la communauté.

### La perspective pour les offices nationaux de statistique

11. Quoique les ONS reconnaissent sans cesse davantage la valeur ajoutée de la communauté des chercheurs quant à la collecte et au traitement de leurs données, et sont de plus en plus conscients de l'importance que revêt l'appui à la communauté des chercheurs,

il reste toutefois un certain nombre de sujets relatifs à l'accès aux microdonnées que les ONS doivent traiter. Outre la question de la confiance, fondamentale au succès de l'ONS dans son entreprise, se posent celles de l'autorité légale, de la qualité et des coûts.

12. Les ONS doivent conserver la confiance des répondants s'ils veulent que celles-ci continuent de collaborer à leurs collectes de données. La protection de la confidentialité est l'aspect clef de cette confiance. Une autre préoccupation des ONS est de disposer de l'autorité suffisante, soit par le biais d'un mandat légal ou toute autre forme d'autorisation, pour pouvoir appuyer l'accès des chercheurs aux microdonnées.

13. Certains ONS craignent que la qualité de leurs microdonnées ne soit pas suffisante pour qu'elles puissent faire l'objet d'une plus large diffusion. Si la qualité peut s'avérer suffisante pour permettre l'élaboration d'agrégats statistiques, des incohérences entre les résultats de recherches fondées sur les microdonnées et celles basées sur les données agrégées publiées peuvent toutefois apparaître. Dans certains cas, des ajustements ont été apportés aux statistiques agrégées, au stade de l'édition du produit, sans que les microdonnées aient été modifiées. D'aucuns peuvent s'inquiéter que certains chercheurs peu préoccupés de préserver la validité de leur analyse s'aventurent au-delà du niveau de désagrégation que la catégorie d'échantillon peut supporter.

14. Les ONS peuvent également être préoccupés par la question des coûts, non seulement ceux qu'impliquent la création et la documentation de fichiers de microdonnées, mais aussi ceux associés à la mise en place d'instruments d'accès et de protection, ainsi qu'au soutien et à l'autorisation d'enquêtes réalisées par la communauté des chercheurs ; en effet, les nouveaux utilisateurs de leurs fichiers de données ont besoin d'aide pour s'y retrouver dans les structures de fichier complexes et les définitions de variables. Bien que les coûts en question soient à la charge des ONS, ceux-ci ne disposent généralement pas d'enveloppe budgétaire pour financer les travaux supplémentaires à entreprendre dans ce contexte. Quant aux chercheurs, ils n'ont généralement pas les moyens d'assumer une part substantielle de ces coûts.

15. Permettre un accès international présente parfois un problème bien plus sérieux que l'accès purement national, à cause des restrictions légales. Toutefois, pour les ONS de nombre de pays en développement, les ressources et les capacités à offrir des données analytiques ou non standard manquent ou, au mieux, sont limitées. Ainsi, ce type de résultats doit être produit par des chercheurs résidant hors du pays. Dans le cas contraire, il existe un fort risque que les données d'enquête, souvent collectées à hauts coûts, soient sous-utilisées.

### **La perspective de la communauté des chercheurs**

16. Du point de vue de la communauté des chercheurs, il faudrait que le soutien de la recherche faisant appel aux microdonnées représente un élément important de n'importe quel système statistique officiel. Les avantages qui en découlent sont notamment les suivants:

- a) Les microdonnées permettent aux décideurs de poser et d'analyser des questions complexes ;
- b) En ayant accès aux microdonnées, les analystes peuvent calculer des effets marginaux plutôt que de simples moyennes ;
- c) De manière générale, un large accès aux microdonnées permet de reproduire des recherches importantes ;
- d) L'accès aux microdonnées à des fins de recherche, et les réactions qu'il en résulte, peuvent favoriser l'amélioration de la qualité des données ;
- e) L'accès aux microdonnées élargit la gamme des produits élaborés à partir des statistiques recueillies et, par conséquent, la rentabilité globale des collectes de données.

17. Les ONS peuvent jouer un rôle très utile en devenant pour la communauté des chercheurs une source de données de grande qualité, acceptée et faisant autorité. En l'absence d'une telle source digne de confiance, les chercheurs n'ont autre choix que d'utiliser différents ensembles de données pour analyser certains sujets particuliers. Toutefois, les chercheurs pensent que les ONS se sont généralement montrés trop conservateurs en ce qui concerne l'accès à leurs microdonnées. Ils précisent qu'ils ne sont pas intéressés à identifier des individus et que par conséquent les coûts de protection des microdonnées pourraient être évités.

### III. LES PRINCIPES DE BASE

18. Le sixième des Principes fondamentaux de la statistique officielle de l'Organisation des Nations Unies (ONU) est explicite sur la question de la confidentialité:

«Les données individuelles collectées pour l'établissement des statistiques par les organismes qui en ont la responsabilité, qu'elles concernent des personnes physiques ou des personnes morales, doivent être strictement confidentielles et ne doivent être utilisées qu'à des fins statistiques.»

N'importe quel principe d'accès aux microdonnées doit être conforme à ce Principe fondamental.

19. Les principes ci-après devraient régir la gestion de la confidentialité des microdonnées. Chacun d'eux est examiné plus en détail dans les paragraphes qui suivent:

- a) Principe 1 : On peut exploiter les microdonnées réunies dans le cadre de la statistique officielle, aux fins de l'analyse statistique, en vue d'étayer des recherches pour autant que la confidentialité de ces données soit protégée ;
- b) Principe 2 : Les microdonnées ne devraient être communiquées qu'à des fins statistiques ;
- c) Principe 3 : La fourniture de microdonnées devrait s'effectuer en accord avec les dispositions juridiques et autres qui garantissent la confidentialité des microdonnées communiquées ;
- d) Principe 4 : Il faudrait assurer la transparence des modalités d'accès des chercheurs aux microdonnées, ainsi que des utilisations et utilisateurs de microdonnées, et les rendre publics.

20. Le Principe 1 ci-dessus ne constitue pas une obligation de diffuser les microdonnées, et la communication des microdonnées aux chercheurs n'est pas incompatible avec le sixième Principe fondamental de l'ONU tant qu'il demeure impossible d'identifier les données se rapportant à un individu. D'autres considérations (la qualité des microdonnées, par exemple) peuvent rendre inopportun l'accès aux microdonnées. Il se peut aussi qu'il soit inapproprié de fournir des microdonnées à des personnes ou institutions bien précises. C'est à l'ONS qu'il devrait appartenir de décider s'il convient ou non de fournir les microdonnées.

21. Dans le cas du Principe 2 susmentionné, si l'utilisation escomptée des microdonnées semble ne pas suivre des fins statistiques ou analytiques, l'accès aux microdonnées ne devrait pas être accordé. Dans le cas des exploitations statistiques ou analytiques, l'objectif poursuivi par les chercheurs et autres agences statistiques consiste à établir des statistiques se rapportant à un groupe (qu'il s'agisse de personnes physiques ou morales). Cela comprend l'élaboration d'agrégats statistiques de nature diverse, l'établissement de distributions statistiques, l'ajustement de modèles statistiques, ou l'analyse de différences statistiques entre sous-populations. Ces utilisations pour des recherches dont le but est d'éclairer la prise de décision sont au bénéfice de la société, et devraient à ce titre être

différenciées des utilisations administratives. A l'inverse, le but recherché dans l'utilisation administrative des données est d'obtenir des informations sur une personne physique ou morale en vue de prendre une décision susceptible de profiter ou de nuire à un particulier, comme par exemple des demandes de données individuelles par décision judiciaire. Afin de remporter la confiance du public dans le système statistique officiel, ces demandes, incompatibles avec ce principe, devraient être systématiquement rejetées, au risque de voir la collaboration des personnes interrogées s'étioler et la qualité des statistiques altérée. Des comités d'éthique - ou tout système analogue - peuvent prêter leur concours lorsque le doute concernant l'accessibilité aux microdonnées s'installe.

22. En ce qui concerne le Principe 3, il faudrait idéalement mettre en place des dispositions juridiques visant à protéger la confidentialité avant de publier quelque microdonnée que ce soit. Toutefois, les dispositions légales doivent être complétées par des mesures administratives et techniques tendant à réglementer l'accès aux microdonnées et à assurer que les données personnelles ne puissent être divulguées. L'existence et la visibilité de telles modalités (qu'elles soient consacrées par la loi ou par des règlements supplémentaires, des arrêtés, etc.) sont indispensables pour susciter du public une plus grande confiance dans le bon usage qui sera fait des microdonnées.

23. Le Principe 4 est important pour rassurer le public quant au fait que les microdonnées sont exploitées à bon escient et pour montrer que les décisions touchant à la diffusion des microdonnées sont prises sur une base objective. Il appartient à l'ONS de déterminer si les microdonnées peuvent être divulguées, selon quelles modalités et à quel utilisateur. Néanmoins, il faudrait assurer la transparence de ses décisions. Le site Web de l'ONS constitue un instrument efficace pour garantir le respect des règles établies mais aussi pour fournir des informations sur les modalités d'accès aux rapports d'études fondées sur les microdonnées mises à disposition.

24. Pour que les ONS récoltent les meilleurs fruits de leur partenariat avec la communauté des chercheurs, il faudrait que des arrangements soient conclus avec ceux à qui l'accès aux microdonnées est donné, afin de s'assurer que les produits statistiques de leur travail soient transmis en retour à l'ONS. Les utilisateurs de microdonnées devraient également être encouragés à faire remonter de manière constructive, une fois leur analyse des données effectuée, leur opinion quant à leur qualité. De telles informations peuvent s'avérer précieuses lorsqu'il s'agit d'élaborer de futures collectes.

#### **IV. FONDEMENTS JURIDIQUES ET RESPONSABILITE DE L'ONS EN TANT QUE GARDIEN DE LA CONFIDENTIALITE**

25. Il est capital que la diffusion des microdonnées s'appuie sur des fondements juridiques, ainsi qu'il ressort du Principe 3 (voir le chapitre III du présent document), et ce pour plusieurs raisons:

- a) Pour gagner la confiance du public dans les dispositions établies - en d'autres termes qu'il sache que des contraintes juridiques déterminent ce qui est ou non autorisé ;
- b) Pour qu'une compréhension mutuelle s'instaure entre les ONS et les chercheurs en ce qui concerne ces dispositions ;
- c) Pour qu'une plus grande cohérence soit assurée dans le traitement des projets de recherche ; et
- d) Pour que soient mis en place les fondements d'un système visant à sanctionner les infractions.

La réputation de l'ONS sera compromise s'il n'existe pas une forme quelconque d'autorité s'exerçant sur la divulgation des microdonnées, même anonymisées.

26. Il n'est pas indispensable que les dispositions en question soient énoncées dans une loi. Les détails de la protection des microdonnées peuvent plus aisément être précisés par le biais de règlements, d'arrêtés, etc., qui n'en ont pas moins un effet juridique. En l'absence de dispositions légales, l'une ou l'autre forme d'autorisation est essentielle. Des dispositions spéciales devraient être mises en place hors de l'ONS (par le ministère de la justice, par exemple). Les dispositions devraient comprendre un engagement ou un accord signé à la fois par le(s) chercheur(s) ayant accès aux données et un cadre supérieur de l'institution. L'engagement devrait couvrir les questions énumérées dans le paragraphe 42, et devrait être consultable par le public de sorte qu'aucune suspicion à propos des dispositions ne soit rendue possible.

27. Au minimum, il faudrait que la divulgation de microdonnées bénéficie du soutien d'une forme quelconque d'autorité. Les dispositions juridiques peuvent ne pas être possibles dans certains pays. Dans pareil cas, il faudrait donc alors instituer une autre forme quelconque de dispositions administratives. Il faudrait également que les autorités responsables des questions de confidentialité, dans les pays où il en existe, donnent leur accord aux dispositions juridiques (ou autres) avant que celles-ci ne soient consacrées par la loi. En l'absence d'autorité de cette nature, il peut y avoir des ONG qui exercent une fonction de «surveillance» dans le domaine de la confidentialité. Il serait judicieux d'obtenir qu'elles souscrivent à toute forme de disposition juridique ou autre mise en place, ou tout au moins de répondre à n'importe quelle inquiétude sérieuse qu'elles pourraient avoir.

28. Il importe que la législation (ou l'autorisation) prenne en compte les aspects suivants:

- a) Ce qui est ou non autorisé, et à quelles fins;
- b) Les conditions de la divulgation; et
- c) Les conséquences d'un non-respect de ces conditions.

29. Il faudrait que des accords soient scellés, non seulement avec les chercheurs mais aussi avec les hauts fonctionnaires des institutions qu'ils représentent. Toute infraction devrait être sévèrement sanctionnée. Dans le cas où aucune action en justice ne peut être intentée, d'autres dispositions peuvent certainement être prises. Trois possibilités existent :

- a) interdire tout futur accès au chercheur en question et à son institution ;
- b) informer la haut fonctionnaire de l'institution en question de l'infraction, et exiger que des sanctions administratives soient prises à l'encontre du chercheur ;
- c) refuser l'accès à l'ensemble de la communauté des chercheurs durant une période donnée, de sorte que les institutions et leur personnel se sentent conjointement responsables de la protection de la confidentialité.

30. Il faudrait que les ONS considèrent sérieusement l'ampleur de leur responsabilité en tant que gardiens de la confidentialité des unités individuelles présentes dans leurs ensembles de données, avant d'entreprendre quelconques arrangements en vue de permettre l'accès aux microdonnées au public, aux chercheurs ou aux organisations internationales. Une étape essentielle de ce processus est l'établissement d'une relation de confiance avec les personnes interrogées, les convainquant que les données à caractère confidentiel seront utilisées conformément au sixième Principe fondamental de la statistique officielle de l'ONU. Cette étape est particulièrement déterminante dans le cas des pays pour lesquels la distinction entre utilisation statistique et non statistique des microdonnées ne bénéficie pas d'une solide tradition, ou ne s'appuie sur aucune législation.



## V. MÉTHODES D'APPUI À LA COMMUNAUTÉ DES CHERCHEURS

31. Il y a diverses méthodes qu'un ONS peut mettre en œuvre pour appuyer les travaux de recherche :

### (i) Produits statistiques utilisables en dehors de l'ONS

#### Flux de diffusion

#### Notes

---

Tableaux statistiques et cubes de données	Il peut s'agir à la fois de tableaux types et de tableaux spéciaux (ou, sinon, d'analyses spéciales) établis à la demande du chercheur. Certains services publient à présent des matrices très détaillées, appelées «cubes de données», que les chercheurs peuvent manipuler en fonction de leurs propres besoins. Toutefois, si ces matrices sont très détaillées, le risque qu'elles présentent du point de vue de la confidentialité peut être du même ordre que celui qui se rattache aux microdonnées.
---	---

Fichiers de microdonnées anonymisés - Fichiers à usage public	Il s'agit de fichiers de microdonnées destinés à l'usage du grand public en dehors de l'ONS. Ils ont été anonymisés et sont souvent divulgués sur un support tel qu'un cédérom, parfois par le biais d'une archive de données. Le degré de protection de la confidentialité qu'offrent les fichiers à usage public devrait être tel qu'aucune identification n'est possible, même lorsqu'il sont rapprochés d'autres fichiers de données.
---	---

Fichiers de microdonnées anonymisés - Fichiers sous licence	Les fichiers sous licence sont aussi anonymisés mais se distinguent des fichiers à usage public en ce sens que leur emploi peut être réservé à des chercheurs autorisés. Même s'il est annoncé que ces fichiers sont librement mis à la disposition du public, ils ne sont pas diffusés avant qu'un engagement ou un contrat ne soit signé par le chercheur.
---	--

---

### (ii) Un guichet par le biais duquel les chercheurs peuvent soumettre leur demande de données

#### Service

#### Notes

---

Moyens d'accès à distance	Des dispositions pour autoriser les chercheurs à élaborer des produits statistiques à partir de fichiers de microdonnées par le biais de réseaux informatiques, sans que les chercheurs ne «voient» effectivement les microdonnées. Grâce aux contrôles supplémentaires que les moyens d'accès à distance permettent d'exercer et au fait que les microdonnées ne quittent pas effectivement l'ONS, on peut assurer l'accès à des microdonnées plus détaillées.
---------------------------	---

---

(iii) Dispositions autorisant les chercheurs à travailler dans les locaux de l'Office national de statistique

Service	Notes
Laboratoires de données	Accès sur place à des microdonnées plus aisément identifiables, généralement <i>via</i> un circuit de vérification strict et sous la supervision de l'ONS. L'accès à des données plus détaillées crée certaines complications pour le chercheur dans la mesure où il est tenu de travailler dans les locaux ou une antenne de l'ONS.

32. Un point sur lequel il semble important d'insister est que l'anonymisation des fichiers de microdonnées n'est pas seulement assurée par la suppression des noms et adresses, mais aussi par l'adoption de dispositions complémentaires (par exemple, soustraction d'informations telles que les détails géographiques). Cela revient à éliminer toute possibilité d'identification immédiate. Plus la population est restreinte, plus la possibilité d'identification est forte, et toute divulgation d'information par inadvertance peut avoir des conséquences très sérieuses. Il faudrait également porter une attention particulière aux populations à la distribution fortement asymétrique pour des caractéristiques spécifiques ou en présence de valeurs aberrantes.

33. Quand bien même l'anonymisation et l'adoption d'autres dispositions seraient appliquées afin d'assurer l'improbabilité de l'identification des individus lorsqu'ils sont considérés séparément, certains fichiers pourraient malgré tout contenir des données qui rendent potentiellement possible la mise en correspondance avec d'autres fichiers de microdonnées des secteurs public comme privé, et, par voie de conséquence, l'identification d'individus. Des études ont montré que l'appariement statistique des fichiers de microdonnées des ONS avec des fichiers existants pouvait mener à des correspondances exactes. Leur nombre peut être relativement significatif, selon le niveau de détail des informations disponibles dans le fichiers de microdonnées de l'ONS. En termes relatifs, plus la taille des pays se réduit, plus le nombre de cas uniques augmente. C'est l'une des raisons pour lesquelles un engagement préalable doit être requis avant toute fourniture de données. Ces risques peuvent cependant être réduits si des techniques de bruitage aléatoire ou d'échange de données sont employées par l'ONS.

### **Tableaux statistiques et cubes de données**

34. Les tableaux statistiques restent le moyen le plus économique de satisfaire bon nombre de besoins en matière de recherche. Il ne faudrait donc pas sous-estimer leur importance. Avec l'apparition des cubes de données (des tableaux multidimensionnels très détaillés), l'utilité des tableaux statistiques aux fins de la recherche s'est accrue car les chercheurs peuvent manipuler ces cubes de données en fonction de leurs propres besoins.

35. Des problèmes de confidentialité continuent de se poser en ce qui concerne les tableaux statistiques et cubes de données, et la plupart des dispositions législatives en matière de statistique précisent qu'il n'est interdit de divulguer des données identifiables sous la forme de tableaux statistiques. Toutefois, les données sont confidentialisées avant publication. Il existe des systèmes logiciels qui permettent de confidentialiser les tableaux statistiques, et les méthodes ne cessent de s'améliorer. On les désigne souvent sous le nom de méthodes de non-divulgation.

### **Fichiers de microdonnées anonymisés – Fichiers à usage public**

36. Les chercheurs considèrent qu'ils retirent un service très utile de ces fichiers. Toutefois, compte tenu des possibilités accrues de rapprochement des données, on pourrait

évoluer vers une réduction du volume des données disponibles sous la forme de fichiers à usage public et s'appuyer davantage sur des fichiers de microdonnées anonymisés, des services tels que les moyens d'accès à distance et les laboratoires de données pour permettre aux chercheurs d'avoir accès à l'information. Les fichiers sous licence reposent sur le pari que les chercheurs honoreront l'engagement qu'ils ont pris ou le contrat qu'ils ont signé de ne pas chercher à identifier les individus ou entités auxquels se rapportent les données. Ce type d'engagement fait en général partie intégrante de la publication de fichiers de microdonnées anonymisés (voir la section suivante).

37. Bien que les ONS garantissent généralement un accès égal à tous les utilisateurs de leurs statistiques, ce principe ne prévaut pas nécessairement en ce qui concerne les microdonnées. Une attitude différente peut être adoptée à l'égard d'utilisateurs qui ne sont pas pleinement accrédités en qualité de chercheurs ou qui ont accès à des bases de données par le biais desquelles ils pourraient facilement apparier les fichiers de microdonnées anonymisés. Dans le but de renforcer la crédibilité des ONS et de contraindre les utilisateurs à se conformer aux règles, il serait utile d'échanger les informations à propos des infractions commises par la communauté des chercheurs, et d'interdire tout accord de divulgation de données avec les institutions impliquées.

38. L'accès aux fichiers à usage public est délibérément large, ce qui est très apprécié dans les pays où il en existe et où ils sont amplement exploités. Les chercheurs ont souligné l'importance des fichiers à usage public, mais il ne faut pas qu'ils s'attendent à ce que tous les pays publient de tels fichiers. Une personne qui y est disposée pourrait n'avoir aucune difficulté à identifier certains individus par le biais d'un appariement avec d'autres bases de données. Avant de divulguer les données de fichiers à usage public, il convient d'étudier de près les conditions dans lesquelles ceux-ci sont diffusés pour mieux gérer les risques de violation de la confidentialité. Par exemple, un engagement juridiquement contraignant peut constituer l'une des conditions d'accès. Il devrait être possible de mettre en place ce genre de disposition dans les cas où un engagement préalable doit être signé, même lorsque l'accès au fichier à usage public s'effectue *via* l'Internet.

39. De manière générale, le risque sera beaucoup plus important dans les pays peu peuplés et dans ceux dotés de registres de la population. Le risque d'identification peut être réduit par l'utilisation de techniques telles que l'échange ou la perturbation de données. Ces techniques sont par exemple fréquemment utilisées aux Etats-Unis. L'inconvénient toutefois de telles méthodes est qu'elles peuvent réduire l'utilité des microdonnées sous-jacentes.

40. Il existe une abondante documentation sur les méthodes permettant d'anonymiser les fichiers de microdonnées. On trouve un bon résumé en la matière dans Willenburg, L. & de Waal, T (2001), *Elements of Statistical Disclosure Control*. Le progiciel  $\mu$ -ARGUS sert à protéger les microdonnées de la divulgation. Il propose plusieurs techniques d'anonymisation des fichiers de microdonnées. Il est de bonne pratique de requérir l'avis d'un spécialiste pour savoir si un fichier de microdonnées est suffisamment anonymisé ou non. Cette précaution ne devrait pas causer de retard susceptible d'empêcher de publier les données à temps.

### **Fichiers de microdonnées anonymisés – Fichiers sous licence**

41. Il s'agit d'un système qui autorise une certaine classe d'utilisateurs, détenteurs d'une autorisation obtenue après engagement contractuel ou l'obtention d'une licence, à se servir de fichiers de microdonnées. Bien que ces fichiers aient été anonymisés et que les individus présents dans ces fichiers ne puissent être ni repérés ni identifiés, leur identification peut être rendue possible par la mise en correspondance avec d'autres fichiers. C'est pourquoi une licence est nécessaire. La licence est assortie de certaines conditions, qui peuvent être énoncées dans un engagement ou un contrat signé par le chercheur ou l'organisme duquel il relève. Les conditions peuvent varier d'un pays à

l'autre, voire d'un chercheur à l'autre, selon le projet de recherche et, éventuellement, l'entité à laquelle le chercheur est rattaché.

42. Les conditions prévues peuvent notamment être les suivantes:

- a) Un accord selon lequel le chercheur s'engage à respecter les conditions de publication ;
- b) Un engagement à ne pas chercher à identifier des individus ou des organisations ;
- c) La certification que l'information ne servira qu'à des fins statistiques ou pour la recherche ;
- d) L'engagement de ne pas communiquer les microdonnées à d'autres personnes ;
- e) la promesse de rendre les microdonnées à l'ONS dès l'achèvement du projet de recherche ; et
- f) La renonciation à apparier les statistiques avec d'autres bases de données sans autorisation.

43. Il est de bonne règle que ce genre d'engagement s'appuie sur un certain fondement juridique, par exemple qu'il soit incorporé dans une législation habilitante. Ainsi, des mesures juridiques pourraient être prises à l'égard d'auteurs d'infractions. Cela n'empêche pas l'adoption d'autres mesures s'agissant des infractions, telles que le refus de fournir d'autres services au chercheur concerné et/ou éventuellement à l'organisme dont il relève. Ces questions sont traitées au chapitre VII du présent document.

44. Il devrait être possible de diffuser plus de données par le biais de fichiers sous licence que par l'intermédiaire de fichiers à usage public, dans la mesure où l'on peut aussi se reposer sur l'engagement pris par le chercheur d'assurer la protection de la confidentialité des données. Autrement dit, ce moyen de diffusion est plus fiable dans les cas où certaines données sont potentiellement identifiables par appariement avec d'autres fichiers.

### **Microdonnées pour lesquelles l'identification est possible**

45. Certains pays diffusent à l'extérieur, à des fins statistiques ou de recherche, des fichiers de microdonnées contenant des données susceptibles d'être identifiées, mais toutefois sous accords de licence stricts. Il faudrait que ces accords de licence comprennent les conditions sous lesquelles les données peuvent être utilisées, et la procédure devrait être spécifiquement bordée par la législation. Une procédure stricte est nécessaire pour conserver la confiance des répondants en particulier et du public en général. Les moyens d'accès à distance et les laboratoires de données sont d'autres moyens de traiter ce type de situation.

### **Moyens d'accès à distance**

46. Ces moyens de diffusion revêtent une importance croissante, mais la manière dont ils sont mis en œuvre varie sensiblement d'un pays à l'autre. Leur caractéristique principale réside dans le fait que les chercheurs n'ont pas accès aux microdonnées proprement dites, mais peuvent faire exécuter à distance - par le truchement d'Internet - les tâches nécessitant ces microdonnées. Fréquemment, un arrangement contractuel a été conclu à cette fin entre l'ONS et le chercheur ou l'organisme auquel ce dernier est rattaché.

47. Il existe deux types fondamentaux de système d'accès à distance:

- a) L'exécution à distance, qui permet à un chercheur de soumettre un programme et de recevoir ultérieurement le produit par courriel ;
- b) Les services à distance, grâce auxquels le chercheur exécute lui-même l'analyse et voit immédiatement la réponse s'afficher sur l'écran.

48. À titre d'exemple, Statistique Canada fournit aux chercheurs des fichiers de microdonnées fictifs et les autorise à soumettre des demandes d'exploitation en relation avec le fichier complet via le réseau informatique. Il traite les demandes hors ligne et expédie les résultats par le biais de réseaux informatiques après avoir effectué un contrôle de la confidentialité des données. Bien qu'il existe des dispositions semblables au Bureau australien de statistique, des différences sont notables. Les fichiers de microdonnées sont confidentialisés pour empêcher toute identification spontanée avant d'être rendus accessibles à distance. Toutefois, les exploitations expérimentales sont autorisées en relation avec des fichiers accessibles à distance et un petit nombre d'enregistrements unitaires non identifiables peuvent être téléchargés dans le but d'étudier les valeurs aberrantes, etc. Ce produit est contrôlé avant d'être expédié aux chercheurs. Le système assure actuellement une exploitation par lots mais la mise au point d'une version interactive est en cours. Les modalités établies à Statistics Denmark sont encore différentes. Il s'agit d'un système en ligne grâce auquel les chercheurs peuvent effectuer des analyses en regard du fichier de microdonnées complet. Les modalités sont conçues de telle manière que le téléchargement des microdonnées elles-mêmes est impossible. Pour mieux gérer les risques, elles font plutôt appel aux accords conclus par les institutions et aux sanctions (notamment le refus de tout accès futur) si les règles ne sont pas respectées.

49. Bien qu'ils ne soient jusqu'ici en place que dans quelques pays, et quoique les modèles et démarches varient, comme illustré ci-dessus, l'expérience des moyens d'accès à distance est, à ce jour, généralement positive. Du point de vue des coûts, les moyens d'accès à distance sont préférables aux laboratoires de données (voir ci-après) puisque l'accès sous contrôle dans un tel système exige moins de main-d'œuvre que l'utilisation supervisée dans le cadre des laboratoires de données.

50. Si un tel système n'élimine pas entièrement le risque d'identification, un accord sous l'une ou l'autre forme doit néanmoins être signé par les chercheurs, pour faire en sorte qu'ils soient pleinement conscients de leurs obligations. Il est de bonne règle de réserver l'accès aux données aux chercheurs qui ont signé un accord quelconque énonçant les conditions d'accès. La formation revêt également son importance, de même que le suivi et le contrôle périodiques de l'utilisation de ces moyens.

### **Laboratoires de données**

51. Les laboratoires de données existent depuis de nombreuses années dans quelques ONS et assurent avec efficacité la protection contre le risque d'identification tout en permettant aux chercheurs d'avoir notamment accès à des ensembles de données pour lesquels il n'est pas possible de diffuser un fichier de microdonnées confidentialisé. Ils vont néanmoins de pair avec des conditions d'accès pour garantir un degré de protection suffisant. La principale critique formulée à l'encontre des laboratoires de données concerne leur manque de commodité pour le chercheur qui se voit, par exemple, parfois contraint de se servir de logiciels d'analyses de données avec lesquels ils n'est pas familier. Leur gestion est également coûteuse pour les ONS, comparée à d'autres solutions.

52. Certains ONS ont aménagé de nouveaux locaux pour héberger les laboratoires de données dans des endroits davantage accessibles pour les chercheurs (parfois connus sous le nom de «Centres de recherche de données»). Mais cette solution peut également s'avérer coûteuse, à moins que des fonds spécifiques soient alloués à l'ONS.

53. Quelles sont les conditions essentielles d'accès aux microdonnées par le biais de laboratoires de données? Celles-ci pourraient inclure: a) la fourniture d'une documentation attestant de l'intérêt général qui découlera de la recherche, b) une description de l'accessibilité des résultats par le public, c) des preuves de la bonne foi des chercheurs, d) un engagement juridiquement contraignant, et e) des exigences concernant la supervision exercée par l'ONS.

## **Recrutement d'un chercheur en qualité d'agent temporaire d'un ONS**

54. Un autre moyen de veiller à ce que les chercheurs aient accès aux microdonnées consiste à les recruter comme agents temporaires d'un ONS, et de les soumettre aux mêmes règles relatives à la confidentialité que le reste du personnel. Il ne faudrait avoir recours à cette formule que si l'activité du chercheur représente un véritable apport au travail de l'ONS, sinon on pourrait n'y voir qu'un simulacre. Si un arrangement de cette nature était mis en place et que le public l'apprenne, la crédibilité de l'ONS en souffrirait.

55. Le chercheur peut être associé aux travaux de l'ONS à l'initiative de ce dernier, s'il considère que cette personne est susceptible de le faire bénéficier de compétences particulières et d'accroître l'utilité de l'ensemble de données. A l'inverse, l'initiative peut venir du chercheur. Mais, dans ce cas, l'ONS doit jauger et accepter la proposition selon ses mérites et l'incorporer aux activités de son programme de travail. Il est plus facile de prouver que les chercheurs apportent leur concours à l'ONS si les résultats de leurs travaux sont publiés par le service (même si c'est sous une appellation quelque peu différente de celle de ses produits usuels). Bien entendu, il y aura des retombées pour les chercheurs participant à ce type d'arrangement, et il y peut être convenu que les résultats seront aussi publiés ailleurs (certainement après validation par l'ONS).

## **Données se rapportant aux entreprises**

56. Les données des entreprises, notamment celles des exploitations agricoles, soulèvent quelques problèmes particuliers. Les entreprises, et en premier lieu les plus grandes d'entre elles, sont plus aisément identifiables qu'un ménage ou un individu, surtout de manière spontanée, parce que la distribution de leurs caractéristiques est beaucoup plus asymétrique. Egalement, dans certaines enquêtes auprès des entreprises, les plus grandes sont systématiquement sélectionnées. Dans certains pays, les bases de données sur les entreprises sont souvent plus accessibles, ce qui permet le rapprochement des données. En outre, il arrive que bon nombre de chercheurs fassent également office de consultants auprès des entreprises et, même en bonne et due forme, l'accès de ces chercheurs aux microdonnées des entreprises peut s'avérer incompatible avec leur mission de consultant. Par ailleurs, les pays peuvent être confrontés à des questions de compétitivité économique (voire de sécurité) du fait qu'ils échangent des données d'entreprises identifiables avec des chercheurs d'autres pays.

57. Pour ce qui est de l'accès des chercheurs aux données, la principale différence entre les données se rapportant aux ménages ou aux personnes, d'une part, et les données d'entreprises, d'autre part, tient au fait que les flux de diffusion assurant la plus grande protection concernent surtout les données des entreprises.

58. Quant aux moyens de diffusion:

- a) Les tableaux statistiques restent un moyen intéressant de diffusion de données; toutefois, comme ils présentent un risque d'identification plus élevé dans ce cas, ils ne contiennent généralement pas de données très détaillées lorsqu'il s'agit d'entreprises ;
- b) Les fichiers de microdonnées anonymisés peuvent n'être pertinents que pour les plus petites entreprises. Dans certaines études, ce groupe intéresse particulièrement les chercheurs. Il n'en reste pas moins que quelques données (par exemple, des données financières) devront être «altérées» pour qu'elles ne puissent pas être mises en correspondance avec d'autres bases de données (par exemple, des données fiscales). Une autre solution consiste à présenter les données sous la forme de fourchettes de valeurs. En tout état de cause, les fichiers de microdonnées anonymisés n'auront probablement qu'une utilité limitée ;
- c) Pour des raisons analogues, les moyens d'accès à distance peuvent n'être utiles que dans le cas des fichiers de microdonnées concernant les plus petites entreprises. L'utilisation de ces systèmes permettra tout au moins aux ONS de

contrôler le risque de rapprochement des données, afin qu'il ne soit pas forcément nécessaire d'«altérer» les données pour en protéger la confidentialité. Cependant, si les grandes entreprises sont prises en compte, il peut s'avérer difficile de confidentialiser les produits publiés, même si les chercheurs ne peuvent pas avoir directement accès aux microdonnées ;

- d) Les laboratoires de données sont sans doute le mode le plus pertinent d'accès aux fichiers de microdonnées des entreprises.

59. Des microdonnées pourront sans doute être communiquées pour certaines recherches avec l'assentiment des entreprises concernées

## **VI. GESTION DES DIFFÉRENCES DE POINTS DE VUE ENTRE LES OFFICES NATIONAUX DE STATISTIQUE ET LES CHERCHEURS**

60. La culture et les valeurs des chercheurs sont très différentes de celles d'un ONS. Alors que les chercheurs considèrent souvent que les « contrôles » inhérents aux accords d'accès aux microdonnées constituent une bureaucratie inutile, une violation de la confidentialité a, pour l'ONS, de terribles conséquences. Si les personnes interrogées nourrissent la croyance ou le sentiment que l'ONS n'est pas en mesure d'assurer la confidentialité des données, ils seront moins enclins à coopérer ou à fournir des données précises. Même un incident isolé, en particulier s'il s'accompagne d'une forte couverture médiatique, peut avoir un impact significatif sur la collaboration des personnes interrogées et, par voie de conséquence, sur la qualité des statistiques officielles.

### **Comment pourrait-on concilier les perspectives différentes des ONS et des chercheurs?**

61. Ce sont les ONS qui pourront, avec le plus d'efficacité, concilier ces perspectives différentes, en passant d'une stratégie d'évitement des risques à une stratégie de gestion des risques.

62. De toute évidence, des risques existent et il faut les gérer. La rapide expansion des bases de données, contenant des informations sur des personnes identifiables, signifie qu'il est pratiquement impossible d'éliminer complètement le risque d'identification d'un nombre important de personnes à travers le rapprochement des données, même en supprimant leurs noms et adresses, surtout si la structure du ménage est indiquée dans les fichiers. Les bases de données en question sont pour beaucoup tenues par le secteur privé qui en contrôle généralement l'emploi de manière moins stricte que le secteur public. En outre, les progrès techniques facilitent le rapprochement des données, qu'il s'agisse d'une correspondance exacte ou de méthodes d'appariement statistique (susceptibles de conduire, exceptionnellement, à des correspondances exactes). En substance, l'évitement des risques signifie que les microdonnées identifiables ne doivent pas quitter les locaux de l'ONS, à moins que d'autres mesures tels que l'échange ou la perturbation de données soient mises en oeuvre. Les risques varient, entre autres, selon la taille du pays. Dans les petits pays de taille plus restreinte, le risque est relativement élevé parce qu'il y a plus de cas exceptionnels.

63. Néanmoins, l'accès aux microdonnées assuré par l'ONS ne semble pas avoir donné lieu à une controverse publique. On peut en déduire que le public accepte relativement bien les pratiques actuelles, bien que l'information manque à propos des pays où un débat ouvert sur la question a été ouvert. Toutefois, le souci général du public en matière de protection de la confidentialité donne à penser qu'il y a une limite à ce qu'il est prêt à accepter. Une controverse pourrait aisément être déclenchée (au-delà des frontières nationales) par un seul incident malheureux, ce qui risquerait de nuire à la participation aux collectes ultérieures de données statistiques.

64. La transparence est importante pour pallier les accusations d'excès de confidentialité. Par conséquent, il est souhaitable que les ONS fassent ouvertement savoir que l'une des utilisations des données tirées de certaines collectes consiste à permettre aux chercheurs de se servir de microdonnées confidentialisées dans des conditions strictes et exclusivement à certaines fins. Cet aspect des choses doit être géré avec prudence, sinon les inconditionnels de la confidentialité risquent de retourner l'opinion publique. Il est essentiel que des personnes respectées et faisant autorité prêtent leur appui à cet égard.

### **Comment les ONS gèrent-ils les risques de l'accès aux microdonnées?**

65. Quelques suggestions sont présentées ci-après:

- a) Arrêter une série de principes qu'il faudrait suivre pour donner accès aux microdonnées (notamment ceux énoncés au chapitre III du présent document) ;
- b) Faire en sorte qu'on dispose d'une base juridique et éthique solide (ainsi que des instruments techniques et méthodologiques nécessaires) pour protéger la confidentialité. Cette base juridique et éthique nécessite que l'on mette soigneusement en balance l'intérêt pour le public d'une solide protection de la confidentialité, d'une part, et les avantages que lui apporte la recherche, d'autre part. La décision de savoir s'il convient ou non de permettre à un chercheur d'avoir accès aux données pourrait dépendre des mérites de son projet de recherche et de sa crédibilité, et il faudrait en tenir compte d'une façon ou d'une autre dans les dispositions législatives. On ne doit pas considérer l'accès comme étant automatique ;
- c) Mettre en place une procédure indépendante pour évaluer en regard l'une de l'autre les deux catégories d'avantages susmentionnées. Il serait judicieux de créer un comité interne chargé de débattre de ces questions et d'adresser des recommandations au chef de l'ONS. Des comités d'éthique peuvent également prêter leur concours dans des situations où une certaine latitude doit s'exercer pour déterminer s'il convient ou non de diffuser les données. Les arguments plaidant en faveur de l'intérêt général seront beaucoup plus convaincants s'il est prévu de placer les résultats de la recherche dans le domaine public ;
- d) Assurer une transparence complète concernant les utilisations particulières des microdonnées pour dissiper tout doute quant à une éventuelle utilisation abusive ;
- e) Être prêt à offrir aux chercheurs une plus grande facilité d'accès par le biais des moyens d'accès à distance et des laboratoires de données car il peut s'avérer impossible de rendre les microdonnées destinées à la publication complètement non identifiables sans altérer sensiblement les données. Étudier d'autres possibilités de recours aux progrès technologiques pour améliorer l'accès aux microdonnées de telle sorte qu'une protection suffisante de la confidentialité soit assurée ;
- f) Transmettre une part de la responsabilité à la communauté des chercheurs. Faire en sorte qu'elle comprenne pleinement les raisons pour lesquelles les ONS sont tellement attachés à la protection de la confidentialité. S'assurer que les chercheurs soient conscients des conséquences d'infractions éventuelles pour eux-mêmes et l'organisme dont ils relèvent. Prévoir des sanctions éventuelles en cas d'infraction.

66. De nombreux chercheurs ne voient pas l'intérêt de ces contrôles. S'il n'y a aucun incident connu d'utilisation abusive par les chercheurs de leur accès aux microdonnées pour identifier volontairement des individus, il est arrivé que des chercheurs communiquent à des collègues, sans y avoir été autorisés, des microdonnées qui leur avaient été fournies pour leur usage exclusif, ou que des chercheurs mettent des



microdonnées en correspondance avec d'autres données, sans autorisation préalable, dans le but d'élaborer des ensembles de données plus étoffés. Les chercheurs en question peuvent avoir l'impression qu'ils n'ont rien fait de mal car ils n'ont pas tenté d'identifier des individus. Toutefois, des incidents de cette nature, s'ils sont divulgués, peuvent saper la confiance du public et devraient par conséquent être pris au sérieux. Les ONS et les chercheurs ont des cultures différentes et des conceptions différentes des risques découlant de ce genre d'incidents. Il faut en tenir compte pour définir des procédures de diffusion des microdonnées.

### **Comment les ONS peuvent-ils transférer une partie des risques aux chercheurs?**

67. Le tort potentiel causé par une divulgation de données non-autorisée ne doit pas être sous-estimé, surtout si elle constitue un acte délibéré. De telles situations doivent être prises au sérieux. Les mesures envisageables dans ce cadre pourraient notamment être les suivantes:

- a) Leur demander de prouver leur légitimité en qualité de chercheurs, de démontrer l'intérêt de leurs recherches pour le public et de fournir des preuves que l'usage des microdonnées est nécessaire dans ce cadre ;
- b) Faire en sorte que les chercheurs signent un engagement juridiquement contraignant prévoyant des sanctions analogues à celles qui s'appliquent aux fonctionnaires de l'ONS s'ils enfreignent les règles en matière de confidentialité ;
- c) Expliquer les raisons de la prudence dont font preuve les ONS. S'assurer que les chercheurs sont pleinement conscients de leurs obligations en les informant comme il se doit. Instaurer des procédures de suivi et de surveillance efficaces (même si, étant donné le manque de ressources de nombreux ONS et le manque de transparence de certains chercheurs, cela n'est pas toujours possible). Il pourrait s'avérer utile d'établir un code de conduite en collaboration avec la communauté des chercheurs ;
- d) Lorsque des infractions sont commises, refuser au chercheur et éventuellement à l'organisme dont il relève de leur fournir tout service pendant un certain temps (par exemple jusqu'à ce que l'organisme ait pris les mesures disciplinaires qui s'imposent à l'égard du chercheur en faute). Il est crucial de leur faire comprendre qu'une fronde du public pourrait hypothéquer la divulgation future de microdonnées à la communauté des chercheurs. Entreprendre une action en justice si cela est opportun.

Un facteur à même de décourager les ONS de fournir de telles données est la période de temps qui s'écoule entre l'utilisation abusive des données et la découverte de l'infraction.

68. En réalité, un ensemble de mesures juridiques, administratives et techniques devra être mis en place pour gagner et conserver la confiance du public. En outre, la communauté des chercheurs doit accepter le fait qu'elle ne bénéficie pas d'un droit d'accès automatique. La décision d'autoriser ou non l'accès aux chercheurs devrait être laissée à la discrétion de l'ONS, et le droit d'accès devrait s'accompagner de responsabilités. En particulier, les chercheurs devraient accepter de partager la responsabilité de préserver et défendre les conditions dans lesquelles ils ont obtenu l'accès aux données. Les limites et garanties relatives à ces données sont probablement plus restrictives que celles applicables à d'autres ensembles de données qu'ils ont le droit de consulter mais il y a une bonne raison à cela.

### **Autres questions**

#### Consentement

69. On fait parfois valoir qu'il faudrait obtenir le consentement des répondants avant de diffuser les microdonnées à l'extérieur de l'ONS. Les défenseurs de cette position pensent que les personnes interrogées ont le droit de décider de quelle manière leurs données

doivent être utilisées, quand bien même elles ne sont pas identifiables. Ce genre de démarche devrait être découragé car :

- a) Elle soulève des problèmes pratiques importants liées à la recherche et à la gestion du consentement ;
- b) Les données fournies ne sont pas identifiables et ne servent qu'à un usage statistique, conformément à l'objectif de la collecte des données ;
- c) Il est très difficile de fournir la totalité des informations dont un répondant a besoin pour prendre une décision en toute connaissance de cause – et, par conséquent, bon nombre de répondants s'opposeront à la diffusion de données les concernant, simplement à titre conservatoire. L'échantillon perdra rapidement de sa représentativité s'il repose uniquement sur les données fournies par les répondants qui ont accordé leur consentement.

Toutefois, il est obligatoire, comme indiqué ailleurs dans les présentes lignes directrices, de garantir la transparence des modalités mises en place. Ainsi, on peut faire valoir qu'un consentement passif a été obtenu.

70. Si permis par la loi, un consentement donné en toute connaissance de cause conviendrait dans une situation où la publication de petits agrégats permettrait aux utilisateurs de déduire des conclusions concernant la situation d'une seule unité d'échantillonnage (personne ou entreprise, par exemple) prise en compte dans cet agrégat. La probabilité que le problème se pose est plus grande dans le cas des statistiques des entreprises.

#### Données administratives

71. La question du consentement a aussi une autre facette. Les données d'un ONS peuvent comprendre des informations recueillies directement par le service et des données collectées par les autorités administratives et communiquées à l'ONS. Sauf disposition contraire de la législation ou d'un autre instrument pertinent, un ONS ne devrait pas divulguer des données de source administrative sous la forme de microdonnées sans le consentement de l'autorité administrative intéressée (qui peut se trouver dans l'impossibilité de le donner en raison des engagements qu'elle a pris vis-à-vis des répondants). Même lorsque des données administratives se trouvent déjà dans le domaine public, la courtoisie veut que l'on avise les autorités administratives de leur diffusion éventuelle pour qu'elles aient l'occasion de formuler des observations. Dans le cas contraire, des difficultés peuvent surgir lors de la fourniture de données administratives. Les agences administratives doivent aussi, de leur côté, gérer les questions de confidentialité.

#### Dispositif spécifique

72. Il importe que les ONS prévoient un dispositif spécifique au cas où l'accès aux microdonnées suscite un débat public. Ils ne doivent pas exclure *a priori* l'éventualité qu'un tel débat se déclenche. Quels sont les principaux arguments qu'un ONS peut faire valoir?

- a) Les ONS peuvent mettre l'accent sur le soin qu'ils apportent à la protection de la confidentialité de leurs données, notamment en anonymisant les microdonnées, en dressant une solide barrière de protection physique et en veillant à mettre en place un processus d'évaluation pour peser le pour et le contre entre les avantages conflictuels, pour le public, de la protection de la confidentialité, d'une part, et de la recherche, d'autre part ;
- b) En cas d'infraction, l'ONS devrait être ouvert concernant à la fois l'infraction commise et la sanction infligée, s'il venait à être interrogé. Il devrait indiquer clairement que le responsable de l'infraction est le chercheur mais que l'ONS va prendre les mesures qui s'imposent pour sanctionner cette faute ;

- c) Les ONS devraient appeler l'attention sur l'intérêt public général qu'offre l'accès aux microdonnées, notamment dans le cas où une infraction a été commise, et donner quelques bons exemples ;
- d) Il faudrait solliciter le concours de personnes renommées et respectées qui sont prêtes à adhérer publiquement aux dispositions mises en place. L'aide de hauts fonctionnaires spécialisés en matière de confidentialité pourrait être particulièrement précieuse à cet égard.

## **VII. PROBLÈMES DE GESTION ASSOCIÉS À LA PUBLICATION DES MICRODONNÉES**

### **Gestion de la prise de décisions en matière de confidentialité**

73. Il y a toujours un risque d'identification, même s'il est très faible. Il existe à présent des logiciels permettant d'évaluer la proportion d'enregistrements uniques en leur genre et présentant donc un risque d'identification.

74. C'est au chef du service de statistique ou à son représentant qu'il incombe de se prononcer au sujet de la publication d'un fichier de microdonnées, que ce soit par le biais d'un fichier de microdonnées anonymisé (à usage public ou sous licence), d'un moyen d'accès à distance, ou d'un laboratoire de données. Pour pouvoir prendre cette décision, le chef du service de statistique a besoin d'un avis lui permettant, par exemple, de savoir si:

- a) Le risque d'identification est suffisamment faible ;
- b) Les ajustements apportés aux éléments de données n'ont pas exagérément altéré le fichier de microdonnées le rendant ainsi inutilisable aux fins de la recherche ; et
- c) Les variables qui ont été écrasées ont été choisies à bon escient, compte tenu à la fois des besoins des chercheurs et du risque d'identification.

75. Il faudrait mettre en place un dispositif pertinent pour donner un avis sur la question de manière cohérente. Un tel dispositif doit souvent être appuyé par des moyens de recherche appropriés et pourrait s'inscrire dans un cadre méthodologique.

### **Gestion des métadonnées**

76. Pour que les utilisateurs puissent exploiter efficacement les microdonnées, ils doivent avoir accès aux métadonnées pertinentes. Celles-ci comprendraient:

- a) Une description de l'enquête et notamment toute information utile sur la qualité ;
- b) Une liste des éléments de données et des classifications utilisées (parfois dénommée «dictionnaire des données») ; et
- c) Des définitions des éléments de données.

La disposition visée sous a) garantira que les microdonnées ne seront pas utilisées si les données ne sont pas réellement bien adaptées à l'objectif recherché. Il est aussi crucial que les limites des données soient clairement indiquées, en particulier le niveau d'agrégation supporté par le profil d'enquête.

77. Comme les microdonnées sont fournies sur support électronique, les métadonnées devront être communiquées sous une forme accessible. Si possible, les métadonnées devraient être publiées en même temps que les microdonnées. La copie papier reste un moyen de diffusion efficace bien que le site Web de l'ONS présente une utilité croissante à cette fin.

## **Gestion des infractions commises par le chercheur**

78. Il faudrait s'attacher à réduire la probabilité des infractions telles que décrites dans le chapitre précédent. Néanmoins, des infractions peuvent survenir et il conviendrait de mettre en place des procédures pour y faire face.

79. Les infractions doivent être prises au sérieux. Sinon, le public perdra confiance dans le dispositif institué. En outre, les infractions se répéteront plus fréquemment si elles restent impunies.

80. Il y a plusieurs façons de réagir aux infractions. Par exemple, si une infraction à la loi a été commise, il faudrait envisager d'engager des poursuites, solution certes coûteuse mais essentielle pour démontrer l'importance que l'ONS attache à la confidentialité, et réduire la probabilité d'infractions futures.

81. En outre, il faudrait, au minimum, interdire aux chercheurs d'avoir accès ultérieurement aux microdonnées.

82. Il faudrait également envisager d'arrêter de communiquer des données à l'organisme dont relève le chercheur, tout au moins jusqu'à ce que:

- a) Cet organisme ait pris les mesures qui s'imposent pour sanctionner l'infraction commise par le chercheur ; et
- b) L'ONS ait la conviction que les mesures voulues ont été mises en place au sein de l'organisme pour réduire au minimum les risques d'infractions futures.

83. La communauté des chercheurs est généralement favorable à l'adoption de mesures strictes contre le nombre relativement restreint de chercheurs en infraction qui risquent d'entacher la réputation de la communauté des chercheurs. Il y va de leur intérêt à long terme.

84. Dans le cas des infractions mineures, un avertissement peut s'avérer suffisant.

## **VIII. QUELQUES QUESTIONS PARTICULIÈRES**

### **Accès international**

85. Il importe de procéder à des comparaisons à l'échelon international pour bien comprendre l'efficacité des politiques et programmes adoptés par les différents pays. Les gouvernements, en particulier, jugent ces comparaisons utiles aux fins de l'évaluation des politiques. De toute évidence, il y a avantage à permettre aux chercheurs qui participent à des comparaisons internationales, de même qu'aux organisations internationales, d'avoir accès à des microdonnées mais cela ne va pas sans risques (tels que la transmission des microdonnées sans autorisation). Sauf à EUROSTAT, les fonctionnaires des organisations internationales ne sont soumis à aucune législation nationale ou internationale, en dehors du règlement du personnel en vigueur dans l'organisation. D'un autre côté, la probabilité d'identification est bien plus basse (tant que le chercheur ne transmet pas les microdonnées à une tierce personne dans le pays hôte). Une autre difficulté tient au fait que de nombreux pays ne sont pas légalement autorisés à communiquer des données aux organisations internationales ou aux chercheurs basés hors de leur territoire.

86. Les présentes lignes directrices suggèrent que l'on remplace une stratégie d'évitement des risques par une démarche de gestion des risques dans le contexte de la communication de microdonnées. Les risques sont plus faibles ou perçus comme tels si l'organisme qui reçoit les données jouit d'une réputation de crédibilité et de fiabilité. Ils sont aussi plus faciles à justifier si le pays qui fournit les données tire avantage de l'étude pour laquelle les microdonnées sont communiquées notamment s'il s'agit d'une étude internationale

entreprise par une organisation internationale ou d'un effort de recherche international réputé comme, par exemple, la LIS (Luxembourg Income Study).

87. La mondialisation accentue l'importance de ce genre d'études internationales. Les ONS devraient donc être en droit de soutenir les études en question en fournissant les microdonnées requises. Toutefois, les dispositions instaurées à cette fin devraient n'avoir qu'une fonction habilitante (en ce sens que l'ONS concerné devrait pouvoir décider dans chaque cas s'il convient ou non de fournir les données demandées) et prévoir aussi des garanties et des conditions de publication appropriées. Il faudrait que les ONS soient mieux préparés à communiquer des microdonnées anonymisées dans les cas où les risques sont plus faibles et les avantages plus grands.

88. Quelles sont les diverses possibilités qui s'offrent aux chercheurs d'avoir accès aux ensembles de données d'autres pays? Comment les organisations internationales peuvent-elles obtenir l'accès aux microdonnées à des fins statistiques et de recherche? Les possibilités sont notamment les suivantes:

- a) Les données sont recueillies directement par l'organisation internationale (ou le chercheur) ou par le biais d'intermédiaires (un organisme d'enquête spécialisé, par exemple) de telle sorte que l'on fait savoir au moment de la collecte des données que les microdonnées vont être transmises aux fins de la recherche ;
- b) Les fichiers à usage public lorsqu'il en existe ;
- c) Les fichiers de microdonnées anonymisés sous licence, lorsque les pays sont en mesure d'en produire ;
- d) Les moyens d'accès à distance assortis de mesures de protection appropriées ; et
- e) La collaboration avec un chercheur intégré à l'ONS ou établi dans le pays où se situe l'ONS.

89. Du point de vue de l'accès aux microdonnées, les enquêtes de la catégorie a) sont préférables pour les chercheurs internationaux. L'étude OCDE-PISA en constitue un bon exemple. Toutefois, de manière générale, ces collectes de données ne sont pas effectuées en vertu de la législation statistique en vigueur dans les divers pays. La qualité des microdonnées, et notamment les taux de réponse, pourraient en souffrir dans le cas de certaines études. Cela dépendra de la nature de l'étude et de la réputation de l'organisme qui l'entreprend, de même que de l'engagement contracté par les responsables de la collecte des données. Ce facteur doit être pris en considération par les chercheurs internationaux qu'ils optent ou non pour cette approche. Il peut y avoir des arbitrages à faire entre accès et qualité.

90. Il arrive que l'ONS puisse répondre aux besoins de l'étude en fournissant des données très détaillées à des fins d'analyse, mais pas de microdonnées. Cette démarche est suivie dans le programme de comparaisons internationales et l'étude OCDE/Eurostat sur les parités de pouvoir d'achat.

91. On ne dispose de fichiers à usage public que pour quelques pays. La constitution de fichiers de microdonnées anonymisés sous licence peut être envisageable si elle n'est pas exclue par les règles de l'ONS. Si les ONS sont autorisés à fournir des microdonnées par ce biais, les facteurs qui pourraient être pris en considération sont les suivants:

- a) La confiance qu'inspirent le chercheur et l'organisme dont il relève ;
- b) Le degré d'importance de l'étude pour le pays ; et
- c) La compatibilité ou non de la diffusion de ces données avec les engagements pris vis-à-vis des répondants au moment de la collecte des données.

92. Il serait probablement plus rassurant, pour bon nombre de pays, de communiquer des données à une organisation internationale spécifique ou pour un projet de recherche précis plutôt que de les diffuser de façon plus générale à la communauté internationale des

chercheurs. En outre, il peut y avoir des conditions ne s'appliquant qu'à certains chercheurs en particulier. Par exemple, des pays peuvent ne se sentir en confiance pour communiquer des données aux chercheurs que s'ils passent par l'intermédiaire de l'ONS dans le pays d'origine du chercheur. En tout état de cause, il serait de bonne règle de ne divulguer les données qu'à certaines conditions, soit en prenant un engagement, soit en signant un mémorandum d'accord. Parmi les conditions pourraient figurer:

- a) La limitation de l'accès aux données à certaines divisions des organisations internationales et l'interdiction de transmettre les données des tiers ;
- b) La restriction des utilisations pour lesquelles les microdonnées peuvent être exploitées sans autorisation ;
- c) L'obligation de rendre les microdonnées sur simple demande (par exemple si elles contiennent des erreurs) ;
- d) La possibilité de faire des observations sur des publications s'appuyant sur les microdonnées ; et
- e) L'énonciation claire des conséquences qu'aurait le non-respect des conditions de diffusion.

93. Le moyen le plus efficace pour réagir au non-respect des conditions de diffusion consisterait à suspendre toute communication ultérieure de microdonnées. La question pourrait également être abordée avec de plus hauts fonctionnaires de l'organisme concerné. Dans le cas des organisations internationales, cela pourrait se faire par la voie diplomatique pour les infractions les plus graves. Toutefois, l'essentiel est de ne pas laisser des infractions se produire sans réagir. Sinon, elles se répéteront.

94. Pour de nombreux pays, l'utilisation de moyens d'accès à distance pourrait être la meilleure solution pour permettre aux chercheurs internationaux d'obtenir des données. Dans ce genre de formule, un plus grand nombre de contrôles s'exerce et il est plus facile, en cas de contestation, de défendre la position des ONS concernant l'accès international aux microdonnées. Toutefois, l'applicabilité de ce genre de modalité à l'accès international doit encore être améliorée. L'expérimentation est importante.

95. Il existe encore une autre possibilité. Les chercheurs internationaux, notamment ceux qui œuvrent au sein des organisations internationales, pourraient travailler par le biais des réseaux de chercheurs nationaux pour atteindre leurs objectifs. En effet, ces chercheurs nationaux pourraient mener leurs recherches dans les locaux de l'ONS lorsqu'il s'agit d'études internationales particulièrement importantes.

96. Les ONS devront décider s'il convient ou non d'autoriser les chercheurs internationaux à avoir accès aux données, compte tenu de l'ensemble de la gamme des questions examinées dans la présente section. Ils ne devraient pas perdre de vue qu'il faut encourager l'usage d'une méthode de gestion des risques. Dans certaines applications de la recherche, les avantages pourraient contrebalancer les risques, pour autant que l'arrangement mis en place soit légal. Les risques pourraient être plus limités pour certains organismes que d'autres. Les ONS devront également décider quel est le mode d'accès le plus approprié. Afin de favoriser la cohérence du processus décisionnel, les pays devraient élaborer, en ce qui concerne l'accès des chercheurs internationaux et organisations internationales aux microdonnées, des lignes directrices conformes à leur propre législation. Sinon, ils peuvent décider de modifier leur législation de manière à autoriser l'accès aux microdonnées dans les cas qui le justifient.

97. L'accès des chercheurs internationaux aux microdonnées est bien plus facile à justifier lorsque le pays en retire un bénéfice. Ce bénéfice sera d'autant plus tangible que le pays disposera d'une remontée d'information concernant les produits statistiques. Il est ainsi important que les conclusions utiles de la recherche menée appartiennent au domaine public, ou soient transmises aux pays qui ont fourni les données. C'est un des moyens d'accroître l'utilité des services statistiques nationaux.

## **Accords naissants de publication de données pour certains pays en développement**

98. Les options d'accès aux microdonnées sont très limitées dans d'encore trop nombreux pays en développement. Mis à part pour les ressources limitées pour la collecte de données, le budget touchant à l'analyse et à la diffusion des résultats d'enquête n'est la plupart du temps pas adapté. Il est encore plus improbable que des dispositions aient été prises pour la transmission de microdonnées aux futurs chercheurs, au niveau national ou international. Ces contraintes techniques et de ressources ont même incité de nombreux ONS à prendre en considération des options qui pourraient affaiblir le contrôle qu'ils exercent sur les microdonnées ainsi transmises.

99. Une approche à adopter par les agences de financement ou les institutions qui les représentent, par les organisations internationales, ainsi que par les commissions régionales des Nations Unies, est de devenir les dépositaires de certains fichiers de microdonnées. Une autre approche, à adopter par les ONS, est de conclure des accords avec la recherche privée et/ou les institutions académiques, afin de produire des fichiers de microdonnées anonymisés (ainsi que des fichiers à usage public), en échange de services tels que l'archivage et la préservation des recensements. Certains dépositaires de données offrent des services complémentaires comme la constitution d'un catalogue central d'enquêtes et de recensements.<sup>5</sup> Une partie de ces accords sont le résultat d'accords passés dans le cadre de financements d'enquêtes spécifiques.<sup>6</sup> Cependant, il faut noter, comme dans le paragraphe 85, que ces institutions peuvent ne pas disposer des mesures de protection juridiques garantissant la sécurité des ensembles de données.

100. Certains accords passés prévoient que l'ONS se réserve le droit d'autoriser ou non la divulgation de ses données, tandis que d'autres prévoient que l'ONS renonce à toute autorité sur les données une fois que l'ensemble de celles-ci a été transféré à l'organisation dépositaire. Dans un cas comme dans l'autre, l'ONS a peu ou pas d'autorité pour faire appliquer le respect de l'accord passé, et n'a aucun de recours en cas d'infraction, à part celui de suspendre l'accord. Il est cependant essentiel que l'ONS soit informé dès qu'un accès est accordé. Les ONS impliqués dans de tels accords devraient ainsi s'assurer que l'institution intermédiaire s'engage fermement à prendre les mesures disciplinaires qui s'imposent en cas d'infraction en rapport aux données auxquelles l'accès a été permis. Lorsque la collecte de données est en partie ou intégralement financée par une organisation tierce, les termes qui régissent la divulgation des microdonnées doivent être acceptés par les deux parties, et l'ONS doit pouvoir obtenir l'assurance que la confidentialité du répondant n'est pas compromise.

101. Un argument convaincant et une motivation concernant ce genre d'accord est de s'assurer que le meilleur parti est tiré des collectes de données, ce qui ne peut être entrepris sans coût substantiel. Les bénéfices à espérer d'une permission d'accès à des microdonnées peuvent être remis en cause si l'organisme dépositaire n'accepte pas, à travers l'accord passé, de :

- a) assurer la préservation de la confidentialité ;
- b) exiger la transmission à l'ONS de tous les résultats issus de l'utilisation des données ;
- c) informer les ONS de toute transmission des données ; et
- d) refuser le transfert de microdonnées à des tiers si aucun accord n'a été signé avec l'institution à laquelle ceux-ci sont rattachés.

102. Il faudrait donc que l'accès initial et ultérieur soit conditionnel au retour d'information sur les résultats de recherche, et au respect des règles de la part des

---

<sup>5</sup> [http://www.internationalsurveynetwork.org/home/index.php?option=com\\_frontpage&Itemid=1](http://www.internationalsurveynetwork.org/home/index.php?option=com_frontpage&Itemid=1)

<sup>6</sup> Par exemple, les enquêtes démographiques ou de santé, les enquêtes par grappes à indicateurs multiples, les enquêtes sur les niveaux de vie, etc.

utilisateurs habilités. Les chercheurs, et les organisations internationales, peuvent aussi se faire une idée de la qualité des données, et, dans ce cas, faire remonter l'information de manière constructive afin d'aider à définir les contours des collectes futures. Parmi les mesures à prendre en cas de violation de l'accord passé, on peut citer : le refus à l'avenir de fournir des données à l'organisme dépositaire ; la suspension de l'accord ; déposer plainte auprès de la haute hiérarchie de l'institution hôte.

103. L'archivage d'ensembles de données dans un autre site est généralement considéré comme une bonne pratique pour pallier la destruction accidentelle ou non des ensembles de données. Les pays développés choisissent généralement un autre site à l'intérieur de leurs frontières. Cependant, les pays en développement n'ont pas toujours cette capacité, et, dans ce cas, l'utilisation d'un dépôt de données dans un pays tiers peut se justifier, pourvu que les mesures de protection idoines aient été mises en place.

104. Partout où la législation relative aux statistiques est en cours de développement ou de révision, des dispositions quant aux accords naissants relatifs à la diffusion et au dépôt de données doivent être incorporées.

### **Mise en corrélation des données**

105. La mise en relation des ensembles de données, qu'elle se fasse par correspondance exacte ou par appariement statistique, permet d'élargir sensiblement la gamme des analyses et peut créer une valeur ajoutée considérable. De plus en plus, les chercheurs se tournent vers l'utilisation d'ensembles de données appariées comprenant des liens avec les ensembles de microdonnées de services nationaux de statistique ou d'autres organismes de statistique (y compris les données issues du recensement de la population dans certains pays). La recherche en matière de santé, en particulier, est un domaine où les ensembles de données appariées peuvent revêtir une importance particulière.

106. Bien qu'établir un appariement entre des données comporte des avantages manifestes, une telle pratique comporte aussi des risques, notamment si l'entité qui a la garde du fichier apparié n'a pas mis en place des mesures de protection de la confidentialité semblables à celles qui existent souvent au sein de l'ONS. Les études réalisées dans bon nombre de pays mettent en évidence l'inquiétude que la mise en relation de bases de données suscite aux yeux du public. La manière de percevoir les choses est aussi importante. Il importe particulièrement que les quatre principes énoncés dans le chapitre III du présent document soient respectés dans le cas des ensembles de données appariées.

107. Il est souhaitable que les ONS soient associés à la mise en relation des ensembles de données à des fins statistiques. L'organisme de statistique doit assurer la protection de ces ensembles de données appariées. Il arrive aussi qu'il soit jugé préférable de confier à l'organisme de statistique le soin de conserver les ensembles de données appariées émanant d'autres entités, en raison des garanties de protection qu'il offre et de la confiance qu'il inspire au public.

108. Dans les pays où il existe des commissions chargées de la protection de la confidentialité ou des organes équivalents, ceux-ci devraient souscrire à l'adoption de modalités s'appliquant à la mise en corrélation des données.



## ANNEXE

### LIST OF CASE STUDIES ON SPECIFIC PRACTICES

1. Legislation to support release of microdata - Australia
2. Legislation to support release of microdata - Finland
3. Data cubes - Netherlands
4. Public use microdata - United States
5. Release of anonymised microdata files (licensed files) - Australia
6. Release of licensed microdata files - Netherlands
7. Release of licensed microdata files - Sweden
8. Remote data access facilities - Canada
9. Remote access facility (for microdata access) - Australia
10. Remote access to microdata files - Denmark
11. Research data centre program - Canada
12. Research data centres – United States
13. Data laboratory arrangements - Netherlands
14. Data laboratory microdata access - New Zealand
15. Data laboratory microdata access - Brazil
16. Microdata laboratory analysis - Italy
18. Managing decision making on confidentiality - Australia
19. Microdata access in the OECD programmes for international student assessment (PISA)
20. Policy on international release of microdata - Australia
21. Management of record linkage projects - Canada
22. Data linking when preparing microdata for research - Sweden

## **ANNEX 1. CASE STUDY - LEGISLATION TO SUPPORT RELEASE OF MICRODATA - AUSTRALIA**

### **1. Broad description**

This is delegated legislation (referred to as a ‘Ministerial Determination’, but in effect a regulation) that enables the Australian Bureau of Statistics (ABS) to release microdata to approved users for statistical purposes. It also outlines the conditions of release and the penalties for any breach of those conditions.

### **2. Why is it good practice?**

It provides a degree of certainty to both the ABS and the potential users of microdata about the arrangements for release. The legislation also outlines the arrangements that the Parliament is happy with. As they are enshrined in delegation legislation, they are in the public domain.

### **3. Target audience**

Primarily the research community who are the main users of microdata.

### **4. Detailed description**

The specific legislation is outlined in Part 5. There is also a supporting statement providing policy, rules and guidelines to assist ABS staff involved in the release of microdata.

Each new release of microdata requires the approval of the Australian Statistician in view of the potential sensitivity of releases. Each release to individual clients requires the approval of a senior manager, employing the delegated authority of the Australian Statistician.

A Microdata Review Panel has been established to provide advice to the Australian Statistician on microdata releases, particularly the steps that need to be taken to ensure the release complies with the confidentiality test imposed by the legislation.

### **5. Supporting legislation**

Disclosure of unidentified information:

(1) Information in the form of individual statistical records may, with the approval in writing of the Statistician, be disclosed if:

- (a) all identifying information such as name and address has been removed;
- (b) the information is disclosed in a manner that is not likely to enable the identification of the particular person or organisation to which it relates; and
- (c) the Statistician has been given a relevant undertaking by each person required by sub-clause (2) to give a relevant undertaking in relation to the information.

(2) The persons required to give a relevant undertaking are:

- (a) for information to be disclosed to an individual, the same individual; and
- (b) for information to be disclosed to an official body:
  - (i) the responsible Minister in relation to, or a responsible officer of, the official body; and

- (ii) if the Statistician considers it necessary in a particular case, each individual in the official body who will have access to the information.
  - (c) for information to be disclosed to an organisation other than an official body:
    - (i) a responsible officer of the organisation; and
    - (ii) if the Statistician considers it necessary in a particular case, each individual in the organisation who will have access to the information.
- (3) In this clause: ‘relevant undertaking’ means an undertaking in writing that use of the information in relation to which the undertaking is given is subject to the following conditions:
- (a) no attempt will be made to identify particular persons or organisations to which the information relates;
  - (b) the information will be used only for statistical purposes;
  - (c) for information to be disclosed to an individual, the information will not be disclosed to anyone without the approval in writing of the Statistician;
  - (d) for information to be disclosed to an official body or other organisation:
    - (i) the information will not be disclosed to anyone outside the body or organisation without the approval in writing of the Statistician; and
    - (ii) if the Statistician considers it necessary in a particular case, the information will not be disclosed to an individual in the body or organisation who has not given a relevant undertaking;
  - (e) if the Statistician considers it necessary in a particular case, either or both of the following:
    - (i) the information, and all copies (if any) of the information, will be returned to the Statistician as soon as the statistical purposes for which it was disclosed have been achieved;
    - (ii) access by officers to information, documents or premises will be given as may be necessary for the purpose of conducting a compliance audit concerning observance of the conditions under which the information is disclosed;
  - (f) any other condition that, in the opinion of the Statistician, is reasonably necessary in a particular case.

In a different part of statistics legislation, it is made clear that a person who fails to comply with an undertaking, as prescribed in (2) above, is guilty of an indictable offence punishable on conviction by a fine not exceeding \$5000 or imprisonment for a period not exceeding 2 years, or both.

## **6. Strengths**

- (i) Provides a basis for arrangements that are understandable by both the NSO and researchers.
- (ii) Provides for significant penalties for legal breaches; this may be a reason why no known breaches have occurred.
- (iii) Microdata protection is partly provided by a legally enforceable undertaking. This means that some protection (e.g. prevention of matching) can be provided through the undertaking.
- (iv) Provides wider access to the data than would otherwise be the case, thereby achieving a greater return on the high investment in data collection and respondent burden.

(v) Provides statutory authority and transparency for release practices and a basis for the public defence of those practices.

## **7. Weaknesses**

(i) Researchers still believe the conditions of release are too limiting i.e. the steps taken to make the data confidential result in too much of the detail not being released.

(ii) Disclosure of microdata, even under circumstances demanding strict confidentiality, can alarm the privacy constituency and in the worst case, have the potential to impact on response rates.

(iii) Compliance with the limitations and conditions imposed by legislation can impose an administrative burden on both the NSO and the researchers, delay the release of information, restrict the range of researchers who can have access to the information, restrict the uses to which the information can be put and limit the nature of the information which can be released.

## **8. References**

The supporting statement referred to in Part 4 is available on request from [teresa.dickinson@abs.gov.au](mailto:teresa.dickinson@abs.gov.au)

## **ANNEX 2. CASE STUDY - LEGISLATION TO SUPPORT RELEASE OF MICRODATA - FINLAND**

### **1. Broad description**

Legislation (the Statistics Act) enables Statistics Finland to release microdata to approved users for scientific research and statistical purposes. It also outlines the conditions on the release and the penalties for any breach of these conditions.

### **2. Why is it good practice?**

The law sets out conditions under which microdata can be released. Written guidelines by Statistics Finland give further directions and assure equal treatment of all applicants. The law gives a certain leeway to Statistics Finland in assessing the threat to confidentiality that the data might impose. The principles of data release are well known by all parties (statistical authorities, data suppliers and data users). The practice does not weaken data suppliers' trust in the confidentiality of basic data. The decisions on access to microdata are made solely by the statistical authority.

### **3. Target audience**

A licence to use data may be issued to an official body, an institution or a person in charge of research. In cases where the licence is issued to an official body or an institution, it is granted to a specific person or specific persons.

### **4. Detailed description**

The essential principles and procedures of data release are prescribed in the Statistics Act. Statistics Finland has given more detailed guidelines on data release. These guidelines and the application form for access to microdata are publicly available on Statistics Finland's website.

An application for a licence to use data must be submitted in writing. The applicant must specify the purpose for which the statistical data are to be used, the material requested from Statistics Finland and any other data that will be used. A research plan should be appended to the application.

When considering the granting of a licence to use basic data, Statistics Finland first determines whether the data can be processed in-house to obtain the statistics requested by the applicant. In considering the application, account is also taken of the possibility that the applicant will obtain reliable results on the basis of this material. Particular attention is also paid to data protection issues.

Statistics Finland also takes into consideration any other data that the applicant may already have at their disposal. If a licence is granted and the data in the possession of Statistics Finland are to be combined with other data, this combining must take place at Statistics Finland, which shall remove all identification variables from the combined material.

Statistics Finland will not grant a licence for data covering the whole country or a whole region. Authorisation to use entire data files is generally granted only in exceptional cases, such as specific research purposes and where the material does not contain sensitive data.

Before releasing the data, all identification information is removed from the material for which a licence has been granted, or the data are made less detailed or combined with other data in order to prevent identification. The information to be removed or the manner of combination shall be indicated in the licence decision. Information on age, gender, education and occupation may be released with identification data if the applicant is entitled to collect such data by virtue of the Personal Data Act. This must be indicated in the application. An additional requirement is that the release of these data in identifiable form is considered essential to the study.

The decision to grant access to microdata is made by the Director General when data are to be released abroad. In other cases the decision is made by the director of a statistics department. The licence is granted for a limited period only. Statistics Finland has a Committee on Statistical Ethics which helps decision-makers by giving opinions on complicated data release issues and on all cases where data are to be released abroad.

Each licence is accompanied by the terms and conditions applicable to the use of the data. The data may only be used for the purpose indicated in the decision. The data shall be treated as confidential and may not be handed over to others without authorisation from Statistics Finland. No attempt must be made to identify the data subjects from the material and the data must be destroyed by the set date.

## **5. Supporting legislation**

All statistical data are confidential irrespective of the data source. The release of confidential data is determined by the Statistics Act (Section 13).

The data obtained by a statistical authority for statistical purposes may only be released to a third party on terms laid down in the Statistics Act or in another act concerning especially the National Statistical Service or upon express consent of the subjects of the data.

Confidential data collected for statistical purposes may be released for use in scientific research or statistical surveys concerning social conditions. Such data may not be released for use in an investigation, surveillance, legal proceedings, administrative decision-making or other similar handling of a matter concerning an individual, enterprise, corporation or foundation.

Identification data may not be released. Both direct and indirect identification of personal data must be prevented. As far as other data (e.g. business data) are concerned it is sufficient to prevent direct identification. However, access to business microdata is usually granted only at the premises of Statistics Finland.

The decision to grant access to microdata is always made by the statistical authority concerned. When making the decision, data protection issues must be taken into consideration.

Violation of statistical confidentiality is a punishable offence (Section 24 of the Statistics Act). The punishment may be a fine or imprisonment not exceeding two years.

## **6. Strengths**

Legislation provides a clear basis for arrangements that the National Statistical Institute, data suppliers and researchers can understand.

Data obtained from administrative sources can be released without the permission of the data supplier. This makes the procedures of data release simpler and enables the use of very large data files.

Legislation ensures that the release of data collected for statistical purposes cannot be regulated by any other act than the Statistics Act. This enhances the trust of data suppliers.

Legislation prescribes severe punishments for breaches of law.

## **7. Weaknesses**

From Statistics Finland's perspective:

- Making data non-identifiable demands a great amount of work, which increases their cost to researchers.

From data users' perspective:

- Data are often regarded as expensive by researchers.
- Researchers sometimes think that there are too many restrictions to obtaining and using data.

## **8. References**

The legislation can be found at [http://tilastokeskus.fi/org/index\\_en.html](http://tilastokeskus.fi/org/index_en.html)

## ANNEX 3. CASE STUDY - DATA CUBES - NETHERLANDS

### 1. Broad description

Statistics Netherlands (*Centraal Bureau voor de Statistiek*, or CBS) releases its publishable information in its output database StatLine on the Internet, [www.cbs.nl/en/statline](http://www.cbs.nl/en/statline). Usually, this information takes the form of multidimensional tables, or data cubes. These tabulations are safe from the perspective of statistical confidentiality protection. The user selects and processes his own views on these data cubes. Occasionally, statistical work is commissioned and paid for by third parties, resulting in data cubes.

### 2. Why is it good practice?

Data cubes are the main vehicle for releasing all statistical information. Statistical confidentiality protection is applied in a routine fashion. Moreover, data cubes can be easily linked and compared on a meso level. Conversely, a lack of coherence is easily discovered. Adding data cubes to the StatLine database ensures that statistical information is produced and published to serve the public at large.

### 3. Target audience

Data cubes are primarily made and used to serve the public at large. Even if they are produced and paid for by a third party, as a matter of policy the resulting data cubes are available for all.

### 4. Detailed description

CBS has published several papers on the art of ‘cubism’.

### 5. Supporting legislation

Three sections of the Statistics Netherlands Act ([www.cbs.nl/en-GB/menu/organisatie/statistics-netherlans-act.htm](http://www.cbs.nl/en-GB/menu/organisatie/statistics-netherlans-act.htm)) are relevant, pertaining to its general public task, its commissioned work, and the precondition of statistical confidentiality.

Section 3 states that it is the legal task of CBS “to carry out statistical research for the government for practice, policy and research purposes and to publish the statistics compiled on the basis of such research”.

According to section 5, “CBS may occasionally carry out statistical work for third parties.”

Section 37 reads:

- “1. The data received by the director general in connection with the performance of his duties to implement this act shall be used solely for statistical purposes.
2. The data referred to in the first subsection shall not be provided to any persons other than those charged with carrying out the duties of the CBS.



3. The data referred to in the first subsection shall only be published in such a way that no recognisable data can be derived from them about an individual person, household, company or institution, unless, in the case of data relating to a company or institution, there are good reasons to assume that the company or institution concerned will not have any objections to the publication.”

## **6. Strengths**

CBS is in full control as far as statistical disclosure protection is concerned. The user can rely on the professional quality of the statistical information. It is rewarding for staff to produce information that is in demand. The data cubes make it ever easier to relate various bits of statistical information to each other. Experiences with commissioned work may be fed back into the standard statistical programme as an indication of user preferences.

## **7. Weaknesses**

By definition data cubes are less informative and less flexible than microdata (unit level records) for researchers. As commissioned work has to be paid for, data cubes may appear to be expensive for the commissioning party.

## ANNEX 4. CASE STUDY - PUBLIC USE MICRODATA - UNITED STATES

### 1. Broad description

The U.S. Census Bureau first published public-use microdata for the 1970 Decennial Census. Microdata files of decennial censuses have been released since then, as well as public use microdata files from selected demographic surveys. The Census Bureau does not produce public use microdata from its economic censuses and surveys.

In the mid 1980s the Census Bureau established a Microdata Review Panel to oversee the content of microdata publication. This included ensuring that microdata files met disclosure avoidance conditions. In the mid 1990s, the Microdata Review Panel was replaced by the Disclosure Review Board (DRB), with a greater emphasis on disclosure avoidance. By this time, microdata were the primary publication form for servicing the Census Bureau's more sophisticated public users. Because Census Bureau data products that are released to the public are available to all users, the role of the DRB is to establish disclosure avoidance guidelines for all of the Census Bureau's data products (including microdata) and to ensure that they adequately protect the identity of individual respondents. In practice, a checklist approach is used to assess these data sets. In addition, ongoing research is conducted to ensure that disclosure avoidance techniques are consistent with current conditions.

### 2. Why is it good practice?

Microdata publication changes the role of the NSO, largely eliminating any interpretive function. The NSO is able to accommodate more interests and maintain itself as a neutral party. Interpretation of the data becomes more robust as more parties are able to examine the data in detail.

### 3. Target audience

All users, from sophisticated analysts for micro-simulation modelling and policy evaluation to federal, state, and local governments, academic researchers, market researchers, private businesses, and the general public.

### 4. Detailed description

The Census Bureau has published microdata files from decennial censuses since 1970. The medium of publication for the 1970 and 1980 Public Use Microdata Samples (PUMS) was mainframe tape. The 1990 Census Public Use Files are available on both tape and CD-ROM. Census 2000 microdata are available via CD-ROM and the Internet. Changes in media and technological advances have led to broader access by users in general and by type of user in particular.

For Census 2000 two principal sets of public use files were released – the 5-Percent PUMS and the 1-Percent PUMS. The two sets are mutually exclusive. The 5-Percent file contains data for 5% of all households in the country, is released for public use microdata areas (PUMAs) of at least 100,000, and requires the PUMAs to follow state boundaries. The 1-Percent file contains more detailed characteristics data for 1% of all households and is based on superPUMAs of at least 400,000 that do not cross state boundaries.

In addition to decennial census information, the Census Bureau public-use microdata products, provided through the Internet (FTP) and CD-ROM, include the following ongoing surveys:

- Current Population Survey (CPS);
- Survey of Income and Program Participation (SIPP);
- American Housing Survey (AHS);
- Survey of Program Dynamics (SPD);
- American Community Survey (ACS); and
- Consumer Expenditure Survey.

Personal identifiers are removed from these files and only large geographic areas are identified on microdata records. The Census Bureau uses a basic population threshold of 100,000 in conjunction with other methodologies, to avoid disclosure. Many of the surveys for which Public Use Files are produced use a larger geographic unit (in terms of population) in order to offer more detailed data. To further protect confidentiality, there is limited detail on items such as place of residence, place of work, high incomes, and others. (See Zayatz (2002), for more detail about disclosure avoidance methods used for the Census 2000 PUMS.)

## **5. Supporting legislation**

The Census Bureau’s authorizing legislation is Title 13, United States Code. Section 9(a)(2) of this law prohibits the Census Bureau from making “any publication whereby the data furnished by any particular establishment or individual under this title can be identified.” At the same time, the law states that the Census Bureau is encouraged to make “statistical use” of the data in its possession. Although some thought has been given to offering licensed access to microdata, as a means of expanding access to advanced users while ensuring enhanced protection of the data, legal interpretation of the Census Bureau’s statute suggests that this is not an option. According to the Census Bureau’s legislation, the data either are public or they are not – if they are public then they must be made available to any user; if they are not, they may only be accessed by persons who have taken the Census Bureau’s Oath of Nondisclosure, who use the data only for statistical purposes, and are subject to severe penalties for disclosure.

In the United States, each agency has its own legislation and many statistical agencies do not have specific confidentiality protection as part of their statute. In 2002, the Confidential Information Protection and Statistical Efficiency Act (CIPSEA) was passed, which guarantees that data collected under the CIPSEA with a pledge of confidentiality must be kept confidential, subject to severe penalties for disclosure, and which ensures that data collected for statistical uses may not be used for administrative or compliance purposes. This new legislation helps protect microdata that may be released by other U.S. federal agencies.

## **6. Strengths**

For many data users, the summary tables and tabular and narrative profile reports released meet their needs. Microdata are released for advanced users who want to create or define their own tabulations, to be able to further draw on the richness of detail recorded in the census or survey.

Census Bureau microdata files are available to the general public without restriction on their use, and while the Census Bureau offers limited access to non-public microdata for selected users at its Research Data Centers, the ability to obtain public use microdata files permits users to access these rich data sets in their own settings, without the need for Census Bureau oversight.

## 7. Weaknesses

The methods used to make the data disclosure-proof can be damaging to some characteristics of interest:

- Geography is largely suppressed;
- Variables pertaining to collection are seldom included; and
- Data are being suppressed more often due to the presence of overlapping external data. This problem is likely to worsen.

Unfortunately, the more sophisticated the disclosure avoidance techniques are, the less undisturbed data can be released, ultimately affecting analysis, often in unknown ways. Recent advances in computer technology and data mining techniques increase concerns about the ability to continue to release detailed microdata files, and better methods are needed to measure microdata disclosure risk and the bias added by disclosure avoidance techniques.

## 8. References

Doyle, P. et al. (eds) (2001) *Confidentiality, Disclosure and Data Access: Theory and Practical Applications for Statistical Agencies*; North-Holland.

Duncan, George T; Jabine, Thomas B.; and de Wolf, Virginia A (eds.) (1993) *Private Lives and Public Policy*, Committee on National Statistics Panel on Confidentiality and Data Access, National Academy Press, Washington, DC.

Federal Committee on Statistical Methodology (1994) *Statistical Policy Working Paper 22: Report on Statistical Disclosure Limitation Methodology*, Office of Management and Budget: Washington, DC.

U.S. Census Bureau (2003) *Access to Microdata – Issues, Organisation and Approaches*, Conference of European Statisticians, Geneva, June 10-12, 2003.

Zayatz, L. (2002) “SDC in the 2000 U.S. Decennial Census”, in *Inference Control in Statistical Databases* (Josep Domingo-Ferrer, ed), Springer.

## **ANNEX 5. CASE STUDY - RELEASE OF ANONYMISED MICRODATA FILES (LICENSED FILES) - AUSTRALIA**

### **1. Broad description**

Anonymised microdata files (licensed files) in Australia are referred to as Confidentialised Unit Record Files (CURFs). Key measures undertaken by the Australian Bureau of Statistics (ABS) to protect the data are: requiring anyone who uses the data, and the organisations that employ them, to sign an undertaking with the ABS; obtaining user commitment to confidentiality principles; and perturbing data or reducing detail on files to make it very difficult for units to be identified. CURFs are most commonly made available to users either on a CD-ROM or through a remote access data laboratory (RADL™). CURFs available on RADL™ contain more detail than those on CD-ROM. In selected cases users may have access to a CURF through an on-site data laboratory.

### **2. Why is it good practice?**

Releasing microdata in this manner constitutes good practice as:

- perturbation of data and masking of records is undertaken to maintain the integrity of the data while protecting the confidentiality of an individual's data; and
- placing restrictions on how the data are used, as set out in a legal undertaking to be signed by each user and their organisation, ensures both the user and the organisation accept responsibility for keeping the data confidential and secure.

### **3. Target audience**

CURFs are aimed at Australian researchers and analysts within government, academia and other non-government organisations, who seek to undertake more in-depth analysis than is possible using tabular aggregated data.

CURFs are not generally released to overseas applicants. In very selected instances the ABS allows overseas researchers to access CURFs via the RADL™ if they are sponsored by a suitable Australian organisation. The sponsoring organisation is required to sign an undertaking with the ABS.

### **4. Detailed description**

The ABS has adopted a manner of release for CURFs that protects the data in three ways: confidentialising the unit record file to control the detail available; providing modes of access appropriate to the level of detail available; and requiring users and organisations with access to the data to sign an undertaking that restricts how they use the data.

The unit record files are confidentialised by removing name and address information, by controlling and limiting the amount of detail available, and by perturbing or deleting data where it is likely to enable identification of individuals.

Each CURF release is personally approved by the Australian Statistician, following advice from a Microdata Review Panel consisting of three senior executives. The panel makes a detailed assessment of each CURF to ensure that the disclosure risk is low.

There is protection inherent in the different access modes and in the different levels of data provided in each. The ABS provides three different modes of access for CURFs - CD-ROM, the RADL™ and the ABS Data Laboratory (ABS DL). CURFs available on CD-ROM are labelled Basic CURFs and are restricted to a relatively small number of variables released in broad categories. RADL™ users can also access Expanded CURFs that contain more variables and more detail, with extra protection provided by the automatic logging of RADL activity and subsequent audits of this activity. Specialist CURFs contain the most variables and detail and can only be accessed via on-site ABS Data Laboratories.

Each user must apply to be granted access to a CURF, explaining their intended use of the CURF. Both the User and a Responsible Officer of the employing organisation must sign a legal undertaking in which they agree:

- access to information about individuals will be restricted to officers of the organisation who have signed an individual undertaking with the ABS;
- users will not attempt to identify individuals;
- users will not match the unit data to other files of unit data;
- ABS officers are allowed access as necessary to audit compliance with these rules;
- CURF usage is limited to the specified and approved individual ‘Statistical Purpose’; and
- any sensitive printed data and output will be stored in a secure place.

The organisation must monitor its officers that have access to the CURF and ensure that all have signed an individual undertaking with the ABS. Access to CURFs are for statistical purposes within an organisation. If an individual changes organisations, they must surrender access and notify the ABS.

The responsible officer is generally the head or deputy head of an organisation, department or university. They are required to sign an undertaking about the storage and use of the CURF. Breaches can be addressed by sanctions against both the individual user and the organisation as well, including removal of access to all microdata for all individuals in the organisation.

## **5. Supporting legislation**

The release of microdata by the ABS is governed by legislation; namely, the Census and Statistics Act 1905. This legislation enables the Australian Statistician to release unit record data, provided this is done “in a manner that is not likely to enable the identification of a particular person or organisation to which it relates.” Details are provided in Section 5 of Annex 1.

## **6. Strengths**

- (i) Allows for a range of access mechanisms to suit a range of uses.
- (ii) Allows for access to more detailed data to be granted to users who are able to work with a greater level of environmental protections.
- (iii) Microdata protection is partly provided by a legally enforceable undertaking. This means that some protection (e.g. prevention of matching) can be provided through the undertaking.
- (iv) Sanctions can be applied against users and organisations that breach the undertakings, providing additional motivation to ensure data access and use is appropriate.

## **7. Weaknesses**

- (i) Researchers still believe the protections applied directly to the microdata are too limiting. They believe too much of the detail is not being released, especially for some of the most identifiable sections of the population (e.g. large households).
- (ii) It is more costly to support a range of access mechanisms than a single access mechanism.

## **8. References**

The Census and Statistics Act 1905 <http://scaletext.law.gov.au/html/pasteact/1/580/top.htm>

The Statistics Determination 1983 <http://scaletext.law.gov.au/html/pastereg/0/414/top.htm>

CURF undertakings & the Responsible Access to ABS CURFs Training Manual is at:  
[www.abs.gov.au/websitedbs/D3110129.NSF/85255e31005a1918852558ac00697645/72d92417a0ba71b5ca256d01002c47a4!OpenDocument#Untitled%20Section\\_6](http://www.abs.gov.au/websitedbs/D3110129.NSF/85255e31005a1918852558ac00697645/72d92417a0ba71b5ca256d01002c47a4!OpenDocument#Untitled%20Section_6)

## ANNEX 6. CASE STUDY - RELEASE OF LICENSED MICRODATA FILES - NETHERLANDS

### 1. Broad description

For its social sample surveys Statistics Netherlands (*Centraal Bureau voor de Statistiek*, or CBS) releases about ten standard microdata files each year. The microdata are protected against disclosure but not to the last detail. The remaining risk is dealt with by a contract (or license). The microdata are available to legitimate researchers. They are released on tape or on disk, usually in the SPSS format.

### 2. Why is it good practice?

The community of social researchers is quite large. By releasing standard microdata files from its social sample surveys CBS serves this community. A basic acquaintance with SPSS is widespread among them.

Research on these files:

- reduces expenditure of tax payers' money on data collection efforts;
- reduces response burden;
- provides researchers with readily available microdata;
- turns CBS files and corresponding definitions into a *de facto* standard;
- provides end users within the policy domain with high-quality information within a short turnaround time.

Social sample survey microdata are relatively easy to protect against disclosure.

Two of the national 'planning offices', or independent government research institutes (SCP and CPB) and some five university faculties have a full subscription to these licensed microdata files. In addition over 70 files are released to individual institutes and researchers.

### 3. Target audience

Microdata are released under a contract or license to legitimate researchers only. Section 41 of the law mentions the researchers that are qualified. Amongst them are universities and other research institutes with a legal foundation, but also Eurostat and NSOs within the EU. A residual category of applicants must be formally admitted by the Central Commission for Statistics (CCS), the supervisory body for CBS. The CCS has set its own selection criteria and procedures, in which a focus on statistical (aggregate) research, independence from administrative authorities, and the intention to share results in the public domain are predominant. The CCS has no objection in principle against admitting non-EU universities, for example. A commercial bank or a journalist would not be eligible, however.

### 4. Detailed description

Microdata files are released, nowadays usually on CD-ROM, to interested researchers that are qualified according to the law or to the CCS. The files are compiled and documented from the social sample surveys carried out by CBS. Of course, they do not contain formal identifiers or matching numbers. Other identifying variables are collapsed or protected in other ways. The sampling factor (1% for the Continuous Labour Force Survey being the maximum) by itself protects respondents.



## 5. Supporting legislation

Providing microdata to researchers is legally defined as an exception to the general obligation of statistical confidentiality. The general obligation reads as section 37:

- “1. The data received by the director general in connection with the performance of his duties to implement this act shall be used solely for statistical purposes.
2. The data referred to in the first subsection shall not be provided to any persons other than those charged with carrying out the duties of the CBS.
3. The data referred to in the first subsection shall only be published in such a way that no recognisable data can be derived from them about an individual person, household, company or institution, unless, in the case of data relating to a company or institution, there are good reasons to assume that the company or institution concerned will not have any objections to the publication”.

The microdata release policy is supported by section 41:

- “1. Contrary to the provisions of Section 37 the director general may, on request, provide or grant access to a set of data to a department, organisation or institution as referred to in the second subsection for the purposes of statistical or academic research where appropriate measures have been taken to prevent identification of individual persons, households, companies or institutions from those data.
2. A set of data as referred to in the first subsection may be provided to or made accessible to:
  - a. a university, within the meaning of the Higher Education and Research Act;
  - b. an organisation or institution for academic research established by law;
  - c. planning offices established by or by virtue of the law;
  - d. the Community statistical agency and national statistical agencies of the member states of the European Union;
  - e. research departments of ministries and other departments, organisations and institutions, in so far as the CCS has given its consent.

The importance of statistical confidentiality is apparent in section 42:

“The director general shall only grant a request as referred to in Section 41 if the director general considers that the applicant has taken adequate measures to prevent the set of data being used for purposes other than statistical or academic research.”

The remaining risk of disclosure (considering the adequate measures mentioned in section 42) is dealt with by a contract or license. The contract is signed by the institute that has requested access to the microdata. An appendix to the contract is a confidentiality statement to be signed by each individual researcher with access to the data. There is no legal punishment or fine in the case of a transgression of legal or contractual obligations of confidentiality.

The research community itself has drafted, and agreed upon, codes of conduct for the social and epidemiological sciences. These codes have been accepted by the national privacy authority CBP. They may be interpreted as a sign of awareness on the side of researchers of ethical and legal problems of privacy and confidentiality. One of these codes installs a commission of appeal for respondents, on which a staff member of CBS serves.

Apart from supporting legislation there has been since 1994 a long-term contract with the Netherlands National Science Foundation (NWO). As a broker, it couples data providers, first and foremost CBS, and data users, primarily (but not exclusively) with a focus on the universities. Under this long-term contract, CBS obliges itself to make available at least eight social sample survey microdata files each year. NWO pays £450,000 per annum. Concrete users of microdata pay an additional small fee (varying from £1,000 to £5,000 depending on the size of the file, with a discount for older files, as well as for the full package for a whole year). NWO also organises publicity, user consultation days (on specific files or themes), and an independent formal evaluation every four years.

## **6. Strengths**

The researcher can process and analyse the microdata at his own computer, at his own time, with his own familiar and specialised software.

From the statistician's perspective an initial investment is needed for preparing and documenting the microdata file. But from then onwards, efforts can be quite minimal. The more microdata are used, the more value is added for society at large and for research in particular. Furthermore, the data quality and documentation is enhanced by feedback from intensive use.

## **7. Weaknesses**

From the researcher's perspective the microdata do not always contain sufficient detail. In some cases microdata are even deemed too sensitive to be allowed to leave the statistical office at all. For example, microdata from businesses, fiscal income statistics and causes of death statistics are not permitted to leave the office, which is an extreme example of collapsing the microdata.

Because of the lack of formal identifiers and the collapsing of some of the background variables, the microdata can not flexibly be expanded with new variables.

Some of the contractual conditions (CBS may want to screen draft publications or to inspect the ICT facilities on which the researchers have access to their data) are sometimes interpreted as 'organised distrust' if not outright 'strangulation' by CBS of research.

Some statistical staff consider it a threat that others use 'their' microdata and publish results that should have been on the official statistical programme.

## **ANNEX 7. CASE STUDY - RELEASE OF LICENSED MICRODATA FILES - SWEDEN**

### **1. Broad description**

These are the arrangements for Statistics Sweden's release of confidential microdata (licensed microdata files) to approved users for statistical and research purposes.

### **2. Why is it good practice?**

The arrangements ensure that the release of confidential data are in accordance with the legislation concerning confidentiality and protection of individual's privacy. The legislation, decided by parliament, provides the limits for release of data, e.g. research purposes, and legally underpins and constitutes administrative and technical safeguards.

### **3. Target audience**

Statistics Sweden mainly provides access to microdata to public authorities and people or organisations performing scientific research (universities and research institutions). Statistics Sweden also provides access to microdata to other authorities and municipalities producing statistics.

### **4. Detailed description**

According to the main principle, confidential data may be released to a third party only for the purpose of statistics production, statistical analyses and research. The legislation is outlined in Part 5.

Statistics Sweden provides access to data which do not allow direct or indirect identification of individuals or of other data subjects like enterprises. This means in practice anonymous data or data without name, address and identification number. Both the anonymous and the de-identified data are in principle only available to the researcher for a specified period, for a specified project and for access by specified staff of an institution.

In addition to laws and regulations on data confidentiality, Statistics Sweden follows a screening procedure requiring a written application from the researcher. In the application the researcher is required to describe the project, variables and periods during which data are used in the research, and also specify the people taking part in the project. If the project involves processing of sensitive personal data the researcher is required to add the approval of a research committee.

Heads of Statistics Sweden's departments are the only ones who can decide on the release of confidential data. Furthermore, the Director General shall always decide on matters that are of fundamental importance. An advisory committee has been established to provide advice in difficult cases or matters of principle.

When microdata are released to a researcher at a private institute or organisation, Statistics Sweden imposes legal restrictions limiting the researcher's right to pass on or use the information. If data are released to a researcher in another authority (e.g. a university), data will also be confidential at the authority receiving data, according to the Swedish Secrecy Act. In addition, researchers at other authorities normally sign a general confidentiality statement when receiving the data.

When microdata are released, it is common that a pseudo-identifier replaces the identification number. If the user needs annual series of microdata information for the same individuals, the pseudo-identifier may be connected with the identification number, and the combination is to be stored by Statistics Sweden. The possibility of having new information added by storing the combination of pseudo-identifier and identification number is restricted to research projects and for statistical purposes.

The main method of giving access to microdata for research has been to deliver the data to the user by sending a micro disc by post. The data and the metadata are sent separately.

However, since 2005 it has been possible for researchers to get access to microdata online (remote access). This allows researchers to have online access to specific servers at Statistics Sweden. However, all data processing will be carried out on the server at Statistics Sweden and no downloads are allowed. The results are frequently sent by e-mail to the researcher in the form of tables. The system is similar to the remote access system of Statistics Denmark. The Danish system is further described in the case study from Denmark.

Supply of microdata is not covered by grants provided in the state budget for production of statistics. Consequently, the costs involved in supplying microdata are to be paid by the customers. The principle is that full costs should be reflected in providing the data, i.e. cost recovery. The costs involved are to cover not only direct labour costs, but also overhead such as rental of the premises, office costs, staff costs, EDP costs, marketing costs, development costs and a proportion of the joint costs of the statistical institutes for management and administration.

## **5. Supporting legislation**

According to the Swedish Secrecy Act, any information concerning personal or economical circumstances of private subjects shall be confidential if it is managed within an authority responsible for producing statistics. However, information needed for statistics or research purposes and information which is not directly related to the private subject may be disclosed, if it is evident that the information can be disclosed without the person whom the information concerns suffering loss or other harm.

The obligation of confidentiality will – according to the law or by imposition of a duty of non-disclosure – also apply to the recipient of the data. Breach of confidentiality restrictions is punishable.

However, it is not possible to impose restrictions when data are released to other authorities. It is therefore also important for Statistics Sweden to take into consideration if data will be confidential according to the Swedish Secrecy Act at the authority receiving data.

The Statistics Act regulates the use of statistical information. According to this act, data collected for statistical purposes in accordance with any prescribed obligation to provide information, or which is given voluntarily, may in principle only be used for the production of statistics. From this principle there are exceptions that make it possible to provide access to data for research purposes and public planning. However, a condition for the use for research is that there should be no incompatibility between the purpose of such processing and the purpose for which the data was collected. The processing of data, which includes release of data, must also be in accordance with the regulation concerning the protection of the individual's privacy.

A scientific project involving processing of sensitive personal data without consent is subject to notification to, and approval by, a research committee before such processing can commence. This applies to all surveys, whether conducted by a public administration, individuals or enterprises. If the committee approves the processing, personal data may be released and used in research projects unless otherwise provided by the rules on confidentiality. This means that the statistical office may take other issues into consideration even if the research committee has approved the processing of data.

## **6. Strengths**

The arrangements are understandable by all parties, and transparent.

## **7. Weaknesses**

Researchers sometimes point out that the handling of their requests takes too much time and take the view that Statistics Sweden is too restrictive in releasing microdata.

The framework mainly depends on public confidence in research institutions and researchers. When microdata are released outside Statistics Sweden it is not possible for staff to control the use of the data. The Swedish Data Inspection Agency may observe illegal use of NSO data on their inspections at the institution.

## **8. References**

*The Official Statistics of Sweden – Annual Report 2004*. This report includes relevant Swedish legislation.

[www.scb.se](http://www.scb.se)

## **ANNEX 8. CASE STUDY - REMOTE DATA ACCESS FACILITIES - CANADA**

### **1. Broad description**

Remote data access (RDA) is a mode of indirect access to confidential microdata through which researchers submit their own computer programs via the Internet to Statistics Canada, where they are run by Statistics Canada staff on the internal unscreened microdata. The results are then vetted for confidentiality and sent back to the researcher.

### **2. Why is it good practice?**

RDA fills a gap in the continuum of access to data. On the one hand, direct access to confidential microdata is restricted according to the provisions of the Statistics Act to employees of Statistics Canada and persons deemed to be employed under the Act (see Case Study – Research Data Centre Program – Canada). On the other hand, given limited resources, there can often only be a select number of products made available in an unrestricted manner from any given statistical activity. By having indirect access to the confidential microdata through the output of the computer programs that they submit, researchers from outside Statistics Canada can fulfil their own needs for tabulations or modelling while engaging relatively little of the agency’s resources in the process. Agency staff vets the computer outputs before returning them to the researcher, thus ensuring data confidentiality.

### **3. Target audience**

RDA is available to all researchers who are not Statistics Canada employees and who have a demonstrated need to access microdata for statistical research. To prevent unnecessarily engaging the agency’s resources, researchers must ensure that any products already in the public domain are insufficient to meet their needs.

### **4. Detailed description**

When using RDA, the researcher accesses the data through the output of a computer program that is executed by a Statistics Canada employee.

First, the researcher applies for RDA. At Statistics Canada, RDA is the responsibility of individual subject-matter divisions, and the service is managed at that level. Since no direct access to the microdata is involved on the part of the researcher, the approval process essentially ensures that the output will not be confidential and that information already in the public domain would not suffice to carry out the project.

Once a research project is approved, the subject-matter division provides the researcher the tools necessary to develop the programs before submission. The set of tools includes file names, record layouts and data dictionaries. In best-practice situations, a ‘dummy’ file is also made available by the subject-matter division. This is a data file with artificial data that mimics exactly the internal microdata, and which the researcher uses to develop and test the computer program prior to submitting it to Statistics Canada.

Once development and testing is complete, the researcher sends the program electronically, via e-mail, to the subject-matter division at Statistics Canada. The program is executed by survey staff using the internal microdata file. The program's output and log (containing diagnostics for the researcher to determine whether the program has executed properly) are vetted by agency staff to determine whether any confidential information is included. Any confidential information is deleted. If the amount of confidential information is large, the researcher may be asked to modify the program to reduce the output of confidential information, and to resubmit it. Then the output and log are sent electronically to the researcher.

Depending on the resources available to support RDA within the particular statistical activity, a small fee may be levied for use of the service. The fee, if any, is usually minimal compared to the costs that can be involved in requesting custom tabulations and/or analysis from the subject-matter area.

As a rule, the researcher is solely and fully responsible for the content and accuracy of the computer program. Arrangements can be made in certain cases, where agency staff will be called to participate in the development of the programs, and potentially in the analysis of the results. Such arrangements are negotiated in advance. Because they engage more Statistics Canada resources than basic RDA arrangements, extra fees are likely to be levied.

The vetting process can be time-consuming as it primarily involves manual work. To expedite this step, advance discussions with the researcher can indicate steps that can be taken with the program to reduce the time needed for vetting.

## **5. Supporting legislation**

Since researchers do not have direct access to confidential microdata, no specific legislative authority is invoked, apart from the Statistics Act which governs Statistics Canada in general and sets out the confidentiality requirements applied to all data prior to public release.

## **6. Strengths**

- Allows the use of unscreened microdata by researchers outside of Statistics Canada.
- Provides another mode of access to microdata, and thus is another means of expanding the outputs of the research community.
- Provides another opportunity for researchers to build on their capacity to work with microdata and enhance their analytical skills.
- Can be time-effective for smaller requests.
- Relatively inexpensive compared to other options for data access.

## **7. Weaknesses**

- Inconvenient to use in some ways, as the researcher does not see outputs prior to screening for confidentiality. This can make it more difficult to get a sense of small cell size and/or data accuracy.
- Not all software is supported. Researchers may have to learn new software or work with less familiar software.
- All output must be vetted for confidentiality prior to being returned to the researcher, engaging Statistics Canada resources.

- Requires that researchers learn and understand the content of the survey and microdata file, instead of relying on subject-matter staff as would be the case when requesting custom tabular and/or analytical output.

## **8. References**

The various modes of access, including RDA, that are available for a number of surveys at Statistics Canada are well described in Tambay, J.-L., Goldmann, G., and White, P. (2001). *Providing Greater Access To Survey Data For Analysis At Statistics Canada*. Proceedings of the Annual Meeting of the American Statistical Association, August 5-9 2001.

More information can be obtained by contacting Statistics Canada staff or on the Statistics Canada web site ([www.statcan.ca](http://www.statcan.ca)). See [www.statcan.ca/cgi-bin/statcomment.pl](http://www.statcan.ca/cgi-bin/statcomment.pl)



## **ANNEX 9. CASE STUDY - REMOTE ACCESS FACILITY (FOR MICRODATA ACCESS) - AUSTRALIA**

### **1. Broad description**

The Remote Access Data Laboratory (RADL) is a web-based tool that allows authorised users to access detailed microdata that is stored within the Australian Bureau of Statistics (ABS) secure environment. Built-in automatic checks prevent large-scale release of unit record information, thus maintaining confidentiality of data providers as outlined in Australian legislation.

### **2. Why is it good practice?**

The RADL provides access to more detailed and less confidentialised microdata than can be made available on CD-ROM. It provides greater flexibility in user analysis of microdata.

Access is limited to authorised users. All microdata remains within the ABS computing system. A balanced mix of automatic and manual processes prevent clients from obtaining outputs containing large amounts of unit record information. An audit trail is automatically maintained.

### **3. Target audience**

The RADL is primarily targeted at Australian government agencies involved in policy development and research areas within Australian universities. To a lesser extent, the RADL is also used for research purposes by the private sector and by non-profit institutions.

### **4. Detailed description**

Potential users of microdata are required to sign legal undertakings and read training material provided before RADL access will be granted. Authorised users are required to comply with published data-security guidelines and any further instructions of the ABS.

The RADL operates as a three-stage process. Clients submit batch-style queries via a secure section of the ABS website, which are firstly parsed for illegal commands. If the query is accepted, it is then executed in conjunction with ABS confidentialised microdata files. Finally, all produced output is automatically checked for confidentiality issues before being made available to clients on a secure web page.

A retrospective auditing process manually checks for inappropriate use of ABS microdata, and provides empirical evidence that automatic checks have been applied appropriately.

### **5. Supporting legislation**

The release of microdata by the ABS is governed by legislation, the Census and Statistics Act 1905. This legislation enables the Australian Statistician to release unit record data, provided this is done “in a manner that is not likely to enable the identification of a particular person or organisation to which it relates”. Section 5 of Annex 1 provides more detail.

### **6. Strengths**

- (i) Provides a secure online access point, from which users may access detailed ABS microdata from their own computing environments.
- (ii) Automatic protection of output at time of execution allows quick turnaround.

- (iii) Enables ABS to release more detailed microdata than that which can be released on CD-ROM.
- (iv) Flexibility of user analysis. Users are not restricted to a set of predefined tables.
- (v) Users are alleviated of CD-ROM security and data storage concerns.
- (vi) Statistical software is provided by ABS. Users do not need to supply their own licenses.

## **7. Weaknesses**

- (i) Researchers still believe the conditions of release are too limiting and that the steps taken to make identification unlikely result in too little detail being released.
- (ii) Limited to batch-mode style of programming, lack of graphical-user interface functionality.
- (iii) Time taken to build automatic protections limits variety of statistical software packages made available.
- (iv) Heavy manual auditing load.

## **8. References**

Australian Bureau of Statistics, (2005), *Responsible Access to ABS Confidentialised Unit Record Files (CURFs) Training manual*, Edition 2, Canberra, Australia, also available at [www.abs.gov.au->services we provide->curfs](http://www.abs.gov.au->services we provide->curfs).

Australian Bureau of Statistics, (2004), *The Remote Access Data Laboratory (RADL) User Guide*, Revised Version 2.0, Canberra, Australia, also available at [www.abs.gov.au->services we provide->curfs](http://www.abs.gov.au->services we provide->curfs).

Access to ABS CURFs web pages at [www.abs.gov.au->services we provide->curfs](http://www.abs.gov.au->services we provide->curfs).

## **ANNEX 10. CASE STUDY – REMOTE ACCESS TO MICRODATA FILES - DENMARK**

### **1. Broad description**

Statistics Denmark allows access to licensed (de-identified) microdata files for researchers and analysts. Access is only granted to employees (researchers and analysts) at institutions holding a special authorization issued by the General Director of Statistics Denmark. Special contracts are signed by the head of the institution and the researcher. Data are declared as confidential. Statistics Denmark has developed a remote access system allowing access to data from the researcher's own workplace.

Statistics Denmark does not give access to public-use microdata.

### **2. Why is it good practice?**

The system allows access to very detailed de-identified microdata with a maximum of flexibility both to Statistics Denmark and the research environment. The system has replaced an on-site arrangement used for about 15 years. The researchers no longer have to work from premises in Statistics Denmark, which has allowed many more researchers to start research projects using microdata.

The technical system together with the authorization procedure and signed contracts is considered safe in relation to confidentiality. The basic microdata does not leave the premises of Statistics Denmark at any time, as only the statistical results are allowed to be transferred to the researcher.

The system is supported by the Danish Ministry of Research with a special grant. €800,000 per year is allocated to Statistics Denmark in order to reduce the costs of each project and with the vision that Danish researchers should develop to be among the best in the world to use register data.

### **3. Target audience**

Authorizations can be granted to public research and analysts' environments (e.g. in universities, sector research institutes, ministries etc.) and to research organizations within a charitable organization.

Within the private sector, the following user groups can be granted authorisation if they have a stable research or analysts' environment (with a responsible manager and with a group of researchers/analysts):

- (i) Non-governmental organisations;
- (ii) Consultancy firms;
- (iii) Enterprises, although single enterprises cannot access microdata with enterprise data.

In order to grant an authorisation, Statistics Denmark will evaluate the proposed organization carefully, especially when it is an organization or firm within the private sector. Statistics Denmark will consider the credibility of the applicant in the light of ownership, educational standard among the staff and the research done for others.

Statistics Denmark will not grant authorization to single persons. Furthermore, media organizations are excluded from the scheme.

A ‘need to know’ principle is used as Statistics Denmark does not allow access to more data than needed according to the project description.

Researchers can have access to relevant business data after the “need to know” principle. Very few business data are excluded from remote access.

Only Danish research environments are granted authorisation as Statistics Denmark is not able effectively to enforce a contract abroad. Foreign researchers from well-established research centres can have access to Danish microdata from the on-site arrangement in Copenhagen or Århus. Visiting researchers can have remote access from a workplace in the Danish research institution during their stay in Denmark and under the Danish authorisation.

#### **4. Detailed description**

(i) The scheme is administered centrally by the Division of Research Services. The staff of this unit also creates a substantial part of the inter-disciplinary data sets and have a general (authorized) access to all relevant Statistics Denmark data in order to reduce the administrative and bureaucratic workload. The scheme requires close cooperation between the Division of Research Services and the individual divisions. The advantage of such central organisation is that the individual researcher is fully aware of who to negotiate with and who is responsible for the data set supplied.

(ii) Statistics Denmark has not applied scrambling procedures or special grouping techniques to the data that are made available to the researchers. The data appear as in the basic register. It means that the linked data can be very detailed.

(iii) The technical solution is web-based, as shown on the flow chart at the end of this case study.

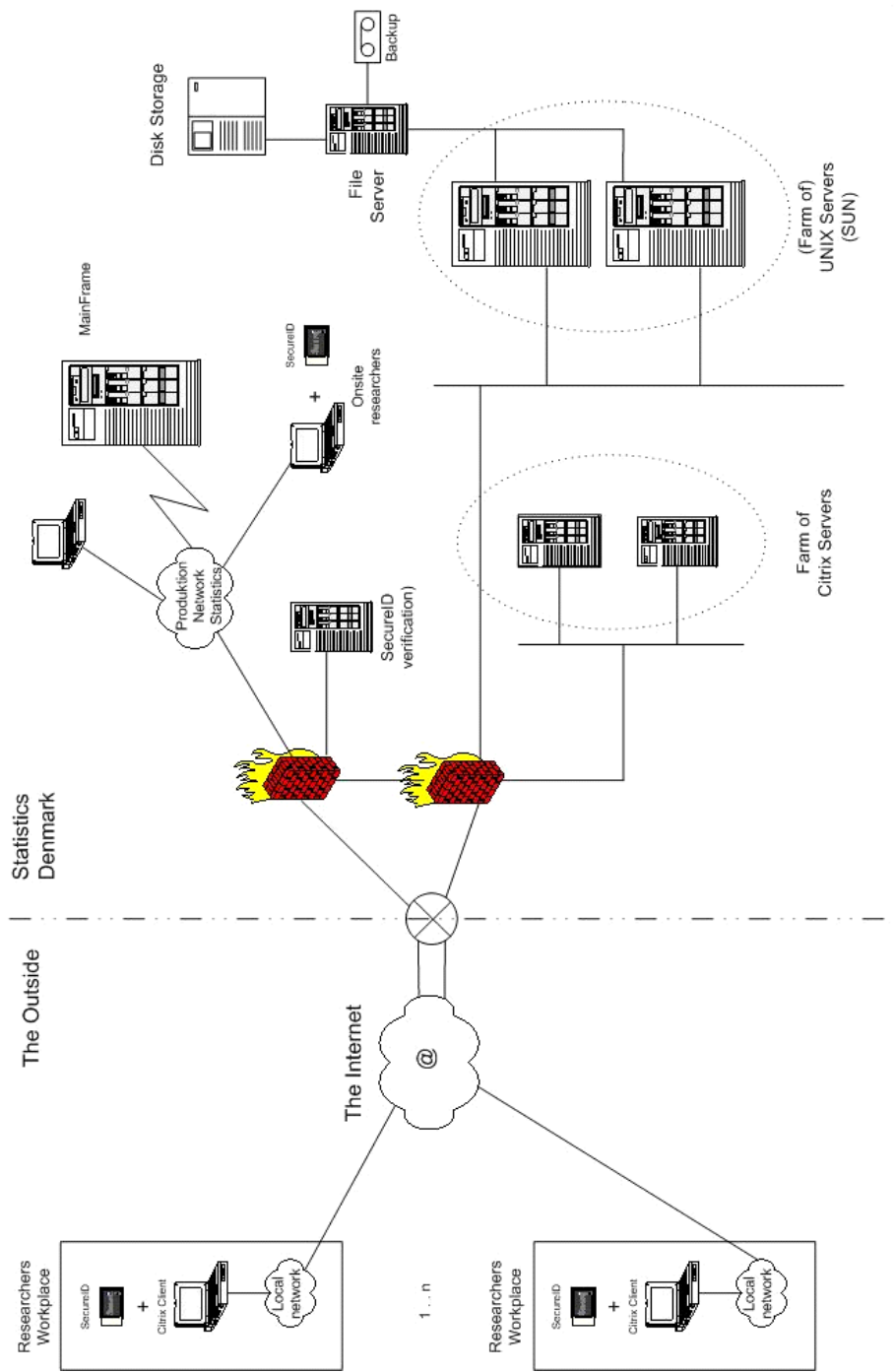
The relevant microdata are produced by Statistics Denmark staff and the de-identified microdata are transferred to the disk storage connected to the special Unix servers. These Unix servers are only used by researchers and are separated from the production network.

Communication via the Internet is encrypted by means of a so-called RSA SecurID card, a component that secures Internet communications against unauthorised access. In practice the researcher rents a password key (a token) from Statistics Denmark. The token ensures that only the authorised person obtains access to the computer system.

A farm of Citrix Servers ensures that the researchers from their own workplace can ‘see’ the Unix environment in Statistics Denmark. All data processing is actually done at Statistics Denmark and data cannot be transferred from Statistics Denmark to the researcher’s computer. The researcher can work with the data quite freely and can make new data sets from the original data sets. The limit is of course the amount of disk space. Statistics Denmark has just increased the total amount of disk space considerably.

All results from the researchers’ computer work can be stored in a special file and printouts are sent to the researchers by e-mail. This is a continuous process (every five minutes) and has proved to be quite effective. The advantage to Statistics Denmark is that all e-mails are logged at Statistics Denmark and checked by the Research Service Unit. If the unit finds printouts with too detailed data, the researcher is contacted to agree on details of the level of output. No severe violation of the rules established in the authorisation formula has so far taken place.

Remote Access to Statistics Denmark. January 2003. Principles of Operation



Rev 1 March 13th, 2002  
ABJ.

The Act  
 processing  
 previous  
 new Act  
 covers all  
 merging,

research has  
 as very  
 the use of  
 1997, 71  
 the access  
 is granted

increasing  
 space is

system is  
 of the data

the Joint  
 2003).

operates.

## **ANNEX 11. CASE STUDY - RESEARCH DATA CENTRE PROGRAM - CANADA**

### **1. Broad description**

Starting in 2000, Statistics Canada, in partnership with participating Canadian universities, the Social Sciences and Humanities Research Council and the Canadian Foundation for Innovation, established a network of Research Data Centres (RDC) in Canadian universities. These centres are enclaves of Statistics Canada, within which researchers have access to household survey data in an environment that respects Statistics Canada's requirements for security and confidentiality. There are currently 15 RDC locations across the country, plus a federal RDC in Ottawa used by statistical researchers in federal government departments.

### **2. Why is it good practice?**

The Chief Statistician and the President of the Social Sciences and Humanities Research Council (a granting council for the human sciences) established a panel of highly qualified individuals to assess how social sciences could become more relevant and more quantitatively oriented. The panel observed that Canada's capacity in the quantitative social sciences was stagnating, due in part to difficulties in accessing the data needed to conduct analyses on some of the important socio-economic and demographic issues facing Canadian society. It was also observed that the advent of complex longitudinal survey data made it very difficult (if not impossible) to create useful public-use microdata files. The Research Data Centre Program successfully addresses the issues of access while respecting the provisions of the Statistics Act for security and confidentiality of the data. The RDC Program makes it possible for researchers outside Statistics Canada to directly access microdata (after satisfying several conditions) that would otherwise not be available to them. Society benefits because insights are gained that would otherwise not be possible; and the statistical system benefits because the visible relevance of available statistical information increases. The following are the basic features:

- Academics wishing to access confidential microdata submit a research proposal which is peer reviewed by the Social Sciences and Humanities Research Council;
- Authors of accepted proposals are sworn in under the Statistics Act as employees of Statistics Canada, subject to all the conditions and penalties of the Statistics Act;
- All work is carried out in an RDC, which in turn is supervised by a regular Statistics Canada employee;
- Academics must submit a short article to SC for potential publication.

The proposal is based on two features of the Statistics Act: first, that it explicitly mandates Statistics Canada to analyse data; and second, it allows the agency to swear in under the Act personnel needed to carry out its mandate.

### **3. Target audience**

The RDC Programme is open to all researchers who are not employees of Statistics Canada and who require microdata for statistical research. This includes established academics, new researchers, graduate students and researchers from federal departments and provincial governments.

#### **4. Detailed description**

A researcher (or research team) seeking access to the detailed microdata must submit a proposal that outlines the analyses to be conducted. The proposal must be a maximum of five pages excluding the CV of the researcher(s) and it must contain the following information:

- Project title;
- Rationale and objectives of the study, including: specific questions or objectives of the project; and how the research will contribute to the knowledge in the field of study;
- Proposed data analysis and software requirements including: the proposed statistical methodology; its suitability for this project; and the software needed;
- Data requirements including: why access to the confidential data (as opposed to public use microdata files) is necessary; the survey file/files or cycles to be used; a description of the specific population of interest; and a list of the variables to be used;
- Expected project start and end dates; and
- References – sources of quotes used in the proposal or for specific analytical methods employed.

All proposed research projects are reviewed by a peer-group committee who determine the academic merit of the work and the suitability of the methods and the data. They also verify that the work can only be undertaken with access to the confidential data files. In cases where the Public Use Files would be suitable or the work lacks rigour or focus, the application will be denied. Approved researchers have access to the required files within a RDC, but only results that have been screened for disclosure protection can be removed from the RDC. Researchers are required to produce a report for Statistics Canada as part of their commitment under the Statistics Act (the so-called “deemed employee” provisions of the Act). Once that obligation is fulfilled, researchers are free to publish other articles that may be based on the research project.

Before being granted access to the data, researchers must undergo a security check; sign the oath/affirmation of secrecy required by the Statistics Act; acknowledge in writing that they have read and understood the relevant sections in the Statistics Act and specifically the policies related to data confidentiality and security; acknowledge in writing that they have read the documentation on conflict of interest and declaring that they will comply with the requirements.

The RDC network has substantially increased the access by researchers to the complex detailed microdata survey files. As of June 2005 there were over 500 active projects and over 1,300 researchers in the centres. Approximately one third of the researchers are students. There are also over 280 articles, book chapters, working papers and theses that have been published from the research conducted in the centres.

#### **5. Supporting legislation**

Section 5 of the *Statistics Act* permits persons carrying out any function or performing work for Statistics Canada to become “deemed employees”, thereby allowing access to the confidential data files.

#### **6. Strengths**

- Allows access to data outside the Statistics Canada offices while continuing to respect the requirements of the Statistics Act.

- Increases the opportunity to conduct research on key socio-economic and demographic issues and expands the quantity and range of research outputs using statistical data.
- Effective in developing the next generation of quantitative social scientists in Canada.
- Provides greater research opportunities for highly qualified analysts who do not reside in cities in which Statistics Canada has offices.
- As the use of the data increases, greater feedback is obtained on the surveys and the data sets that they generate. This results in quality improvements in the data and it opens new possibilities for the use of the data.
- Accelerates the development of advanced statistical methods required to analyse complex survey data.
- Provides Statistics Canada with much more detailed and timely information on the use of its data.
- Locating RDCs in universities reduces the cost of conducting research since it eliminates the need for travel for many researchers.
- The research conducted in the RDCs adds substantially to the body of literature on major social, economic and demographic questions affecting Canadian society. It also serves to inform public policy and debate.

#### **7. Weaknesses**

- RDCs are costly to build, manage and operate. This places them out of the reach of some of the smaller universities in Canada.
- All output must be vetted for confidentiality prior to leaving the RDC. This is a manual effort and, even when prompt attention is given to the vetting, results in some delays to the researcher.
- To date, data sets in the RDCs have been from household surveys. Although the demand exists and there are no technological barriers, access to data from the census of population and from business surveys are not placed in the RDCs.

#### **8. References**

Statistics Canada's Policy on the Use of Deemed Employees is available on request. More information on the Research Data Centre Program can be viewed at the Statistics Canada web site at: [www.statcan.ca/english/rdc](http://www.statcan.ca/english/rdc).



## ANNEX 12. CASE STUDY - RESEARCH DATA CENTRES – UNITED STATES

### 1. Broad description

Research Data Centres (RDCs) offer qualified researchers restricted access to confidential economic and demographic data collected by the U.S. Census Bureau in its surveys and censuses. All projects must offer benefits to U.S. Census Bureau programmes. These projects are carried out at U.S. Census Bureau headquarters, or at one of eight other secure locations around the U.S.

### 2. Why is it good practice?

The statutory provisions under which the U.S. Census Bureau collects data prevent the release of the full details of survey data (e.g. names, addresses) in order to protect the confidentiality of respondents. The microdata provided by businesses are never released to the public; public use microdata samples of household surveys include limitations on geography, topcodes on income, collapsing of occupational categories, and so forth. Nevertheless, some research would benefit from access to this additional information. A ‘research enclave’ where data dissemination is tightly controlled allows the estimation of statistical models based on the full data set.

### 3. Target audience

RDCs are aimed at researchers in academia; at independent research organizations such as the National Bureau of Economic Research; and in federal, state, and local government agencies. Tabulations of confidential data are generally not allowed to be removed from the RDCs, and therefore estimation of statistical models is the focus of their activities. All researchers are required to become Special Sworn Status employees of the U.S. Census Bureau, and as such are subject to the penalty provisions of its authorizing legislation (e.g. a fine of US\$250,000), should there be a confidentiality violation.

### 4. Detailed description

The objective of the U.S. Census Bureau and the RDCs is to increase the utility and quality of U.S. Census Bureau data products. Access to microdata encourages knowledgeable researchers to become familiar with U.S. Census Bureau data products and data collection methods. More importantly, providing qualified researchers access to confidential microdata enables research projects that would not be possible without access to respondent-level information. This increases the value of data that has already been collected. Access to the microdata also allows for data linking that is not possible with aggregates – both cross-survey linkages and longitudinal linkages. These linkages leverage the value of existing data. Creative use of microdata can address important policy questions without the need for additional data collection.

In addition, the best means by which the U.S. Census Bureau can check the quality of the data it collects, edits, and tabulates is to make its microdata records available in a controlled, secure environment to sophisticated users who, by employing the microdata records in the course of rigorous analysis, will uncover the strengths and weaknesses of those records. Each set of observations is the end result of many decision rules covering definitions, classifications, coding procedures, processing rules, editing rules, disclosure rules, and so forth. The validity and consequences of all these decision rules only become evident when the U.S. Census Bureau’s micro databases are tested in the course of analysis. Exposing the conceptual and processing assumptions that are embedded in the U.S. Census Bureau’s micro databases to the light of research constitutes a core element in the U.S. Census Bureau’s commitment to quality.

The opportunities for researchers to carry out unique research come at a price. Research conducted at RDCs takes place under a set of rules and limitations that are considerably more constraining than those prevailing in typical research environments. The process is described below.

Working closely with an RDC administrator, researchers develop a preliminary research proposal that includes information about the researcher(s), site where the research will be carried out, its purpose, funding source, requested data sets, desired software, a brief narrative description of the research project and proposed benefits to the U.S. Census Bureau. The researcher enters this information via the online proposal management system. Once a preliminary proposal has been submitted, the RDC administrator reviews it and advises the researcher of any suggestions for improvement or refinement. The administrator must approve the preliminary proposal before the researcher can submit a final proposal to the U.S. Census Bureau's Center for Economic Studies (CES) for final review.

Research proposals submitted to CES are reviewed on the basis of five major criteria:

- **Benefit to U.S. Census Bureau programmes.** Proposals must demonstrate that the research is likely to provide one or more benefits to the U.S. Census Bureau. These benefits can include:
  - Understanding and/or improving the quality of data produced through a Title 13, Chapter 5 survey, census, or estimate [Title 13 is the U.S. Census Bureau's authorizing legislation];
  - Leading to new or improved methodology to collect, measure, or tabulate a Title 13, Chapter 5 survey, census, or estimate;
  - Enhancing the data collected in a Title 13, Chapter 5 survey or census, for example
  - Improving imputations for non-response, or developing links across time or entities for data gathered in censuses and surveys authorized by Title 13, Chapter 5;
  - Identifying the limitations of, or improving, the underlying Business Register, Household Master Address File, and industrial and geographical classification schemes used to collect the data;
  - Identifying shortcomings of current data, collection programmes and/or documenting new data collection needs;
  - Constructing, verifying, or improving the sampling frame for a census or survey authorized under Title 13, Chapter 5;
  - Preparing estimates of population and characteristics of population as authorized under Title 13, Chapter 5;
  - Developing a methodology for estimating non-response to a census or survey authorized under Title 13, Chapter 5; and
  - Developing statistical weights for a survey authorized under Title 13, Chapter 5.
- **Scientific merit.** This criterion relates to the project's likelihood of contributing to existing knowledge. Evidence that a federal agency such as the National Science Foundation or the National Institutes of Health has approved the proposal for support constitutes one indication of scientific merit.
- **Clear need for non-public data.** The proposal should demonstrate the need for and importance of non-public data. The proposal should explain why publicly available data sources are not sufficient to meet the proposal's objectives.
- **Feasibility.** The proposal must show that the research can be conducted successfully with the methodology and requested data.

- **Risk of disclosure.** Output from all research projects must undergo and pass disclosure review.
  - Tabular and graphical output presents a higher risk to disclosure of confidential information than do coefficients from statistical models.
  - The U.S. Census Bureau is required by law to protect the confidentiality of data collected under its authorizing legislation.
  - Some data files are collected under the sponsorship of other agencies. In providing restricted access to these data, the U.S. Census Bureau Center for Economic Studies (CES) must adhere to all applicable laws and regulations.
  - Researchers may be required to sign non-disclosure documents of survey sponsors or other agencies that provide data for their research projects.

Both U.S. Census Bureau and external experts on subject matter, data sets and disclosure risk review all proposals. Relevant data sponsors and data custodians also review proposals that request certain data sets. Any proposals seeking to use data sets that contain Federal Tax Information must also be reviewed for approval by the Internal Revenue Service.

All of the actual processing of data for approved proposals is conducted on servers located in the U.S. Census Bureau's secure central computer facility. Researchers located in the RDCs use 'thin client' terminals to access these servers via encrypted communication lines.

## 5. Supporting legislation

Title 13, United States Code, permits the U.S. Census Bureau to employ Special Sworn Status employees for the purpose of carrying out its mission. Specifically, Section 23(c) states:

“The Secretary [of Commerce] may utilize temporary staff, including employees of Federal, State, or local agencies or instrumentalities, and employees of private organizations to assist the Bureau in performing the work authorized by this title, but only if such temporary staff is sworn to observe the limitations imposed by section 9 of this title.”

## 6. Strengths

- (i) As administrative data about individuals becomes more and more available through the Internet, statistical agencies must reduce the detail about individuals available through public use microdata. The availability of such data through the RDCs as research enclaves can help ensure that valuable research can continue.
- (ii) Since business microdata has never been in the public domain, the RDCs allow microeconomic research on businesses that could not otherwise take place.
- (iii) There is potential for expansion to allow the confidential data of other federal agencies to be available through the RDCs.

## 7. Weaknesses

- (i) Operating the RDCs has costs, some of which must be absorbed by the U.S. Census Bureau.
- (ii) The proposal review process is cumbersome and time consuming, and the consequent delays in getting access to the data at the RDCs are frustrating to researchers.

(iii) All projects must, by law, have a benefit to the U.S. Census Bureau. Therefore, some worthy research projects with questionable benefits must be rejected.

## **8. References**

The CES web site contains additional information about the RDC programme:  
<http://www.ces.census.gov/ces.php/rdc#objectives>.

Prepared by Dr. Daniel Weinberg, Chief, Center for Economic Studies, and Chief Economist,  
U.S. Census Bureau, October 13, 2005.

## **ANNEX 13. CASE STUDY - DATA LABORATORY ARRANGEMENTS - NETHERLANDS**

### **1. Broad description**

After the initial success of releasing licensed microdata files from its social sample surveys from 1994 onwards, researchers also developed a demand for accessing other microdata files: business survey microdata, fiscal income data, cause-of-death data, and the like. Such data are much less easy to protect against disclosure because important variables are very skewed in their distributions, samples are much more stratified and even integral in some (or all) strata, and so on. The solution to serve these researchers was to create a separate research facility, a data laboratory, within the safe walls of Statistics Netherlands' (Central Bureau voor de Statistiek, or CBS) two establishments, with most universities within an hour's reach. So with this solution the microdata does not go to the researcher but the researcher comes to the microdata. In 1998 the Centre for Research on Economic Microdata (Cerem) was established after fairly long consultations with business representatives who needed to be convinced of the utility and the safety of academic on-site analysis of business microdata. Subsequently on-site facilities were also used by researchers on social microdata with more detail than can be found in the licensed microdata files, and by researchers on social microdata from matched administrative data.

More recently the Centre for Policy Statistics (CPS) was set up as a department of Statistics Netherlands in 2002 in response to an increasing demand for statistical information by government policymakers and national planning agencies. One important factor in this respect was the demand for statistics to measure the effects of policy measures, and to gain insight into possible effects of a change in policy measures.

These demands are mostly of a short-term character. Almost inevitably the statistical programme of a national statistical agency like Statistics Netherlands (SN) is not suited for short term changes. Instead the programme is based on producing statistics that can be compared over time and therefore have a slow rate of change. This makes it difficult to fulfil the needs of government departments and planning offices in this respect.

The CPS was set up to improve the fulfilment of these demands. Flexibility was achieved by making the working programme of the Centre dependent on the demands of the departments and planning offices. Only a few of the staff are paid directly from the budget of SN. Other demands for statistics are paid directly by the departments. A pilot project was set up with the Ministry of Social Affairs and Employment in 2002. This pilot was successful and led to a further increase in services.

### **2. Why is it good practice?**

The data laboratory arrangement makes it possible to have microdata analysed in a safe setting. The microdata themselves cannot always be protected; for example, the producer of light bulbs from Eindhoven will always be recognisable and indispensable at the same time. But the settings in which these microdata are analysed are fully controlled. The number of days spent in the data laboratories is increasing each year by more than 20% and has now surpassed 750.

### 3. Target audience

Microdata are made accessible under a contract or license to legitimate researchers only. Section 41 of the law cites the researchers that are qualified. These include the universities and other research institutes with a legal foundation, but also Eurostat and the EU NSOs. A residual category of applicants must be formally admitted by the Central Commission for Statistics (CCS), the supervisory body for CBS. The CCS has set its own criteria and procedures for deciding, in which a focus on statistical (aggregate) research, independence from administrative authorities, and the intention to share results in the public domain are predominant. The CCS has no principal objection against admitting non-EU universities, for example, but a commercial bank or a journalist would not be eligible. In practice, researchers seem to have better methodological qualifications when working on site, if only because their microdata and statistical models and software are complex in comparison with the social analysis of official social sample survey microdata at the universities. At present only researchers affiliated with Dutch research institutes are allowed.

### 4. Detailed description

The services of CPS can be divided into three groups.

- First there is the advisory function. The Centre can give advice about the possibilities of doing research on a specific question. Because the CPS staff have a broad knowledge of the available data sources, this can help to reduce data collection costs.
- Secondly, as mentioned above, CPS can itself conduct research on request. This research is done solely on existing data material; no additional survey activity is undertaken in this respect.
- A third activity is the possibility to provide access to microdata for researchers from outside SN. The microdata are made available at the level of individual records where, of course, direct identifiers are removed.

The datasets are all well documented, making it possible for researchers to gain access to the material efficiently and to evaluate the relevance of the dataset for their research.

Furthermore, precautions are taken to ensure that the security of the process is maximised.

Most microdata are made available for analysis on-site: i.e. researchers work at one of the offices of Statistics Netherlands on a dedicated infrastructure. For reasons of security, this infrastructure is physically disconnected from Statistics Netherlands' production environment and visitors only have access to the micro datasets they need for their specific research.

A second type of microdata service is *remote execution*. Using this service, researchers may send in scripts to be executed on well-defined sets of micro data.

For all types of microdata services, checks on the possibility of statistical disclosure are performed before results are made available to researchers for use outside the secure environment.

From mid-2005 a *remote access* facility has been developed, making it possible for researchers to analyse microdata present at SN through a secure connection from workstations in their own institute. This facility is much like the facility in use in Denmark.

Part of the security regime here is the use of a secure Internet connexion and the application of biometric identification (fingerprints) and PKI certificates.

The on-site facilities for microdata analysis within SN developed in recent years originate from different departments, and were designed slightly differently. Apart from the on-site facility within the CPS, there were separate facilities within the department for social statistics and a facility for economic statistics, known as CEREM (Centre for Research on Economic Microdata). At the end of 2005 all the activities for microdata services were pooled within the CPS, enabling a more transparent and more efficient microdata access. This means that, although CEREM as such is no longer in existence, CPS offers the same facilities and availability for microdata analyses.

The use of microdata is expected to grow rapidly the coming years. In this respect, the remote access facilities in particular are promising.

## **5. Supporting legislation**

In 2003 the statistical legislation allowing the release of microdata was rephrased to make formally possible the analysis of microdata on site in a data laboratory. Section 41 now makes it possible “to provide or grant access to a set of data”.

## **6. Strengths**

The main strength from the perspective of the researcher is that there is hardly a limit to the amount and nature of microdata that can be analysed.

## **7. Weaknesses**

The main remaining weakness is the restriction to the premises of CBS. This restriction entails travelling time, working within standard office hours, and the use of hardware and software as they are available at CBS. Another weakness, at least from an international perspective, is the language used for documentation. Because the main use of the (meta)data is by staff from CBS, the number of Dutch researchers on specific microdata sets is limited, and foreign researchers are not allowed, there is no push to provide high quality metadata in English.

## **8. References**

The Centre for Policy statistics can be reached by e-mail at [CvB@CBS.nl](mailto:CvB@CBS.nl). Within the CPS, contact persons are Frans Hoeve (+31 70 337 5609 of [FHVE@CBS.nl](mailto:FHVE@CBS.nl)) and Gerhard Meinen (+31 70 337 4228 or [GMNE@CBS.nl](mailto:GMNE@CBS.nl)).

## **ANNEX 14. CASE STUDY - DATA LABORATORY MICRODATA ACCESS - NEW ZEALAND**

### **1. Broad description**

Access to anonymised unit record data is provided to researchers in a secure environment within the regional offices of Statistics New Zealand (SNZ).

Access to microdata is governed by the provisions of the New Zealand Statistics Act 1975, and is implemented in accordance with SNZ's microdata access protocols (see [www.stats.govt.nz/about-us/policies-and-guidelines/general/microdata-access-protocols.htm](http://www.stats.govt.nz/about-us/policies-and-guidelines/general/microdata-access-protocols.htm)). All microdata access requests are subject to the approval of the Government Statistician.

Microdata access can be supplied to New Zealand government departments for bona fide research or statistical purposes, or to researchers contracted to SNZ (who must provide some output from their work that is of direct value to the Official Statistics System), and to other government agencies and bodies in New Zealand when data has been collected jointly. The Government Statistician can also permit access to microdata when written consent has been obtained from all the people who supplied the data.

To request access to unit record data through the data laboratory, a researcher must complete an application form which includes adequate detail on the nature of the intended research, what variables are required, and the proposed outcomes of the research, such as publications, presentations, or a contribution to ongoing research. An initial application form is completed by the applicant. This is assessed by relevant staff of SNZ, who will work with the applicant to produce a final application that is feasible and complies with the department's microdata access criteria. Once an application is in a form which meets the department's criteria, it is submitted to the Government Statistician, who makes a decision to approve or refuse the request. If an application is refused on some grounds, the applicant can address that issue and resubmit an altered application.

### **2. Why it is good practice?**

The data laboratory balances the need to ensure that New Zealanders have confidence in SNZ's ability to protect their identities and personal information with the value this information has for conducting research and developing Government policy.

The data laboratory gives sophisticated researchers access to unit record data that is not otherwise available. The rigorous process for approving applications ensures that the provisions of the Statistics Act 1975 are always taken into account when access to unit record data is granted, and that access to the unit record data is necessary for the proposed work.

A number of techniques are used to limit the disclosure risk. Unit record data are anonymised and modified to protect respondent identities. Data sets are made available in a secure physical and computing environment to prevent unauthorised access to the data. Statistical outputs generated in the data laboratory are checked to guard against disclosure risks. Finally, all papers and reports produced based on data laboratory research are checked prior to publication.



### **3. Target audience**

The data laboratory is aimed at researchers and analysts working in New Zealand. In some instances a visiting foreign academic, who can point to benefits to New Zealand's Official Statistical System from their study, may be given consideration.

### **4. Detailed description**

The following steps outline the assessment and approval process that follows the receipt of an initial data laboratory application form. During this process, staff at SNZ and the researchers seeking access to microdata may be involved in frequent communication. The data laboratory administrator coordinates communication and ensures that agreements and decisions are recorded.

1. The subject-matter area (SMA) unit responsible for the data to which access is requested examines the proposal in terms of the fitness for purpose of the proposed data set and variables requested for the study. Depending on the basis for permitting access to the microdata relevant issues may include sample sizes, data quality, confidentiality, and whether the research will benefit the official statistical system. SMA staff provide an assessment, and the manager of the SMA unit then makes a recommendation on whether the requested access to microdata should be approved or not.
2. The Statistical Methods unit examines the proposal for potential breaches of confidentiality, and specifies modifications to the data (typically removal or aggregation of geographic variables and randomisation of IDs) to minimise these risks. The manager of the Statistical Methods unit then makes a recommendation on whether the requested access to microdata should be approved or not.
3. A staff member from Strategic and Financial Services determines if the application is consistent with the requirements of the Statistics Act 1975 and SNZ's microdata access protocols.
4. The Microdata Access Manager prepares a summary of the issues raised for consideration by senior management.
5. The Group Manager responsible for the SMA provides their comments, and a recommendation to the Government Statistician to approve or reject the requested access to microdata.
6. The Government Statistician approves or rejects the application for microdata access through the data laboratory. The researcher is then advised of the decision.

If the application is refused, the researcher will be notified of the reasons for the refusal. The researcher can subsequently resubmit an application. This is usually done after modifying the proposal to address the particular grounds for refusal.

If the proposal is accepted, the SMA unit creates a customised data set designed to provide only the information needed for the research. Statistical Methods staff check this data set before it is copied to the data laboratory. A contract is drafted and signed prior to researchers beginning their work. The restrictions on how data may be used are set out in the contract, and these obligations are made clear to each user who is given access to data. All researchers must also sign the statutory declaration of secrecy, required under the Statistics Act 1975, before beginning to work with the data. Once an agreement has been signed, changes such as the addition of new researchers to the agreement, are managed by way of letter of variation. Signatory rights are limited to Deputy Government Statistician level.

7. While research is underway, Statistical Methods staff check all outputs to ensure that there are no confidentiality breaches. All draft publications are also submitted to SNZ for checking.

## **5. Supporting legislation**

The release of microdata into the data laboratory environment is governed by the Statistics Act 1975.

## **6. Strengths**

(i) The data laboratory allows for access to the most detailed data available for users working within the secure environment.

(ii) Contracts provide a legal framework to ensure confidentiality protection for these data sets.

(iii) Sanctions can be applied to users and organisations that breach the agreements, and this helps to ensure use of data sets is appropriate.

## **7. Weaknesses**

(i) Researchers complain that the timeframe for approval is too lengthy. SMAs have found that it can be difficult to balance their regular work programme with the uneven demands placed on them by data laboratory projects.

(ii) The recovery of costs for access, support and initial data set development is problematic for some academic researchers.

(iii) The care and attention given to the approval of proposals and the checking of outputs can be expensive and time-consuming.

## **8. References**

Datalab: [www.stats.govt.nz/products-and-services/datalab.htm](http://www.stats.govt.nz/products-and-services/datalab.htm)

Statistics Act 1975: [www.legislation.govt.nz/](http://www.legislation.govt.nz/)

Microdata access protocols: [www.stats.govt.nz/about-us/policies-and-guidelines/general/microdata-access-protocols.htm](http://www.stats.govt.nz/about-us/policies-and-guidelines/general/microdata-access-protocols.htm)

## **ANNEX 15. CASE STUDY – DATA LABORATORY MICRODATA ACCESS - BRAZIL**

### **1. Broad description**

Statistical dissemination in the Brazilian Institute of Geography and Statistics (IBGE) was traditionally carried out in two ways: for the general public, by means of media communication, assisted by media releases or press conferences; and for the general users, through printed publications and electronic publications. For more specialized users and government agencies, the requirements are met through customized tables and public use microdata files.

A policy of free dissemination of all products through Internet has been adopted in IBGE, since 2001. There has been outstanding growth in this communication channel.

As well as the electronic publications, the IBGE web page contains two important databases: Aggregated Statistical Tables (SIDRA) – a database with information grouped at territorial level that allows the users to construct tables according to selected information; and Multidimensional Statistical Database (BME) – a database with microdata information that allows users to construct tables according to selected information and confidentiality constraints. This database requires Internet subscription.

IBGE has been releasing public use microdata files for households' statistics since the early 1990s. Measures taken to protect the confidentiality of these microdata include suppression of geographical detail. However, no public use microdata files are released for businesses data, or for the 1996 Agricultural Census and the short form 2000 Population Census.

The pressure of increasing demand, the advance of technology and the increase of sensitivity to privacy issues have encouraged the development of arrangements to provide restricted access for researchers to data files that the statistical agency does not release to the general public. These arrangements permit a more in-depth analysis than was possible when using tabular aggregated data. This is done in IBGE via on-site access at the headquarters of the agency.

This Case Study provides short summaries of the procedures that have been implemented and are currently in use by IBGE since 2003, in order to permit external researchers, analysts within government, academia and other organizations to access restricted data.

### **2. Why is it good practice?**

Confidentiality is a key element of respondents' trust, thus maintaining their cooperation in the provision of accurate data. As a result, the policy for the release of data is to prevent disclosure of information about individual persons or businesses, consistent with IBGE's legislation supporting confidentiality.

But it is also essential to try to reach the needs of the research community while maintaining confidentiality and security.

To provide restricted data access for analysis requires collaboration between all involved parties and preparation to deal with a variety of situations and questions.

Technical developments may allow for new ways of achieving the needs of the research community whilst maintaining confidentiality and security.

### **3. Target audience**

The target audience is researchers requiring special data access to information not available through the web site or public use data files.

### **4. Detailed description**

The following describes the administrative and technical measures to regulate the access of restricted microdata and to ensure that the output is released with an adequate level of protection so that individual data cannot be disclosed. The procedures cover the following steps:

#### **(1) - application**

The researcher submits the research project to be evaluated if it is for public or academic interest, for statistical purposes and also whether it is feasible.

#### **(2) - evaluation of the project**

A Committee of Assessment of Restricted Data Access evaluates the project, based on submissions of the thematic area responsible for the survey microdata. The Committee authorizes (or not) the access to internal data files under the appropriate conditions.

The Committee is chaired by the Deputy Director for Surveys and composed of senior staff members dealing with business, methodology and dissemination coordination.

#### **(3) - formal agreements to access**

Once a project has been authorized, formal agreements between the researcher and the agency are established. These agreements involve a written contract (contractual arrangement), and an agreement form outlining the conditions of access and setting out fees for the proposed work.

#### **(4) - on-site access**

The databases are installed in the room with special computers for the researchers. The security features of the computers include a blockade to external networks to prevent transfer of data. Furthermore, the external disk drives and serial parallel ports are disabled. The identification of the enterprises is recoded in the databases from businesses surveys of IBGE or from external sources.

The researchers do the work and save the output in the hard disk of the special computer and then prepare a report document. A CD-Rom with this information is prepared by IBGE staff, to be analysed by the thematic survey area.

(5) - evaluation of output

The statistical output must be analysed before its release to the researcher to ensure the technical assessment of disclosure risks and confidentiality requirements. The analysis is undertaken by the thematic area responsible for the survey microdata, the same that gave submissions for the committee decision.

(6) - releasing the output

Once the output of the project has been approved, i.e. the thematic area judges that there is no risk of disclosure, another formal agreement is established. This new agreement outlines the conditions of use of the data generated by the special access, i.e. the user has to recognize that data are the property of IBGE and has to provide advice of this special access when releasing the results and analysis involving these data.

Table 1 shows the number of projects analysed by the Committee from September 2003 to February 2006. In 37 projects analysed, 3 projects involved data from the long form of the 2000 Population Census. In this case, the researcher needed different geographical areas from the weighting areas used in the sampling weighting process. One project involved data from an annual trade survey; one from an annual services survey; 30 projects from manufacturing surveys; and 2 projects involved data from manufacturing, trade or services surveys simultaneously.

**Table 1** – Number of Projects Analysed by the Committee (September 2003 – February 2006)

<b>Thematic area</b>	<b>Number of projects</b>
<b>Total</b>	<b>37</b>
Population Census	3
Trade Survey	1
Services Survey	1
At least 2 businesses surveys	2
Manufacturing surveys	30

## **5. Supporting legislation**

The regulations for the provision of restricted data access were established by IBGE using the following expedients:

- Resolution of the Board of Directors, n. 7, of May 29, 2003 – that created the Committee of Assessment of Restricted Data Access.
- Regulation of the Chief Statistician, n. 485, of July 8, 2003 – that appointed the members of the Committee.
- Regulation of the General Coordinator of the Centre for Documentation and Dissemination of Information, n.1, of September 10, 2003 – that established the objectives of the rooms for use in the on-site restricted access.

## 6. Strengths

Provides a secure way of providing researcher access to IBGE data for projects that are of clear statistical or academic benefit.

## 7. Weaknesses

Although about 40 projects have been working on this on-site system at IBGE since 2003, we have had a lot of difficult tasks to face. It has been:

- time-consuming to analyse projects because, in many cases, there is a need to contact the proponents to redesign the project or to provide detailed explanations of why the project is not feasible;
- time-consuming to prepare user-friendly documentation;
- time-consuming to analyse the outputs due to faults in the documentation.

In general, the expected work time is underestimated.

Another issue involves managing the tension between the agency and the researchers in regard to the acceptability of the current practice. The culture and value system of the research community is very different from that of a National Statistical Office.

Researchers still think of microdata access arrangements as unnecessary bureaucracy, too limiting and inconvenient. This lack of convenience for the researcher includes the requirement to work at the agency. That can be an expensive option, especially for researchers living in other cities or countries. Another point is that sometimes the researcher is forced to use unfamiliar data analysis software.

There is an internal debate about the acceptability of this practice. Even under measures to regulate the access of restricted microdata, there is a worry that it could still alarm public opinion with suspicion of disclosure. The reaction of respondents would have some impact on response rates.

Increasingly, researchers are looking to link data sets with the data sets of the agency. Although matching of databases brings benefits, the identification risks increase.

There are some issues concerning transparency. The IBGE web site was an effective way to provide information on how to make access available for researchers. However, information about the procedures is only provided through Intranet and the users learn about the procedures only when asking for special data.

Therefore, it is a challenge for us to be transparent about the arrangements of providing access to data for researchers under controlled conditions for specific purpose. But the visibility of such arrangements is necessary to increase public confidence that microdata will be used properly. We would want to be completely transparent about the specific uses of microdata to avoid suspicion of misuse and ensure that researchers are aware of the consequences for them and their institution if there are breaches of confidentiality. On the other hand, there is a fear of excessively increasing the demand.

There is a demand to install rooms for on-site access outside the headquarters of the agency, especially in the big cities like São Paulo and Brasília. But to meet this demand requires investment in resources to train staff and prepare the infrastructure.

## **8. References**

IBGE (2003), Resolução do Conselho Diretor nº 7, de 29.05.2003. (Resolution of the Board of Directors of IBGE, n. 7, of May 29, 2003 – that created the Committee of Assessment of Restricted Data Access).

IBGE (2003), Portaria do Presidente nº 485, de 08.07.2003. (Regulation of the IBGE's Chief Statistician, n. 485, of July 8, 2003 – that appointed the members of the Committee).

IBGE (2003), Norma de Serviço CDDI n.º 1, de 10.09.2003. (Regulation of the General Coordinator of the IBGE's Centre for Documentation and Dissemination of Information, n.1, of September 10, 2003 – that established the objectives of the rooms for use in the on-site restricted access).

Lei nº 5534, de 14 de novembro de 1968. Brasília, Diário Oficial da União. (Law 5534 of November 14, 1968. Law on the obligatory character of providing statistical data and confidentiality).

## ANNEX 16. CASE STUDY - MICRODATA LABORATORY ANALYSIS - ITALY

### 1. Broad description

The Statistics Law 332/1989 allowed for the first time the Italian national statistical institute (ISTAT) to release microdata to external users. These are essentially data from social surveys where protection is chosen according to a statistical model; the complete list is on the Internet at [www.istat.it/servizi/infodati/index.html#standard](http://www.istat.it/servizi/infodati/index.html#standard). It was soon clear that this product was not able to cover all requests for access to microdata especially for research purposes. For this reason in 1999 ISTAT created the Laboratory for Analysis of Microdata (Laboratorio ADELE, an abbreviation of *Analisi Dati ELEMENTARI*), an on-site facility where researchers perform statistical analysis on confidential microdata files stemming from both social and business ISTAT surveys.

### 2. Why is it good practice?

Very often researchers need business microdata or social microdata with the maximum information content; therefore, restricting the detail in data (as in the released microdata file) is not a feasible solution. The restriction has to be made on the access, using administrative, legal, statistical and IT measures to avoid any breaches of confidentiality. In the Laboratory the users have access to the whole collection of validated microdata of the Institute with the maximum information content.

### 3. Target audience

Access to the Laboratory is allowed for research purposes only; projects are welcome from universities or research institutes or from bodies who can prove a recognized research attitude. Projects have also been accepted from ministries or national authorities who demonstrate that the proposed project has clear research intentions. Researchers from foreign universities and institutes are also allowed.

### 4. Detailed description

The Laboratory for Analysis of Microdata is located in Rome at the ISTAT premises; plans are in place to open new branches in regional offices of ISTAT in order to decentralise access.

A researcher or a team of researchers seeking access to one or more microdata sets must complete a form containing the following information: the institution where they work, the name of the person responsible for the research project (because, very often, research students themselves carry out the analysis of the data), description, rationale and objective of the study, data to be analysed, statistical methods chosen to analyse the data, statistical software needed, and the expected type of output to be taken away from the Laboratory.

All proposals are reviewed inside ISTAT to establish the admissibility and purpose of the request, the admissibility of the institution, the need for confidential data as opposed to available microdata products, the acceptability of the expected output with respect to confidentiality. This latter analysis is done to avoid fruitless analysis where it is known in advance that the type of output requested is far too detailed to be taken away from the Laboratory without a protection that will completely destroy the information content.



Data are provided in a safe setting: a room with PC on a network separated from the internal ISTAT one, where any input/output procedures are disabled to users. The most common statistical software is available and any other commercial statistical software brought by the user will be installed on production of a valid licence.

The users sign a contract that ties researchers to their institution and together they are responsible for maintaining confidentiality. In accordance with the Statistics Law, every research project is authorized by the President of ISTAT.

Access to the Laboratory is controlled and supervised and the final output of the research is released after checking for confidentiality by ISTAT staff. The results of the research cannot be considered official statistics.

The number of projects is increasing steadily every year; in 2005 ISTAT approved more than 30 projects with more than 100 days of work.

A complete description of the Laboratory together with the form to request access is available at [www.istat.it/dati/pubbsci/documenti/Documenti/doc\\_2004/2004\\_9.pdf](http://www.istat.it/dati/pubbsci/documenti/Documenti/doc_2004/2004_9.pdf)

## **5. Supporting legislation**

The renewal of the legal framework on privacy protection in Italy, finalised by the adoption of the Personal Data Protection Code (Law 196/2003), led to the development of the Code of Ethics and Good Conduct for any party that is in some way involved in the processing of personal information (journalists, historians, statisticians, police, health services, etc). The Code of Ethics and Good Conduct for Public Statistics (Provvedimento del Garante no. 13, 7/2002) has the status of law (Annex A.3 of the Personal Data Protection Code) and applies to all the processing of confidential data for the purpose of statistics and research in the framework of the National Statistical System. It sets criteria for assessing the identification risk of a statistical unit, the rules to be followed when providing information to subjects not involved in the National Statistical System (Laboratory and anonymous microdata - art. 7), and when exchanging confidential microdata inside the System, security measures and so on. The Statistics Law and the Code of Ethics provide a complete framework for access to microdata inside and outside the Statistical System.

## **6. Strengths**

Users can study the complete microdata set (except for direct identifiers) stemming from all social-demographic and business surveys as well as censuses conducted by ISTAT. There is no limit on the type of analysis that can be carried out at the Laboratory; this allows for more in-depth analysis of phenomena being studied, especially as far as business data are concerned.

## **7. Weakness**

The Rome location of the Laboratory is a barrier for certain researchers; plans to add other laboratories in regional offices of ISTAT will only partly resolve this problem. The metadata and documentation are mostly provided in Italian and this represents a major problem for foreign researchers.

## **8. References**

The Statistics Law (Legislative Decree no. 322, 6 September 1989), is available at [www.istat.it/dlgs322.pdf](http://www.istat.it/dlgs322.pdf)

Personal Data Protection Code (Legislative Decree no.196, 30 June 2003) available for download at [www.garanteprivacy.it/garante/document?ID=1169255](http://www.garanteprivacy.it/garante/document?ID=1169255)

*Code of Ethics and Good Conduct when processing personal data for the purposes of statistics and scientific research within the National Statistical System* also at [www.garanteprivacy.it/garante/document?ID=1169255](http://www.garanteprivacy.it/garante/document?ID=1169255), Annex A.3 pp. 130-141.

## **ANNEX 17. CASE STUDY - MANAGING DECISION MAKING ON CONFIDENTIALITY - SLOVENIA**

### **1. Broad Description**

The Case Study presents the management issues at the Statistical Office of the Republic of Slovenia (SORS) associated with the release of microdata to researchers. Tasks of the Data Confidentiality Committee and the system of rules and procedures regarding the release of microdata to researchers are presented.

With the procedure described, the Director-General of SORS has the necessary advice before deciding on the release of microdata to researchers and all the researchers are treated in the equal standardised way.

### **2. Why is it Good Practice?**

It provides the necessary advice to the Director-General of SORS before deciding on the release of microdata.

Researchers are treated in equal way.

Trust in SORS regarding confidentiality of data is maintained.

SORS's staff is well informed about the procedure and can monitor the decision process and outcome which is applied in a routine fashion.

### **3. Target Audience**

Target audience are researchers in research and government bodies as well as individual researchers and social science data archives.

### **4. Detailed Description**

#### **4.1 Data Confidentiality Committee**

The Data Confidentiality Committee deals with the problems of data confidentiality at SORS and was established as an advisory body of the Director-General.

The Committee has the following tasks:

- To take care of the implementation of the Rules on the Procedures and Measures for the Confidentiality of Data Collected Under the Program of Statistical Surveys by SORS
- To deal with various matters and to give advice to the Director-General of SORS regarding issues that cannot be solved by general rules from the field of data confidentiality
- To report to the Director-General of SORS and the Statistical Council of the Republic of Slovenia regarding the situation in the field of data protection at SORS.

With reference to its tasks, the Data Confidentiality Committee adopts findings, positions and opinions and forwards them to the Director-General of SORS. Members of the Data Confidentiality Committee are experts from SORS and authorised producers

of national statistics as well as external data protection experts. Committee members are appointed by the Director-General of SORS.

## **4.2 The system of rules and procedures regarding the release of microdata to eligible users**

### **4.2.1 Organizational rules and procedures**

All requests received by SORS for the release of microdata are transmitted to the Data Confidentiality Committee, which prepares the opinion about the possibility of releasing the requested microdata and forwards it to the Director-General of SORS for approval. In preparing the data, subject matter specialists must take into account the »need to know« principle.

### **4.2.2 Rules for the release of non-anonymised microdata**

#### **a. Release of microdata within the system of national statistics**

Good practice: for implementing the Annual Program of Statistical Surveys, it is possible to exchange microdata between SORS and authorised producers of the program of statistical surveys.

#### **b. Release of microdata collected with combined questionnaires to partner institutions**

In some cases SORS sends together with one of the government institutions to the reporting units a combined questionnaire, thus decreasing the burden of reporting the same or similar microdata twice to government institutions.

Good practice: SORS collects microdata with a combined questionnaire together with a partner institution only if SORS and the partner institution have a legal basis to do this and if SORS's interest is not threatened by this method of microdata collection.

The legal basis for microdata collection by SORS and a partner institution must be printed on the questionnaire and the information letter must explain the purpose of microdata collection for the partner institutions.

#### **c. Release of microdata to observation units requesting own microdata**

In some cases observation units ask SORS for own microdata that they sent to SORS in the past.

Good practice: if SORS has these microdata, it transmits them to the observation unit within its technical and financial capacity. For the 2002 Population Census, SORS transmits prints of scanned census questionnaires.

#### **d. Release of microdata about their members to commercial and interest associations**

To rationalise microdata collection and decrease the burden of reporting units, some commercial and interest associations do not collect microdata for various analyses themselves but ask SORS to transmit these microdata to them.

Good practice: SORS transmits individual microdata on a member of an association after obtaining written consent from the member.

e. Release of microdata for the purpose of interviewing

For the purpose of interviewing, SORS may transmit to registered scientific research organisations and registered individual researchers only the following personal microdata: name and family name, address, year of birth, sex and occupation (see National Statistics Act).

#### **4.2.3 Rules for the release of anonymised microdata**

a. Release of microdata to scientific research institutions and individual researchers

Good practice: microdata for scientific research and analytical purposes (secondary data analysis) are transmitted only to scientific research institutions and registered researchers that can prove their registration.

b. Release of microdata to researchers in government bodies

Government bodies are statistical microdata users that have great and specific needs for microdata, so SORS facilitates their work regarding policymaking by enabling them to use microdata.

Good practice: microdata are transmitted to the government body if the purpose of microdata use is research or analysis.

The request is denied if the purpose of microdata use is to determine administrative advantages or disadvantages for business entities or natural persons.

c. Release of microdata to social science data archives

By transmitting microdata to data archives, SORS enables analytical and research work.

Good practice: microdata transmitted to various social science data archives have the highest level of confidentiality based on the contract between SORS and the data archive.

## **5. Supporting Legislation**

### **5.1 National Statistics Act**

National statistics shall be implemented on the different principles among others on statistical confidentiality (Article 2).

The professional tasks performed by the Office within the framework of its basic functions shall among others develop methods and techniques for data protection (Article 7).

Dissemination of data shall be carried out in such a way that the persons or businesses cannot be identified (Article 34, 47).

For the purpose of conducting surveys, the Office may transmit to registered scientific research organizations and registered individual researchers only the following personal

data: first name and family name of an individual, his/her place of residence, year of birth, sex and occupation (Article 41).

Statistics may be published in aggregate form only, by way of exception, data may also be published individually:

- upon written consent of the reporting unit as regards publication of the data in such a way;
- if data have been collected from public (generally accessible) data collections (records, registers, databases, etc.);
- if data are published in such a way that the person or business involved cannot be directly identified (Article 50).

## **5.2 Rules on procedures and measures for the protection of data collected through programmes of statistical research at the Statistical Office of the Republic of Slovenia**

In communicating data to users, the principle of statistical confidentiality shall be respected. The principle of statistical confidentiality means that no data may be communicated to users

outside the system of national statistics, which can be ascribed to a particular observation unit or which could indirectly enable this (Article 5)

Before communicating data referred to in the previous paragraph, the research organisation or registered individual researcher shall sign the declaration on data protection (Article 16).

Data for research purposes may only be used by a registered research organisation or registered individual researcher that has concluded an appropriate contract with the Office, which must contain the status of the user, the intended use of the data, protection of data and the manner and time of publication of the data (Article 17)

A proposal for concluding a contract shall be discussed by the Committee for Data Protection before the contract is concluded (Article 17).

## **6. Strengths**

- It provides the necessary advice to the Director-General of SORS before deciding on the release of microdata.
- Researchers are treated in equal way.
- Rules and procedures for microdata release are transparent (they are published on intranet and internet)
- Procedures are easy to understand for the staff of SORS and researchers.
- Trust in SORS regarding confidentiality of data is maintained.
- Staff of SORS is adequately informed about the procedure for managing decision making on confidentiality and can monitor the decision process and outcome which is applied in a routine fashion.
- There are clear responsibilities for the upgrading of the system for managing decision making on confidentiality.

## **7. Weaknesses**

- Time lag between the data request and approval

## **8. References**

National Statistics Act ( [http://www.stat.si/doc/drzstat/ZAKON\\_O\\_DSTA\\_ENG.PDF](http://www.stat.si/doc/drzstat/ZAKON_O_DSTA_ENG.PDF) )  
Description of access to microdata on SORS's home page  
[http://www.stat.si/eng/drz\\_stat\\_mikro.asp](http://www.stat.si/eng/drz_stat_mikro.asp)  
Rules on procedures and measures for the protection of data collected through  
programmes of statistical research at the Statistical Office of the Republic of Slovenia  
[http://www.stat.si/doc/stat\\_urad/pravilniki/06-0471pravilnik\\_varstvo\\_podatkov\\_en.pdf](http://www.stat.si/doc/stat_urad/pravilniki/06-0471pravilnik_varstvo_podatkov_en.pdf)

## ANNEX 18. CASE STUDY - MANAGING DECISION MAKING ON CONFIDENTIALITY - AUSTRALIA

### 1. Broad description

Special governance arrangements have been put in place to ensure the Australian Statistician has sound advice before making decisions on whether to release anonymised microdata files.

The recommendation comes from the statistical area responsible for the statistical collection on which the microdata are based. They make judgements based on the demands from users of the information. It must be accompanied by:

- (a) a positive recommendation from a Microdata Review Panel (chaired by a senior methodologist) that the microdata are not identifiable; and
- (b) a positive recommendation from the Policy Secretariat area that the proposal conforms with policy and legislation requirements.

### 2. Why is it good practice?

It provides the necessary assurances to the Australian Statistician before he makes decisions on release of microdata. In practice, he approves in principle the release of microdata from a particular collection (e.g. a Household Expenditure Survey). Australian legislation requires each release to an individual researcher to be approved. This responsibility has been delegated but only to senior executives.

### 3. Target audience

Microdata releases are targeted to the research community, particularly those located in government agencies, universities and other research institutes.

### 4. Detailed description

To assist uniformity in the process, standard templates have been developed for documentation.

The relevant statistical area will take the initiative in developing a proposal. For many surveys it will be a standard output, although there may still be consultation on the exact nature of the microdata release. In other cases, the decision to provide a microdata release could depend on representations from users and subsequent discussions with them.

The statistical area will then develop a proposal for a microdata release. It must first be cleared with a Microdata Review Panel. This is chaired by senior methodologists and they have developed criteria to assist them with their assessment. They will also do empirical analysis to help determine identifiability. If the result is unacceptable, they will make recommendations on how to reduce identifiability (e.g. by combining classifications). This will be done in collaboration with statistical areas.

Wherever possible consistent classifications on identifying variables such as age and occupation are used across different microdata releases. This simplifies the assessment task but is also of benefit to researchers working with several microdata sets.

The Microdata Review Panel is chaired by a senior methodologist. Its membership includes confidentiality experts and representatives from statistical areas.



One important component of the submission is the conditions that must be included in the Undertaking to be signed by the recipients of the microdata release. Some are prescribed in legislation; others can be determined by the Australian Bureau of Statistics (ABS) (e.g. non-matching with other data sets). The Microdata Review Panel may recommend conditions as part of their deliberations.

The next step is to get clearance from Policy Secretariat. They will check that the proposal conforms with legislation. They will also check that the proposal conforms with ABS policy on microdata release.

## **5. Supporting legislation**

The relevant legislation is described in Annex 1.

## **6. Strengths**

It provides appropriate checks and balances and the full range of information required for the Australian Statistician to make an informed decision.

## **7. Weaknesses**

The assessment of some proposals can be labour-intensive. Also the investigation may take effort. This can result in delays in decision making particularly when multiple proposals are being considered at the same time.

## **ANNEX 19. CASE STUDY - MICRODATA ACCESS IN THE OECD PROGRAMMES FOR INTERNATIONAL STUDENT ASSESSMENT (PISA)**

### **1. Broad Description**

OECD's Programmes for International Student Assessment (PISA) are conducted every three years in order to collect student achievement indicators in a number of areas, such as reading, mathematics and science. Information is collected both on students and their schools. PISA is currently in its third project cycle: the first being conducted in 42 countries in 2000 (PISA 2000), the second in 41 countries in 2003 (PISA 2003), and the third cycle in 57 countries in 2006 (PISA2006). Data and instruments for all PISA cycles are available on the OECD PISA web site ([www.pisa.oecd.org](http://www.pisa.oecd.org)). Released data include microdata files, statistical tables published in the international reports, and special tables generated at the request of researchers.

### **2. Why is it Good Practice?**

An Agreement concerning the confidentiality in the use of PISA materials is established between the OECD and the countries participating in PISA. This agreement specifies that the use of all materials from the OECD/PISA is permitted solely for the national implementation of PISA in the participating country, preparation of national reports or documents, with the provision that no information derived from these materials shall be published or otherwise disseminated to any individual other than those identified in the Agreement prior to the publication of the first international PISA report by the OECD, or without prior consent from the OECD. The OECD reserves the right to terminate the Agreement at any time with immediate effect, for the reasons of failing to meet any requirements of the Agreement.

In the microdata files, student and school information are kept anonymous through the use of randomly assigned identification numbers and codes. This system has ensured anonymity while maintaining high levels of accuracy.

Released PISA data provide reliable and internationally comparable indicators that meet high technical standards. Only data concerning participating countries that have fully satisfied PISA Technical Standards in the areas of sampling (including population coverage, exclusions and response rates), translation and translation verification, test administration, quality monitoring, coding, data entry and data submission, are included in PISA international microdata files. Since a number of same items and instruments are used across all cycles, researchers have the opportunity to compare indicators over time.

The PISA microdata files are released publicly through the PISA web site in the first week of December in the year following that of data collection. This occurs concurrently with the release of the initial PISA international reports of each cycle. Researchers worldwide are immediately able to replicate the analysis presented in the international reports. Concerning PISA 2006, the data set is planned to be released on December 4, 2007. Participating countries are currently required to strictly maintain the embargo on releasing any results until that date.

### **3. Target Audience**

All stakeholders involved in education: policy makers, researchers, teachers, school principals, parents and students.

### **4. Detailed Description**

In the PISA web site, four data functions are available for each programme cycle:

- **Downloading of microdata files:** user can download questionnaires, code books, microdata files in TXT format, SPSS and SAS control files, and compendia. With these microdata files, researchers can conduct analysis and run models using statistical software such as SPSS and SAS. The PISA 2003 student microdata file includes more than 400 variables for approximately 276000 students. The PISA 2003 school microdata file includes 190 variables for approximately 10000 schools.
- **Interactive data selection:** user can construct tables by selecting countries and variables. Tables are immediately generated through the website. Included are estimates for the variable selected, student performance determined by the selected variable, as well as standard errors.
- **Multi-dimensional data request:** user can access more complex analytical results by selecting multiple variables. Results can be mailed directly to users through an email service based on the website.
- **PISA data service:** more advanced or customised analysis is available for a fee.

## 5. Strengths

All data files and data functions are available on the PISA website without requiring special registration. The entire data set is available publicly free of charge through the website. Various on-line functions (as described above) are available for handling and interpretation of PISA data. Users can select an on-line data function depending on their technical ability and the aim of analysis.

There is sufficient confidence in the arrangements for protecting confidentiality in the project. The high participation in PISA ensures the quality of the resulting statistics.

## 6. Weaknesses

Analysis of the PISA microdata may be complicated because it requires understanding and application of high-level statistical knowledge. In order to support researchers in conducting analysis, *PISA 2003 Data Analysis Manual* has been published. The Manual explains the methodological approach applied by PISA as well as SPSS and SAS macros and syntax for correct computation.

Since the data found in PISA microdata files can be quite extensive, computation time may be lengthy depending on a computer used. It is recommended that user defines cases selected and variables necessary for the analysis as narrowly as possible to ensure effective analysis.

## 7. References

OECD (2005) PISA 2003 Data Analysis Manual. OECD. Paris.

Further information on PISA is available on the PISA web site ([www.pisa.oecd.org](http://www.pisa.oecd.org)).

## **ANNEX 20. CASE STUDY – POLICY ON INTERNATIONAL RELEASE OF MICRODATA - AUSTRALIA**

### **1. Broad description**

The Australian Bureau of Statistics (ABS) is receiving a small, but growing, number of requests from overseas researchers for access to microdata.

There are two types of access sought: individual researchers seeking access for research projects, and requests to add Australian data to international databases. The Luxembourg Income Study (LIS) is a long-standing example of the latter type of request.

While granting of access to microdata to overseas researchers will remain a matter of judgement, a policy has been developed to provide guidance on when such requests might reasonably be considered.

### **2. Why is it good practice?**

Increasingly comparisons with other countries are being used to inform policy. It is why Australia is an active participant in organisations like OECD and other international collaborations with worthwhile objectives. Often these studies require access to microdata to achieve their research objectives.

The ABS can legally release microdata internationally under specified conditions. As well as legal requirements, there is the issue of public acceptability. To maintain the trust and confidence of respondents, there have to be assurances that their data is safe and being put to good use.

The policy statement provides a decision making framework to allow individual decisions on research access to be made on a consistent basis.

### **3. Target audience**

The international research community but particularly international agencies.

### **4. Detailed description**

For data to be released internationally, two key conditions should be fulfilled.

(i) The study should be of interest to Australia. While this would always be a matter of judgement, some examples of work meeting this criteria might include: producing international comparisons in an area of topical interest; an overseas organisation undertaking policy relevant work on behalf of Australia; methodological work that might lead to improved data collection practices and methods in Australia; and research that is relevant to Australian policy.

(ii) The recipient organisation and person should be trustworthy. While this also remains a matter of judgement a 'threshold' criteria may be that the organisation has recognised international standing in the relevant field.

Unless the above two conditions are fulfilled, access should not be provided.

Even in these situations our Remote Access Data Laboratory (RADL) would be the preferred option if practicable. For requests made by individual researchers, access should only be granted through RADL.

The organisation receiving the microdata may want to provide access to other researchers outside their organisation to support the international study. They cannot do this legally. Each request should come to the ABS for consideration.

The process of granting access proceeds in two stages: an "approval in principle stage" which assesses the usefulness of the project and trustworthiness of the applicant, followed by an "approval" stage which involves signing of appropriate undertakings.

Where it is found that researchers or organisations have breached conditions of undertakings made, sanctions will be applied. Doing so can reduce the risk of further breaches by the relevant researchers/organisation as it acts as a deterrent to others' breaching their undertakings.

There will be a graded series of sanctions as follows:

1. for minor breaches, issue a warning to the individual in breach of an undertaking and their organisation (where there is suspicion rather than proof of a breach, this approach might be taken);
2. remove data access from the individual in breach of an undertaking, either in perpetuity or for a fixed length of time (e.g. three years);
3. remove data access from all researchers from the offending organisation, or in the case of ABS microdata being part of an international study prohibiting further access to this data, either in perpetuity or for a fixed length of time (e.g. three years);
4. advising the researcher's managers, or other persons of authority, of the breach and the sanction;
5. publicising, to the relevant international research communities, that an organisation has been in breach of their undertaking in relation to ABS microdata and that they are prohibited from using ABS microdata.

Which sanction to apply would remain a matter of judgement; however, the factors to consider would be:

1. whether the breach was intentional or not;
2. the nature of the breach;
3. the breadth of the breach (one researcher only as against multiple researchers);
4. the length of time that the breach had been occurring before detection.

## **5. Supporting legislation**

Microdata is released under the provisions of Clause 7 of the Ministerial Determination (see References).

There is nothing in these provisions which prevents release to a person or organisation residing outside Australia. We have been reluctant to do so because legal sanctions against breaches could not be applied.

Each release to a person or organisation should be approved by the Australian Statistician or delegate within the ABS (at present the Deputy Australian Statisticians).

Although legal sanctions may not be possible, there are other sanctions that could be used. The most powerful (and easy to apply) is to withdraw access to all ABS microdata services.

## **6. Strengths**

It provides a publicly defensible basis as to how Australia might participate in international research studies involving microdata. Previously, as an abundance of caution, we had provided virtually no microdata access to international researchers.

It provides a clear statement to the international research community on the ABS position.

It provides a clear statement of the ABS position to staff who might be collaborating with international researchers. They know what is allowable and what is not allowable and discussions can proceed on the basis of that understanding.

## **7. Weaknesses**

The risk of actual identification is very small. The most likely breach is that the recipient of microdata may pass the microdata on to other researchers including those in Australia who are not authorised by the ABS to access the data.

If this happened, it might lead to perceptions about the security of microdata. This in turn could affect response rates and hence the quality of ABS statistical collections.

## **8. References**

A copy of the policy statement can be obtained through [teresa.dickinson@abs.gov.au](mailto:teresa.dickinson@abs.gov.au).

## **ANNEX 21. CASE STUDY - MANAGEMENT OF RECORD LINKAGE PROJECTS - CANADA**

### **1. Broad description**

Since the mid-1980s, Statistics Canada has had in place a Record Linkage Policy designed to protect the privacy of individuals while, at the same time, permitting record linkage under certain circumstances. Record linkage can be undertaken for research and statistical purposes only, and where the public benefits of the proposed linkage are judged to outweigh the privacy intrusion inherent to the linkage. All record linkage proposals must follow a prescribed review process that culminates with approval by Policy Committee, the senior executive committee chaired by the Chief Statistician.

### **2. Why is it good practice?**

The Policy ensures that an appropriate balance is maintained between two competing public goods: the public good resulting from information that can only be developed through record linkage; and the minimising of privacy intrusion – which, however, is inevitably involved at any time when information about people is used in ways that they have not authorised.

A standardized approach to record linkage is implemented throughout the agency. By following this strict protocol, Statistics Canada has avoided any negative public reaction that could jeopardize or interfere with the agency's current or future activities. Transparency, strong governing procedures and an ethical position on the undertaking of record linkages has led to the sound management of this important statistical activity, which can shed light on important issues of public interest, and has contributed to the maintenance of public trust in the agency.

### **3. Target audience**

The Statistics Canada Record Linkage Policy applies to all proposed record linkage activities to be carried out by employees of Statistics Canada, regardless of the purpose or extent of the linkage activity.

### **4. Detailed description**

The Record Linkage Policy provides a definition that captures all types of linkages. Record linkage is defined as the bringing together of two or more micro-records to form a composite record, where a micro-record contains information about an identifiable individual respondent or unit of observation, such as a person, family, household, dwelling, farm, company, business, establishment, institution, etc.

In deciding which applications to approve, Policy Committee looks for a high likelihood that the linkage would result in significant public benefits; a methodology that would yield valid results; and ensures that no disadvantage affecting the subjects of the linkage, individually or collectively, would result. In addition, for linkages thought to be especially sensitive, the Committee will seek out the view of the Privacy Commissioner(s), as well as the degree of public support from key client groups or other stakeholders. Furthermore, in order to ensure transparency, the Record Linkage Policy requires that all approved applications, and their expected public benefits, be listed on the agency's web site.

All record linkage proposals to Policy Committee must include the following information:

- A concise description of the intended linkage project and an outline of the proposed research plan. The purpose for undertaking the proposed record linkage must be fully discussed, including the key reasons for conducting the linkage and the intended use of the results. How the public interest is served must be clearly demonstrated, namely by asking and answering the question: “So what?” It is important to indicate whether the linkage study findings are to be used in the context of public policy development, adjustments to existing federal or provincial programmes (e.g. funding or administrative arrangements), administrative decision-making, programme or project evaluation, changes to medical procedures, improvements in workplace safety procedures and so on. Policy issues that may be supported by the results of the proposed linkage must also be identified. Where linkages involve the use of personal information, how the public interest benefits will outweigh any possible privacy intrusions must be demonstrated. Research projects that are dependent on the linkage must be described in detail, including the research hypotheses.
- An indication of whether the proposed linkage is once-only or ongoing.
- An indication of whether survey respondents or those involved in the study have provided consent for the record linkage activity, or have been notified of any intended record linkage activity. Direct approval by Policy Committee may not be required when informed consent has been obtained. The Director of the Division in Statistics Canada responsible for the implementation of the Record Linkage Policy has been mandated to determine whether fully informed consent was obtained, in which case the linkage project may proceed without further review, or whether special circumstances require that the linkage project be approved by Policy Committee. If obtaining consent is not feasible, any consultations or communication strategies with respondents, the target population, or the selected proxy representatives, if applicable, should be mentioned.
- An indication of whether a privacy impact assessment or an evaluation by an ethics review board has been conducted.
- An indication of any efficiencies or savings in terms of costs, resources, timeliness, and reduced response burden.
- The names, sources, and years of all the files to be linked are to be supplied. A summary of the file contents should also identify the variables from these files that will be used in the linkage.
- A detailed description of the methodology to be employed in the linkage, including a description of the models or statistical tests being undertaken, linkage techniques and any generalised linking systems that are to be used.
- In addressing the methodological issues, a discussion of the appropriateness of using record linkage as opposed to other methods. In this regard, it is especially important to highlight what other alternative sources were considered and why these were rejected in favour of record linkage.
- The ability of the data sources to support, with an appropriate level of statistical confidence, the expected findings of the research.
- Whether entire populations are being linked or whether only a sample is to be included. This is an especially important consideration as in some cases the privacy intrusion of a record linkage can be diminished by using a sample of the total population.
- Details regarding the outputs of the linked file.
- The maximum retention period for the composite file, after which the linkage file must be destroyed. In the event that a linkage project is not completed within the approved retention period, it is necessary to seek Policy Committee approval to retain the linked file for a longer period of time.



- In general, there is no analytical requirement to retain the identifiers on the linked composite file that is used for the data analysis. If there is a reason to retain the identifiers, an adequate justification must be provided.

Each submission must be accompanied by a one-page summary, which is included in Statistics Canada's *Annual Report to Parliament on Access to Information and Privacy*, and is also posted on the Statistics Canada web site.

## 5. Supporting legislation

The Record Linkage Policy is a major component of Statistics Canada's legislative and policy framework, and embodies several principles and provisions of the Statistics Act, the agency's governing legislation, as well as of the federal Privacy Act.

## 6. Strengths

The Policy ensures:

- that the trade-off between the expected public benefit and the degree of privacy invasion which may be involved is applied consistently across all linkages, projects and over time;
- that record linkages are carried out with great care, while pursuing selected key public interest objectives;
- that openness and transparency are maintained, from approval of the linkage to dissemination of the results;
- that every record linkage proposal is evaluated and approved based on its own merit, regardless of its source of funding;
- that for on-going linkages, the objectives are reassessed at set periods;
- that all analytic results are placed in the public domain and accessible to everyone;
- that linked files will be destroyed once the study is completed and the results released;
- that in the eventuality of a major public controversy, Statistics Canada would be in a position to convince Canadians that it had been very sensitive about their legitimate privacy concerns and gone to great lengths to minimize the intrusiveness of the linkage while still carrying out its mandate, thereby, hopefully, maintaining the public trust in the statistical office.

## 7. Weaknesses

- The Policy is viewed in some circles as being too conservative and in effect an impediment to research.
- The Policy sets out a rigorous review and approval process which involves the submission of documented proposals. Approval of record linkages may be seen as requiring an inordinate amount of time and effort.

## 8. References

Statistics Canada's Policy on Record Linkage is available on its web site at *Record linkage at Statistics Canada*. The web site also includes a summary of all approved record linkages, as well as a document on *Privacy-related policies and practices at Statistics Canada*, by Dr. Ivan Fellegi, Chief Statistician of Canada. See <http://www.statcan.ca/english/recrdlink/>

## **ANNEX 22. CASE STUDY - DATA LINKING WHEN PREPARING MICRODATA FOR RESEARCH - SWEDEN**

### **1. Broad description**

When creating a statistical register for research, data linking is used for two different purposes:

- Different sources are combined to create an object set, the register population, with good coverage.
- Different sources are used to create the variables in the new register.

Different sources, such as administrative registers or pre-existing statistical registers, can consist of different object types. It may then be necessary to define the statistical units or objects in the new register in a suitable way so that data from sources with different kinds of units can be used together. Data linking can be used in the same way to combine microdata from sample surveys with data from administrative or statistical registers.

The case study is based on a report mentioned in section 8 below, which illustrates how different sources with agricultural data can be combined into a new kind of Farm Register with variables from many administrative and statistical registers. In the report data linking is discussed from a methodological point of view.

### **2. Why is it good practice?**

The microdata at National Statistical Offices have not been created to meet the needs of academic research. To meet these needs, new sets of microdata should be created, where existing sets of microdata are combined so that data sets with richer content are created. Exact linking with identifying variables is used to create this kind of microdata for research.

### **3. Target audience**

Persons at National Statistical Offices who prepare microdata for research and potential users of microdata for research.

### **4. Detailed description**

The original aim of the case study was to investigate how data linking can be used to create a new Farm Register at Statistics Sweden based on administrative data instead of a census. A new Farm Register can be linked to the Business Register in two steps:

- Integrating the census-based Farm Register and the administrative IACS Register with data from the Integrated Administrative and Control System, which is the system for agricultural subsidies used within the European Union.
- Linking the records in the integrated register with the records in the Business Register. After this linkage all variables in all statistical registers, which are linked to the Business Register, can be used to analyse the agricultural sector.

The role of the Business Register is to define the object set of all enterprises, including those belonging to the agricultural sector. To be able to create a set of microdata describing the agricultural sector, statistically interesting variables must be imported from other registers linked to the Business Register:

- Crop areas and subsidies of different kinds from the IACS Register.

- Persons employed by age and sex from the PAYE Register. The PAYE Register is based on the annual income verifications in which all employers provide information on wages paid to all persons employed.
- A large number of economic variables from the Register of Standardised Accounts, which is based on annual income statements from all firms: data from profit and loss statements, balance sheets, investments and labour costs.
- Turnover and other economic variables from the VAT Register, which is based on monthly or yearly VAT declarations from all firms.
- A large number of variables describing different kinds of vehicles owned by the agricultural unit from the Vehicle Register, which contains data about vehicles owned by businesses and individuals.

The conclusions of the case study can be summarised as follows:

The matching process must be carefully planned, considering which linking variables should be used, and in which order the different sources should be combined. The quality of the linking variables is important, and editing of these variables is an important part of the work. Causes and extent of mismatch should be investigated, and it must be decided if the non-matching units should be excluded or included in the register population. If they are included, mismatch will result in units with missing values for some variables. Seemingly matching objects should also be checked, since false hits will otherwise give rise to gross errors in data.

- The identifying variables should be edited before matching. Before editing of telephone numbers, only 47% of the farmers in the Farm Register could be matched to corresponding units in the IACS register. After corrections 64% could be matched.
- By combining two identifying variables (telephone number to the farm and the farm's tax identity number) the matching result is improved so that 96% of the units in the IACS register could be matched to units in the Farm Register.
- By combining these two identifying variables the matching result is improved so that more relevant agricultural units can be defined. Matching with only the farm's tax identity number resulted in (almost) only one-to-one matches between objects in IACS and the Farm Register. However, matching with both the tax identity number and telephone number resulted in a number of one-to-many matches and many-to-many matches. After data linking, new units should be created in the following way:
  - In some cases husband and wife, relatives or companions on the same holding make separate IACS applications for different parts of the holding's activities. As the relationships between these persons are informal and can change over the years, it is appropriate to combine all IACS applications and all legal units in the Business Register connected with these applications.
  - In other cases a number of holdings and IACS applications refer to the same telephone number. This is an indication that all objects have the same administration. If all holdings, all IACS applications and all legal units in the Business Register connected to the same group are combined, we will get an agricultural unit, which can be described by all statistical variables in the register system.
- Linkages must be checked. First the one-to-one linkages were checked. A match between identification variables is not sufficient proof that the IACS and Farm Register objects are identical. If the IACS object has a larger crop area than the FR object this can indicate that the IACS object should be linked with two FR objects and vice versa. The linkages were checked by comparing total arable area, reliable crop area and location described by parish.

- It was found that there was serious under-coverage in the agricultural part of the Business Register. By combining the Business Register with the PAYE Register, the Register of Standardised Accounts and the VAT Register, this undercoverage was reduced from 25% to 3%. These administrative sources are not used by the Business Register today.

## **6. Strengths**

By combining microdata from different sources, the relevance or scientific value of the data can be increased to a great extent.

## **7. Weaknesses**

Mismatch and/or false hits will give rise to quality problems.

## **8. References**

This case study is based on the following report:

Anders Wallgren and Britt Wallgren: *Administrative Registers in an Efficient Statistical System – New Possibilities for Agricultural Statistics? How Can We Use Multiple Administrative Sources?* Statistics Sweden and Eurostat 1999. The report is available at <http://www.scb.se/Grupp/Allmant/IACS2.pdf>

## ANNEX 2.1 STANDARD TERMINOLOGY

This should be read in conjunction with the Glossary on Statistical Disclosure Control developed by the Joint UNECE/Eurostat Work Session on Statistical Data Confidentiality. (Available at: [www.unece.org/stats/documents/ece/ces/ge.46/2005/wp.45.e.pdf](http://www.unece.org/stats/documents/ece/ces/ge.46/2005/wp.45.e.pdf).)

### **National Statistical Office (NSO)**

Although the term is used in the singular, it is meant to incorporate all statistical agencies, or statistical units within government departments, who produce official statistics and provide access to microdata for statistical or research purposes.

### **Research community**

Although this mainly refers to people working in research institutions such as universities, it also includes researchers working in government agencies, NGOs, international agencies and the private sector. Some countries may want to define the research community more narrowly and only include those working in research institutions.

### **Statistical purposes**

It is particularly important to make a distinction between statistical and administrative uses. In the case of statistical use, individual data are used as an input to derive statistics that refer to a group of persons or legal entities. It may also incorporate support for other activities within a NSO (e.g. sample selection off a business register). Administrative uses concern decisions about a particular person or legal entity which may bring benefit or harm to the individual.

The statistics referred to above include statistical aggregates, statistical distributions, parameters for models and other forms of statistical analysis that may refer to groups of individuals or organisations without identifying them.

Microdata used for research is consistent with statistical purposes if it is being used to produce the type of statistics referred to in the previous paragraph.

### **Anonymised microdata files - Public Use Files**

These are microdata files that are disseminated for general public use. They have been anonymised and are often released on a medium such as CD-ROM sometimes through a data archive. The term anonymised implies that not only are names and addresses removed but that other steps are taken to ensure that identification of individuals is highly unlikely.

### **Anonymised microdata files - licensed files**

The term anonymised implies that not only are names and addresses removed but that other steps are taken to ensure that identification of individuals is highly unlikely.

Licensed files are distinct from Public Use Files in that use is restricted to approved researchers for approved purposes. A legal undertaking is signed before files are provided to them.

### **Remote Access Facilities**

These are facilities that provide researchers with the ability to produce statistical outputs from microdata through computer networks without researchers actually 'seeing' the microdata. The microdata itself does not leave the National Statistical Office. Remote Access Facilities may be of two types.

- (a) Remote execution where a researcher submits a programme and receives the output later by email.
- (b) Remote facilities where the researcher performs the analysis and can immediately see the answer on the screen.

### **Data laboratories**

This involves working on-site at the National Statistical Office, or one of its Branches, to obtain access to microdata. Access could be direct or indirect through staff of the National Statistical Offices. If access is direct, the researcher is in effect being treated as a temporary employee of the National Statistical Office with the inherent responsibilities.

### **Data swapping**

A disclosure control method for microdata that involves the swapping the values of records that match on selected records. The techniques maintain statistics such as means, variances and univariate distributions but can affect multivariate distributions.

### **Data perturbation**

Techniques for the release of microdata which change the data before dissemination in such a way that the disclosure risk for the microdata is decreased but the information content is retained as far as possible. Perturbation methods falsify the data by introducing an element of error purposely for confidentiality reasons. Possible perturbation methods are:

- rounding,
- addition of random noise.

### **Risk avoidance**

This approach tries to eliminate all risks. In the case of microdata confidentiality, it requires the confidentiality of the data to be absolute, not only in its own right, but in association with other available data.

### **Risk management**

Within the constraints provided by legislation, it involves identification of the risks and managing them in accordance with their significance (impact) and their likelihood. More effort is put into managing the high impact, strong likelihood risks. Microdata confidentiality may not be absolute when considered in association with other data. Confidentiality could be considered in association with other means of reducing the risk.

**Data linking**

Data can be linked by exact matches (e.g. using an identifier such as name and address or ID number) or by statistical matches (using probabilistic matches). They may be NSO data sets only, a NSO and administrative data sets, or administrative data sets only. Data sets for a particular collection could be linked longitudinally. All these possibilities are incorporated within data linking.

### ANNEX 3.1 ACKNOWLEDGEMENTS

This work is the result of the efforts of a Task Force set up by the Conference of European Statisticians (CES). The Task Force members are: Dennis Trewin (Australia), Ivan Fellegi (Canada), Otto Andersen (Denmark), Teimuraz Beridze (Georgia), Luigi Biggeri (Italy) and Tadeusz Toczynski (Poland). Dennis Trewin is the Chairman of the Task Force. He has made a significant contribution to the work by drafting the text and incorporating the inputs from countries and international organisations throughout the several consultation stages of the document.

Tiina Luige and Gauri Khanna of the Statistics Division of the ECE were of great assistance to the Task Force and their contributions were much appreciated.

Svante Öberg and Heinrich Brünger have also provided considerable assistance to the Task Force during the course of their work.

Several countries have provided case studies to support the Guidelines and their efforts are greatly appreciated. They certainly make these guidelines more useful.

Finally, the Bureau of the CES has provided constructive guidance throughout this project.

\* \* \* \* \*