MPHEC
Maritime Provinces
Higher Education
Commission

CESPM
Commission de
l'enseignement supérieur
des Provinces maritimes

The Council of Maritime Premiers
Le Conseil des premiers ministres
des Maritimes

Norme de la Commission de l'enseignement supérieur des Provinces maritimes relative à la confidentialité

But

Protéger la confidentialité des renseignements que la Commision de l'enseignement supérieur des Provinces maritimes (CESPM) a en sa possession et qui peuvent permettre d'identifier (directement ou indirectement) un particulier. Les renseignements de la CESPM sont des informations que la CESPM a recueilli ou obtenu à l'aide de méthodes ou de systèmes variés, y compris :

- SISCU (système d'information statistique sur la clientèle universitaire);
- SIAE (système d'information amélioré sur l'éducation);
- Bases de données sur les enquêtes de la CESPM auprès des diplômés.

Norme

Le personnel qui accomplit ses activités quotidiennes et communique des renseignements au public doit, en s'appuyant sur les principes énoncés dans le Code type sur la protection des renseignements personnels de l'Association canadienne de normalisation (ACNOR) qui se trouve à l'annexe 1, s'assurer de ne divulguer aucun renseignement qui puisse permettre d'identifier un particulier.

Exigences réglementaires

La protection de la confidentialité des renseignements identificateurs de particuliers que la CESPM recueille ou a sous sa garde, est assujettie à la *Loi sur la Commission de l'enseignement supérieur des provinces Maritimes*. Cette loi n'est cependant pas en vigueur. Les données du SIAE sont épurées et compilées par la CESPM pour Statistique Canada, et elles sont, de ce fait, assujetties à la *Loi sur la statistique*.

Procédures

La directrice générale de la CESPM assume la responsabilité du respect de la norme. Afin de maintenir le caractère confidentiel des renseignements de la CESPM, les conditions suivantes doivent être respectées.

RENSEIGNEMENTS GÉNÉRAUX

1. Conservation

En raison de la nature archivistique des bases de données conservées à la CESPM, les données renfermant des renseignements identificateurs de particuliers doivent être conservées indéfiniment.

Quant à l'enquête de la CESPM auprès des diplômés, les listes de diplômés contenant des renseignements identificateurs de particuliers sont recueillies auprès des établissements participants afin que l'on puisse communiquer avec les diplômés pour des entrevues de suivi. Pour chaque classe de diplômés, ces listes originales seront détruites à la fin de chaque cycle d'enquête (c.-à-d. à la parution du rapport final de l'enquête de cinq ans).

2. Accès aux données

SISCU/SIAE : La CESPM reçoit les fichiers de données codés de chaque établissement, selon un protocole de transfert de fichiers de données exclusifs (pour plus d'information, voir le document sur le réseau local de la CESPM). Dans le cadre du programme, les fichiers .txt sont codés à l'aide d'un algorithme cryptographique que seule la CESPM connaît. Lorsque les fichiers ont été téléchargés et déchiffrés, ils sont emmagasinés et protégés par un mot de passe. Lorsque ces fichiers de travail sont finalisés, les fichiers originaux sont enregistrés sur des CD-ROM avec protection d'un mot de passe, une copie est déposé dans un classeur fermé à clé sur place et une copie est déposée dans un coffret de sûreté à l'extérieur. Les versions finalisées sont emmagasinées sur un serveur distinct.

Seuls les employés qui exécutent les tâches de programmation ou de gestion de la base de données ont accès à l'ensemble de la base de données du SIAE, y compris aux fichiers qui contiennent des renseignements identificateurs de particuliers. Les chercheurs qui consultent la base de données du SIAE n'ont pas accès à ces fichiers.

L'accès aux données conservées dans le fichier du SIAE et la communication des données permettant d'identifier un particulier sont seulement autorisés aux fins suivantes :

1) Dresser une liste d'étudiants ou de diplômés qui peuvent participer à une enquête de la CESPM;
2) Satisfaire aux obligations imposées par la loi;
3) Communiquer avec les établissements pendant le processus de validation des données du SIAE et avec Statistique Canada.

Enquêtes de la CESPM auprès des diplômés : Les identificateurs directs des étudiants doivent être enlevés des données d'enquête, et l'accès doit être restreint aux employés chargés de l'analyse des données et de l'administration de la base de données. Un fichier de données renfermant les identificateurs directs des étudiants doit être conservé sur CD-ROM sous forme codée, ou protégé par un mot de passe. Comme c'est le cas avec les données originales du SIAE, l'accès aux données d'enquête protégées est seulement permis aux fins indiquées ci-dessus; de plus, les données peuvent aussi être consultées lorsqu'il faut vérifier l'exactitude de données longitudinales.

Processus de validation des données du SIAE : La collecte des données du SIAE auprès des établissements comprend un processus de validation selon lequel la CESPM vérifie les données et collabore étroitement avec les établissements en vue de l'épuration des données. De plus, dans le cadre du mandat de la CESPM qui est de fournir à Statistique Canada les données du SIAE recueillies auprès des établissements d'enseignement des Maritimes, la CESPM entretient une correspondance avec Statistique Canada concernant les données. Dans les deux cas, le personnel de la CESPM qui gère la base de données doit souvent utiliser les numéros de matricule des étudiants et d'autres identificateurs personnels comme référence. Dans de tels cas, la CESPM transmet les données permettant d'identifier un particulier par protocole de transfert de fichiers sécuritaire.

3. Renseignements à communiquer aux personnes interrogées

Les renseignements suivants doivent être communiqués aux personnes interrogées dans le cadre des enquêtes de la CESPM : but de l'enquête, usage prévu des renseignements fournis, protection des renseignements et ententes sur le partage des données.

4. Couplage d'enregistrements

Le couplage d'enregistrement est le fusionnement d'au moins deux micro-enregistrements de la CESPM provenant de différentes bases de données ou enquêtes pour former un enregistrement composite. Un micro-enregistrement est un registre d'information sur un particulier interrogé ou une unité d'observation. Lorsqu'une activité de couplage proposé implique le couplage d'enregistrements existants (p. ex. les données du SIAE) aux renseignements recueillis directement par la CESPM auprès des particuliers interrogés (p. ex. l'enquête de suivi auprès des diplômés), les intéressés doivent être informés de l'activité de couplage proposée au moment de la collecte des données. Il faut obtenir leur consentement pour coupler leurs réponses au sondage à leur dossier scolaire dans le SIAE. Les intéressés doivent aussi être informés des fins du couplage et de la valeur de l'information qui sera obtenue.

Le personnel de la CESPM et les personnes engagées à contrat doivent utiliser des méthodes de collecte et d'analyse des données qui protègent le caractère confidentiel des renseignements identificateurs de particuliers. Entre autres, cela signifie que les fichiers de données, les questionnaires et les autres rapports qui renferment des renseignements personnels sur des particuliers doivent être protégés, en tout temps, au moyen de mots de passe, de la séparation de l'identité des personnes et des autres renseignements qui les concernent, et de la gestion et du stockage sûrs de l'information.

COMMUNICATION ET DIFFUSION

Renseignements non identificateurs

Ces renseignements ne révèlent pas d'information précise sur une personne en particulier. Ils décrivent habituellement un groupe de personnes (p. ex. données agrégées sur l'effectif scolaire) sans identifier un particulier. Il peut aussi s'agir de dossiers personnels dénués de tout renseignement qui rendrait possible l'identification de la personne décrite.

5. Communication de microdonnées

Lorsque des données d'enquête sont communiquées ou que des fichiers de données sont préparés pour un usage public ou institutionnel (fichiers dépersonnalisés contenant les dossiers individuels des participants), la probabilité de pouvoir identifier les personnes qui ont répondu doit être faible. Il importe de ne pas oublier qu'il existe une possibilité de divulguer par inadvertance des renseignements qui puissent permettre d'identifier les particuliers, même s'il y a plus d'un fichier dans une catégorie.

a) La procédure d'examen et de communication de fichiers de microdonnées d'usage public assure que les enregistrements, même faits à un niveau individuel, ne permettent

pas d'identifier les particuliers. Les fichiers préparés en vue de leur communication doivent être soumis à une analyse de divulgation statistique. Toutes les modifications qui sont nécessaires à la suite de l'analyse doivent être apportées, et tout le processus doit être documenté.

b) Lorsqu'il s'agit de fichiers de données d'usage public, il faut interroger toutes les variables peu ordinaires à inclure au fichier (comme les salaires très élevés) et les sources de données qui peuvent être utilisées dans les secteurs public ou privé aux fins de recoupement.

Renseignements identificateurs de particuliers

Ces renseignements ne permettent pas toujours d'identifier directement un particulier mais ils contiennent de l'information qui rendrait l'identité du particulier, et toute autre information le concernant, facile à reconnaître, par exemple le nom, l'adresse, le numéro de téléphone, le numéro d'assurance sociale ou le matricule de l'étudiant (identificateur particulier de l'étudiant).

6. Tout le personnel de la CESPM, sans exception, doit prendre l'engagement de ne communiquer, sous aucun prétexte, un renseignement identificateur à une personne qui n'a pas prêté le serment de confidentialité. Les renseignements identificateurs de particuliers sont confidentiels et protégés par voie légale, et ils ne peuvent être divulgués sans le consentement préalable obtenu par écrit de la personne concernée.

7. Tous les titulaires de contrat, qui pourraient consulter ou utiliser des renseignements identificateurs de particuliers dans l'exercice de leurs fonctions, doivent fournir aux agents de projet de la CESPM une liste de toutes les personnes qui pourraient prendre connaissance de ces données et une entente de confidentialité signée par chaque particulier. De telles ententes doivent être signées chaque fois que de nouvelles personnes sont affectées à des projets de la CESPM.

8. La direction générale de la CESPM peut, à sa discrétion, autoriser des employés à communiquer des renseignements identificateurs de particuliers à des personnes qui en ont besoin à des fins statistiques (p. ex. aux personnes engagées par contrat pour mener des enquêtes longitudinales) compatibles avec les fins auxquelles les données ont été recueillies, si ces personnes signent des ententes de confidentialité et répondent aux autres exigences jugées nécessaires.

9. La communication de renseignements identificateurs de particuliers à des chercheurs extérieurs de la CESPM doit être considérée comme un prêt de renseignements (les destinataires n'ont pas la propriété des renseignements) et les renseignements doivent être remis ou les copies doivent être détruites lorsque les chercheurs ont terminé leur travail.

10. Lorsque des renseignements sont transmis à l'extérieur de la CESPM, les destinataires doivent signer une attestation certifiant qu'ils utiliseront les renseignements en respectant les conditions établies dans la demande de renseignements et qu'ils ne communiqueront ni ne transmettront l'information à une autre personne ou organisation.

ACCÈS À L'INFORMATION

SIAE

11. Statistique Canada et les établissements individuels doivent informer les étudiants sur les buts de la collecte des données au moyen du SIAE et sur la possibilité qu'ils ont d'exercer l'option de refus de la collecte de renseignements les concernant.

12. À la demande d'un étudiant, Statistique Canada supprimera de la base de données du SIAE l'information personnelle qui le concerne (nom, adresse, numéro de téléphone, numéro d'assurance sociale, SIAE_NSN, adresse électronique). À la suite du retrait de cette information, les utilisateurs ne pourront pas identifier ce particulier. La CESPM sera avisée de tout changement par Statistique Canada. Les étudiants qui désirent présenter une telle demande doivent communiquer avec Statistique Canada comme suit :

Par courrier :	Section de l'éducation postsecondaire et de la formation aux adultes Centre de la statistique de l'éducation Statistique Canada, Édifice Jean-Talon, 1-B-9 Parc Tunney, Ottawa (Ontario) K1A 0T6
Par téléphone :	Du lundi au vendredi De 8 h à 17 h 1 613 951-1666
Par courrier électronique :	ESIS-SIAE_contact@statcan.ca
Source :	http://www.statcan.ca/francais/concepts/ESIS/contacts-f.htm

La *Loi sur les renseignements privés* prévoit qu'un particulier a le droit d'avoir accès à l'information qui le concerne conservée par le gouvernement fédéral. Les étudiants peuvent demander de voir l'information qui les concernent dans le Système d'information amélioré sur les étudiants à l'aide de l'information ci-dessus.

13. Toute personne peut avoir accès à son dossier pour vérifier l'exactitude des renseignements qui s'y trouvent. Les particuliers qui désirent le faire doivent présenter une demande par l'entremise de leur établissement. Tous changements devant être apportés aux fichiers du SIAE doivent être envoyés à la CESPM par l'établissement.

14. Les établissements peuvent avoir accès à leurs dossiers pour vérifier l'exactitude des renseignements qui s'y trouvent. Si elle le juge raisonnable, la CESPM fournit l'accès, sur réception d'une demande écrite indiquant la nature et le but de la demande, le motif de crainte que les renseignements soient inexacts ou incomplets et les dossiers qui doivent être consultés.

Annexe 1

Code type de l'ACNOR sur la protection des renseignements personnels

Plusieurs entreprises canadiennes ont appliqué des codes volontaires afin de préserver le droit de leurs clients à la protection des renseignements personnels. Ces codes reposent sur le principe que les renseignements personnels sur les clients ne devraient pas être mal utilisés et que les particuliers devraient avoir accès aux renseignements qui les concernent.

En 1996, l'Association canadienne de normalisation (ACNOR) a établi un code volontaire basé sur les *Lignes directrices régissant la protection de la vie privée et les flux transfrontaliers de données de caractère personnel* établies par l'Organisation de coopération et de développement économiques (OCDE). La version de l'ACNOR, son code type sur la protection des renseignements personnels, a été adoptée par plusieurs entreprises canadiennes comme la norme nationale sur la protection des renseignements personnels.

Voici les dix principes de base du code :

1.	Responsabilité	Un organisme est responsable des renseignements personnels dont elle a la gestion et elle doit désigner une ou des personnes qui devront s'assurer que l'organisme respecte les principes énoncés ci-dessous.
2.	Détermination des fins de la collecte de renseignements	L'organisme devra déterminer les fins auxquelles les renseignements personnels sont recueillis avant la collecte ou au moment de celle-ci.
3.	Consentement	Les particuliers devront être informés de toute collecte, utilisation ou communication de renseignements personnels qui les concernent et y consentir, à moins qu'ils ne soient pas appropriés de le faire.
4.	Limitation de la collecte	L'organisme ne peut recueillir que les renseignements personnels nécessaires aux fins déterminées. L'organisme devra recueillir les renseignements personnels de façon honnête et licite.
5.	Limitation de l'ulitisation de la communication et de la conservation	L'organisme ne doit pas utiliser ou communiquer des renseignements personnels à des fins autres que celles auxquelles ils ont été recueillis à moins que la personne concernée n'y consente ou que la loi ne l'exige. L'organisme ne doit conserver les renseignements personnels qu'aussi longtemps que nécessaire pour la réalisation des fins déterminées.
6.	Exactitude	Les renseignements personnels doivent être aussi exacts, complets et à jour que l'exigent les fins auxquelles ils sont destinées.
7.	Mesures de sécurité	L'organisme doit protéger les renseignements personnels au moyen de mesures de sécurité qui correspondent à leur degré de sensibilité.

8.	Transparence	L'organisme doit faire en sorte que les renseignements précis sur ses politiques et ses pratiques concernant la gestion des renseignements personnels soient facilement accessibles à ses clients et employés.
9.	Accès aux renseignements personnels	L'organisme doit informer tout client ou l'employé qui en fait la demande de l'existence de renseignements personnels qui le concernent, de l'usage qu'il en est fait et du fait qu'ils ont été communiqués à des tiers, et lui permettre de les consulter. Un client ou un employé aura aussi la possibilité de contester l'exactitude et l'intégralité des renseignements, et d'y faire apporter les corrections appropriées.
10.	Possibilité de porter plainte à l'égard du non-respect des principes	Tout particulier doit être en mesure de se plaindre du non-respect des principes énoncés ci-dessus, en communiquant avec la ou les personnes responsables au sein de l'organisme, et de faire respecter ces principes conformément au code.