Codes et guides internationaux des études

CHECK-LIST ESOMAR PROTECTION DES DONNEES PERSONNELLES

ESOMAR, l'association mondiale des études de marché et sondages d'opinion, rassemble près de 4900 membres dans plus de 130 pays et est l'organisation principale pour encourager, promouvoir et faire progresser les études de marché. Ses codes et guides sont disponibles à www.esomar.org

SYNTEC Etudes est le syndicat représentatif des professionnels des études en France. Il a pour objet la représentation, la promotion et la défense des intérêts collectifs professionnels, moraux et économiques des personnes morales exerçant de façon prépondérante une activité d'études de marché et opinion auprès d'entités et entreprises, publiques ou privées.
www.syntec-etudes.com

Sommaire

1 INTRODUCTION

Les chercheurs qui travaillent dans un contexte mondial sont de plus en plus confrontés à un kaléidoscope de lois nationales visant à assurer le respect de la vie privée et la protection des données personnelles. Ils ont la responsabilité d'examiner et de se conformer non seulement aux exigences légales dans le pays où ils opèrent, mais aussi aux exigences locales de protection des données dans tous les pays où ils exercent leurs activités d'étude set/ou de traitement de données.

Dans le même temps, le développement continu des nouvelles technologies dans tous les aspects de nos existences a non seulement augmenté le volume des données personnelles potentiellement disponibles pour les chercheurs, mais aussi introduit de nouveaux types de renseignements personnels qui doivent être protégés.

Un point qui n'a pas changé est la nécessité pour ces professionnels de protéger la réputation des études de marché et sondages d'opinion grâce à des pratiques qui garantissent la transparence pour les répondants et les clients, maintiennent la confiance dans les informations fournies, et démontrent leur considération pour les participants des études.

2 PERIMETRE

L'objectif de ce document est de fournir aux chercheurs, notamment ceux travaillant dans les plus petites organisations n'ayant pas de ressource dédiée ou d'expérience des obligations de protection de données, les principes généraux de leurs responsabilités dans un cadre global de protection des données qui garantisse aux participants aux études le contrôle de leurs informations personnelles. Le cadre général utilisé a été développé par l'Organisation pour la Coopération et le Développement Economique (OCDE). Ce cadre comprend une liste de huit principes pour concevoir un programme garantissant la confidentialité et la protection des données personnelles :

- collecte limitée
- qualité des données
- finalité spécifiée
- utilisation limitée
- garanties de sécurité
- transparence
- participation individuelle
- responsabilité

Ces grands principes se retrouvent dans la plupart des lois existantes ou en préparation sur la vie privée et la protection des données.

Cependant, les chercheurs peuvent noter que les principes OCDE sont proches des obligations de l'UE en protection des données, par conséquence les chercheurs travaillant sur d'autres zones géographiques ont besoin de consulter d'autres documents. Ceux-ci incluent les références suivantes *: Asia-Pacific Co-operation (APEC) Privacy Framework, US Safe Harbour Privacy Principles* (si un accord entre l'Union européenne et les Etats-Unis est en cours d'application)*, Generally Accepted Privacy Principles (GAPP)* développé par *American Institute of CPAs (AICPA)* et *Canadian Institute of Chartered Accountants (CICA).*Bien que ces documents n'aient généralement pas force de loi, ils expriment cependant les principes fondamentaux que les chercheurs doivent suivre quand ils travaillent dans la région concernée.

De plus, les chercheurs doivent vérifier et respecter chacune des lois nationales de protection des donnée set des exigences d'autorégulation des organisations professionnelles d'études de marché et d'opinion dans les pays où ils prévoient de collecter ou de traiter des données, puisqu'il peut exister des différences dans la manière d'appliquer localement ces principes fondamentaux. Les recommandations fournies par ce document sont un minimum standard qui peut avoir besoin d'être complété par des mesures additionnelles dans le contexte d'une étude spécifique. Les chercheurs peuvent avoir besoin de consulter un conseil juridique local dans la zone où l'étude doit être conduite afin d'assurer une conformité totale. Ils peuvent aussi trouver utile de consulter le site The Data Protection Laws of the World, une ressource en ligne hébergée par DLA Piper et mise à jour annuellement.

Enfin, les chercheurs réalisant des études dans des domaines spécialisées comme la santé peuvent consulter les guides spécialisés comme le EphMRA Adverse Event Reporting Guidelines 2014 pour avoir des recommandations plus détaillées.

3 UTILISATION DE « DOIT » ET « DEVRAIT »

A travers ce document, le terme « doit » est utilisé pour désigner les exigences impératives. Nous utilisons le terme « doit » pour décrire un principe ou une pratique que les chercheurs sont obligés de suivre pour être conformes au Code international ICC/ESOMAR des études de marché et d'opinion. Le terme « devrait » est utilisé pour décrire une bonne pratique. Cet usage permet de reconnaître que les chercheurs peuvent choisir de mettre en œuvre un principe ou une pratique de différentes manières selon la conception de leur étude.

4 DEFINITIONS

Etude en entreprise (B2B) désigne la collecte de données sur des entités juridiques comme des entreprises, des établissements scolaires, des sociétés caritatives, etc.

Etude grand public (B2C) désigne la collecte de données concernant des individus.

Consentement désigne l'agrément librement consenti et informé d'une personne pour la collecte et le traitement de ses données personnelles. Dans les études de marché, sociales et d'opinion, ce consentement repose sur la communication aux participants à l'étude d'une information claire sur la nature des données collectées, l'objectif pour lequel elles sont utilisées et l'identité de la personne ou de la société détenant ces données personnelles. Les participants à l'étude peuvent retirer à tout moment leur consentement.

Responsable de traitement désigne une personne ou une organisation responsable pour définir comment les données personnelles sont traitées. Par exemple, le client de l'étude pourrait être le responsable de traitement des données personnelles de ses propres clients et consommateurs ; un organisme public de santé serait le responsable du traitement des données collectées auprès de ses bénéficiaires ; un fournisseur de panel serait le responsable de traitement des données collectées auprès des membres du panel en ligne; et un institut d'études serait le responsable de traitement sur les données collectées sur les participants à une enquête omnibus.

Sous-traitant des données désigne la partie qui collecte, enregistre, conserve ou réalise des opérations (y compris des analyses) sur les données personnelles pour le compte et sous la supervision du responsable de traitement. Comme indiqué ci-dessus, un institut d'études pourrait être à la fois responsable de traitement et sous-traitant pour une enquête omnibus.

Les lois protégeant la vie privée désignent les lois et règlements nationaux dont l'application a pour effet de protéger les données personnelles, en cohérence avec les principes directeurs de ce document.

L'étude de marché*,* qui comprend l'étude sociale et le sondage d'opinion, désigne la collecte systématique et l'interprétation d'informations sur des personnes physiques ou morales. Elle s'appuie sur les méthodes et les techniques statistiques et analytiques des sciences sociales

appliquées, afin de développer des connaissances ou d'aider à la prise de décision. L'identité des personnes interrogées ne doit pas être révélée aux utilisateurs des informations sans consentement explicite et aucune démarche commerciale ne devra être tentée auprès d'elles en conséquence directe de leur participation à l'étude.

Mesures passives des données désigne des données collectées sans passer par les traditionnelles questions et réponses.

Le terme ***données personnelles*** désigne toute information relative à une personne physique (une personne privée, par opposition à une entreprise ou une autre entité) identifiée ou identifiable. Une personne identifiable est quelqu'un pouvant être identifié directement ou indirectement, en particulier en référence à un numéro d'identification ou aux caractéristiques physiques, physiologiques, mentales, économiques, culturelles ou sociales de la personne. Dans certains types d'études de marché, les enregistrements de données peuvent inclure des cas où les individus peuvent être identifiables par des photographies, enregistrements vidéo ou audio, ou d'autres informations personnelles collectées au cours de l'étude de marché.

Traitement des données personnelles inclut, sans être limitatif, la collecte, l'enregistrement, l'organisation, la conservation, l'adaptation ou la modification, l'extraction, la consultation, l'utilisation, la communication par transmission, diffusion ou toute autre forme de mise à disposition, le rapprochement ou l'interconnexion, ainsi que le verrouillage, l'effacement ou la destruction, par des moyens automatiques ou autres.

Participant à l'étude désigne toute personne physique ou morale auprès de qui des informations sont collectées dans le cadre d'une étude de marché, que ce soit par interview active ou par mesures passives.

Chercheur désigne une personne physique ou morale menant une étude de marché, ou ayant un rôle de conseil dans le cadre de cette étude; cette catégorie comprend également les collaborateurs de la société cliente qui interviennent dans le cadre de l'étude de marché et tous les sous-traitants, comme par exemple les fournisseurs technologiques.

Client de l'étude ou ***Utilisateur des données*** désigne toute personne physique ou morale faisant la demande, commissionnant ou souscrivant à tout ou partie d'une étude de marché.

Le terme ***Données sensibles*** désigne toute information relative à l'individu concernant la race, l'origine ethnique, la santé, la vie sexuelle, les antécédents criminels, les opinions politiques, les croyances religieuses ou philosophiques ou l'appartenance syndicale Des informations additionnelles peuvent être définies comme sensibles selon les juridictions. Aux Etats-Unis par exemple, les informations personnelles relatives à la santé, au revenu et autres informations financières, aux identifiants financiers, aux documents d'identification financière et documents provenant du gouvernement sont aussi considérées comme sensibles.

Le terme ***Transfert*** en relation avec les données fait référence à toute divulgation, communication, copie ou envoi de données d'une partie à une autre, quel que soit le moyen utilisé, notamment et de manière non limitative les envois de données par réseau, les transferts physiques, les transferts d'un média ou appareil à un autre, ou les accès à distance aux données.

Le terme ***Transfert transfrontières de données personnelles*** désigne les échanges de données personnelles au-delà des frontières nationales, en incluant l'accès aux données en dehors du pays où elles ont été collectées et l'utilisation des technologies dans le nuage (« *cloud* »).

5 CHECK-LIST DESREGLES ET PROCEDURES DE PROTECTION DE DONNEES

Les utilisateurs de la check-list ci-dessous peuvent noter que les rubriques et l'ordre des éléments ne sont pas les mêmes que ceux utilisés par l'OCDE. Le but ici est d'exprimer les

principes dans une formulation et dans un ordre plus familiers aux chercheurs. Les utilisateurs peuvent également noter que les points sont interdépendants et se chevauchent parfois. **Néanmoins, il est essentiel que la liste de contrôles soit considérée au global et pour chaque article comme complémentaire plutôt qu'exclusive, en accordant une attention particulière aux différences si l'organisme agit comme responsable du traitement ou sous-traitant. Toute question dont la réponse n'est pas «oui» signale un manque potentiel dans un programme de protection de la vie privée et donc un risque potentiel de violer une ou plusieurs lois de protection des données personnelles.**

5.1 Impact minimal

1. *Lors de la conception d'un projet d'étude, limitez-vous la collecte de données personnelles aux seuls éléments nécessaires à l'objectif d'étude en vous assurant qu'ils ne sont pas utilisés d'une manière incompatible avec ces objectifs ?*

Les chercheurs ne doivent recueillir et/ou détenir des données personnelles que pour assurer que l'interview a été menée avec cette personne spécifique, et/ou réaliser un contrôle qualité, un échantillonnage et/ou une analyse. Dans le cas d'étude en entreprise, cela inclut des données personnelles sur le titre ou le poste du participant individuel dans l'organisation, puisque cela peut être nécessaire à l'objectif d'étude.

Ce même principe vaut pour les méthodes passives de collecte de données où les données personnelles peuvent être recueillies sans les traditionnelles questions et réponses. Par conséquent, il est de la responsabilité du chercheur de s'assurer que les seules données personnelles collectées sont celles nécessaires à l'objectif d'étude. Dans le cas où d'autres données personnelles sont reçues, ces éléments doivent être filtrés et supprimés.

2. *Mettez-vous en place des procédures pour garantir que les participants à l'étude ne subissent aucun dommage ou préjudice découlant directement de leur collaboration à un projet d'étude de marché ?*

Le chercheur doit veiller à ce que l'identité d'un individu ne puisse être déduite via des analyses croisées, des petits échantillons, ou de toute autre manière à travers les résultats d'étude. Cela inclut par exemple la fusion avec des renseignements auxiliaires tels que les informations géographiques ou l'identification possible d'un employé particulier dans une enquête de satisfaction clients.

3. *Si vous prévoyez d'utiliser des sous-traitants ou d'autres fournisseurs tiers pour effectuer des services en votre nom, fournissez-vous le minimum de renseignements personnels nécessaires pour qu'ils puissent 'effectuer le service convenu ? Avez-vous des contrats en place pour assurer un niveau de protection similaire de leur part?*

Lors de l'utilisation d'un sous-traitant, il faut lui fournir seulement la quantité minimale de données personnelles nécessaires pour effectuer le service convenu, en clarifiant toujours via des contrats et des instructions les responsabilités du sous-traitant quand il est en possession de ces données. Tous les sous-traitants doivent se conformer aux mêmes règles et règlements que l'organisme d'études. En outre, le transfert de données personnelles à un sous-traitant ou à un autre fournisseur tiers ne doit être fait qu'avec le consentement préalable ou sur instruction du client de la société d'études.

Ce qui précède suppose que les participants à l'étude auront l'assurance que toutes les données recueillies rester ont confidentiel les et ne seront analysées et publiées qu'à un niveau agrégé. Si les participants à l'étude donnent leur consentement pour relier leurs réponses et leurs données personnelles, ils doivent être alors informés de la manière dont ces données seront partagées et utilisées.

5.2 Information et consentement

4. Obtenez-vous le consentement de tous les participants dont les données personnelles sont collectées?

Selon les lignes directrices régissant la vie privée de l'OCDE, toute donnée personnelle devrait être obtenue par des moyens licites et loyaux et, le cas échéant, avec information et consentement du participant à l'étude. Si les législations nationales prévoient généralement un certain nombre de motifs licites et loyaux, les chercheurs sont obligés d'obtenir un consentement dans la plupart des cas.

Dans certains cas, cette responsabilité d'obtenir le consentement repose sur d'autres parties. Les exemples courants incluent l'utilisation de panel tiers ou l'utilisation d'une base de données client. Dans ces circonstances et celles similaires, le chercheur doit obtenir l'assurance que le consentement a été obtenu régulièrement.

Le consentement doit être:

• libre (volontaire et capable d'être retiré à tout moment);

• spécifique (lié à un ou plusieurs objectifs identifiés); et

• éclairé (en pleine connaissance des conséquences du consentement).

Le consentement doit également être clairement notifié par une déclaration ou une action du participant à l'étude après réception des informations ci-dessous. En résumé, il devrait être informé : (a) de l'utilisation qui sera faite de ses données personnelles; (b) des données précises à collecter; (c) du nom, de l'adresse et du contact dans l'entreprise ou l'organisation collectant les données et de celle du responsable de traitement si différent; et (d) le cas échéant de la communication des données à des tiers.

Les chercheurs devraient examiner attentivement le mécanisme qu'ils utilisent pour obtenir le consentement, exprimé habituellement en opt-out (droit d'opposition), opt-in (option d'adhésion), implicite, éclairé ou explicite. La méthode spécifique retenue devrait être documentée.

En général, plus les données collectées sont sensibles, intrusives, ou non-évidentes, plus le niveau de consentement requis est élevé. Dans certaines juridictions, il existe des classes de « données personnelles sensibles » qui nécessitent le consentement explicite des personnes concernées avant qu'elles puissent être recueillies.

Il peut exister des cas où les chercheurs collectent ou reçoivent involontairement des données personnelles, ou des renseignements personnels sur des individus non définis comme participants. Cela comprend par exemple les informations fournies spontanément par les participants; les fichiers fournis par le client contenant plus d'informations que celles nécessaires pour mener l'étude ; et les non-participants capturés en photos ou vidéo. Les chercheurs devraient traiter ces informations de la même manière que les autres données personnelles. Ces données devraient être anonymisées ou détruites immédiatement, en particulier en l'absence de moyen d'informer les personnes dont les données personnelles ont été recueillies de la localisation de ces données, de leur conservation et de leur utilisation. Dans certaines juridictions, il est obligatoire de supprimer ces données ou de les gérer exactement de la même manière que d'autres informations collectées intentionnellement.

5. Êtes-vous clair sur les finalités pour lesquelles les données sont collectées et conservées?

Le secteur des études établit une claire distinction entre les études de marché et la collecte de données à d'autres fins telles que la publicité, la promotion des ventes, la création de fichier, le marketing direct et la vente directe. Cette distinction est essentielle dans la différenciation des finalités et la promotion d'une image positive auprès des organismes de régulation et du grand public. Au cours des dernières années, l'émergence de nouvelles technologies a augmenté les occasions de recueillir des renseignements personnels grâce à des techniques telles que le traçage en ligne et les applications mobiles téléchargeables. Dans tous les cas, il est essentiel que, préalablement à la collecte des données, les participants éventuels à l'étude soient informés de(s) l'objectif(s) pour le(s)quel leurs données seront utilisées et de toutes les conséquences qui pourraient en découler, y compris pour un recontact de suivi qualité.

Lorsque les chercheurs recueillent des données personnelles d'un participant à des fins d'études de marché, la transparence vis-à-vis du participant est cruciale dans la notice d'information. Le participant à l'étude doit recevoir suffisamment de renseignements sur l'utilisation prévue des données personnelles collectées et sur tout partage des données avec des tiers. A titre d'exemple, si l'utilisation prévue des données personnelles est de relier une réponse de l'enquête à un profil de client, cela doit être communiqué au participant de l'étude au moment où les données personnelles sont collectées.

Les engagements de confidentialité doivent être réexaminés régulièrement afin de garantir que le type de données collectées et les utilisations prévues n'ont pas changé. Les chercheurs doivent veiller à ce que les pratiques et les technologies utilisées au sein de leur organisation soient conformes aux engagements pris avec les participants, et en adéquation avec l'évolution des exigences réglementaires. Chaque utilisation possible des données personnelles doit être analysée pour s'assurer de sa conformité avec les lois locales concernant la vie privée, le Code ICC / ESOMAR et les Guides ESOMAR, et les engagements de confidentialité faits aux participants à l'étude.

6. Êtes-vous clair sur les données précises à collecter?

Compte tenu de la large définition des données personnelles dans certaines juridictions, il faut tenir compte de toutes les informations personnelles pouvant être recueillis pour préparer la notice d'information des participants à l'étude. Les données personnelles peuvent inclure le nom, l'adresse, l'email, le numéro de téléphone, le numéro de téléphone mobile, la date de naissance, l'identifiant de l'appareil mobile, l'adresse IP, les photographies et enregistrements audio et vidéo, les numéros d'identification nationale (permis de conduire, sécurité sociale, assurance nationale), l'identifiant d'utilisateur affecté par votre organisme, le nom d'utilisateur dans les réseaux sociaux, les données stockées dans un cookie ou tracking pixel / tag. Rappelez-vous aussi qu'un seul élément de données peut ne pas être considéré comme permettant une identification personnelle dans certaines législations locales, mais lorsqu'il est combiné avec d'autres données (par exemple, le code postal, le sexe, le lieu de travail ou d'études, le poste et le salaire), il peut permettre d'identifier un individu.

En outre, il faut tenir compte de tous les destinataires possibles des données personnelles. Les chercheurs, les organismes de recherche, les tiers fournisseurs de services, et/ou les clients finaux peuvent tous avoir la capacité de collecter et/ou utiliser les données personnelles dans le cadre d'un projet d'étude.

7. Clarifiez-vous de quelle manière les données seront recueillies, y compris toute collecte par mesures passives dont le participant peut ne pas être conscient?

Historiquement, les études s'appuient sur des interviews comme principale méthode de collecte de données personnelles. Comme indiqué dans le point 5 ci-dessus, les nouvelles technologies ont rendu possible le recueil d'un plus large éventail de données personnelles sans informer les personnes dont ces données sont collectées. Tous les participants à l'étude doivent être informés des données précises recueillies et de la méthode(s) utilisée(s) pour les collecter, que ce soit par des moyens actifs tels que des interviews, ou des moyens passifs tels que ceux issus d'une application mobile ou du traçage des comportements en ligne par cookie.

Les chercheurs devraient examiner quels éléments de données collectées et/ou quelle méthode de collecte de données peuvent être non évidentes pour un participant à l'étude et devraient en fournir une description approfondie. Il faut privilégier une série de « notices brèves » plutôt qu'une notice de confidentialité plus détaillée des données collectées ou de leur utilisation pouvant être inattendues ou intrusives. Les applications mobiles, en particulier celles utilisant la géolocalisation, l'écoute passive, et/ou la mesure du système d'exploitation du périphérique mobile, exigent toutes une description détaillée et le consentement explicite du participant à l'étude pour ces activités.

5.3 Intégrité / Sécurité

8. *Des procédures sont-elles en place pour assurer que toutes les données personnelles collectées sont exactes, complètes et à jour?*

Les contrôles qualité devraient être effectués à chaque étape du processus d'étude. Lors de l'élaboration des questionnaires ou des applications d'étude, des tests devraient être effectués avant le lancement du terrain afin de réduire le risque d'erreurs dans la collecte de données. Pendant la phase de terrain, le suivi et la validation des données entrantes telles que les interviews devraient se dérouler en conformité avec les normes qualité applicables aux études. Pendant les phases de traitement statistique et de création de rapport, des contrôles qualité supplémentaires devraient être effectués pour s'assurer que les données sont correctes et que l'analyse, les conclusions et les recommandations sont cohérentes avec les données.

Les chercheurs fournisseurs de panels devraient veiller à ce que les membres du panel soient en mesure d'examiner et de mettre à jour leurs données de profil à tout moment, et devraient leur rappeler périodiquement de le faire. Les échantillons constitués à partir de panel devraient inclure des informations démographiques à jour. Une bonne source de pratiques standard à cet égard est la norme ISO26362:2009 Access panels pour les études de marché, études sociales et d'opinion.

9. *Vous assurez-vous que les données personnelles ne sont pas conservées plus longtemps que nécessaire aux fins pour lesquelles elles ont été collectées ou traitées? Avez-vous des procédures pour conserver séparément ou supprimer les identifiants d'enregistrements de données une fois qu'ils ne sont plus nécessaires?*

Les chercheurs devraient fixer des durées de conservation des données aussi courtes que possible, en suivant dans tous les cas les lois applicables pour la source des données personnelles qu'ils collectent, qu'ils agissent en tant que responsable de traitement ou sous-traitants des données. Dans ce dernier cas, les clients peuvent imposer par contrat des durées de conservation.

En ce qui concerne la source des données personnelles, les informations provenant d'études longitudinales ou des profils panélistes seront typiquement utilisées et conservées pendant toute la durée pendant laquelle ils restent des membres actifs. En revanche, une période de conservation plus courte devrait s'appliquer aux données personnelles de non-panélistes participant aux études ad hoc. Bien sûr, il est important de ne pas détruire leurs données personnelles trop rapidement car des contrôles qualité doivent être effectués lors de la phase de traitement statistique pour s'assurer de l'exactitude des données et satisfaire aux exigences du principe d'intégrité des données.

Lorsque des données personnelles sont utilisées, une bonne pratique pour les chercheurs est d'utiliser des identifiants pseudonymes. Un fichier maître reliant les noms des participants, adresses ou numéros de téléphone avec leur numéro d'identification généré en interne doit être conservé en toute sécurité avec un accès limité à un petit nombre de personnes, par exemple le personnel en charge de l'échantillonnage ou de la gestion du panel. Ainsi, les chercheurs, le personnel de traitement statistique et de codification qui ont besoin d'analyser les données au niveau des participants peuvent le faire sans voir les noms, adresses ou numéros de téléphone des participants.

Lorsque les réponses de l'enquête ont été traitées et publiées dans un rapport en résultats statistiques agrégés, les données personnelles concernant les participants avec leurs identifiants pseudonymes devraient être supprimées, de sorte que l'organisation en charge de l'étude ne détienne plus ces données personnelles.

10. *Avez-vous des procédures en place pour répondre aux demandes des particuliers au sujet des données personnelles que vous avez recueillies auprès d'eux ? Vos procédures de gestion des demandes d'accès provenant d'individus comprennent-elles une authentification de leur identité, et permettent-elles de répondre aux demandes dans un délai raisonnable en corrigeant les données inexactes ou en supprimant entièrement les données?*

Des procédures formalisées devraient être élaborées, communiquées et suivies pour répondre aux personnes souhaitant accéder aux données personnelles que les organisations détiennent sur eux. S'assurer de l'identité des personnes qui font des demandes d'accès est important pour éviter la divulgation de données personnelles à d'autres personnes de façon inappropriée.

Une fois authentifiée l'identité d'une personne faisant une demande d'accès - la personne est celle qu'elle prétend être et a un droit légal d'accéder aux données personnelles en question - les chercheurs devraient s'efforcer de répondre à la demande d'accès le plus rapidement possible, par exemple dans les 10 à 30 jours selon les lois applicables. Si la société d'études a besoin d'un délai supplémentaire pour répondre à la demande, il peut être possible d'étendre le délai prévu légalement, à condition que l'individu soit informé et que les raisons de la prolongation du délai soient valides. Un délai supplémentaire peut être nécessaire afin, par exemple, de mener des consultations ou pour recueillir les informations demandées à partir de plusieurs bases de données.

Alors que les lois de protection des données peuvent inclure des exceptions qui imposent aux organisations de refuser l'accès à des renseignements personnels dans certaines situations, ces exceptions sont peu susceptibles de s'appliquer aux informations personnelles traitées dans le cadre d'études de marché. Par exemple, les lois applicables peuvent permettre aux organisations de refuser les demandes d'accès si ces informations relèvent du secret professionnel. A titre d'autre exemple, si l'organisation a divulgué des renseignements à une institution gouvernementale pour l'application de la loi ou pour des raisons de sécurité nationale, cette institution peut exiger de l'organisation qu'elle refuse l'accès ou qu'elle ne révèle pas que l'information a été communiquée.

11. Avez-vous des protocoles de sécurité en place pour chaque ensemble de données afin de maitriser les risques tels que la perte et l'accès non autorisé, la destruction, l'utilisation, la modification ou la divulgation non autorisés ?

S'acquitter de ces responsabilités commence par l'élaboration et l'application d'une politique de sécurité pour protéger les informations personnelles et d'autres types d'informations confidentielles. La norme ISO 27001 est un standard reconnu de sécurité de l'information sur lequel une politique de sécurité renforcée peut être basée.

L'utilisation de mesures de sécurité appropriées pour assurer la protection requise comprend:

- des mesures physiques (armoires fermées, accès restreint aux bureaux, systèmes d'alarme, caméras de sécurité) ;
- des outils technologiques (mots de passe, cryptage, pare-feu) ;
- des contrôles organisationnels (vérification des antécédents, règles relatives à la prise de contrôle des ordinateurs hors site, accès restreint sur le principe du «besoin de connaître», formation du personnel, accords avec les clients et sous-traitants).

La politique de sécurité devrait également inclure une procédure pour faire face à une violation potentielle de sécurité qui donnerait lieu à une divulgation de données personnelles. Si les données ont été recueillies et fournies par une tierce partie, comme dans le cas d'une base de données d'un client, cette tierce partie doit être immédiatement informée. Les participants dont les données ont été divulguées doivent également être informés si la divulgation les expose à un risque (par exemple, le vol d'identité) et les mesures appropriées doivent être prises pour les protéger contre ce risque.

12. Avez-vous un dispositif clair sur le délai de conservation des données personnelles ?

Le délai de conservation des données personnelles peut varier d'un projet d'étude à l'autre selon une diversité des circonstances indiquée précédemment dans la réponse à la question 9.

Alors que les pratiques générales de conservation devraient être incluses dans les politiques de confidentialité, il n'est pas toujours pratique de communiquer les délais précis de conservation pour les différents types d'études. Par conséquent, les chercheurs devraient également

envisager de communiquer des informations de conservation des données dans les matériaux de recrutement de l'enquête, les introductions de questionnaires ou formulaires d'agrément spécifique par enquête. Ils devraient toujours être prêts à communiquer sur demande les délais de conservation des données d'un projet donné.

5.4 Transfert de données personnelles

13. Avez-vous défini des règles et procédures régissant l'utilisation et la divulgation des données personnelles?

Ces règles et procédures sont clairement définies dans les lois locales sur la vie privée et la protection des données existant dans votre pays. Une explication de leurs implications devrait être clairement documentée, avec des procédures et documents écrits pour garantir que le personnel peut mettre en œuvre les procédures de gestion des données personnelles, et qu'il est au fait de ces règles et procédures. Par exemple, cela comprendra le principe que le consentement du participant à l'étude est nécessaire avant que de telles données puissent être communiquées, même à des clients ou à des chercheurs dans les organisations clientes.

14. Les conditions dans lesquelles les données personnelles peuvent être communiquées sont-elles claires et sans ambiguïté?

Les participants à l'étude doivent savoir ce qui est fait avec leurs données personnelles, et cela doit être expliqué soit verbalement, soit fourni dans un format écrit ou un document que les participants à l'étude doivent accepter–avec un consentement enregistré comme preuve qu'ils ont accepté.

15. Votre personnel connaît-il ces règles et est-il formé pour mettre en œuvre les procédures?

Votre politique de confidentialité décrit les pratiques de collecte et de gestion des données de votre organisation. Il est également important d'élaborer des procédures opérationnelles standard pour garantir que les engagements de confidentialité faits aux participants soient bien tenus.

La formation du personnel sur la vie privée devrait inclure un aperçu des lois applicables, les codes de conduite sectoriels, la politique de confidentialité des consommateurs dans votre organisation, et vos procédures opérationnelles standard. La formation à la protection de la vie privée devrait être faite au moins annuellement et les attestations de présence devraient être conservées.

Tout le personnel qui interagit avec les participants devraient être en mesure d'expliquer en profondeur les politiques et les procédures de l'organisation. Il devrait savoir qui contacter en interne pour les assister sur les demandes auxquelles ils ne sont pas en mesure de répondre.

Il devrait y avoir une supervision claire et une description des responsabilités, avec un contrôle formalisé du suivi des procédures.

5.5 Flux transfrontières de données personnelles

16. Si des données personnelles doivent être transférées d'une juridiction à l'autre, est-ce fait conformément aux exigences de protection des données à la fois dans les juridictions d'origine et de destination?

Ceci est souvent désigné comme un «transfert transfrontalier des données personnelles». Cela se produit lorsque les données sont collectées au-delà des frontières nationales, et/ou lorsque le traitement des données est délocalisé ou sous-traité à un autre pays ; par exemple quand un client engage un chercheur dans un autre pays pour réaliser une étude utilisant des données fournies par le client sur ses consommateurs ou utilisateurs. Chaque pays a ses propres règles sur la façon dont ces données doivent être traitées et protégées, les chercheurs devant s'y conformer. Bien que cela puisse sembler complexe, les problèmes de conformité rencontrés par les chercheurs peuvent utilement être décomposés en trois difficultés principales:

- S'assurer que les transferts transfrontaliers de données personnelles sont effectués en conformité avec la législation nationale applicable. Les fondements les plus courants pour assurer une protection adéquate lors d'un transfert transfrontalier seront le consentement ou l'utilisation de clauses contractuelles appropriées et, si requis par la loi nationale applicable, l'obtention de l'autorisation préalable à utiliser ces contrats par l'Autorité de protection des données personnelles nationale ou autre autorité de régulation de la vie privée. Comme mesure de sécurité supplémentaire et afin de réduire davantage les risques quand le traitement statistique est délocalisé, l'identifiant des données personnelles doit être si possible retiré de sorte que seul un numéro d'identification pseudonyme est utilisé pour relier les données individuelles et l'identité des participants.
- La possibilité pour un chercheur de procéder à des transferts transfrontaliers lorsqu'il est sous-traitant des données personnelles, par exemple lors d'une enquête utilisant un échantillon fourni par le client. Même lorsque les chercheurs ont pris soin de s'assurer que les transferts transfrontaliers respectent les règles régissant ces transferts, ils devraient garder à l'esprit que lors du traitement des données personnelles en tant que sous-traitant du responsable de traitement (le client de l'étude par exemple), celui-ci peut refuser le transfert transfrontalier des données personnelles qu'il détient, ce qui peut avoir un impact sur la manière de réaliser le projet. Il devrait y avoir un accord écrit entre les deux parties dessus.
- Les transferts transfrontaliers de données personnelles lors de la collecte de données personnelles des participants à l'étude dans d'autres pays ; par exemple des enquêtes en ligne destinées à des participants à l'étude résidant dans un pays différent de celui du chercheur en charge de l'enquête. Les lois applicables sur la confidentialité seront normalement les lois nationales du pays où est basé le chercheur. Cependant, le chercheur doit également veiller à la conformité de l'étude ou du panel avec toutes les autres lois nationales applicables dans les pays où les données ont été recueillies. Les pratiques recommandées consistent notamment à vérifier que : (1) les renseignements juridiques du chercheur (nom de l'entreprise, adresse postale, etc…), dont le pays, sont clairement communiqués dans tous les documents de recrutement ; (2) la politique de confidentialité en ligne comprend une déclaration simple mais claire décrivant les transferts transfrontaliers qui auront lieu suite à la participation à l'étude ou au panel ; et (3) il existe une référence au transfert(s) transfrontalier(s) dans la question de consentement du recrutement du panel.

5.6 Externalisation et sous-traitance

17. Avez-vous des exigences précises, y compris une surveillance appropriée pour tous les prestataires en charge d'un traitement de données personnelles et autres sous-traitants?

Des exigences précises doivent être communiquées à tous les sous-traitants en charge d'un traitement de données personnel les selon les règles de protection des données personnelles relatives au transfert. Une protection supplémentaire devrait concerner le transfert de toute donnée, qu'elle soit individuelle ou agrégée, via un processus informatique dédié tel que le cryptage des données transférées ou l'utilisation de plates-formes de transfert FTP sécurisé. Si des copies de sauvegarde des données sont faites par les sous-traitants ou les prestataires de traitement, des procédures précises doivent protéger ces données pendant le stockage, et prévoir leur suppression une fois leur durée de conservation expirée.

5.7 Politique de confidentialité

18. Les informations sur votre programme de protection des données personnelles et de la vie privée sont-elles facilement disponibles et sous une forme facilement compréhensible par les participants?

De nombreuses juridictions exigent que l'information soit disponible via une politique de confidentialité facilement disponible pour les participants à l'étude. Bien que le contenu et les détails requis puissent varier d'un pays à l'autre, les chercheurs doivent toujours s'identifier clairement auprès des participants de l'étude et veiller à expliquer le but de l'étude, la manière dont les données personnelles sont collectées, comment elles seront gérées (collectées, stockées, utilisées, consultées et divulguées) et comment obtenir de plus amples renseignements ou déposer une plainte.

Les chercheurs doivent veiller à ce que les politiques soient faciles à comprendre, pertinentes pour le lecteur, faciles à trouver, aussi concises que possible, et adaptées aux activités de l'organisation. Ceci inclut la mise à disposition de politiques dans toutes les langues utilisées, la révision régulière des politiques et leur mise à jour le cas échéant.

19. L'identité et la responsabilité du responsable de traitement de données sont-elles claires?

Les chercheurs doivent veiller à ce que leurs propres rôles et responsabilités pour la gestion des données personnelles soient clairs pour les participants à l'étude. Ceci comprend l'identification du responsable du traitement de données et des éventuels prestataires en charge d'un traitement de données personnelles. Les participants ne doivent pas être laissés dans le doute quant à l'organisation responsable en dernier ressort de la gestion de leurs données.

Certaines juridictions exigent également qu'une personne en particulier dans l'organisation soit identifiée comme ayant la responsabilité des pratiques de protection des données de l'organisation.

Dans le cas d'enquêtes « en aveugle » à l'aide d'échantillons fournis par le client, les participants doivent être informés au début d'interview que le nom du client sera révélé à la fin de l'enquête parce que la divulgation de cette information au préalable pourrait introduire un biais de réponse. Puisque de nombreuses lois nationales de protection des données personnelles accordent aux participants un droit de savoir de qui le chercheur a obtenu leurs données personnelles, les chercheurs doivent être prêts à fournir le nom du client à tout moment sur demande des participants.

20. Est-il clair que le responsable du traitement des données est responsable des données personnelles sous son contrôle indépendamment de leur localisation ?

Si les chercheurs sont susceptibles de sous-traiter une partie des traitements, ou de transférer des données personnelles en dehors de leur juridiction, ils doivent être prêts à fournir au responsable de traitement la description des sous-traitants et la localisation du traitement, en obtenant le consentement écrit préalable du responsable de traitement si nécessaire. Lorsque la société d'études est le responsable de traitement de données, elle devrait inclure dans sa politique de confidentialité les références aux sous-traitants utilisés pour le traitement de données et, le cas échéant, la liste des pays ou régions où ils se situent. Les chercheurs devraient être vigilants sur le fait que certaines juridictions interdisent aux chercheurs de transférer des données personnelles vers des pays ou des régions qui ne disposent pas des niveaux équivalents en matière de loi sur la protection des données personnelles. Sous réserve du respect des règles relatives aux transferts transfrontaliers imposées par la législation locale pertinente (qui peut imposer des formalités préalables), transférer des données personnelles à travers un groupe multinational est autorisé par la plupart des juridictions, bien que certaines exigent que les personnes concernées soient informées de la localisation de leurs données

6 POINTS SPECIFIQUES

6.1 Collecte de données auprès d'enfants

Les règles nationales fixant les âges à partir desquels une autorisation parentale n'est plus nécessaire varient considérablement. Pour déterminer quand l'autorisation parentale est nécessaire, ou lorsque les sensibilités culturelles nécessitent un traitement particulier, les chercheurs doivent consulter les lois nationales et les codes professionnels d'autorégulation des

juridictions où les données seront collectées. En l'absence de lignes directrices nationales, consulter le guide ESOMAR, Interviewing Children and Young People.

La collecte de données auprès des enfants nécessite l'autorisation vérifiable du responsable légal de l'enfant. Le parent ou un adulte responsable doit recevoir suffisamment d'information sur la nature du projet d'étude pour lui permettre de prendre une décision éclairée au sujet de la participation de l'enfant. Le chercheur doit enregistrer l'identité de l'adulte responsable et son lien avec l'enfant.

6.2 Etude en entreprise (B2B)

Un nombre important de projets d'étude implique la collecte de données auprès d'entités juridiques telles que les entreprises, les établissements scolaires, les organismes à but non lucratif et autres organisations similaires. Cette recherche nécessite souvent la collecte d'informations sur l'entité telles que le chiffre d'affaires, le nombre d'employés, le secteur, la localisation, et ainsi de suite.

Dans tous ces cas, les organisations participantes ont droit au même niveau de protection dans la divulgation d'identité dans le rapport que celles offertes aux personnes individuelles dans les autres types d'études.

Il est à noter que de nombreuses lois nationales de protection des données personnelles considèrent que le titre et les coordonnées du lieu de travail d'un individu sont des données personnelles. Certaines lois de protection des données personnelles vont plus loin en appliquant leurs exigences aux personnes physiques et entités juridiques (personnes individuelles et personnes morales).

6.3 Photographies, enregistrements audio et vidéo

Plusieurs nouvelles techniques d'enquêtes créent, stockent et transmettent des photographies et enregistrements audio et vidéo dans le cadre du processus d'étude. Deux exemples marquants sont l'ethnographie et les études mystères.

Les chercheurs doivent reconnaître que les photographies et enregistrements audio et vidéo sont des données personnelles et doivent être traités comme tels le cas échéant. Si les chercheurs demandent aux participants de fournir des informations sous ces formes, ils devraient également indiquer comment réduire la collecte de données personnelles non sollicitées, en particulier celles de non-participants (membres du foyer…).

Enfin, certains types d'étude par observation peuvent impliquer de photographier, filmer ou enregistrer dans les lieux publics impliquant des personnes qui ne sont pas recrutées comme participants à l'étude. Dans ces cas, les chercheurs doivent demander l'autorisation aux individus concernés de partager leurs images si les visages sont clairement visibles et peuvent être identifiés. Si l'autorisation ne peut être obtenue, l'image de l'individu doit être pixélisée ou rendue anonyme. De plus, des panneaux clairs et lisibles devraient être placés pour indiquer que la zone est sous observation en indiquant comment contacter la personne ou l'organisation responsable. Les caméras devraient être situées de manière à surveiller uniquement les zones destinées à l'observation.

6.4 Stockage en nuage (« *cloud storage* »)

La décision de stocker des données personnelles dans le nuage doit être examinée attentivement. Les chercheurs doivent évaluer les contrôles de sécurité du fournisseur de service de stockage dans le nuage et ses conditions générales d'utilisation. Beaucoup de fournisseurs de services de stockage en nuage offrent des indemnités faibles en cas de violation de la sécurité et de compromission les données personnelles. Cela signifie que l'organisation du chercheur

prendrait un risque considérable de dommages financiers et de pertes suite aux violations graves de la vie privée portant atteinte aux personnes concernées.

Les chercheurs devraient donc mettre en place des contrôles compensatoires pour se protéger contre de tels risques. Par exemple, ils devraient crypter les flux de données personnelles (transférées depuis/vers le nuage) et les dépôts (stockés sur les serveurs du fournisseur de nuage). Les chercheurs devraient aussi envisager la souscription d'une police d'assurance du risque numérique.

Les chercheurs doivent aussi considérer les emplacements physiques où les données personnelles sont stockées afin de déterminer si l'utilisation du stockage en nuage est un transfert transfrontalier. Reportez-vous à la section 5.5 du présent document pour davantage d'information. Certains fournisseurs de services dans le nuage offrent des emplacements de stockage spécifiques à chaque pays pouvant être appropriés à certains cas.

Enfin, les chercheurs devraient stocker des données personnelles sur un nuage privé plutôt que public. Un nuage privé est celui dans lequel un équipement dédié dans un centre de données particulier est attribué à l'organisation du chercheur. Le principal avantage d'un nuage privé est que le chercheur sait toujours où se trouvent les données personnelles. En revanche, un nuage public peut conduire à des données situées dans deux ou plusieurs centres de données et deux ou plusieurs continents, ce qui soulève des problèmes potentiels de conformité à la fois aux exigences des lois de protection des données personnelles et aux contrats conclus avec les responsables de traitement spécifiant où les données personnelles doivent être situées.

6.5 Anonymisation et pseudonymisation

Un élément clé de la responsabilité en protection des données personnelles d'un chercheur est d'anonymiser les données avant de les envoyer à un client ou même au grand public. L'anonymisation est l'une des mesures de sauvegarde qui implique soit la suppression soit la modification des identifiants personnels pour rendre les données sous une forme qui ne permette pas d'identifier les individus. Il s'agit par exemple de brouillage des images pour masquer les visages, et de résultats sous forme agrégée dans les rapports pour s'assurer qu'ils ne permettront pas d'identifier un individu en particulier.

La pseudonymisation consiste à modifier les données personnelles d'une manière telle qu'il est toujours possible de distinguer des individus dans un ensemble de données en utilisant un identifiant unique comme un numéro d'identification ou des algorithmes de hachage, tandis que leurs données personnelles sont conservées séparément à des fins de vérification (voir Q9).

Lors de l'utilisation de ces techniques, les chercheurs devraient consulter les lois nationales et locales et les codes professionnels d'autorégulation pour déterminer quels éléments doivent être enlevés pour se conformer à la norme juridique d'anonymisation / pseudonymisation de ces données.

7 SOURCES ET REFERENCES

DLA Piper, Data Protection Laws of the World

EphMRA Adverse Event Reporting Guidelines 2014

ICC/ESOMAR International Code on Market and Social Research

ESOMAR Interviewing Children and Young People Guideline

ISO 26362:2009 – Access panels in market, opinion, and social research

ISO 20252 – Market, Opinion and Social Research

OECD Privacy Principles

8 L'EQUIPE PROJET

Co-présidents:

- Reg Baker, consultant au ESOMAR Professional Standards Committee et au Marketing Research Institute International
- David Stark, Vice-President, Integrity, Compliance and Privacy, GfK

Membresde l'équipe Projet:

- Debrah Harding, Managing Director, Market Research Society
- Stephen Jenke, Consultant
- Kathy Joe, Director of International Standards and Public Affairs, ESOMAR
- Wander Meijer, Global COO, MRops
- Ashlin Quirk, General Counsel SSI
- Barry Ryan, Director - Policy Unit, MRS
- Jayne Van Souwe, Principal, Wallis Consulting Group