Politique du Groupe Ipsos de Protection et de Confidentialité des Données

(en vigueur le 25 mai 2018)

Politique du Groupe Ipsos de Protection et de Confidentialité des Données

Table des Matières

1. Introduction

Dans le cadre de sa responsabilité sociale, Ipsos s'engage à respecter les lois et les réglementations applicables en matière de protection des données personnelles. Cette politique de protection des données (« **Politique »** ou « **Politique de Protection des Données »**) s'applique à l'ensemble du Groupe Ipsos et repose sur des principes de base de protection des données acceptés dans le monde entier.

Cette Politique adopte les principes fondamentaux du Règlement Général sur la Protection des Données[1] (« **RGPD** ») de l'Union Européenne comme norme minimale à laquelle le Groupe Ipsos, ses collaborateurs et ses prestataires doivent se conformer.

Ipsos collecte et analyse des informations sur des individus (« **Personnes Concernées** ») pour réaliser des études de marché et des activités connexes. Maintenir la confiance des Personnes Interrogées (voir ci-après au paragraphe 5.1) et du public exige que les répondants ne subissent pas de conséquences négatives ou des dommages résultant de la communication à Ipsos de leurs informations ou de leurs Données Personnelles traitées pour les besoins de l'activité d'Ipsos (pour avoir une définition et une explication des termes en majuscules utilisés dans cette Politique, veuillez vous référer au **Glossaire**). Ipsos interroge tout type d'individu ou d'organisation.

Dans le cadre de ses activités, Ipsos a également besoin de collecter et de traiter certains types d'informations sur les personnes avec lesquelles Ipsos intéragit pour les besoins de ses activités. Il s'agit notamment des collaborateurs actuels, passés et futurs, des prestataires, des clients et d'autres personnes avec lesquelles Ipsos pourrait communiquer. En outre, Ipsos peut être tenu par la loi de traiter certains types de Données Personnelles pour se conformer à certaines exigences légales.

La présente Politique définit les normes minimales relatives au traitement, à la collecte, à la manipulation et à la conservation des Données Personnelles afin de satisfaire aux principes applicables en matière de protection des données d'Ipsos.

Les Utilisateurs de Données sont tenus de se conformer à la présente Politique lors du traitement des Données Personnelles pour le compte d'Ipsos.Tout manquement à cette Politique peut entraîner des mesures disciplinaires pouvant aller jusqu'au licenciement.

2. Champ d'application

La Politique est applicable à l'ensemble des entités du Groupe Ipsos, quelle que soit leur localisation. Au sein d'Ipsos, cette Politique constituera la norme minimale à laquelle l'ensemble des entités, des collaborateurs et des prestataires d'Ipsos devront adhérer, que le RGPD s'applique directement ou non à une activité ou à un territoire spécifique.

Toute personne travaillant pour Ipsos a la responsabilité de s'assurer que les Données Personnelles sont collectées, conservées et manipulées de manière appropriée.

Il est de la responsabilité de chacun que les Données Personnelles soient manipulées et traitées conformément à la présente Politique et à ses principes de protection des données.

Ipsos attend également de ses prestataires/fournisseurs qu'ils se conforment aux principes énoncés dans la présente Politique.

3. Application des Lois et des Codes de Conduite Nationaux

Cette Politique de Protection des Données adopte les principes de protection de la vie privée acceptés à l'échelle internationale, tels que renforcés par le RGPD. Cette Politique complète

[1] Règlement (UE) 2016/679 du Parlement européen et du Conseil du 27 avril 2016

toute législation nationale applicable. Les lois nationales applicables prévaudront en cas de conflit avec la présente Politique ou si leurs exigences sont plus strictes que la présente Politique. Toute obligation d'enregistrement, de notification ou de déclaration pour le traitement des données en vertu de la législation nationale doit être respectée. Le contenu de la présente Politique doit également être respecté en l'absence de législation nationale relative à la protection des Données Personnelles.

Chaque entité du Groupe Ipsos est responsable du respect de la présente Politique de Protection des Données et des obligations légales applicables. S'il y a lieu de croire que les obligations légales sont en conflit avec les obligations découlant de la présente Politique, l'entité Ipsos concernée devra en informer le Délégué à la Protection des Données (« ***Data Protection Officer*** » ou « **DPO** ») du pays et le *Global Chief Privacy Officer* (« **CPO** »). En cas de conflit entre la législation applicable et la Politique de Protection des Données, Ipsos travaillera avec l'entité Ipsos concernée pour trouver une solution pratique qui réponde aux exigences et aux objectifs de cette Politique ainsi qu'à la législation applicable.

En complément de cette Politique, pour ses activités d'études de marché, Ipsos adhère aux exigences du Code international ICC/Esomar des études de marché, études sociales et d'opinion et de l'analytique des données, disponible ici.

4. Principes relatifs au Traitement des Données Personnelles

Toutes les Données Personnelles doivent être traitées de manière appropriée, quel que soit le procédé utilisé pour la collecte, l'enregistrement et le traitement que ce soit sur papier, dans un fichier informatique, dans une base de données ou sur d'autres supports.

Il existe des règles assurant cette protection, comme indiqué dans les Lignes Directrices de l'OCDE sur la Protection de la Vie Privée et les Flux Transfrontières de Données Personnelles, ainsi que des lois nationales sur la protection des Données Personnelles applicables dans différents pays, y compris dans le cadre du RGPD.

Ipsos considère que le traitement licite et sécurisé des Données Personnelles et le maintien de la confiance vis-à-vis des personnes participant aux études sont les éléments essentiels de son activité. Ainsi, Ipsos s'engage à agir de manière éthique et responsable à l'égard du Traitement des Données Personnelles et à toujours assurer un niveau élevé de confidentialité et de sécurité des Données.

Ipsos s'engage à respecter les principes relatifs au traitement des Données Personnelles figurant dans le RGPD qui sont eux-mêmes le reflet des principes de l'OCDE. Le traitement des Données Personnelles par Ipsos s'effectue selon les principes suivants, dont l'explication détaillée est fournie ultérieurement dans la Politique :

- Les données sont traitées de façon licite, loyale et transparente.
- Les données sont traitées pour des finalités déterminées, explicites et légitimes .
- Les données collectées sont adéquates, pertinentes et non excessives au regard des finalités pousuivies.
- Les données sont exactes.
- Les données sont conservées pendant une durée qui n'excède pas la durée nécessaire aux finalités auxquelles elles sont traitées.
- Les données sont traitées de manière conforme aux droits des Personnes Concernées.
- Les données sont traitées de manière sécurisée.
- Les données ne sont pas transférées à des personnes ou à des organisations situées dans des pays ne bénéficiant pas d'un niveau adéquat de protection.

4.1. Licéité, Loyauté et Transparence

Les Données Personnelles doivent être traitées et collectées de manière licite, loyale et transparente au regard de la Personne Concernée. En outre, les Personnes Concernées

doivent être informées de la manière dont leurs données sont traitées. En général, les Données Personnelles sont collectées directement auprès de la Personne Concernée. A défaut, la base juridique sur laquelle le traitement est fondé doit être documentée. Le DPO concerné doit être consulté pour savoir si une **Analyse d'Impact relative à la Protection des Données** (« **DPIA** ») doit être réalisée (voir également les directives distinctes sur les DPIA qui se trouvent sur l'intranet Groupe sous Privacy & Data Protection).

4.2. Limitation des Finalités

Les Données Personnelles doivent être collectées pour des finalités déterminées, explicites et légitimes et ne doivent pas être traitées ultérieurement d'une manière incompatible avec ces finalités. Toute modification ultérieure des finalités n'est possible que de manière restreinte et requiert une justification et une validation. Le DPO concerné doit être consulté pour savoir si un DPIA doit être réalisé.

4.3. Minimisation des Données

Les Données Personnelles doivent être adéquates, pertinentes et limitées à ce qui est nécessaire au regard des finalités pour lesquelles elles sont traitées. Il faut déterminer si, et dans quelle mesure, le traitement des Données Personnelles est nécessaire pour atteindre la finalité pour laquelle le traitement est effectué. Lorsque les finalités le permettent et que les dépenses engagées sont proportionnelles à l'objectif poursuivi, les données anonymes doivent être utilisées en lieu et place des Données Personnelles.

4.4. Exactitude

Les Données Personnelles doivent être exactes et, le cas échéant, tenues à jour. Toutes les mesures raisonnables doivent être prises pour que les Données Personnelles qui sont inexactes, eu égard aux finalités pour lesquelles elles sont traitées, soient effacées ou rectifiées sans délai.

4.5. Limitation de la Conservation des Données

Les Données Personnelles ne doivent pas être conservées sous une forme permettant l'identification des Personnes Concernées pendant une durée excédant celle nécessaire au regard des finalités pour lesquelles elles sont traitées. Ipsos ne conservera pas les Données Personnelles pendant une durée excédant celle nécessaire au regard des finalités pour lesquelles elles ont été collectées. Ipsos prendra toutes les mesures raisonnables pour détruire ou effacer de ses systèmes toutes les Données Personnelles qui ne sont plus nécessaires.

4.6. Intégrité et Confidentialité

Les Données Personnelles doivent être traitées de façon à garantir une sécurité appropriée des Données Personnelles contre la divulgation, la diffusion, l'accès ou la manipulation. Par conséquent, lorsque cela est possible d'un point de vue méthodologique et que le coût n'est pas disproportionné au regard des risques encourus par la Personne Concernée, les données pseudonymisées doivent être utilisées pour le traitement. **RAPPEL : les données pseudonymisées sont des Données Personnelles.**

4.7. Restriction sur les Transferts

Les Données Personnelles ne doivent pas être transférées vers des pays (même vers d'autres entités Ipsos situées dans ces pays) qui n'assurent pas un niveau adéquat de protection. Ipsos a mis en place diverses mesures pour assurer un tel niveau adéquat de protection (voir également le paragraphe 6 pour plus de détails). Cependant des pays peuvent avoir des exigences supplémentaires et/ou différentes qui doivent être respectées.

4.8. Mesures et Considérations Générales

En outre, dans le cadre de ses activités d'études de marché, Ipsos se conforme au Code International ICC/ESOMAR des Etudes de Marché, Etudes Sociales et d'Opinion, et de l'Analytique des Données et la Check-list de Protection des Données d'Esomar.

5. Base Juridique pour le Traitement des Données

Ipsos ne collectera, ne traitera et n'utilisera les Données Personnelles qu'en vertu des bases juridiques suivantes, à condition qu'une telle base juridique soit prévue par la loi nationale applicable. L'une de ces bases juridiques est également nécessaire si la finalité de la collecte, du traitement et de l'utilisation des Données Personnelles doit être modifiée par rapport à la finalité initiale, à moins qu'il n'y ait une compatibilité claire entre la finalité initiale et la nouvelle finalité. Veuillez vous référer également au paragraphe 4.2 et à toute exigence de conformité supplémentaire éventuelle.

5.1. Données des Personnes Interrogées

Les Personnes Interrogées (ou les interviewés) sont les Personnes Concernées les plus fréquentes dans l'activité d'Ipsos. En conséquence, le traitement correct de leurs Données Personnelles est au cœur de l'activité d'Ipsos.

5.1.1. Consentement au Traitement des Données

Les Données Personnelles peuvent être traitées après obtention du consentement de la Personne Concernée. Avant de donner son consentement, la Personne Concernée doit être informée conformément au principe de transparence énoncé au paragraphe 4.1. La déclaration de consentement doit être établie sous forme écrite ou électronique à des fins de documentation. Dans certains cas, notamment en cas d'enquête téléphonique, le consentement peut être donné verbalement. L'octroi du consentement doit dans tous les cas être correctement documenté.

Tout consentement ne sera valide que s'il constitue une manifestation de volonté libre, spécifique, éclairée et univoque par laquelle la Personne Concernée accepte, par une déclaration ou par un acte positif clair, que des Données Personnelles la concernant fassent l'objet d'un traitement.

5.1.2. Traitement des Données dans le cadre d'une Relation Contractuelle

En dehors du consentement, leurs Données Personnelles peuvent être traitées lorsque cela s'avère nécessaire dans le cadre de l'exécution d'un contrat auquel ces Personnes Concernées sont parties, afin de satisfaire aux droits et obligations applicables. Cela s'applique également lorsque ce traitement est nécessaire à l'établissement ou à la résiliation d'un contrat. Cela s'applique en particulier aux Personnes Interrogées (y compris les clients mystères) dans le cadre de l'inscription aux panels Ipsos.

Certains pays considèrent que la conclusion d'un contrat est une forme de consentement.

5.1.3. Traitement des Données conformément à une Obligation Légale

Le traitement des Données Personnelles est également autorisé si la législation nationale le demande, l'exige ou le permet. Le type et l'étendue du traitement des données doivent être nécessaires à l'activité de traitement des données légalement autorisée et doivent être conformes aux dispositions légales applicables.

5.1.4. Traitement des Données aux fins des Intérêts Légitimes

Les Données Personnelles peuvent également être traitées si cela s'avère nécessaire au regard des intérêts légitimes du groupe Ipsos et si la législation nationale le prévoit (par exemple, l'Article 6(1) (f) du RGPD). La base juridique pour justifier du traitement des données effectué aux fins des intérêts légitimes n'est pas reconnue dans tous les pays, et la législation nationale applicable prévaudra. En règle générale, des catégories particulières de Données Personnelles ne peuvent pas être traitées aux fins des intérêts légitimes. En tout état de cause, les Données Personnelles ne peuvent être traitées aux fins des intérêts légitimes si, dans un cas particulier, il est prouvé que les intérêts de la Personne Concernée justifient d'être protégés et que cette protection prévaut. Avant que les Données Personnelles ne soient traitées aux fins des intérêts légitimes, il est nécessaire d'évaluer s'il existe un intérêt qui mérite d'être protégé et une analyse des intérêts légitimes (sous la forme d'un DPIA en insistant particulièrement sur l'intérêt légitime) doit être menée par l'entité du Groupe Ipsos concernée. Toute analyse de ce type doit être validée par le DPO ou le CPO concerné.

5.1.5. Traitement portant sur les Catégories Particulières de Données Personnelles

Les catégories particulières de Données Personnelles ne peuvent faire l'objet d'un traitement que si la loi l'exige ou si la Personne Concernée a donné son consentement explicite. Les catégories particulières de Données Personnelles peuvent également être traitées si elles sont obligatoires pour faire valoir, exercer ou défendre des revendications légales. Au sein de l'Espace Economique Européen, les catégories particulières de Données Personnelles peuvent également être traitées à des fins de recherche scientifique et historique et à des fins statistiques (Article 9(2) (j)), sous réserve de mesures supplémentaires appropriées. Avant de s'appuyer sur ces dispositions, il est nécessaire d'obtenir l'avis du DPO ou du CPO.

5.1.6. Données de l'Utilisateur et Internet

Lorsque des Données Personnelles sont collectées, traitées et utilisées sur des sites Internet ou dans le cadre d'applications, la Personne Concernée doit en être informée au moyen de mentions relatives à la protection des données et, le cas échéant, relatives à l'utilisation de cookies ou à d'autres mesures techniques similaires.

Les mentions relatives à la protection des données et aux cookies doivent être intégrées de manière à être facilement repérables, immédiatement accessibles, facilement compréhensibles et disponibles à tout moment par et pour la Personne Concernée.

Si des profils utilisateurs (« traçage ») sont générés pour analyser le comportement des utilisateurs de sites Internet et d'applications, les Personnes Concernées doivent dans tous les cas en être informées dans les mentions relatives à la protection des données. Le traçage des Personnes Concernées en ligne ne peut avoir lieu que si la législation nationale l'autorise ou si la Personne Concernée y a consenti. Même si le traçage s'effectue sous un pseudonyme pour identifier la Personne Concernée, la Personne Concernée doit se voir offrir une option de retrait (« *opt-out* ») qui figurera dans les mentions relatives à la protection des données. En ce qui concerne les mesures d'audience en ligne sans option d'adhésion (« *opt-in* ») préalable, Ipsos adhère également aux principes promulgués par researchchoices.com.

Si, dans le cadre de la visite de sites Internet ou de l'utilisation d'applications, il est donné la possibilité d'accéder à des Données Personnelles via un espace réservé aux utilisateurs/personnes interrogées inscrits, l'identification et l'authentification de la Personne Concernée doivent s'effectuer sous une forme offrant une protection appropriée pour le type d'accès considéré.

Dans le cadre de l'engagement d'Ipsos à respecter le Code Esomar, les règles et exigences énoncées dans les Directives de Recherches sur les Médias Sociaux, les Directives sur les Recherches en Ligne et les Directives sur les Recherches et l'Analytique de Données auprès

d'Enfants, de Jeunes Personnes et de Personnes Vulnérables s'appliquent également à Ipsos dans le cadre de cette politique.

5.2. Données Personnelles Fournies par les Clients

La transmission de Données Personnelles à Ipsos par ses clients est courante. Cela passe habituellement par la fourniture d'un échantillon ou l'enrichissement un échantillon existant. En ce qui concerne les Données Personnelles collectées de cette façon, Ipsos sera le Sous-Traitant et devra Traiter ces Données Personnelles conformément aux instructions convenues avec le client. Ces instructions peuvent inclure des restrictions sur les transferts à d'autres parties (y compris d'autres entités Ipsos) ou des transferts vers d'autres pays, ainsi que des exigences spécifiques en matière de sécurité. Ces restrictions doivent être respectées. Il est impératif que ces instructions soient documentées par écrit et convenues avant l'acceptation par Ipsos de tout accord contractuel pertinent, afin de s'assurer qu'Ipsos est effectivement en mesure de se conformer aux restrictions ou exigences spécifiques du client.

Indépendamment des exigences du client, les Données Personnelles fournies par un client :

a) ne peuvent être traitées que dans la finalité pour laquelle elles ont été fournies ;
b) ne doivent pas être conservées pendant une durée qui excède la durée nécessaire aux finalités auxquelles elles sont destinées ;
c) doivent être soumises aux mêmes exigences de sécurité que celles applicables aux Données Personnelles d'Ipsos.

5.3. Données des Collaborateurs

5.3.1. Traitement des Données dans le cadre d'une Relation de Travail

Le traitement des Données Personnelles nécessaires à la conclusion, à l'exécution ou à la cessation du contrat de travail est autorisé dans le cadre de la relation de travail. De même, le traitement des Données Personnelles des candidats est licite pendant la phase de recrutement. Les données d'un candidat qui n'a pas été retenu doivent être supprimées dans le respect des délais de conservation obligatoires, excepté lorsque le candidat a donné son consentement à une prolongation de l'enregistrement de ses données dans l'optique d'une procédure de recrutement ultérieure. Le consentement du candidat est également nécessaire pour permettre l'utilisation des données dans le cadre d'autres procédures de recrutement ou pour les communiquer à d'autres sociétés du Groupe.

Dans le cadre d'une relation de travail existante, le traitement des données doit toujours être rattaché à la finalité du contrat de travail, si aucune des circonstances suivantes pour un traitement des données ne s'applique.

Si, au cours de la phase de candidature, un complément d'information sur le candidat doit être obtenu auprès d'un tiers, il convient alors de respecter les dispositions légales applicables. En cas de doute, il est nécessaire de solliciter le consentement du candidat.

Le traitement de Données Personnelles effectué dans le contexte de la relation de travail, sans pour autant servir en premier lieu à l'exécution du contrat de travail, doit être justifié par un motif juridique légitime. Il pourra s'agir d'exigences légales, de réglementations collectives applicables, d'un consentement du collaborateur ou d'intérêts légitimes de l'entreprise.

5.3.2. Traitement des Données du fait d'une Autorisation Légale

Veuillez vous reporter au paragraphe 5.1.3 ci-dessus pour de plus amples informations à ce sujet.

5.3.3. Accord collectif relatif au Traitement des Données

Si le traitement des données dépasse le cadre de la simple exécution d'un contrat de travail, il est licite à condition qu'il soit légitimé par un accord collectif dans le cadre des possibilités offertes par le droit du travail applicable. Les accords, qui doivent couvrir la finalité concrète du traitement souhaité, peuvent être conclus dans le cadre des dispositions prévues par la législation nationale relative à la protection des données.

5.3.4. Consentement au Traitement des Données

Le traitement de données de collaborateurs peut s'effectuer sur la base du consentement donné par la Personne Concernée. Les déclarations de consentement doivent être formulées selon le principe du consentement libre et éclairé. Au sein de l'UE/EEE, le consentement ne constitue généralement pas une base juridique valable pour le traitement des données dans le cadre de la relation de travail, car il existe une présomption selon laquelle ce consentement n'a pas été donné de manière libre par le colaborateur. Dans cette situation, tout traitement devra s'appuyer sur l'une des autres bases juridiques disponibles. Tout consentement donné sur une base non volontaire est réputé sans effet. Dans la mesure où le consentement constitue une base valable pour le traitement, veuillez vous reporter au paragraphe 5.1.1 ci-dessus pour plus d'informations à ce sujet. Dans la mesure où le consentement peut être retiré à tout moment par le collaborateur, tout traitement ultérieur des données ne sera plus autorisé.

5.3.5. Traitement des Données aux fins des Intérêts Légitimes

Le traitement des Données Personnelles est également possible lorsqu'il sert un intérêt légitime du Groupe Ipsos et quand la loi applicable permet le traitement des Données Personnelles aux fins desdits intérêts légitimes. Dans le contexte professionnel, les intérêts légitimes sont généralement d'ordre juridique ou financier.

Veuillez vous reporter au paragraphe 5.1.4 ci-dessus pour obtenir plus d'informations sur les conditions et les limites de l'intérêt légitime.

Les mesures de contrôle ou de surveillance nécessitant le traitement de données de collaborateurs ne peuvent être appliquées qu'en présence d'une obligation légale ou d'un d'intérêt légitime. Même en cas d'intérêt légitime, il convient de vérifier que le principe de proportionnalité est respecté avant que ces mesures ne soient appliquées. À cet effet, il convient de pondérer les intérêts légitimes de l'entreprise quant à l'exécution de la mesure de contrôle (respect des dispositions légales et des politiques internes à l'entreprise, par exemple) avec les éventuels intérêts du collaborateur. Les contrôles ne devront être effectués que s'ils sont proportionnés. L'intérêt légitime de l'entreprise et les éventuels intérêts des collaborateurs doivent être déterminés et documentés avant toute mesure. Par ailleurs, il convient, le cas échéant, de prendre en considération les exigences complémentaires découlant de la législation nationale (droit à l'information des intéressés, par exemple).

5.3.6. Traitement des Catégories Particulières de Données Personnelles

Les catégories particulières de Données Personnelles ne peuvent être traitées que si la loi l'exige ou si la Personne Concernée a donné son consentement explicite. Ces données peuvent également être traitées si cela s'avère être obligatoire pour faire valoir, exercer ou défendre des revendications légales.

5.3.7. Décisions Automatisées

Dans le cadre de la relation de travail, les procédures de traitement automatisé de Données Personnelles s'accompagnant d'une évaluation de certains critères touchant à la personne (par exemple dans le cadre du recrutement de candidats ou de l'évaluation de profils de compétence) doivent satisfaire à des conditions particulières. Elles ne doivent pas constituer l'unique fondement de décisions susceptibles d'avoir des conséquences négatives pour le collaborateur concerné ou de lui porter un préjudice majeur. Afin d'éviter toute décision erronée,

il convient, dans le cadre d'une procédure automatisée, de garantir que les éléments sont évalués par une personne physique et que la décision est prise sur la base de cette évaluation. En outre, la Personne Concernée doit être informée du fait qu'une décision automatisée a eu lieu et du résultat de cette décision, et doit également avoir la possibilité de prendre position à ce sujet.

5.3.8. Télécommunications et Internet

Les installations téléphoniques, adresses électroniques, sites Intranet et Internet ainsi que les réseaux sociaux internes sont en premier lieu mis à disposition par Ipsos dans le cadre d'une mission professionnelle. Ce sont à la fois des moyens de travail et des ressources pour l'entreprise. Ces moyens peuvent être utilisés dans le cadre de la réglementation en vigueur et des directives internes à l'entreprise, en particulier la politique *Information Security and Acceptable Use Policy*. Dès lors que l'usage à titre privé de ces moyens est autorisé, il convient de respecter le secret des télécommunications ainsi que la législation nationale en vigueur en la matière, dans la mesure où ces dispositions s'appliquent.

Ipsos utilise une technologie de filtrage Web pour assurer le respect de la politique *Information Security and Acceptable Use Policy* et des obligations légales, pour mesurer et analyser le trafic Internet et pour se défendre contre les attaques contre le système informatique ou les utilisateurs individuels. Des mesures de protection peuvent être mises en place au niveau des interfaces avec le réseau Ipsos. Il pourra s'agir de dispositifs assurant le verrouillage de contenus pouvant causer des dommages techniques ou de mesures servant à analyser les schémas d'attaque informatique. Pour des raisons de sécurité, l'utilisation des installations téléphoniques, des adresses électroniques, de l'intranet/Internet et des réseaux sociaux internes peut être verrouillée de manière permanente ou temporaire. Toute analyse de données de ce type s'intéressant à une personne donnée doit reposer sur des soupçons fondés d'infraction aux lois ou aux directives du Groupe Ipsos. Ces contrôles ne peuvent être effectués que par des services habilités et ce, dans le respect du principe de proportionnalité (voir également la politique *IT Information Management Policy*) ainsi que de la législation applicable et les politiques du Groupe Ipsos en vigueur.

5.4. Contacts Marketing

Dans l'ensemble, les contacts marketing sont traités de la même façon que les Personnes Interrogées en ce qui concerne la protection de la vie privée qui leur est accordée. Leurs coordonnées constituent des Données Personnelles, même si elles sont liées à l'entreprise. Seules les adresses qui sont vraiment génériques, telles que "contact@acme.com", ne seront pas soumises à cette Politique.

Les communications marketing sont souvent soumises à des exigences légales spécifiques, en particulier si elles sont effectuées par voie électronique ou par téléphone.

Il faut partir du principe que les contacts marketing n'ont pas demandé d'informations marketing. En d'autres termes, les destinataires n'ont pas demandé à recevoir des communications marketing provenant d'Ipsos. Pour agir en toute légalité, les conditions relatives à la base juridique, en particulier les exigences en matière de consentement énoncées au paragraphe 5.1.1 s'appliquent ici aussi.

À titre exceptionnel, un consentement implicite « *Opt-out* » peut être appliqué, si les conditions ci-dessous sont remplies :

- lorsque les coordonnées de la Personne Concernée ont été obtenues dans le cadre d'une prestation de services ou d'une négociation de prestations de services Ipsos ;
- lorsque les messages sont uniquement destinés à la commercialisation de services similaires ; et

- lorsque la personne a la possibilité de s'opposer au marketing au moment où ses données sont collectées, et si elle ne se retire pas à ce moment, elle aura la possibilité de le faire de façon simple dans tous les prochains messages.

6. Transmission des Données Personnelles

La transmission de Données Personnelles à des destinataires externes ou internes au Groupe Ipsos est soumise aux conditions d'autorisation de traitement des Données Personnelles conformément au paragraphe 4.7 Restriction sur les Transferts. Le destinataire des données (qu'il s'agisse d'une autre entité Ipsos ou d'un sous-traitant) doit s'engager à n'utiliser les données que pour les finalités définies. Pour les transmissions externes, les exigences du présent paragraphe et celles du paragraphe 7 Traitement des Données par des Sous-traitants ou des Tiers s'appliquent de manière cumulative.

En cas de transmission des Données Personnelles à un destinataire externe au Groupe Ipsos se trouvant dans un État tiers, celui-ci est tenu d'accepter par écrit de garantir un niveau de protection des données équivalent à la présente Politique de Protection des Données ou à celui exigé par la loi applicable. Par exemple, le RGPD énonce diverses exigences qui doivent être respectées avant qu'une transmission puisse avoir lieu. Cela ne s'applique pas dans le cas où la transmission résulte d'une obligation légale. Une telle obligation légale peut découler du droit du pays où siège l'entitédu Groupe Ipsos qui transmet les données, à moins que le droit du pays où siège l'entité du groupe Ipsos ne reconnaisse pas l'objectif de la transmission de données poursuivi à travers l'obligation légale imposée à un pays tiers.

En cas de transmission des Données Personnelles de tiers (comme un fournisseur d'échantillons) à une société du Groupe Ipsos, il doit être garanti que l'utilisation des Données Personnelles aux fins prévues est licite.

Dès lors que des Données Personnelles sont transmises d'une entité du Groupe Ipsos dont le siège se situe dans un pays à une société du groupe Ipsos dont le siège se situe dans un autre pays, l'entité importatrice de données est tenue de répondre à toutes les demandes des autorités de contrôle compétentes du pays dans lequel l'entité exportatrice de données a son siège social et de respecter les directives des autorités concernant les données transmises.

Si une Personne Concernée constate une infraction à la présente Politique de Protection des Données par une société du Groupe Ipsos importatrice de données ayant son siège dans un pays tiers, l'entité du Groupe Ipsos exportatrice de Données Personnelles s'engage à aider la Personne Concernée à clarifier les faits et à exercer les droits dont elle peut se prévaloir en vertu de la présente Politique de Protection des Données à l'encontre de l'entité du groupe Ipsos ayant importé les données. Par ailleurs, la Personne Concernée peut légitimement faire valoir ses droits à l'encontre de l'entité du Groupe Ipsos ayant exporté les données. En cas d'infraction constatée, l'entité exportatrice doit apporter à la Personne Concernée la preuve qu'aucune infraction à la présente Politique de Protection des Données n'est imputable à l'entité ayant importé les Données Personnelles.

Chaque entité du Groupe Ipsos transmettant des Données Personnelles à une autre entité du Groupe Ipsos ayant son siège dans un autre pays, restera responsable de toute violation de la présente Politique de Protection des Données commise par l'entité du groupe Ipsos ayant reçu les Données Personnelles, comme si la violation avait été commise par l'entité du Groupe Ipsos transmettant les Données Personnelles.

Tout transfert de Données Personnelles au sein du Groupe Ipsos ne peut être effectué qu'après l'inscription dans le JobBook du projet dans le cadre duquel le transfert a eu lieu. Cette entrée créera un contrat dans le cadre de l'accord-cadre de services intragroupe d'Ipsos et rendra automatiquement les Clauses Contractuelles Types de l'UE applicables à ce transfert.

7. Traitement des Données par des Sous-traitants ou des Tiers

Dans de nombreux cas, Ipsos fait appel à des prestataires externes pour le traitement des Données Personnelles. Dans ces cas, un accord sur le traitement des données pour le compte d'Ipsos doit être conclu avec ce prestataire. Cela peut se faire soit en incluant des dispositions appropriées dans l'accord régissant la relation avec le prestataire, soit dans un document séparé et spécifique. En ce qui concerne le traitement pour le compte d'Ipsos, le prestataire ne peut traiter les Données Personnelles que s'il respecte les instructions d'Ipsos. Au moment d'informer le prestataire, les exigences suivantes doivent être respectées :

- Lorsque les Données Personnelles en question relèvent du paragraphe 5.2 (données client), toutes les exigences pertinentes du client doivent être transmises au prestataire.
- Le prestataire doit être choisi en fonction de sa capacité à couvrir les mesures de protection techniques et organisationnelles requises et conformément au processus d'approbation des prestataires d'Ipsos.
- Le prestataire ne doit pas sous-traiter le traitement sans avoir obtenu l'accord préalable et écrit d'Ipsos.
- Les instructions doivent être données par écrit au moyen d'un contrat approprié. Les instructions sur le traitement des données et les responsabilités d'Ipsos et du prestataire doivent être documentées.
- Avant le début du traitement des données, Ipsos doit s'assurer que le prestataire se conformera à ses obligations. Un prestataire peut documenter sa conformité aux exigences en matière de sécurité des données, notamment en présentant une certification appropriée. En fonction du risque lié au traitement des données, les analyses doivent être effectuées régulièrement pendant la durée du contrat. Ipsos doit conserver le droit de vérifier la conformité du prestataire.
- En cas de traitement transfrontalier de données contractuelles, les exigences nationales pertinentes relatives au transfert de Données Personnelles à l'étranger doivent être respectées. En particulier, les Données Personnelles provenant de l'Espace Economique Européen ne peuvent être traitées dans un pays tiers que si le prestataire peut démontrer qu'il dispose d'un niveau de protection des données équivalent à la norme RGPD et à la présente Politique de Protection des Données. Les outils appropriés peuvent être :
    - un accord avec le prestataire fondé sur des clauses contractuelles types de l'UE pour le traitement des données dans les pays tiers. Des accords similaires seront exigés pour tout sous-traitant du prestataire.
    - La participation du prestataire à un système de certification accrédité par l'UE pour la fourniture d'un niveau de protection des données suffisant.

8. Droits de la Personne Concernée

Chaque Personne Concernée peut faire valoir les droits exposés ci-après. L'examen, par l'entité Ipsos concernée, des droits revendiqués doit avoir lieu sans délai et ne doit causer aucun préjudice à la Personne Concernée. Lorsque les Données Personnelles pertinentes sont traitées par Ipsos en vertu du paragraphe 5.2 Données Personnelles Fournies par les Clients, il convient de se reporter au contrat du client concerné pour connaître la procédure à suivre et le client doit être immédiatement informé d'une telle demande.

- **Droit d'accès :**
    - Les Personnes Concernées peuvent exiger des renseignements sur les Données Personnelles collectées les concernant, leur origine et l'usage auquel elles sont destinées.
    - En cas de transmission de Données Personnelles à des tiers, il convient également d'indiquer l'identité du destinataire ou les catégories de destinataires, y compris d'autres sociétés Ipsos.

- **Droit de rectification** : s'il s'avère que des Données Personnelles sont inexactes ou incomplètes, la Personne Concernée est en droit d'exiger qu'elles soient rectifiées ou complétées.
- **Droit de rétractation** : Lorsque les Données Personnelles sont traitées sur la base du Consentement, les Personnes Concernées peuvent s'opposer au traitement à tout moment. Ces Données Personnelles doivent être verrouillées pour l'usage qui a fait l'objet d'une opposition.
- **Droit à l'effacement**. La Personne Concernée est en droit d'exiger la suppression de ses données s'il s'avère que le traitement de ces données n'a pas ou plus de base légale. Il en va de même si la finalité du traitement des données est devenue caduque ou n'a plus lieu d'être pour d'autres raisons. Il convient de tenir compte des obligations légales de conservation des données et des intérêts sensibles s'opposant à la suppression des données.
- **Droit d'opposition** : Les Personnes Concernées disposent d'un droit d'opposition au traitement de leurs données qu'il convient de respecter dès lors que leur intérêt légitime prévaut, en raison de leur situation personnelle particulière, sur l'intérêt du traitement. Cette disposition ne s'applique pas si une disposition légale exige que les Données Personnelles soient traitées.
- **Droit à la portabilité des données**. La Personne Concernée est en droit d'exiger que les Données Personnelles qu'elle a fournies soient mises à sa disposition dans un format facilement lisible, comme un document Word ou Excel.

9. Confidentialité du Traitement

Les Données Personnelles sont soumises à la confidentialité des données. Toute collecte, traitement ou utilisation illicites de ces données par les collaborateurs est interdit. Est considéré comme illicite tout traitement entrepris par un collaborateur sans y avoir été dûment autorisé dans le cadre de l'exercice de ses fonctions. Il convient d'appliquer le principe du « besoin d'en connaître » (*need to know*). Les collaborateurs ne sont autorisés à accéder aux Données Personnelles que dans la mesure où cela est nécessaire dans le cadre de leurs fonctions respectives. Cela implique une répartition et une séparation minutieuses, ainsi qu'une limitation des rôles et des responsabilités. En outre, les dispositions de la politique *Information Management Policy* s'appliquent.

Il est interdit aux collaborateurs d'utiliser les Données Personnelles à des fins privées ou commerciales, de les transmettre à des personnes non autorisées ou de leur en concéder l'accès d'une toute autre façon. Les supérieurs hiérarchiques doivent informer leurs collaborateurs, dès le début de la relation de travail, de l'obligation d'observer la confidentialité des données. Cette obligation reste en vigueur également au-delà de la fin du contrat. Les contrats de travail du personnel d'Ipsos doivent comporter des obligations de confidentialité appropriées.

10. Sécurité du Traitement

Les Données Personnelles doivent être protégées contre tout accès non autorisé, divulgation (interne ou externe), tout traitement illicite ainsi que contre toute perte, falsification ou destruction. Cela s'applique aussi bien au traitement des données sous forme électronique que sur papier. Outre la sécurisation des Données Personnelles existantes conformément aux politiques d'Ipsos en la matière (voir le chapitre 7 du *Book of Policies and Procédures d'Ipsos*, applicable à cet égard), avant l'introduction de nouvelles méthodes de traitement des données, et notamment de nouveaux systèmes informatiques, il convient de définir et de mettre en œuvre des mesures techniques ou organisationnelles appropriées visant à assurer la protection des Données Personnelles. Ces mesures doivent être conformes aux évolutions techniques, aux risques inhérents au traitement et au degré de protection requis pour les données.

Il conviendra de définir ces mesures techniques et organisationnelles en concertation avec le responsable de la Sécurité de l'Information (*Information Security Officer)* ainsi que le DPO

concerné. Les mesures de protection des Données Personnelles d'ordre technique et organisationnel font partie d'un système de gestion de la Sécurité de l'Information de l'Entreprise (*Corporate Information Security Management*) et doivent sans cesse être adaptées au développement et à l'évolution technique ainsi qu'aux changements structurels.

Au minimum, Ipsos traitera toutes les Données Personnelles qu'il détient conformément à sa Politique de Sécurité (*Security Policy*) et prendra les mesures de sécurité appropriées contre le traitement illégal ou non autorisé des Données Personnelles, et contre la perte accidentelle ou l'endommagement des Données Personnelles.

11. Audit de la Protection des Données

Le respect de la présente Politique de Protection des Données ainsi que la législation applicable en matière de protection des données est régulièrement vérifié par le biais d'audits et autres contrôles de sécurité des données. L'exécution de ces contrôles est du ressort du CPO, du DPO, de l'audit interne ou ou d'auditeurs externes mandatés à cet effet. Plusieurs clients d'Ipsos disposent également de droits d'audit dans le cadre de leurs contrats avec Ipsos. Les résultats des audits de protection des données doivent être communiqués au CPO et au Responsable de la Conformité (*Head of Compliance*). Sur demande, les résultats des audits de protection des données seront mis à la disposition des autorités de surveillance compétentes en matière de protection des données.

12. Incidents liés à la Protection des Données

Chaque collaborateur est tenu de signaler sans délai au DPO ou au CPO tout cas d'infraction à la présente Politique de Protection des Données ou à d'autres dispositions en matière de protection des Données Personnelles, conformément à la Procédure de Gestion des Violation de Données Personnelles (Personal Data Breach Management Procedure). Tout manquement grave aux termes de la présente Politique peut également être signalé par le biais du système d'alerte d'Ipsos (Whistle-blowing system).

En cas de :

- transmission illicite de Données Personnelles à des tiers ;
- transmission illicite de Données Personnelles à l'étranger ;
- accès illicite, y compris par des tiers, aux Données Personnelles, ou
- perte de Données Personnelles (y compris le fait d'être rendues publiques en raison de défaillances internes)

Une notification de la violationà la protection des données doit immédiatement être effectuée pour s'assurer que a) toute obligation de déclaration en vertu de la législation nationale peut être respectée, b) tout client affecté peut être informé et c) toute communication avec les parties prenantes peut être gérée. Toute atteinte à la Protection des Données constituera également un incident de sécurité de l'information en vertu de la politique de Gestion des Incidents Informatiques (*IT Incident Management Policy*).

13. Responsabilités et Sanctions

13.1. Management

Les organes exécutifs des entités du Groupe Ipsos sont responsables du traitement des données dans leur domaine de responsabilité. Ils sont ainsi tenus de veiller au respect des dispositions légales et des exigences contenues dans la présente Politique de Protection des Données (par exemple, les obligations de déclaration nationales).

Il appartient à la direction, dans le cadre de ses missions de management, de garantir, par la mise en place de mesures organisationnelles, RH et techniques un traitement des données en bonne et due forme, respectant les exigences en matière de protection des données.

Le respect de ces exigences relève également de la responsabilité du collaborateur compétent.

En cas d'audits de protection des données réalisés par une autorité publique, le CPO doit en être immédiatement informé.

L'entité Ipsos concernée doit informer le CPO du nom du DPO.

Dans de nombreux pays, le traitement illicite de Données Personnelles ou autres violations de la législation sur la protection des données peuvent faire l'objet de poursuites judiciaires et peuvent donner lieu au versement de dommages et intérêts. En outre, toute infraction imputable à des collaborateurs peut entraîner des sanctions prévues par le droit du travail applicable.

13.2. Délégué à la Protection des Données

Chaque pays Ipsos sera tenu de nommer un ou plusieurs Délégués à la Protection des Données ou *Data Protection Officer*s (« **DPO** »). Les DPO sont les interloctuteurs internes et externes dans le pays concernant la protection des données. Ils peuvent procéder à des contrôles et sont tenus de porter à la connaissance des collaborateurs le contenu de la présente Politique de Protection des Données et de la législation applicable. La direction concernée est tenue d'assister les DPO dans leurs tâches. Les principales tâches du DPO sont les suivantes :

- *Informer et conseiller l'organisation et ses collaborateurs sur leurs obligations de se conformer aux lois applicables en matière de protection des données et à la présente Politique de Protection des Données. Cette tâche sera soutenue et assistée par le Groupe et par le réseau des DPO sous la direction du CPO et par le biais de formations.*
- *Contrôler le respect de la législation en matière de protection des données, y compris la gestion des activités internes de protection des données, guider (mais pas mener) les analyses d'impact de la protection des données, former le personnel et mener des audits internes. Cette mission sera soutenue et assistée par le Groupe. Les audits, autres que les vérifications ponctuelles, devront être coordonnés avec le service d'audit interne du Groupe.*
- *Être le premier point de contact pour les autorités de contrôle et pour les personnes dont les données sont traitées (collaborateurs, clients, etc.).*

Au sein de chaque pays Ipsos, le DPO devra :

- rendre compte au plus haut niveau de management de l'entité Ipsos, c'est-à-dire au niveau du comité de local ou d'un membre du comité de direction.
- agir en qualité d'organe indépendant et ne pourra être licencié ou sanctionné dans le cadre de l'exécution de sa mission.
- disposer de ressources suffisantes pour lui permettre de remplir ses obligations en vertu des lois applicables en matière de protection des données et de la présente Politique de Protection des Données.

Le DPO informera rapidement le CPO de tout risque en matière de protection des données.

13.3. Chief Privacy Officer (CPO)

Le Chief Privact Officer (« **CPO** »), organe interne indépendant, s'emploie à faire respecter la conformité avec les autorités de contrôle nationales et internationales de la protection des données. Il/Elle est responsable de la présente Politique et veille à son respect.

Toute Personne Concernée peut s'adresser à tout moment au CPO ou au DPO compétent pour faire part de ses préoccupations, poser des questions, demander des informations ou formuler

des plaintes relatives à la protection des données ou à la sécurité des données. Sur demande, les préoccupations et les plaintes seront traitées de façon confidentielle.

Si le DPO concerné ne peut pas régler une plainte ou parer une atteinte à la Politique de Protection des Données, le CPO doit être immédiatement consulté. Les décisions prises par le CPO pour pallier les atteintes à la protection des données doivent être confirmées par la direction de l'entreprise en question. Les demandes de renseignements des autorités de contrôle doivent toujours être signalées au CPO.

14. Dérogation

Dans certains cas exceptionnels, il est possible d'obtenir une dérogation à la présente Politique, avant tout traitement des Données Personnelles concernées. Une telle dérogation ne peut être accordée qu'après une analyse d'impact relative à la protection des données afin de définir et d'évaluer les risques encourus par toute Personne Concernée, les risques juridiques et l'impact sur la réputation. Cette dérogation est soumise à l'approbation *du Ipsos President Support Services*.

15. Glossaire

Responsable du Traitement / Responsable Conjoint du Traitement

Il s'agit de la personne ou de l'organisation qui détermine les finalités et les moyens dont les Données Personnelles sont traitées. Il est chargé de définir les pratiques et les politiques conformes aux exigences légales applicables.

Généralement quand Ipsos reçoit un échantillon de données du client, Ipsos agit en qualité de responsable conjoint du traitement des données collectées. Cela s'étend aux données que nous avonsc ollectées, même lorsque nous avons assuré aux Personnes Interrogées que leurs réponses étaient confidentielles. Les responsabilités et les obligations des responsables conjoints du traitement doivent être documentées et faire l'objet d'un accord écrit.

Certaines juridictions utilisent d'autres expressions pour désigner la même notion, comme **Personne Responsable, Organisation, Opérateur**[2], etc.

Utilisateurs de Données

Il s'agit de nos collaborateurs dont le travail implique le traitement de Données Personnelles. Les utilisateurs de données doivent protéger les données et les Données Personnelles qu'ils traitent conformément à la présente Politique et aux procédures en matière de sécurité des données applicables à tout moment.

Sous-Traitant

Il s'agit de la personne ou de l'organisation qui n'est pas un Utilisateur de Données et qui traite les Données Personnelles pour le compte et sur instructions du Responsable du Traitement. Les collaborateurs des responsables du traitement des données sont exclus de cette définition, mais elle pourrait inclure les fournisseurs qui traitent les Données Personnelles. Ipsos sera soit un Responsable du Traitement (par exemple, en ce qui concerne les membres de nos panels ou un échantillon collecté par Ipsos pour répondre à un besoin spécifique dans le cadre d'une enquête), soit un Sous-Traitant(par exemple, dans le cas d'un échantillon fourni par les clients). Certaines juridictions utilisent d'autres expressions pour le même concept, comme **Tiers, Intermédiaire, Opérateur**[3], etc.

[2] Singapour
[3] Afrique du Sud

Personnes Concernées

Aux fins de la présente Politique, il s'agit de tous les individus au sujet desquels une société Ipsos détient des Données Personnelles. Il n'est pas nécessaire qu'une Personne Concernée soit un ressortissant ou un résident d'un pays. Toutes les Personnes Concernées ont des droits légaux concernant leurs informations personnelles.

Données Personnelles

La définition des Données Personnelles du RGPD (Article 4 (1) du RGPD) clarifie la notion de Données Personnelles et indique qu'elle doit être interprétée de manière large comme suit :
« …toute information se rapportant à une personne physique identifiée ou identifiable (« Personne Concernée ») ; une personne physique identifiable est une personne physique qui peut être identifiée, directement ou indirectement, notamment par référence à un identifiant tel qu'un nom, un numéro d'identification, des données de localisation, un identifiant en ligne ou à un ou plusieurs éléments spécifiques propres à son identité physique, physiologique, génétique, psychique, économique, économique, culturelle ou sociale ».

Une personne physique est une personne vivante et le RGPD lui-même ne s'applique pas aux personnes décédées. Toutefois, chaque État membre peut prévoir des règles concernant le traitement des Données Personnelles, même en ce qui concerne les personnes décédées.

Les informations concernant une entreprise ne constituent pas des Données Personnelles.

Il faut reconnaître qu'il n'est pas toujours possible de déterminer avec une certitude absolue si une information individuelle constitue une Donnée Personnelle. Il sera nécessaire de vérifier l'ensemble des informations détenues sur la personne en question ou les moyens raisonnablement susceptibles d'être utilisés pour identifier une personne. Avec l'amélioration constante des moyens technologiques, davantage de données deviendront des Données Personnelles.

Traitement

Le traitement représente toute opération qui implique l'utilisation des données. Cela comprend la collecte, l'enregistrement ou la conservation des données, ou l'exécution de toute opération ou ensemble d'opérations sur les données, y compris l'organisation, la modification, la récupération, l'utilisation, la diffusion, l'effacement ou la destruction des données. Le traitement comprend également le transfert de Données Personnelles.

Catégories Particulières de Données Personnelles (aussi connues sous le nom de « données personnelles sensibles »)

L'expression « Catégories Particulières de Données Personnelles » est la nouvelle expression utilisée dans le RGPD et était auparavant désignée sous le nom de « données sensibles ». Elles sont désormais définies à l'Article 9 du RGPD comme étant les données révélant :

l'origine raciale ou ethnique, les opinions politiques, les convictions religieuses ou philosophiques, ou l'appartenance syndicale, les données génétiques [voir ci-dessous], les données biométriques [voir ci-dessous] dans le but d'identifier de manière unique une personne physique, les données relatives à la santé [voir ci-dessous] ou les données concernant la vie sexuelle ou l'orientation sexuelle d'une personne physique

Des définitions plus détaillées de certaines de ces expressions ont été fournies dans le RGPD :

« données génétiques » : les Données Personnelles relatives aux caractéristiques génétiques héréditaires ou acquises d'une personne physique qui donnent des informations uniques sur la physiologie ou l'état de santé de cette personne physique et qui résultent, en particulier, de l'analyse d'un échantillon biologique de la personne physique en question ;

« données biométriques » : les Données Personnelles résultant d'un traitement technique spécifique, relatives aux caractéristiques physiques, physiologiques ou comportementales

d'une personne physique, qui permettent ou confirment son identification unique, telles que les images faciales ou les données dactyloscopiques ;

« données concernant la santé » : les Données Personnelles relatives à la santé physique ou mentale d'une personne physique, y compris la prestation de services de soins de santé, qui révèlent des informations sur l'état de santé de cette personne ;

Données Anonymes

Il s'agit d'informations qui ne concernent pas une personne physique identifiée ou identifiable ou des Données Personelles rendues anonymes de telle sorte que la Personne Concernée n'est pas ou plus identifiable (Considérant 26 du RGPD). Il faut faire la distinction avec les données qui, couplées à l'utilisation d'informations supplémentaires (par exemple une clé), pourraient être utilisées pour identifier une personne physique. Dans ce cas, les données sont simplement pseudonymisées.

Les données pseudonymisées relèvent toujours de la définition des Données Personnelles et les principes et exigences du RGPD s'appliqueront toujours à ces données.

Pseudonymisation

On entend par pseudonymisation le traitement des Données Personnelles de telle façon que celles-ci ne puissent plus être attribuées à une Personne Concernée spécifique sans avoir recours à des informations supplémentaires, pour autant que ces informations supplémentaires soient conservées séparément et fassent l'objet de mesures techniques et organisationnelles afin de garantir que les Données Personnelles ne sont pas attribuées à une personne physique identifiée ou identifiable. (Article 4(5) du RGPD)

Les données pseudonymisées sont des données à partir desquelles les identifiants d'un ensemble d'informations sont remplacés par des identifiants artificiels, ou pseudonymes, qui sont conservés séparément et soumis à des mesures de protection techniques. Les données pseudonymisées restent des Données Personnelles et, par conséquent, toutes les autres exigences en matière de protection des données continuent de s'appliquer à ces données.

PII ou Personally Identifiable Information

Ce terme provient de la législation américaine sur la protection de la vie privée. Bien que d'un point de vue pratique applicable au travail quotidien d'Ipsos, les expressions Données Personnelles et IPI peuvent être considérées comme synonymes, l'utilisation de l'expression PII dans le contexte du RGPD doit être évitée, car elle a un impact négatif sur notre obligation de démontrer notre conformité. Les régulateurs sont très attachés à la cohérence et à l'exactitude dans l'utilisation des expressions.

PHI ou Protected Health Information

Ce terme provient également de la législation américaine sur la protection de la vie privée, en particulier la HIPPA (« Loi sur la Transférabilité et la Responsabilité en matière d'Assurance Maladie », « *Health Insurance Protability and Accountability Act* »). Bien que d'un point de vue pratique applicable au travail quotidien d'Ipsos, les expressions « catégories spéciales de Données Personnelles » et « IPI » doivent être considérées comme synonymes, l'utilisation des IPI dans le contexte du RGPD devra être évitée.

Dans ce contexte le principal élément qui doit être pris en compte est qu'une certaine Donnée Personnelle qui relèverait de la définition légale de l'Information Médicale Protégée, dans le cadre du RGPD, constituerait une Donnée Personnelle plutôt que des catégories spéciales de données. Par exemple, la HIPPA considérerait tous les renseignements contenus dans un ensemble de données qui devaient contenir le nom et l'orientation sexuelle comme des PHI, alors que le RGPD ne considérerait que l'orientation sexuelle comme faisant partie des catégories spéciales de Données Personnelles.

PSI (*Personal Sensitive Information*) ou Données Personnelles Sensibles

Cette expression est aujourd'hui obsolète, car elle provient d'une législation antérieure. Elle est largement synonyme de « catégories particulières de Données Personnelles » telles que définies à l'Article 9 du RGDP, et cette expression doit être utilisée. Les organes régulateurs attendront d'Ipsos qu'il utilise la terminologie correcte pour démontrer notre conformité dans le cadre de notre obligation de rendre compte (*accountability*).