Politique opérationnelle de protection des données à caractère personnel

Historique des versions

Version	Date	Rédacteur	Objet
0.1	20 mai 2018	Sia Partners - toutapprendre	Création

1. Introduction

1.1. Objet du document

Le présent document définit les règles applicables pour assurer la conformité des traitements de données à caractère personnel dans le cadre des activités de TOUTAPPRENDRE.

La Politique opérationnelle de protection des données à caractère personnel a pour principaux objectifs :

- de rappeler le contexte réglementaire et les principales obligations relatives aux lois et règlements en la matière,
- de définir les principes clés qui régissent la protection des données,
- de prévoir les dispositifs de pilotage et de suivi,
- de présenter les procédures générales liées à la protection des données personnelles.

La présente politique s'applique à l'ensemble des salariés permanents et des personnels temporaires qui traitent de la donnée personnelle au sein de TOUTAPPRENDRE. Elle prend en compte aussi bien les fonctions supports que les lignes métiers.

Contractuellement ou par le biais de conventions, cette politique s'applique également aux partenaires et fournisseurs de prestations de services ainsi qu'aux sous-traitants qui exécutent pour le compte de TOUTAPPRENDRE certaines opérations et pour lesquelles ils peuvent être amenés à traiter de la donnée personnelle.

1.2. Mise en œuvre de la politique opérationnelle de protection des données personnelles

Il est important de rappeler que les règles énoncées dans la présente politique constituent une cible à atteindre. La formulation des différents items de la politique ne présage donc pas de leur implémentation effective à la date de rédaction de la politique. Il appartient à l'organisation et à la gouvernance mise en place de suivre et mesurer le niveau de déploiement effectif des règles de la présente politique.

2. Contexte, enjeux et validation

2.1. Contexte réglementaire

Le Règlement Général sur la Protection des Données à caractère personnel (RGPD), aussi connu sous le nom de General Data Protection Régulation (GDPR), est entré en application le 25 mai 2018 dans tous les Etats membres de l'Union Européenne. Cette nouvelle réglementation remplace la directive européenne sur la protection des données personnelles (95/46/CE). Dans ce cadre, la loi dite « Informatique et Libertés » de 1978 a été modifiée.

Les principaux apports de cette nouvelle réglementation sont l'élargissement de la définition d'une donnée personnelle, le renforcement des droits des personnes, la désignation d'un Délégué à la Protection des Données pour certains organismes, le renforcement des sanctions qui peuvent atteindre jusqu'à 4% du chiffre d'affaires global d'une entreprise, l'obligation de notification de violation des données ainsi que l'introduction de nouvelles notions telles que la protection de la vie privée dès la conception (« privacy by design ») et la protection de la vie privée par défaut (« privacy by default »).

Une donnée à caractère personnel est définie par les lois et règlements en la matière comme, « toute information se rapportant à une personne physique identifiée ou identifiable (ci-après dénommée « **personne concernée** »); est réputée être une «personne physique identifiable» 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, culturelle ou sociale;

Les **objectifs de la réforme** sur la protection des données sont de :

- renforcer les droits des personnes concernées, notamment par la création d'un droit à la portabilité des données personnelles et de dispositions propres aux mineurs,
- responsabiliser les acteurs traitant des données (responsables de traitement, responsables conjoints et sous-traitants),
- renforcer la coopération avec l'autorité de contrôle (CNIL)

Le renforcement de la réglementation, les contraintes imposées concernant la collecte, le traitement et la conservation de données, ainsi que les sanctions infligées par l'autorité de contrôle pour tout manquement, conduisent TOUTAPPRENDRE à adopter pour ses clients et elle-même un dispositif en la matière pour protéger sa réputation.

2.2. Contexte interne

Sur l'ensemble de ses activités, TOUTAPPRENDRE collecte et manipule pour ses clients particuliers et professionnels des données personnelles. L'efficacité et la pertinence du dispositif de protection des données personnelles représentent un enjeu important pour TOUTAPPRENDRE et ses clients.

2.3. Approbation et réexamen de la politique

La Politique opérationnelle de protection des données à caractère personnel prend effet après avoir été validée par le Directeur Général de TOUTAPPRENDRE.

Cette politique est revue par la Direction des risques, en cas de :

- **changements significatifs du contexte** métier, ou de la stratégie de protection des données à caractère personnel de TOUTAPPRENDRE (par exemple, nouvelles priorités métier, changement d'organisation…) ;
- changements significatifs de **l'exposition aux risques** (par exemple, nouvelles menaces, nouvelles tendances…) ;
- évolution significative **des lois ou de la règlementation** applicable.

3. Les principes de la protection des données personnelles

Les principes clés doivent être définis tout au long du cycle de vie de la donnée, lors de chacune des étapes de collecte, de stockage, de traitement et de transmission.

3.1. Traitement de données à caractère personnel

Principe de finalité :

Le traitement de données à caractère personnel doit être réalisé pour atteindre une finalité précise, laquelle doit être déterminée au moment de la collecte des données (*cf. 4.2. Collecte des données*).

Principe de licéité :

Le traitement de données à caractère personnel doit répondre à trois principes fondamentaux des lois et règlements sur la protection des données : **licéité**, **loyauté** et **transparence**.

Le traitement n'est **licite** que si, et dans la mesure où, au moins une des conditions suivantes est remplie:

- la personne concernée a consenti au traitement de ses données à caractère personnel pour une ou plusieurs finalités spécifiques ;
- le traitement est nécessaire à l'exécution d'un contrat auquel la personne concernée est partie ou à l'exécution de mesures précontractuelles prises à la demande de celle-ci ;
- le traitement est nécessaire au respect d'une obligation légale à laquelle le responsable du traitement est soumis ;
- le traitement est nécessaire à la sauvegarde des intérêts vitaux de la personne concernée ou d'une autre personne physique ;
- le traitement est nécessaire à l'exécution d'une mission d'intérêt public ou relevant de l'exercice de l'autorité publique dont est investi le responsable du traitement ;
- le traitement est nécessaire aux fins des intérêts légitimes poursuivis par le responsable du traitement ou par un tiers, à moins que ne prévalent les intérêts ou les libertés et droits fondamentaux de la personne concernée qui exigent une protection des données à caractère personnel, notamment lorsque la personne concernée est un enfant.

Ainsi, pour tous les traitements reposant sur l'une des conditions citées ci-dessus, le recueil du consentement de la personne concernée n'est pas nécessaire.

Registre des activités de traitement :

Par ailleurs, il est de la responsabilité de chaque responsable du traitement, de tenir un **registre des activités de traitement** effectuées sous sa responsabilité.

Ce registre des activités de traitement doit comporter des éléments tels que le responsable du traitement, les finalités du traitement, le service chargé de sa mise en œuvre, une description des catégories de personnes concernées, des catégories de données à caractère personnel, la présence de données sensibles, le recours à la sous-traitance, les flux transfrontaliers, les modalités d'exercice des droits des personnes, la durée de conservation des données, et les mesures de sécurité.

Le responsable du traitement doit également s'assurer que son ou ses sous-traitants tiennent un registre de toutes les catégories d'activités de traitement réalisées pour son compte.

3.2. Collecte des données personnelles

Collecte directe et indirecte :

Deux types de collectes sont à distinguer dans les lois et règlements en la matière : la collecte directe et la collecte indirecte.

- On parle de collecte **directe** lorsque les données à caractère personnel relatives à une personne concernée sont collectées auprès de cette personne.

- La collecte est **indirecte** lorsque les données à caractère personnel n'ont pas été collectées auprès de la personne concernée. Un fichier de prospection acheté correspond par exemple à une collecte indirecte.

Afin de garantir un traitement équitable et transparent à l'égard de la personne concernée, le responsable de traitement, lors de chaque collecte de nouvelles données (sauf rafraichissement), doit fournir les informations suivantes à celle-ci:

- l'identité et les coordonnées du **responsable du traitement** ;
- les **finalités du traitement** auquel sont destinées les données à caractère personnel ainsi que **la base juridique** du traitement ;
- **les intérêts légitimes** poursuivis par le responsable du traitement ou par un tiers ;
- **les catégories de données** à caractère personnel concernées (uniquement en cas de collecte indirecte)
- **les destinataires** ou les **catégories de destinataires** des données à caractère personnel ;
- l'intention d'effectuer un **transfert de données** à caractère personnel vers un pays tiers ou à une organisation internationale, et l'existence ou l'absence d'une décision d'adéquation rendue par la Commission ou, la référence aux garanties appropriées ou adaptées et les moyens d'en obtenir une copie ou l'endroit où elles ont été mises à disposition ;
- la **durée de conservation** des données personnelles ou critères utilisés pour déterminer cette durée ;
- l'existence du droit de demander au responsable du traitement **l'accès** aux données à caractère personnel, la **rectification** ou l'**effacement** de celles-ci, ou une **limitation** du traitement relatif à la personne concernée, ou du droit de **s'opposer** au traitement et du droit à la **portabilité** des données;
- les **conséquences** éventuelles, à son égard, d'un défaut de réponse ;
- la capacité de **retirer son consentement (hors finalité contractuelle)** à tout moment, sans porter atteinte à la licéité du traitement fondé sur le consentement pour le traitement des données particulières ;
- le droit d'introduire une **réclamation** auprès d'une autorité de contrôle ;
- le **caractère réglementaire ou contractuel** de fournir les informations et conséquences en cas de refus (uniquement pour collecte directe) ;
- l'existence d'une **prise de décision automatisée**, y compris le profilage ;
- l'intention d'effectuer un **traitement ultérieur** des données à caractère personnel pour une autre finalité ;
- **la source** des données (uniquement pour collecte indirecte).

Dans l'hypothèse où le responsable du traitement collecte **directement** les données, l'information de la personne concernée doit être réalisée **au moment** de la collecte.

En cas de **collecte indirecte**, le responsable du traitement fournit ces informations :

- sous un mois, après obtention des données à caractère personnel ;
- au plus tard au moment de la première communication avec la personne concernée ;
- s'il est envisagé de communiquer les informations à un autre destinataire, au plus tard lorsque les données à caractère personnel sont communiquées pour la première fois.

<u>Exceptions</u> :

Cette obligation d'information ne s'applique pas dans certains cas particuliers, notamment si la fourniture de ces informations se révèle impossible ou exige des efforts disproportionnés, ou si les données doivent rester confidentielles.

Il n'est pas nécessaire d'informer à nouveau la personne si elle dispose déjà de ces informations.

3.3. Consentement

Le **consentement** est défini comme : « toute 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 à caractère personnel la concernant fassent l'objet d'un traitement ».

Un **consentement** doit être exigé lorsque le traitement vise une autre fin que celle pour laquelle les données ont été initialement collectées.

Lorsque le traitement repose sur le consentement, le responsable du traitement doit être en mesure de démontrer que la personne concernée a donné son consentement au traitement de données personnelles la concernant.

Pour être valide, le consentement doit être :

- **Donné librement** : la personne concernée par le traitement doit pouvoir exercer un choix réel et avoir un certain degré de contrôles sur ses données à caractère personnel
- **Spécifique** : le consentement ne peut être donné que pour une finalité prédéterminée
- **Eclairé** : la personne concernée par le traitement a donné son consentement en toute connaissance des caractéristiques du traitement (*cf. 4.2. Collecte des données*)
- **Univoque** : le consentement doit consister en un acte positif (signature, case à cocher, etc.)

3.4. Conservation de données

Principe de minimisation de données :

Les données à caractère personnel doivent être **adéquates**, **pertinentes** et **limitées** à ce qui est nécessaire au regard des finalités pour lesquelles elles sont traitées. Cela exige, notamment, de garantir que la durée de conservation des données soit limitée au strict minimum. Il s'agit du principe de **minimisation de données**.

En d'autres termes, la minimisation des données consiste à ne pas collecter et conserver des données dont le responsable du traitement n'a pas besoin pour la finalité. Concrètement, il faut veiller à limiter la quantité de données traitée dès le départ.

Dans le cadre de la collecte et de la conservation des données, les données non structurées (mails, enregistrements audio, photocopies, etc.) doivent également être prises en compte. Le principe de minimisation s'applique également pour cette typologie de données. Leur traitement doit ainsi se limiter au strict nécessaire.

Principe de conservation de données :

S'agissant de la durée de conservation de données, celle-ci est variable et dépend de la nature des données et de leur finalité.

Les données à caractère personnel peuvent être conservées :

1) Sous une forme permettant l'identification des personnes concernées pendant une **durée n'excédant pas celle nécessaire au regard des finalités** pour lesquelles elles sont traitées. En effet, une fois que la finalité est atteinte, il n'y a plus lieu de conserver les données et elles doivent **être supprimées**.

2) Au-delà de la durée nécessaire à la finalité du traitement, lorsqu'elles présentent encore un **intérêt administratif pour l'entité**. Cela consiste à en prolonger la durée de conservation des données au-delà du délai jugé pertinent pour la finalité de collecte initiale. Ce prolongement doit donc être dûment **justifié et documenté**.
   Il convient également de mettre en place des **habilitations** afin de **limiter** le nombre de personnes pouvant consulter ces données (exemple : le contentieux).
   Les données peuvent encore être conservées en vue de respecter des **durées légales de prescription**, des **durées de conservation particulières** (conservation des documents comptables et pièces justificatives, archivage des contrats électroniques, etc.), essentiellement à **des fins probatoires**, ou encore afin d'être en capacité de **répondre aux demandes de communication** susceptibles d'être adressées par certains tiers autorisés légalement habilités (l'administration fiscale, les organismes sociaux, etc.)

3) Pour des **durées plus longues** dans la mesure où les données à caractère personnel seront traitées exclusivement à des **fins archivistiques** dans l'intérêt public, à des **fins de recherche scientifique** ou **historique** pour autant que soient mises en œuvre les mesures techniques et organisationnelles appropriées requises par le présent règlement afin de garantir les droits et libertés de la personne concernée, telles que **l'anonymisation** ou la **pseudonymisation**.

Il est à noter que la durée de conservation s'applique pour l'archivage physique et numérique.

3.5. Sensibilité des données et des traitements

Définition d'une donnée sensible :

Les lois et règlements sur la protection des données encadrent particulièrement les données sensibles, lesquelles sont :

- Appartenance syndicale
- Données de santé
- Origine raciale ou ethnique
- Opinions philosophiques, politiques, religieuses
- Vie et orientation sexuelle
- Données génétiques
- Données biométriques

Si le **Numéro d'Inscription au Répertoire (NIR)** n'est pas une donnée sensible au sens des lois et règlements en la matière, cette donnée bénéficie tout de même d'un encadrement spécifique.

Traitement de donnée sensible : [à modifier si l'amendement 128 est voté]

Le traitement de ces données sensibles n'est pas autorisé par les lois et règlements sur la protection des données. Cependant, il peut être considéré comme licite si :

- la personne a donné son consentement explicite au traitement de ces données à caractère personnel ;
- le traitement est nécessaire aux fins de l'exécution des obligations et de l'exercice des droits propres au responsable du traitement ou à la personne concernée en matière de droit du travail

3.6. Sécurité du traitement

Principe de sécurisation des traitements :

Les lois et règlements en matière de protection des données imposent au responsable du traitement et à ses éventuels sous-traitants de garantir la mise en œuvre de « **mesures techniques et organisationnelles appropriées** » afin d'assurer la protection des données sur son périmètre de responsabilité.

La mise en place de mesures de protection implique la prise en considération de critères tels que la nature des données, les finalités du traitement et les risques associés.

Exemples de mesures de protection : pseudonymisation, chiffrement des données à caractère personnel, renforcement de la sécurité des systèmes d'information, etc.

Principe de « Privacy Impact Assessment » :

Par ailleurs, les lois et règlements en matière de protection des données imposent la réalisation d'une **analyse d'impact sur la vie privée** (aussi connu sous le nom de **Privacy Impact Assessment – PIA**) lorsque le traitement peut entraîner un risque élevé pour les droits et libertés des personnes physiques.

S'agissant du traitement de données sensibles, cette exigence s'applique. Ainsi, une analyse d'impact sur la vie privée est réalisée **avant le traitement** de ces catégories de données particulières.

Les critères suivants sont pris en compte pour identifier les finalités des traitements nécessitant une analyse d'impact :

- l'évaluation ou la notation (y compris le profilage et la prédiction) ;
- la prise de décision automatisée ;
- la surveillance systématique ;
- les données sensibles ;
- les données traitées à grande échelle ;
- l'ensemble de données qui ont été rapprochés ou combinés ;
- les données concernant les personnes concernées vulnérables ;
- l'utilisation innovante ou la mise en œuvre des solutions technologiques ou organisationnelles ;
- le transfert de données en dehors de l'Union Européenne ;
- les traitements empêchant les personnes concernées d'exercer un droit ou d'utiliser un service ou un contrat.

La méthode pour appliquer une analyse d'impact sur la vie privée est inscrite dans le document « **Note sur la PIA** ».

3.7. Principe de notification de violation de données :

En cas de violation de données à caractère personnel, il est de la responsabilité du correspondant ou de tout collaborateur informé de la situation de remonter la situation au Directeur Général de TOUTAPPRENDRE. Ce dernier, doit notifier la violation en question à l'autorité de contrôle compétente **au plus tard 72h après en avoir pris connaissance**.

Lorsqu'une violation de données à caractère personnel est susceptible d'engendrer un risque élevé pour les droits et libertés d'une personne, l'entreprise (responsable de traitement) est tenue d'informer la personne concernée de la violation de données dans les meilleurs délais.

3.8. Transferts de données à caractère personnel

Transfert de données à caractère personnel vers un pays tiers ou à une organisation internationale :

En cas de transferts de données à un pays tiers ou à une organisation internationale, TOUTAPPRENDRE doit :

- Soit insérer dans les contrats ou conventions les **clauses contractuelles** types de la Commission Européenne
- Soit recueillir le **consentement** de la personne concernée

Transfert de données à caractère personnel à un sous-traitant :

Les lois et règlements en matière de protection des données apportent une vigilance particulière concernant le recours à la sous-traitance.

Afin d'être en conformité avec ces lois et règlements, le délégant doit être en mesure de vérifier les mesures techniques et organisationnelles mises en œuvre par le sous-traitant au titre de la protection des droits de la personne concernée.

Concernant la subdélégation, le sous-traitant doit au préalable, **demander l'autorisation** au responsable de traitement et notifier par écrit sa demande. Le responsable de traitement est autorisé à émettre une objection quant à la demande de subdélégation du sous-traitant. Ces dispositions peuvent être encadrées dans le **contrat de sous-traitance** (clauses de confidentialité, clause sur la protection des données à caractère personnel).

Les principales obligations à la charge du sous-traitant sont la sécurisation des traitements et la tenue d'un registre des traitements.

Il doit également **notifier** au responsable du traitement toute violation de données à caractère personnel, dans les meilleurs délais après en avoir pris connaissance.

La notification à l'autorité de contrôle est à la charge du responsable de traitement.

Les **modèles de clauses contractuelles** encadrant le transfert de données à caractère personnel à un sous-traitant sont intégrées dans **l'annexe** de la présente politique.

3.9. Droits des personnes concernées

3.9.1 Droit d'accès

L'article 15 du RGPD précise le **droit d'accès** de la personne concernée. Celle-ci a le droit d'obtenir la confirmation que des données à caractère personnel la concernant sont ou ne sont pas traitées et, lorsqu'elles le sont, l'accès aux dites données à caractère personnel.

Informations à communiquer :

Suite à l'exercice d'une demande de droit d'accès par une personne concernée, les informations suivantes doivent être communiquées :

- Une copie des données à caractère personnel en cours de traitement ;
- Les finalités du traitement ;
- Les catégories de données personnelles utilisées ;
- Les destinataires ou catégories de destinataires auxquels les données à caractère personnel ont été ou seront communiqués ;
- La durée de conservation des données à caractère personnel envisagée lorsque cela est possible, ou les critères utilisés pour déterminer cette durée ;
- L'existence de droits (rectification, effacement, opposition et limitation) ;
- Le droit d'introduire une réclamation auprès d'une autorité de contrôle ;
- La source des données à caractère personnel, uniquement lorsque les données à caractère personnel ne sont pas collectées auprès de la personne concernée ;
- L'existence d'une prise de décision automatisée, y compris le profilage ;
- Les garanties appropriées lors d'un transfert vers un pays tiers ou à une organisation internationale.

Limites du droit d'accès :

Ce droit ne devrait pas porter atteinte aux droits ou libertés d'autrui, y compris au secret des affaires ou à la propriété intellectuelle

Si les données demandées par le droit d'accès **ne sont pas conservées pour des raisons techniques** ou bien si la demande intervient **après le délai légal de conservation** des données, TOUTAPPRENDRE répond négativement à la demande

Lorsque les demandes d'une personne concernée sont manifestement infondées ou excessives, notamment en raison de leur caractère répétitif, TOUTAPPRENDRE peut **exiger le paiement** des coûts de production ou refuser de donner suite à ces demandes

Par ailleurs, le Règlement Européen prévoit en cas de traitement d'une grande quantité de données relatives à la personne concernée, la possibilité de demander à celle-ci des précisions quant au **périmètre souhaité** (sur quelles données ou quelles opérations de traitement).

3.9.2 Droit de rectification

Définie à l'article 16 du RGPD, **le droit de rectification** est le droit d'obtenir la rectification des données à caractère personnel la concernant dans le cas où elles sont inexactes. Compte tenu des finalités du traitement, la personne concernée a le droit d'obtenir que les données à caractère personnel incomplètes soient complétées, y compris en fournissant une déclaration complémentaire.

TOUTAPPRENDRE notifie à chaque destinataire auquel les données à caractère personnel ont été communiquées toute rectification à moins qu'une telle communication se révèle impossible ou exige des efforts disproportionnés.

3.9.3 Droit à l'effacement (« droit à l'oubli »)

Le droit à l'oubli, aussi connu sous le nom de **droit à l'effacement** est mentionné à l'article 17 du RGPD.

Il s'agit du droit d'obtenir, sous certaines conditions, l'effacement de données à caractère personnel la concernant. Dans ces cas, TOUTAPPRENDRE a l'obligation d'effacer ces données à caractère personnel dans les meilleurs délais.

Conditions d'applicabilité :

Ce droit est applicable dans l'un des cas suivants :

- les données à caractère personnel ne sont plus nécessaires au regard des finalités pour lesquelles elles ont été collectées ou traitées d'une autre manière ;
- la personne concernée retire le consentement sur lequel est fondé le traitement, il ne doit pas exister d'autre base juridique au traitement considéré ;
- lorsque la personne concernée s'oppose au traitement et il n'existe pas de motif légitime impérieux pour le traitement ;
- les données à caractère personnel ont fait l'objet d'un traitement illicite ;
- les données à caractère personnel doivent être effacées pour respecter une obligation légale ;
- les données à caractère personnel ont été collectées dans le cadre de l'offre de services de la société de l'information aux enfants.

Pour résumer, avant de procéder à une suppression de données à caractère personnel, TOUTAPPRENDRE doit donc analyser :

- les traitements opérés sur lesdites données,
- la présence d'un délai légal de conservation afin de vérifier l'existence ou non d'une limite à l'exercice du droit par la personne concernée.

Limites du droit à l'effacement :

Le droit à l'effacement **ne s'applique pas** si le traitement est nécessaire :

- à l'exercice du droit à la liberté d'expression et d'information ;
- pour respecter une obligation légale ;
- pour des motifs d'intérêt public dans le domaine de la santé publique ;
- à des fins archivistiques dans l'intérêt public, à des fins de recherche scientifique ou à des fins statistiques ;
- à la constatation, à l'exercice ou à la défense de droits en justice.

TOUTAPPRENDRE doit informer les autres responsables de traitement qui traitent ces données à caractère personnel, que la personne concernée a demandé l'effacement de tout lien vers ces données à caractère personnel, ou de toute copie ou reproduction de celles-ci.

TOUTAPPRENDRE notifie à chaque destinataire auquel les données à caractère personnel ont été communiquées tout effacement de données à caractère personnel, à moins qu'une telle communication se révèle impossible ou exige des efforts disproportionnés.

3.9.4 Droit d'opposition

Le droit d'opposition de la personne concernée est consacré à l'article 21 du RGPD. Il s'agit du droit de s'opposer à tout moment, pour des raisons tenant à sa situation particulière, à un traitement des données à caractère personnel la concernant, y compris le profilage.

Conditions d'applicabilité :

Le RGPD énonce trois types de traitements pour lesquels la personne concernée peut exercer son droit d'opposition :

1) **Le cas des traitements fondés uniquement sur des intérêts légitimes ou publics :**

Toute personne concernée a le droit de s'opposer pour des raisons tenant à sa situation particulière, à un traitement des données à caractère personnel la concernant et qui est

- nécessaire à l'exécution d'une mission d'intérêt public ou relevant de l'exercice de l'autorité public dont est investi TOUTAPPRENDRE ;
- nécessaire aux fins des intérêts légitimes poursuivis par TOUTAPPRENDRE ou par un tiers.

Il appartient donc à la personne concernée de justifier sa demande à l'aide de raisons tenant à sa situation particulière qui prévalent sur les fondements du traitement auquel elle s'oppose.

Les raisons invoquées par la personne concernée peuvent être l'atteinte à la vie privée, la collecte illicite, etc.

2) **Le cas des traitements à des fins de prospection :**

Toute personne concernée a le droit de s'opposer au traitement des données à caractère personnel la concernant dès lors que le traitement est considéré à des fins de prospection, y compris au profilage lié à une telle prospection.

Après opposition de la personne concernée, les données à caractère personnel ne doivent plus être traitées à ces fins.

3) **Le cas des traitements à des fins de recherche scientifique ou statistique**

Toute personne concernée a le droit de s'opposer au traitement des données à caractère personnel la concernant dès lors que le traitement est considéré à des fins de recherche scientifique ou statistique.

Limites du droit d'opposition :

TOUTAPPRENDRE peut refuser la demande d'opposition de la personne concernée, s'il démontre qu'il existe des **motifs légitimes et impérieux** pour le traitement qui prévalent sur les intérêts et les droits et libertés de la personne concernée, ou pour la constatation, l'exercice ou la défense de droits en justice.

Exemples d'intérêts légitimes proposés par le G29 :

- prospection directe conventionnelle et autres formes de prospection commerciale ou de publicité ;
- messages non commerciaux non sollicités
- exécution de demandes en justice, y compris le recouvrement de créances via des procédures extrajudiciaires
- prévention de la fraude, de l'utilisation abusive de services ou d'un blanchiment d'argent
- surveillance du personnel à des fins de sécurité ou de gestion
- traitement à finalité scientifique ou statistiques
- traitement à des fins de recherche
- …

En conséquence, un intérêt peut être considéré comme légitime dès lors que TOUTAPPRENDRE est en mesure de poursuivre cet intérêt dans le respect de la législation sur la protection des données et d'autres législations. Autrement dit, un intérêt légitime doit être « acceptable au regard du droit ».

Un intérêt légitime doit donc :

- être licite (c'est-à-dire conforme au droit en vigueur dans l'Union et dans le pays concerné)
- être formulé en termes suffisamment clairs pour permettre l'application du critère de mise en balance avec l'intérêt et les droits fondamentaux de la personne concernée (c'est-à-dire suffisamment précis)
- constituer un intérêt réel et présent (c'est-à-dire non hypothétique)

3.9.5 Droit de limitation de traitement

Le droit de limitation de traitement est énoncé à l'article 18 du RGPD. Il s'agit d'un nouveau droit permettant à la personne concernée d'obtenir la limitation du traitement.

Conditions d'applicabilité :

Ce droit s'applique lorsque :

- l'exactitude des données est contestée par la personne concernée, pendant une durée permettant à TOUTAPPRENDRE de vérifier l'exactitude des données à caractère personnel ;
- le traitement est illicite et la personne concernée s'oppose à leur effacement et exige à la place la limitation de leur utilisation ;
- TOUTAPPRENDRE n'a plus besoin des données à caractère personnel aux fins du traitement mais celles-ci sont encore nécessaires à la personne concernée pour la constatation, l'exercice ou la défense de droits en justice ;
- la personne concernée s'est opposée au traitement, pendant la vérification portant sur le point de savoir si les motifs légitimes poursuivis par TOUTAPPRENDRE prévalent sur ceux de la personne concernée.

En cas de limitation de traitement, le **seul traitement autorisé** sur ces données à caractère personnel est la **conservation**.

Les **méthodes visant à limiter le traitement** de données à caractère personnel pourraient consister, entre autres à :

- Déplacer temporairement les données sélectionnées vers un autre système de traitement
- Rendre les données à caractère personnel sélectionnées inaccessibles aux utilisateurs
- Retirer temporairement les données publiées d'un site internet.

Dans les fichiers automatisés, la limitation du traitement devrait en principe être assurée par des moyens techniques de façon à ce que les données à caractère personnel ne fassent pas l'objet d'opérations de traitements ultérieures et ne puissent pas être modifiées.

Notification à la personne concernée :

Une personne concernée qui a obtenu la limitation du traitement est informée par TOUTAPPRENDRE avant que la limitation du traitement ne soit levée.

Limites du droit à la limitation de traitement :

La limitation du traitement peut être soulevée dans les cas suivants :

- avec le consentement de la personne concernée ;
- pour la constatation ;
- pour l'exercice ou la défense de droits en justice ;
- pour la protection des droits d'une autre personne physique ou morale ;
- pour des motifs importants d'intérêt public de l'Union ou d'un Etat membre.

TOUTAPPRENDRE notifie à chaque destinataire auquel les données à caractère personnel ont été communiquées toute limitation de traitement de données à caractère personnel effectué, à moins qu'une telle communication se révèle impossible ou exige des efforts disproportionnés.

3.9.6 Le droit de portabilité des données

L'article 20 du RGPD évoque le **droit à la portabilité des données**. Les personnes concernées ont le droit de recevoir les données à caractère personnel les concernant qu'elles ont fournies à un responsable de traitement, dans un format structuré, couramment utilisé et lisible par machine, et ont le droit de transmettre ces données à un autre responsable de traitement sans que le responsable de traitement auquel les données à caractère personnel ont été communiquées y fasse obstacle.

Conditions d'applicabilité :

Le droit à la portabilité s'applique si ces trois conditions sont toutes réunies :

- Le droit à la portabilité est limité aux données personnelles fournies par la personne concernée. Sont exclues ainsi du droit à la portabilité, les données personnelles qui sont dérivées, calculées ou inférées à partir des données fournies par la personne concernée.
- Il ne s'applique que si les données sont traitées de manière automatisée (les fichiers papiers ne sont donc pas concernés) et sur la base du consentement préalable de la personne concernée ou de l'exécution d'un contrat conclu avec la personne concernée.
- L'exercice du droit à la portabilité ne doit pas porter atteinte aux droits et libertés de tiers, dont les données se trouveraient dans les données transmises suite à une demande de portabilité.

3.9.7 Recours en cas de demandes infondées/excessives de la part des personnes concernées

Lorsque les demandes d'une personne concernée sont manifestement infondées ou excessives, notamment en raison de leur caractère répétitif, TOUTAPPRENDRE peut :

- exiger le paiement de frais raisonnables qui tiennent compte des coûts administratifs supportés pour fournir les informations, procéder aux communications ou prendre les mesures demandées; ou
- refuser de donner suite à ces demandes.

Toutefois, il incombe à TOUTAPPRENDRE de démontrer le caractère manifestement infondé ou excessif de la demande.

3.9.8 Délai de réponse :

En ce qui concerne la réponse, celle-ci doit être fournie dans un **délai d'un mois** à compter de la réception de la demande. Ce délai peut être prolongé de 2 mois compte tenu de la complexité et du nombre de demandes.

Les lois et règlements relatifs à la protection des données prévoient en cas de demandes infondées ou excessives des personnes concernées, la possibilité pour le responsable du traitement soit d'exiger le paiement de frais raisonnables qui tiennent compte des coûts administratifs supportés pour fournir les informations, procéder aux communications ou prendre les mesures demandées, soit de refuser de donner suite à ces demandes.
Cependant, il incombe au responsable du traitement de démontrer le caractère manifestement infondé ou excessif de la demande.

3.10. Contrôle

Afin de surveiller l'application du Règlement européen, l'autorité de contrôle a le pouvoir d'ordonner au responsable du traitement et au sous-traitant de lui communiquer toute information dont elle a besoin pour l'accomplissement de ses missions. Celle-ci peut également demander l'accès à toutes les données à caractère personnel et à tous les locaux du responsable du traitement et du sous-traitant.

3.11. « Privacy by design » et « privacy by default »

Principe de protection de la vie privée par défaut (« privacy by default ») :

Les lois et règlements relatifs à la protection des données exigent du responsable du traitement de mettre en place des mesures techniques et organisationnelles appropriées pour garantir que, par défaut, seules les données à caractère personnel qui sont nécessaires au regard de chaque finalité spécifique du traitement sont traitées. Il s'agit du principe de **protection de la vie privée par défaut (privacy by default)**. Les lois et règlements obligent également à garantir par défaut le plus haut niveau de protection des données.

Principe de protection de la vie privée dès la conception (« privacy by design ») :

Quant au concept de **protection de la vie privée dès la conception (privacy by design)**, il s'agit de garantir le plus haut niveau de protection des données dès la conception du produit ou du traitement. Cela vise à agir de manière proactive et préventive avant qu'une nouvelle technologie n'entraîne de nombreuses violations de la protection des données. Le Délégué à la Protection des Données sera impliqué dans la phase de lancement du projet et pourra ainsi donner son accord ou désaccord sur le projet ou le produit en question.

Glossaire

Les définitions données ci-dessous sont celles retenues par la Commission Nationale Informatique et Libertés (CNIL).

Donnée personnelle : *Toute information identifiant directement ou indirectement une personne physique (ex. nom, numéro d'immatriculation, numéro de téléphone, photographie, date de naissance, commune de résidence, empreinte digitale...).*

Les personnes physiques chez TOUTAPPRENDRE sont principalement des clients ou prospects, des fournisseurs, des collaborateurs et des actionnaires.

Donnée personnelle « sensible » : Information concernant l'origine raciale ou ethnique, les opinions politiques, philosophiques ou religieuses, l'appartenance syndicale, la santé ou la vie sexuelle. En principe, les données sensibles ne peuvent être recueillies et exploitées qu'avec le consentement explicite des personnes.

Traitement de données à caractère personnel : Toute opération, ou ensemble d'opérations, portant sur de telles données, quel que soit le procédé utilisé (collecte, enregistrement, organisation, conservation, adaptation, modification, extraction, consultation, utilisation, communication par transmission diffusion ou toute autre forme de mise à disposition, rapprochement ou interconnexion, verrouillage, effacement ou destruction, ...).

Responsable de traitement de données personnelles : Le responsable d'un traitement de données à caractère personnel est, sauf désignation expresse par les dispositions législatives ou réglementaires relatives à ce traitement, la personne, l'autorité publique, le service ou l'organisme qui détermine ses finalités et ses moyens. En pratique et en général, il s'agit de la personne morale incarnée par son représentant légal.

Sous-traitant : *Le sous-traitant (au sens de la réglementation sur les données personnelles) est une personne traitant des données personnelles pour le compte du responsable du traitement.*

CNIL (*Commission Nationale Informatique et Libertés) : La CNIL est une autorité administrative française indépendante qui a pour missions essentielles de proposer des mesures législatives et réglementaires, d'émettre des avis sur lesdits projets traitant de l'informatique et des libertés, d'établir des normes simplifiées ou dispense de déclaration pour certains traitements, de contrôler la bonne application de la loi.*

Elle a également pour mission d'aider toute personne dans l'exercice de ses droits, de tenir à la disposition du public la liste des traitements déclarés, et de gérer les autorisations de traitement de données « à risques ».

Elle dispose en outre d'un pouvoir de contrôle sur place des traitements déclarés par les responsables de traitement et peut prononcer différentes sanctions en cas de non-respect de la réglementation, sanctions qu'elle peut publier sur son site ou dans les journaux.