



Politique générale de protection des données personnelles

Table des matières

1. Objectif et champ d'application	2
1.1 <i>Objectifs de la Politique</i>	2
1.2 <i>Champ d'application</i>	2
1.3 <i>Révision</i>	3
2. Rôles et responsabilités	3
3. Les principes de protection des Données personnelles	4
3.1 <i>Licéité, loyauté et transparence</i>	4
3.2 <i>Consentement</i>	4
3.2.1 <i>Les conditions de validité du Consentement (caractéristiques et modalités de collecte)</i>	5
3.2.2 <i>La gestion du Consentement (durée, preuve, retrait)</i>	5
3.3 <i>Limitation des finalités</i>	6
3.4 <i>Minimisation et adéquation</i>	6
3.5 <i>Conservation limitée</i>	6
3.6 <i>Sécurité des Données personnelles</i>	7
3.7 <i>Transfert des Données personnelles en dehors de l'Union européenne</i>	8
3.8 <i>Traitement de Données personnelles sensibles</i>	8
3.9 <i>Le registre des traitements en qualité de Responsable de traitement</i>	9
3.10 <i>Protection des données dès la conception et par défaut (« Privacy by Design/by default »)</i>	9
3.11 <i>L'Analyse d'impact sur la vie privée</i>	10
4. Relations avec les Personnes concernées.....	11
4.1 <i>Information des Personnes concernées</i>	11
4.1.1 <i>Quelles informations donner aux Personnes concernées ?</i>	11
4.1.2 <i>Quand informer les Personnes concernées ?</i>	12
4.1.3 <i>Comment informer les Personnes concernées ?</i>	13
4.1.4 <i>Informations en cas de traitement ultérieur</i>	13
4.2 <i>Droits des Personnes concernées</i>	14
5. Gestion des Violations de Données personnelles	15
6. Gestion des sous-traitants.....	15
7. Relations avec l'autorité de contrôle.....	16
8. Sensibilisation et formation du personnel.....	16
9. Le contrôle de la conformité	17
9.1 <i>Contrôle interne</i>	17
9.2 <i>Contrôle externe : audit des Sous-traitants</i>	17
Annexe 1 Définitions	18

1. Objectif et champ d'application

Les termes commençant par une majuscule utilisée dans la présente politique générale de protection des données personnelles (ci-après la « Politique ») sont définis en Annexe 1 « Définitions ».

1.1 Objectifs de la Politique

ATAX CONSULTANTS s'engage à garantir la protection des Données obtenues dans le cadre de son activité, ainsi qu'à se conformer aux lois et réglementations applicables en matière de Traitement de Données à caractère personnel et Données à caractère personnel sensibles.

Cette Politique a pour objectifs de :

- Définir les engagements de ATAX CONSULTANTS au sujet des principes imposés par la Législation applicable, et notamment le Règlement Européen n°2016/679 relatif à la protection des Données à caractère personnel, en date du 27 avril 2016, applicable depuis le 25 mai 2018 ;
- Définir les rôles et responsabilités des principaux contributeurs ; et
- D'assurer la mise en place de méthodes et procédures adéquates ainsi que des structures de gouvernance et de contrôle appropriées pour garantir le respect engagements et de la Législation applicable.

Si pertinent, la section est sanctionnée par un encart de règle, ayant pour objectif de synthétiser l'engagement de ATAX CONSULTANTS sur le point concerné. La conformité de ATAX CONSULTANTS avec ces règles sera auditée dans les termes et conditions définis à la Section 8.

Cette Politique est complétée par les politiques et procédures suivantes :

- Procédure de gestion des droits des personnes
- Procédure générale de sécurité des données et gestion des failles de sécurité.

1.2 Champ d'application

La Politique a vocation à s'appliquer à l'ensemble des collaborateurs de ATAX CONSULTANTS de ses bureaux et établissements secondaires.

Elle s'applique à toutes les Données à caractère personnel recueillies, traitées, partagées par ATAX CONSULTANTS en ligne et hors ligne, y compris :

- Les sites internet opérés par ATAX CONSULTANTS ;
- Les emails échangés au sein de la société ;
- Les conversations ou correspondances ;
- Les documents papiers.

Cette politique s'applique également aux Tiers.

Conformément au droit du travail applicable, la présente politique est rendue obligatoire et exécutoire auprès de tous les collaborateurs de ATAX CONSULTANTS par l'une des conditions suivantes :

- En respectant les politiques internes contraignantes de ATAX CONSULTANTS ;
- Par le respect de la convention collective Syntec à laquelle sont soumis les collaborateurs de ATAX CONSULTANTS ;
- Par le respect d'une clause du contrat de travail.

Par conséquent, ATAX CONSULTANTS peut prendre des mesures disciplinaires à l'égard de ses propres collaborateurs, notamment en cas de non-respect des standards minimum de protection des Données à caractère Personnel établis par la présente politique.

En cas de conflits entre la présente Politique et la Législation applicable, les règles suivantes s'appliqueront :

- Si la Politique est plus protectrice, elle a vocation à primer sur la Législation applicable ;
Si la Législation applicable est plus protectrice, elle s'appliquera sur les points concernés en lieu et place de la Politique.

1.3 Révision

Cette politique peut être mise à jour afin de prendre en compte les évolutions de la Législation applicable et des pratiques au sein de ATAX CONSULTANTS en matière de protection des Données personnelles.

Une communication adéquate sera effectuée aux collaborateurs de ATAX CONSULTANTS en cas de modifications.

2. Rôles et responsabilités

Chaque responsable de pôle est soumis aux obligations suivantes :

- Fournir toute documentation relative aux Traitements dans leur périmètre d'intervention ;
- Inscrire tout nouveau Traitement dans le registre des traitements de ATAX CONSULTANTS.

3. Les principes de protection des Données personnelles

Conformément à la Législation applicable, ATAX CONSULTANTS s'engage à respecter les principes établis ci-après lors de la collecte et du Traitement de Données personnelles.

3.1 Licéité, loyauté et transparence

Les Données à caractère personnel doivent être collectées et traitées de manière licite, loyale et transparente. A ce titre, ATAX CONSULTANTS garantit que tout Traitement repose sur l'une des bases légales suivantes :

- La Personne concernée a donné son consentement au Traitement de ses Données personnelles pour une ou plusieurs finalités spécifiques (sous réserve du respect des exigences supplémentaires détaillées à la section 3.2 "Consentement") ;
- Le Traitement est nécessaire à l'exécution d'un contrat auquel la Personne concernée est partie ou pour prendre les mesures appropriées à la demande de la Personne concernée avant de conclure un contrat.
- Le Traitement est nécessaire au respect des obligations légales auxquelles ATAX CONSULTANTS est soumis.
- Le traitement est nécessaire aux fins d'intérêts légitimes poursuivis par ATAX CONSULTANTS

Lorsqu'un traitement est basé sur l'intérêt légitime de ATAX CONSULTANTS, ATAX CONSULTANTS procède à une analyse pour déterminer si cet intérêt légitime prime ou non sur les intérêts ou les droits et libertés fondamentaux des Personnes concernées. Cette évaluation et ses résultats doivent être documentés et consignés à des fins probatoires (accountability).

A titre subsidiaire, ATAX CONSULTANTS peut être amené à traiter des Données personnelles lorsque ce traitement est nécessaire :

- Afin de protéger les intérêts vitaux de la Personne concernée.
- Pour l'exécution d'une mission d'intérêt public.

Exceptionnellement, ATAX CONSULTANTS peut traiter des Données personnelles sensibles, auquel cas ATAX CONSULTANTS veille à respecter les exigences de la Section 2 de la présente Politique.

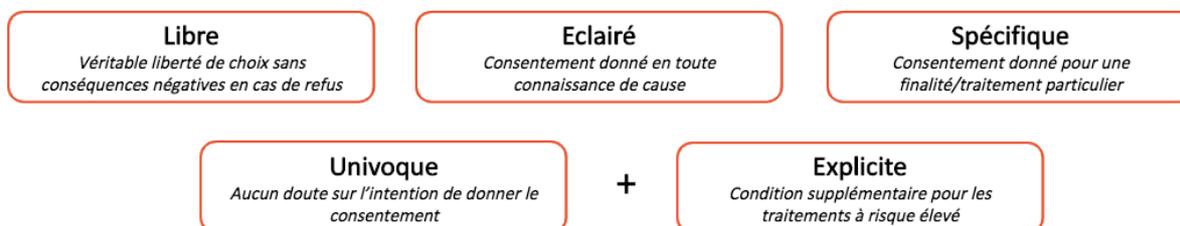
De plus, ATAX CONSULTANTS s'assure que les activités de Traitement des Données personnelles sont effectuées de manière apparente et transparente. À cette fin, ATAX CONSULTANTS fournit des informations accessibles et intelligibles aux Personnes concernées sur la façon dont leurs Données personnelles sont utilisées, conformément aux termes et exigences de la section 3.1 de cette Politique.

3.2 Consentement

Lorsque le Traitement est fondé sur le Consentement de la Personne concernée, ATAX CONSULTANTS s'assure que ce Consentement a été obtenu légalement (voir Section 3.2.1 sur les « Conditions de validité du Consentement ») et est correctement géré pendant toute la durée du Traitement (voir Section 3.2.2 « Gestion du Consentement »).

3.2.1 Les conditions de validité du Consentement (caractéristiques et modalités de collecte)

Pour être valide, le Consentement doit présenter les caractéristiques suivantes :



En outre, ATAX CONSULTANTS doit le cas échéant s'assurer du respect des lois locales sur les conditions de validité du Consentement.

Ce Consentement doit être obtenu avant la collecte des Données et, a minima, concomitamment à la collecte des Données.

Par écrit, le consentement peut être obtenu de différentes façons :

- ✓ Mention et/ou signature manuscrite sur un formulaire de consentement
- ✓ Déclaration écrite par voie électronique ;
- ✓ Une case à cocher non-pré-cochée
 - J'accepte que mes données soient traitées à des fins de...*

À l'oral, le consentement peut être obtenu grâce à une déclaration :

- *Un collaborateur peut demander à l'oral à recevoir des emails sur les activités organisées par la société. Un email devra être envoyé à ce dernier pour s'assurer qu'il a bien consenti à recevoir les emails.*

3.2.2 La gestion du Consentement (durée, preuve, retrait)

ATAX CONSULTANTS est en mesure de démontrer que le consentement a bien été donné.

ATAX CONSULTANTS veille également à la durée de validité du Consentement : lorsque les modalités de traitement changent ou évoluent, le Consentement original n'est plus valide. Un nouveau consentement doit alors être obtenu.

La Personne concernée doit être en mesure de **retirer son consentement à tout moment**. Le consentement doit :

- Pouvoir être **retiré aussi facilement qu'il a été donné**
- Répondre au **parallélisme des formes** dans la mesure du possible

3.3 Limitation des finalités

Avant toute collecte de Données personnelles, ATAX CONSULTANTS définit de façon claire l'ensemble des finalités poursuivies par la collecte, lesquelles doivent être déterminées, explicites et légitimes. ATAX CONSULTANTS s'assure également que la ou les finalités ainsi définies sont compatibles avec ses activités.

Ces Données ne doivent pas être traitées pour une finalité ultérieure incompatible avec la finalité initiale pour laquelle les Données ont été collectées. ATAX CONSULTANTS effectue un test de compatibilité pour vérifier si la finalité ultérieure est compatible avec la finalité initiale ; ce test est documenté et prend en compte :

- L'existence d'un lien entre les deux finalités ;
- Le contexte dans lequel les Données personnelles ont été collectées, en particulier en ce qui concerne la relation entre les Personnes concernées et ATAX CONSULTANTS ;
- La nature des Données Personnelles, en particulier si des Données personnelles sensibles sont traitées ;
- Les conséquences possibles du traitement ultérieur envisagé pour les Personnes concernées ;
- L'existence de garanties appropriées.

Lorsque la finalité ultérieure est incompatible avec la finalité initiale, ATAX CONSULTANTS s'assure de recueillir le consentement de la Personne concernée, conformément aux exigences de la Législation applicable (Article 6 (4) du RGPD).

3.4 Minimisation et adéquation

Les Données à caractère personnel collectées doivent être adéquates, pertinentes et non excessives par rapport à la finalité poursuivie par le Traitement. En d'autres termes, ATAX CONSULTANTS s'assure que la collecte porte uniquement sur les Données strictement nécessaires pour atteindre la finalité.

Dans le cadre de la gestion du projet de nouveau traitement, une évaluation spécifique doit être effectuée afin de minimiser les Données personnelles collectées et traitées, de manière à s'assurer que le principe de minimisation des données est appliqué dès le début du projet (privacy by design).

Enfin, ATAX CONSULTANTS s'assure que les Données collectées sont exactes, complètes et, si nécessaire, mises à jour.

3.5 Conservation limitée

Les Données à caractère personnel ne doivent pas être conservées plus longtemps que nécessaire au regard des finalités pour lesquelles elles sont collectées.

Afin d'assurer le respect de ce principe, ATAX CONSULTANTS définit les durées de conservations applicables à chaque Traitement. Les éléments suivants doivent être pris en compte pour la détermination de la durée de conservation de chaque catégorie de données collectées :

- Les obligations légales ;
- Les recommandations de la CNIL ;
- Les meilleures pratiques dans chaque domaine concerné ;
- Les besoins de l'entreprise.

Ces durées sont revues et mises à jour en tant que de besoin pour refléter les évolutions de la Législation applicable et/ou des pratiques au sein de ATAX CONSULTANTS

Les Données peuvent être conservées pendant une durée supplémentaire résultant d'une obligation légale de conservation des Données et/ou d'un intérêt administratif (notamment en cas de contentieux et/ou en application de mesures précontractuelles spécifiquement requises par la Personne concernée.

ATAX CONSULTANTS établit des modes opératoires pour la suppression des données, en tenant compte des contraintes techniques, des coûts et délais d'implémentation. A l'exception des cas dans lesquels il existe une obligation d'archivage, les Données qui ne présentent plus d'intérêt doivent être supprimées sans délai.

Cette suppression peut être opérée par destruction des Données et/ou anonymisées. En cas de suppression par destruction, ATAX CONSULTANTS s'assure que les Données sont effectivement détruites des systèmes (en ce inclus lorsque les systèmes concernés sont ceux d'un Tiers en requérant notamment de l'établissement un certificat de destruction).

Pour la destruction des documents papiers, une broyeuse est mise à disposition des collaborateurs de ATAX CONSULTANTS.

3.6 Sécurité des Données personnelles

ATAX CONSULTANTS prend des mesures techniques et organisationnelles dans le but d'assurer la sécurité, la confidentialité et l'intégrité des Données personnelles pendant toute la durée du Traitement. Sont pris en compte dans la détermination de ces mesures :

- La gravité et la probabilité du préjudice éventuel pouvant résulter de la perte, de l'altération et/ou de l'accès non autorisé aux Données ;
- Les éléments caractéristiques du Traitement concerné ;
- L'état de l'art ;
- Les coûts d'implémentation.

ATAX CONSULTANTS a établi une politique de sécurité du système d'information (PSSI) détaillant l'ensemble des mesures de sécurité techniques et organisationnelles mises en œuvre. Cette PSSI est régulièrement revue et mise à jour. ATAX CONSULTANTS s'engage également à évaluer de façon régulières les mesures de sécurité afin de tester, d'évaluer et de mesurer leur efficacité et d'entreprendre toute amélioration nécessaire.

De plus, ATAX CONSULTANTS s'assure que toute Violation des Données est gérée correctement conformément à la Section 4 de la présente Politique.

Enfin, ATAX CONSULTANTS veille à réaliser une Analyse d'impact sur la vie privée si le Traitement de Données à caractère personnel est susceptible de causer un risque sur les droits et libertés des Personnes concernées (voir Section 5.4).

3.7 Transfert des Données personnelles en dehors de l'Union européenne

Les Transferts de Données personnelles exigent une attention et des garanties supplémentaires. ATAX CONSULTANTS s'assure que tout Transfert de Données personnelles est sécurisé de façon adéquate et encadré juridiquement conformément aux exigences de la Législation applicable.

A ce titre, ATAX CONSULTANTS veille à :

- Identifier tout Transfert de Données personnelles, y compris, dans la mesure du possible, les Transferts ultérieurs opérés par les Sous-traitants (de 1^{er} rang) ;
- Encadrer dans le contrat avec le prestataire les Transferts de Données ainsi que, le cas échéant, le lieu d'hébergement des Données (lequel doit être par principe sur le territoire de l'Union européenne). Le prestataire doit ainsi garantir l'application de mesures permettant d'assurer un niveau de protection des Données personnelles équivalent à celui fourni par le RGPD ;
- Sécuriser tout Transfert par des mesures techniques et organisationnelles adaptées ;
- Lorsque le Transfert n'est pas à destination d'un pays reconnu comme d'adéquat (en vertu d'une décision d'adéquation de la Commission européenne), encadrer juridiquement le Transfert par la signature de clauses contractuelles types de la Commission européenne.

3.8 Traitement de Données personnelles sensibles

Les Données personnelles sensibles ne peuvent être collectées que si l'une des conditions spéciales suivantes s'applique :

- La Personne concernée a donné son consentement explicite ;
- Le Traitement est nécessaire aux fins de l'exécution des obligations et de l'exercice des droits propre à ATAX CONSULTANTS ou à la personne concernée en matière de droit du travail, sécurité sociale et protection sociale ;
- Le Traitement est nécessaire à la sauvegarde des intérêts vitaux de la Personne concernée ;
- Le Traitement porte sur des Données personnelles qui sont manifestement rendues publiques par la Personne concernée ;
- Le Traitement est nécessaire à la constatation, à l'exercice ou à la défense d'un droit en justice ou lorsque les juridictions agissent ;
- Le Traitement est nécessaire pour des motifs d'intérêt public importants, sur la base du droit de l'Union européenne ou d'un Etat membre qui doit être proportionné à l'objectif poursuivi, respecter l'essence du droit à la protection des données et prévoir des mesures appropriées et spécifiques pour la sauvegarde des droits fondamentaux et des intérêts de la Personne concernée ;

- Le Traitement est nécessaire aux fins de la médecine préventive, ou de médecine du travail, de l'appréciation de la capacité de travail du travailleur, des diagnostics médicaux, de la prise en charge sanitaire ou sociale, ou de la gestion des systèmes et services de soins de santé.

ATAX CONSULTANTS doit prévoir des mesures de sécurité particulières pour ces Données au regard du risque qu'elles peuvent représenter pour la Personne concernée.

Les données relatives aux condamnations pénales, aux infractions ou aux mesures de sûreté connexes ne doivent pas, par principe être recueillies, sauf dans des cas très exceptionnels et (par exemple la collecte du casier judiciaire pour vérifier les informations concernant un candidat à un emploi en raison de la nature spécifique de l'offre d'emploi). En tout état de cause, ce type de Données personnelles sensibles ne peut pas être traité (ainsi la copie du casier judiciaire, si elle peut être collectée, ne peut être conservée).

3.9 Le registre des traitements en qualité de Responsable de traitement

ATAX CONSULTANTS tient à jour un registre des Traitements mis en œuvre en qualité de Responsable de traitement. Ce registre détaille pour chaque Traitement :

- Les finalités du Traitement ;
- Une description des catégories des Personnes concernées et des catégories de Données à caractère personnel ;
- Les catégories de destinataires auxquels les Données personnelles ont été ou seront communiquées, y compris les destinataires dans des pays tiers ou à une organisation internationale ;
- Le cas échéant, les transferts de Données personnelles vers un pays tiers ainsi que les documents attestant de l'existence de garanties appropriées ;
- Les délais prévus pour l'effacement des différentes catégories de Données ;
- Une description générale des mesures de sécurités techniques et organisationnelles mises en œuvre.

Le registre des activités de Traitement est mis à jour lorsque (i) de nouvelles activités de Traitement sont mises en œuvre ou (ii) en cas d'évolution d'un Traitement existant (en ce inclus l'arrêt du Traitement).

3.10 Protection des données dès la conception et par défaut (« Privacy by Design/by default »)

Pour tout nouveau projet impliquant le Traitement de Données personnelles, ATAX CONSULTANTS met en place des mesures visant à protéger les Données personnelles dès la conception du Traitement, mais aussi tout au long du projet et du cycle de vie de la Donnée personnelle (de la collecte à la destruction).

A cette fin, tout collaborateur de ATAX CONSULTANTS pilotant un projet devra suivre les étapes suivantes :

- Etape 1 : Vérifier que les principes définis en Section 2 de la présente Politique sont bien respectés.
- Etape 2 : Liste les mesures techniques et organisationnelles existantes et envisagées, conformément à la Politique de Sécurité du Système d'Information de ATAX CONSULTANTS.
- Etape 4 : Réaliser si nécessaire l'Analyse d'impact sur la vie privée (voir Section 5.4).
- Etape 5 : Implémenter les mesures de sécurité adaptées au niveau de risque.

En outre, ATAX CONSULTANTS s'assure, à ce que, la vie privée des personnes soient respectées au plus haut degré possible, sans toutefois empêcher le Traitement d'atteindre sa finalité.

Lorsque le projet implique de confier tout ou partie du Traitement à un Sous-traitant, ATAX CONSULTANTS s'assure que les exigences de la section 6.2 "La gestion des Sous-traitants" sont respectées.

3.11 L'Analyse d'impact sur la vie privée

Lorsqu'un Traitement est susceptible d'engendrer un risque élevé pour les droits et libertés des Personnes concernées, ATAX CONSULTANTS effectue une Analyse d'impact sur la vie privée (AIPD) sur le Traitement, en amont de la mise en place du Traitement.

Le RGPD impose la réalisation d'une AIPD sur la vie privée dans les trois cas suivants :

- Le Traitement est fondé sur l'évaluation systématique et approfondie d'aspects personnels concernant des personnes physiques, y compris le profilage, et sur la base duquel des décisions sont prises produisant des effets juridiques à l'égard de la personne physique ou affectant de manière significative de façon similaire.
- Le Traitement est un traitement à grande échelle de catégories Données sensibles, ou de Données à caractère personnel relatives à des condamnations.
- Le Traitement est basé sur une surveillance à grande échelle d'une zone accessible au public.

ATAX CONSULTANTS prend en compte, outre le RGPD, les cas obligatoires définis par la CNIL.

En complément du RGPD, le Comité européen de la protection des données a établi que si au moins deux des critères suivants sont présents dans le Traitement, alors une analyse d'impact devra être réalisée :

- Évaluation/scoring (y compris le profilage) ;
- Décision automatique avec effet légal ou similaire ;
- Surveillance systématique ;
- Collecte de Données sensibles ;
- Collecte de Données personnelles à grande échelle ;
- Croisement de données ;
- Personnes vulnérables ;
- Exclusion d'un bénéfice d'un droit/contrat

A contrario, une Analyse d'impact ne sera pas nécessaire, selon la CNIL, dans les cas suivants :

- Le Traitement ne présente pas de risque élevé pour les droits et libertés des Personnes concernées.
- La nature, la portée, le contexte et les finalités du Traitement envisagé sont très similaires à un Traitement pour lequel une autre Analyse d'impact sur la vie privée a déjà été menée.
- Le Traitement répond à une obligation légale ou est nécessaire à l'exercice d'une mission de service public.
- Le Traitement fait partie d'une liste adoptée par la CNIL concernant les traitements dispensés de mener ce type d'analyse. Cependant, aucune liste n'a été publiée à ce jour.

L'AIPD est un processus continu et doit être adaptée en fonction de l'évolution du Traitement, De même, si un traitement ne nécessite pas une AIPD dans un premier temps mais que les opérations de traitement évoluent, un DPIA peut devoir être effectué dans un second temps.

4. Relations avec les Personnes concernées

ATAX CONSULTANTS s'engage à respecter les droits des Personnes concernées qui leur sont accordés par la Législation applicable.

4.1 Information des Personnes concernées

Dans le cadre du principe de transparence, ATAX CONSULTANTS s'engage à fournir aux Personnes concernées une information écrite, claire, accessible et intelligible sur la manière dont leurs Données personnelles sont utilisées.

Le contenu de l'information fournie et le moment de leur communication sont détaillés dans les sous-sections suivantes.

4.1.1 *Quelles informations donner aux Personnes concernées ?*

Lorsque la collecte de Données personnelles est directement effectuée auprès de la Personne concernée, la Législation applicable impose au Responsable de traitement d'informer la Personne concernée sur le Traitement et les conditions de mise en œuvre (Article 13 du RGPD).

A cet égard, ATAX CONSULTANTS s'assure de fournir aux Personnes concernées les informations suivantes :

- L'identité et les coordonnées de ATAX CONSULTANTS en tant que Responsable de traitement ;
- La ou les finalités du Traitement
- La base légale du Traitement et, lorsque le Traitement est fondé sur l'intérêt légitime, les détails concernant l'intérêt poursuivi par ATAX CONSULTANTS ;
- La durée de conservation des Données personnelles ou les critères de détermination de cette durée ;
- Les destinataires ou catégories de destinataires, le cas échéant ;
- Les droits des Personnes concernées (droit d'accès, droit à la rectification, à l'effacement, à la limitation, à l'opposition et à la portabilité) ;

- Le cas échéant, l'existence d'un transfert de données hors Union Européenne, ainsi que les informations (pays, entité) et garanties (Privacy Shield, Clauses contractuelles types) qui s'y rattachent ;
- Le cas échéant, le fait que la fourniture de Données dépende d'une exigence à caractère réglementaire ou contractuel ou conditionne la conclusion d'un contrat, l'existence d'une obligation pour la personne concernée de fournir ses données et les conséquences de la non-fourniture des données ;
- Le cas échéant, l'existence d'une décision automatisée et les informations qui s'y rattachent ;
- Le cas échéant, l'existence d'un Traitement ultérieur pour une autre finalité et les informations qui s'y rattachent.
- Le droit de retirer son consentement, si le Traitement est basé sur le consentement ;
- Le droit d'introduire une réclamation auprès de l'Autorité de contrôle (CNIL).

En outre, dans le cadre d'une collecte indirecte des Données personnelles, ATAX CONSULTANTS s'engage à fournir, en plus des informations mentionnées ci-dessus, les informations suivantes spécifiques à la collecte indirecte :

- Les catégories de Données personnelles concernées ;
- La source d'où proviennent les Données personnelles ;
- L'indication du fait que la source est ou non accessible au public.

ATAX CONSULTANTS s'assure que les mentions d'information sont régulièrement contrôlées et, le cas échéant, mises à jour pour tenir compte des changements législatifs et réglementaires ainsi que des changements apportés aux activités de Traitement de ATAX CONSULTANTS

Les mises à jour importantes affectant matériellement la manière dont ATAX CONSULTANTS utilise les Données personnelles doivent être notifiées aux Personnes concernées, si possible individuellement, afin de leur permettre d'examiner les modifications apportées, de les évaluer et, si nécessaire, de s'y opposer ou, le cas échéant, de se retirer d'un service ou d'une fonctionnalité.

4.1.2 *Quand informer les Personnes concernées ?*

- En cas de collecte directe

Les informations doivent être communiquées, au plus tard, au moment de la collecte des Données à caractère personnel, de façon concise, transparente, compréhensible, aisément accessible et en des termes clairs et simples.

- En cas de collecte indirecte

Lorsque les Données personnelles sont collectées auprès d'un tiers, ATAX CONSULTANTS fournit les informations :

- Dans un délai raisonnable, et au plus tard un mois, après avoir obtenu les Données ;
- Si les Données personnelles doivent être utilisées pour la communication avec la Personne concernée, au plus tard au moment de la communication ;
- Si une divulgation à un tiers est envisagée, au plus tard lors de la première divulgation des Données personnelles.

L'obligation d'information ne s'applique pas lorsque :

- La Personne concernée dispose déjà de l'information ;
- Il serait impossible de fournir l'information à la Personne concernée ;
- L'information de la Personne concernée nécessiterait un effort disproportionné ;
- L'information de la Personne concernée rendrait impossible ou compromettrait gravement la réalisation des finalités du Traitement ;
- ATAX CONSULTANTS est tenu par la loi d'obtenir ou de divulguer les Données personnelles.

Tout recours à ces exceptions doit être validé et documenté par le Délégué à la protection des données de ATAX CONSULTANTS.

4.1.3 Comment informer les Personnes concernées ?

L'information doit être fournie de préférence par écrit ou par d'autres moyens y compris, lorsque cela est approprié, par voie électronique. ATAX CONSULTANTS veille à :

- Fournir une information compréhensible : l'information doit être rédigée de la manière la claire, précise et simple possible ;
- Concevoir un format lisible d'information : l'information doit être concise et les éléments doivent être priorisés ;
- Assurer l'accessibilité de l'information ;
- Donner une vision globale sur les traitements de données.

Dans tous les cas, ATAX CONSULTANTS s'assure que cette information est fournie en utilisant une combinaison de techniques adaptées tenant compte du contexte de la collecte et de la relation avec la Personne concernée, telles que :

- Une approche en plusieurs niveaux ;
- Des tableaux de bord ;
- Des menus dépliants,
- Des pop-ups d'information contextuelles ;
- Des icônes ou vidéos ; ou encore
- Des fonctionnalités (type QR Code) de smartphones.

Pour les Traitements effectués dans le cadre des ressources humaines, l'information des collaborateurs sur les Traitements faits de leurs Données personnelles est réalisée au moyen d'une Charte RH de protection des données personnelles. En outre, des mentions d'information sont inscrites sur les offres d'emploi pour informer les candidats lors des campagnes de recrutement.

4.1.4 Informations en cas de traitement ultérieur

Lorsque ATAX CONSULTANTS a l'intention de traiter les Données Personnelles à des fins autres que celles pour lesquelles elles ont été initialement collectées, ATAX CONSULTANTS fournit à la Personne concernée, préalablement à ce Traitement ultérieur, des informations sur cette autre finalité et toute autre information pertinente pour remplir son obligation d'information définie ci-dessus.

4.2 Droits des Personnes concernées

ATAX CONSULTANTS fait droit aux droits des Personnes concernées. La Législation applicable accorde aux Personnes concernées les droits suivants :

- **Droit d'accès** : le droit d'obtenir une copie des Données personnelles que le Responsable de traitement détient sur le demandeur.
- **Droit de rectification** : le droit de faire rectifier les Données personnelles si elles sont inexactes ou obsolètes et/ou de les compléter si elles sont incomplètes.
- **Droit à l'effacement / droit à l'oubli** : le droit, dans certaines conditions, de faire effacer ou supprimer les données, à moins que ATAX CONSULTANTS ait un intérêt légitime à les conserver.
- **Droit d'opposition** : le droit de s'opposer au Traitement des Données Personnelles par ATAX CONSULTANTS pour des raisons tenant à la situation particulière du demandeur (sous conditions).
- **Droit de retirer son consentement** : le droit à tout moment de retirer le consentement lorsque le Traitement est fondé sur le consentement.
- **Droit à la limitation du traitement** : le droit, dans certaines conditions, de demander à ce que le traitement des Données personnelles soit momentanément suspendu.
- **Droit à la portabilité des données** : le droit de demander à ce que les Données personnelles soient transmises dans un format réexploitable permettant de les utiliser dans une autre base de données.
- **Droit de ne pas faire l'objet d'une décision automatisée** : le droit pour le demandeur
- **Droit de définir des directives post-mortem** : le droit pour le demandeur de définir des directives relatives au sort des Données Personnelles après sa mort.

A cette fin, ATAX CONSULTANTS définit et met en œuvre une procédure de gestion des droits des personnes conformes aux exigences de la Législation applicable. Cette procédure établit :

- Les exigences légales qui doivent être respectées ;
- Les moyens autorisés pour présenter une demande pour chaque droit, selon la catégorie de Personnes concernées ;
- Les processus opérationnels pour traiter ces demandes conformément aux exigences susmentionnées ;
- Les parties impliquées dans ces processus, leurs rôles et responsabilités.

Les demandes admissibles sont consignées dans un registre central et sécurisé à des fins de preuve de la conformité. Et comprend :

- Date des demandes
- Nom du demandeur
- Type de demande
- Statut de la demande
- Date de clôture de la demande

5. Gestion des Violations de Données personnelles

Conformément à son obligation de sécurité, ATAX CONSULTANTS définit, documente et met en œuvre un processus pour détecter, qualifier et répondre aux Violations de Données personnelles. La procédure documentée doit comprendre :

- Une matrice d'évaluation des risques pour les droits et libertés des Personnes concernées, en tenant compte des critères définis par l'Autorité de contrôle et le Comité européen de protection des données ;
- Une répartition des rôles et des responsabilités entre toutes les parties concernées par le plan de réponse, y compris celles des Sous-traitants de ATAX CONSULTANTS;
- Les conditions, modalités et délais concernant la notification d'une Violation de Données à l'Autorité de contrôle compétente et/ou aux Personnes concernées.

Des moyens techniques et organisationnels adéquats sont mis en œuvre pour détecter, enquêter et signaler les Violations de Données personnelles. De plus, afin de mieux détecter et gérer les Violations, les employés de ATAX CONSULTANTS sont sensibilisés et formés à la procédure à suivre en cas de Violation avérée ou suspectée.

Toute personne découvrant une violation de sécurité des Données personnelles doit en informer dans les plus brefs délais :

- La Présidente de ATAX CONSULTANTS.

Si la Violation présente un risque pour les Personnes concernées, ATAX CONSULTANTS doit notifier l'Autorité de contrôle compétente dans un délai maximum de 72 heures après avoir pris connaissance de la Violation. En cas de retard, ATAX CONSULTANTS justifie à l'Autorité de contrôle les raisons du retard.

De plus, ATAX CONSULTANTS établit un registre des Violations de Données personnelles à des fins d'accountability, qu'une notification soit requise ou non.

6. Gestion des sous-traitants

Conformément à la Législation applicable, ATAX CONSULTANTS s'engage à choisir des prestataires qui présentent des garanties suffisantes quant à la mise en œuvre de mesures techniques et organisationnelles appropriées.

A ce titre, ATAX CONSULTANTS vérifie en amont les garanties présentées par tout Sous-traitant envisagé, au moyen notamment de questionnaires et/ou analyse de documentation. Cette vérification doit permettre d'évaluer les conditions de mise en œuvre du Traitement chez le Sous-traitant : modalités de réalisation des opérations de Traitement confiées, sécurité technique, maturité du Sous-traitant sur la question de la protection des Données personnelles.

ATAX CONSULTANTS s'assure qu'un contrat écrit est systématiquement signé avec chacun de ses Sous-traitants, lequel définit clairement les rôles et responsabilités de chacune des parties. Ce contrat intègre au minimum les clauses requises par la Législation applicable (notamment le RGPD) et détaille le ou les Traitements confiés au Sous-traitant en déterminant :

- L'objet et la durée du Traitement ;
- La nature et la finalité du Traitement ;
- La ou les catégories de Données à caractère personnel ;
- La ou les catégories de Personnes concernées ;
- Les instructions relatives aux opérations de Traitement.

Les Sous-traitants sont audités dans les conditions de la Section 10.2.

7. Relations avec l'autorité de contrôle

ATAX CONSULTANTS coopère avec toute Autorité de contrôle lorsque cela est requis et fournit toutes les preuves de sa conformité avec la Législation applicable.

Le Délégué à la protection des données de ATAX CONSULTANTS agit en qualité de point de contact de l'Autorité de contrôle et pilote à ce titre :

- La consultation de l'Autorité de contrôle concernée dans le cas où un Traitement de Données implique un risque (résiduel) élevé pour la vie privée ;
- Le signalement de Violations de Données à l'Autorité de contrôle chef de file et/ou à l'Autorité de contrôle locale compétente ;
- Le traitement de toutes demandes (telles que les demandes d'accès aux registres de traitements, les demandes d'information, etc.)

ATAX CONSULTANTS définit une procédure en cas d'audit par une Autorité de contrôle.

8. Sensibilisation et formation du personnel

ATAX CONSULTANTS s'assure que l'intégralité de ses collaborateurs est sensibilisée à la problématique de la protection des Données personnelles et comprend l'intention et la portée de la Législation applicable ainsi que les risques en cas de non-conformité.

Dans ce cadre, ATAX CONSULTANTS assure une sensibilisation générale à tous ses collaborateurs et des formations plus spécifiques aux pôles et collaborateurs qui ont vocation à traiter des Données personnelles au quotidien.

Les collaborateurs sont régulièrement informés des évolutions législatives ou jurisprudentielles en matière de protection des Données à caractère personnel.

Tout nouveau collaborateur suit une sensibilisation/formation appropriée eu égard à ses missions et à son niveau de connaissance.

9. Le contrôle de la conformité

9.1 Contrôle interne

ATAX CONSULTANTS garantit respect de la présente Politique générale de protection des données ainsi que de ses procédures de mise en œuvre et des politiques supplémentaires relatives à la protection des données.

A cette fin, une analyse annuelle de conformité avec les encarts de règles est réalisée, ainsi que l'adéquation des activités de Traitement mis en œuvre avec le registre des Traitements.

Lorsque des manquements sont identifiés au cours de cette analyse, un plan de remédiation est défini et toutes les parties prenantes concernées afin de remédier aux déficiences détectées, en tenant compte des risques encourus, des coûts de mise en œuvre, des contraintes commerciales existantes et prévisibles et des ressources humaines disponibles. Les mesures correctives du plan de remédiation sont mises en œuvre sans retard injustifié par les parties prenantes concernées.

9.2 Contrôle externe : audit des Sous-traitants

ATAX CONSULTANTS mène des audits auprès de ses Sous-traitants afin de vérifier qu'ils respectent leurs obligations légales et contractuelles.

Pour toute question / demande, merci de nous adresser un mail à :
contact@ataxconsultants.fr

Annexe 1 Définitions

Analyse d'impact relative à la protection des données (AIPD) : analyse à effectuer par ATAX CONSULTANTS pour les traitements susceptibles d'engendrer un risque élevé pour les droits et libertés des personnes physiques.

Autorité de contrôle : autorité publique indépendante instituée par un Etat membre en vertu de l'article 51 du RGPD, chargée de surveiller l'application du RGPD, afin de protéger les libertés et droits fondamentaux des personnes physiques à l'égard du traitement et de faciliter le libre flux des données à caractère personnel de l'Union européenne.

Consentement : 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.

Destinataire : personne physique ou morale, l'autorité publique, le service ou tout autre organisme qui reçoit communication de Données à caractère personnel, qu'il s'agisse ou non d'un Tiers.

Données à caractère personnel/Données personnelles : toute information se rapportant à une Personne concernée notamment par référence à un identifiant tel qu'un nom, un numéro d'identification, un numéro de carte d'identité, un salaire, des dossiers de santé, des informations de compte bancaire, des habitudes de conduite ou de consommation, des données de localisation, un identifiant en ligne, etc. Le terme « Données personnelles » inclut les Données à caractère personnel sensibles.

Données à caractère personnel sensibles/Données personnelles sensibles : désigne les Données à caractère personnel révélant ou reposant sur :

- L'origine raciale ou ethnique, les opinions politiques, religieuses ou philosophiques
- L'appartenance à une organisation syndicale
- La santé physique ou mentale
- L'orientation sexuelle ou la vie sexuelle
- Les données génétiques et biométriques
- Des données relatives aux condamnations pénales, aux infractions ou aux mesures de sûreté connexes.

Législation applicable : ensemble de réglementation relative à la protection des données personnelles, à savoir le Règlement européen n°2016/679 relatif à la protection des Données à caractère personnel (RGPD), la Loi informatique et libertés modifiée, et toute autre réglementation qui y serait relative, applicable aux Traitements de Données personnelles effectués par ATAX CONSULTANTS.

Personne concernée : individu sur lequel porte les Données à caractère personnel et qui peut être identifié ou identifiable, directement ou indirectement, grâce à ces Données personnelles. Cela inclut les clients, prospects, et collaborateurs anciens et actuels.

Responsable de traitement : personne physique ou morale qui, individuellement ou conjointement, décide quelles Données à caractère personnel sont collectées, pourquoi et comment elles sont collectées et traitées.

Au sens du RGPD, le Responsable de traitement sera entendu au sens général comme la représentante légale de la société, et par délégation de pouvoir, les associés ou les responsables métier ou toute personne désignée comme tel par la représentante légale de la société.

RGPD : abréviation du Règlement européen n°2016/679 du 27 avril 2016 relatif à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données.

Sous-traitant : toute personne physique ou morale, l'autorité publique, le service ou un autre organisme qui traite des Données à caractère personnel au nom du Responsable de traitement et selon ses instructions (par exemple des prestataires ou fournisseurs).

Tiers : toute personne physique ou morale, autorité publique, agence ou tout autre organisme autre que la Personne concernée, le Responsable du traitement, le Sous-traitant et les personnes qui, sous l'autorité directe du Responsable du traitement ou du Sous-traitant, sont habilités ou autorisés à traiter les données.

Traitement : toute opération ou ensemble d'opérations effectuées ou non à l'aide de procédés automatisés et appliquées à des Données personnelles telle que la collecte, l'accès, l'enregistrement, la copie, le transfert, la conservation, le stockage, le croisement, la modification, la structuration, la mise à disposition, la communication, l'enregistrement, la destruction, que ce soit de manière automatique, semi-automatique ou autre. Cette liste n'étant pas exhaustive.

Transfert de données : toute communication, toute copie ou déplacement de données par l'intermédiaire d'un réseau, ou toute communication, toute copie ou déplacement de ces données d'un support à un autre, quel que soit ce support, de Données personnelles vers un pays tiers à l'Union européenne ou à une organisation internationale qui font ou sont destinés à faire l'objet d'un Traitement après ce transfert.

Violation de données à caractère personnel : violation de la sécurité entraînant, de manière accidentelle ou illicite, la destruction, la perte, l'altération, la divulgation non autorisée de Données à caractère personnel transmises, conservées ou traitées d'une autre manière, ou l'accès non autorisé à de telles données.