POLITIQUE D'ENTREPRISE DE PROTECTION DES DONNÉES D'AGEM

1. Objet et finalité

AGEM adopte la présente Politique afin de garantir le respect basique et proportionné du **Règlement (UE) 2016/679 (RGPD)** et, s'agissant de la législation espagnole de référence du groupe, de la Loi Organique 3/2018 (LOPDGDD), en ce qui concerne le traitement des données à caractère personnel des salariés, candidats, clients, fournisseurs et autres contacts liés à son activité commerciale.

Dans la mesure où AGEM ne traite pas de données de catégories particulières et n'exerce pas d'activités soumises à une supervision spécifique en matière de confidentialité, la présente Politique établit uniquement les contrôles minimaux nécessaires pour assurer une conformité adéquate sans charges administratives disproportionnées.

Cette Politique s'intègre au Système de Conformité Pénale conformément à la norme UNE 19601, et s'articule avec le Code d'Éthique, la Politique de Conformité Pénale et la Politique du Canal Éthique.

2. Champ d'application

Cette Politique s'applique à :

- AGEM et l'ensemble de ses filiales et délégations.
- L'ensemble des salariés, dirigeants et collaborateurs.
- Les tiers traitant des données à caractère personnel pour le compte d'AGEM (sous-traitants), par le biais d'une clause contractuelle.

3. Rôles et responsabilités

Administrateur Unique

- Approuve cette Politique et garantit les ressources minimales nécessaires à sa mise en œuvre.
- Supervise, de manière générale, le respect des obligations légales en matière de confidentialité.

Compliance Officer

- Assume les fonctions de référent en matière de protection des données.
- Tient à jour la documentation minimale de conformité (clauses, contrats avec les fournisseurs, registre d'activités de base).
- Traite les demandes, incidents et requêtes d'exercice des droits.

- Coordonne la réponse en cas de violation de sécurité.

Responsables de traitement

- Garantissent que les données de leur domaine sont traitées avec licéité, minimisation et sécurité.
- Veillent à l'utilisation des formulaires et clauses d'information approuvés par le Compliance Officer.

4. Principes de base du traitement

AGEM appliquera de manière proportionnée les principes suivants :

4.1. Licéité, loyauté et transparence

Les personnes concernées seront informées, de manière claire et simple, des éléments suivants :

- identité du responsable du traitement,
- finalité des données,
- base juridique,
- éventuelles communications,
- durée minimale de conservation,
- droits disponibles.

Ces clauses figureront dans les contrats de travail, les formulaires de contact, les relations commerciales et tout point de collecte de données.

4.2. Minimisation

Seules les données strictement nécessaires au développement de l'activité commerciale et professionnelle d'AGEM seront collectées.

4.3. Exactitude

Les données seront tenues à jour lorsque cela est nécessaire (par exemple, données professionnelles, fiscales ou de contact).

4.4. Limitation de la conservation

Les données seront conservées uniquement pendant :

- la durée de la relation contractuelle, et
- les délais légaux de prescription applicables (droit du travail, droit commercial ou droit fiscal).

Ce délai écoulé, les données seront supprimées ou conservées sous forme bloquée en cas d'obligation légale.

4.5. Sécurité

AGEM appliquera des mesures techniques et organisationnelles basiques et proportionnées :

- Mots de passe robustes.
- Contrôle des accès par utilisateur.
- Antivirus et mises à jour périodiques.
- Sauvegardes.
- Utilisation restreinte des dispositifs et supports externes.

Compte tenu du faible risque des données traitées, des mesures avancées (chiffrement intégral, anonymisation avancée, etc.) ne sont pas requises, sauf appréciation contraire du Compliance Officer.

5. Registre de base des traitements

AGEM tiendra, de manière simplifiée, un **Registre des Activités de Traitement (RAT)** indiquant au minimum :

- le nom du traitement,
- la finalité,
- les catégories de données et de personnes concernées,
- la base juridique,
- les délais de conservation,
- les sous-traitants externes, le cas échéant.

Aucune analyse d'impact (AIPD) ne sera réalisée, sauf si un traitement à haut risque venait à être mis en place ultérieurement.

6. Droits des personnes

AGEM garantit les droits d'accès, de rectification, d'effacement, d'opposition, de limitation et de portabilité, conformément aux dispositions du RGPD.

Le Compliance Officer gérera les demandes via la messagerie d'entreprise dédiée à la confidentialité, en vérifiant l'identité du demandeur et en répondant dans le délai légal maximal.

7. Sous-traitants du traitement

Lorsqu'un fournisseur a accès à des données à caractère personnel (logiciels, cabinets comptables, services cloud, maintenance), un contrat de sous-traitance sera formalisé, comprenant :

- des instructions claires,
- un devoir de confidentialité,
- des mesures de sécurité proportionnées,
- l'obligation de notifier les incidents,
- la restitution ou la suppression des données à la fin du service.

AGEM sélectionnera des sous-traitants offrant des garanties raisonnables sans nécessiter d'audits complexes.

8. Violations de sécurité

En cas de perte, d'accès non autorisé ou d'incident affectant des données à caractère personnel :

- il en sera immédiatement informé le Compliance Officer,
- la gravité sera analysée,
- l'incident sera documenté,
- l'autorité de contrôle compétente sera notifiée uniquement en cas de risque pour les personnes concernées (critère RGPD),
- les mesures correctives seront communiquées.

9. Diffusion et formation minimale

AGEM dispensera une formation de base et brève sur la confidentialité à l'ensemble du personnel, en particulier dans les processus où des données à caractère personnel sont gérées (administration, RH, commercial).

Un rappel annuel sera suffisant compte tenu de la faible exposition au risque.

10. Entrée en vigueur, révision et mise à jour

La Politique entrera en vigueur après son approbation par l'Administrateur Unique.

Elle sera révisée tous les trois ans, ou plus tôt si :

- les activités d'AGEM changent,
- les traitements de données changent,
- une mise à jour réglementaire pertinente intervient.

11. Engagement de conformité

L'ensemble du personnel devra connaître cette Politique et s'y conformer.

Les tiers ayant accès aux données l'accepteront au moyen d'une clause contractuelle.

Annexe I – Procédure Opérationnelle de Protection des Données d'AGEM

Version simplifiée et proportionnée au risque

Cette Annexe établit les étapes pratiques, les contrôles minimaux et les responsabilités nécessaires à l'application de la Politique d'Entreprise de Protection des Données d'AGEM. Elle vise à garantir une conformité efficace et proportionnée, en évitant une bureaucratie inutile, en cohérence avec la norme UNE 19601 et les risques réels de l'activité d'AGEM.

1. Identification de base des traitements (RAT simplifié)

Le Compliance Officer tiendra un Registre des Activités de Traitement de base, qui comprendra uniquement :

- Le nom du traitement (ex. RH, clients, fournisseurs).
- La finalité.
- La base juridique (contrat, obligation légale, intérêt légitime, etc.).
- Les catégories minimales de données (identification, contact, facturation, professionnelles).
- Les destinataires (cabinet comptable, logiciel de comptabilité, cloud).
- Le délai de conservation.

Responsable de chaque domaine : informer le Compliance Officer lors de la création d'un nouveau traitement ou de la modification d'un traitement existant.

2. Procédure de collecte des données et clauses d'information

Avant de collecter des données à caractère personnel de salariés, candidats, clients, fournisseurs ou tout autre tiers, il convient de s'assurer de ce qui suit :

2.1. Utilisation obligatoire de clauses d'information brèves

Le responsable du domaine remettra/émettra la clause d'information correspondante approuvée par le Compliance Officer.

Modèles existants (utilisation obligatoire) :

- Contrat de travail
- Processus de recrutement

- Formulaires clients
- Formulaires fournisseurs
- Formulaires de contact du site Internet

2.2. Éléments minimaux de la clause

Toutes les clauses doivent comprendre :

- L'identité du responsable du traitement (AGEM).
- La finalité du traitement.
- La base juridique (ex. contrat, obligation légale).
- Les destinataires.
- Le délai de conservation.
- Les droits et l'adresse de contact du Compliance Officer.

3. Procédure de traitement des demandes d'exercice de droits (accès, rectification, effacement, opposition, portabilité)

3.1. Canal habilité

Toutes les demandes d'exercice de droits seront gérées par courrier électronique adressé au responsable Compliance : dgomez@agemsa.com

3.2. Étapes obligatoires

- Enregistrer la demande.
- Vérifier l'identité.
- Examiner avec le domaine concerné si le droit demandé est applicable.
- Répondre dans un délai maximal d'1 mois.
- Archiver la preuve de la réponse.

3.3. Réponses types

Le Compliance Officer tiendra à jour des modèles de réponse pour :

- Accès
- Rectification
- Effacement
- Opposition
- Limitation
- Portabilité

- Impossibilité de faire droit à la demande (motivée)

4. Sélection et gestion des fournisseurs ayant accès aux données (sous-traitants)

4.1. Avant la contractualisation

Le domaine proposant le fournisseur devra vérifier auprès du Compliance Officer :

- Si le fournisseur traite des données à caractère personnel pour le compte d'AGEM.
- S'il offre des garanties raisonnables de sécurité (déclaration, certification de base, réputation).

4.2. Contrat de sous-traitance obligatoire

Un contrat devra être formalisé, comportant au minimum :

- Le traitement uniquement selon les instructions d'AGEM.
- La garantie de confidentialité.
- L'adoption de mesures de sécurité de base.
- La notification des incidents.
- L'interdiction de sous-traiter sans autorisation.
- La suppression ou la restitution des données à la fin du service.

Le Compliance Officer conserve une copie de l'ensemble des contrats.

5. Mesures de sécurité minimales applicables à AGEM

Compte tenu de son activité et de son niveau de risque faible, AGEM applique des mesures techniques et organisationnelles de base :

5.1. Mesures techniques

- Équipements protégés par un mot de passe fort.
- Mises à jour automatiques des logiciels.
- Antivirus actif.
- Sauvegardes automatiques.
- Accès aux données limité aux profils autorisés.

5.2. Mesures organisationnelles

- Interdiction de partager les mots de passe.
- Verrouillage d'écran obligatoire.

- Utilisation limitée des dispositifs externes.
- Conservation responsable de la documentation papier.
- Élimination sécurisée de la documentation.

5.3. Sans papier dans la mesure du possible

La documentation physique ne sera imprimée que si cela est strictement nécessaire.

6. Procédure de notification et de gestion des violations de sécurité

Une violation de sécurité est tout incident de perte, vol, destruction ou accès non autorisé à des données à caractère personnel.

6.1. Communication immédiate

Tout salarié doit informer immédiatement le Compliance Officer.

6.2. Étapes internes

- Enregistrer l'incident.
- Identifier les données concernées.
- Évaluer s'il existe un risque pour les personnes concernées.
- Adopter des mesures de confinement.
- Le cas échéant, notifier l'autorité de contrôle compétente dans un délai de 72 heures.
- Informer les personnes concernées si le risque est élevé.
- Documenter et clôturer l'incident.

7. Procédure de base pour les transferts internationaux

AGEM ne réalisera de transferts internationaux que dans les cas suivants :

- Existence d'une décision d'adéquation, ou
- Mesures appropriées (Clauses Contractuelles Types), ou
- Support technique ponctuel de fournisseurs européens utilisant des infrastructures certifiées.

Il est interdit de contracter avec des fournisseurs situés en dehors de l'EEE sans validation du Compliance Officer.

8. Conservation et suppression des données

Chaque domaine respectera les critères suivants :

8.1. Conservation minimale

- Données professionnelles : selon la réglementation (4 à 10 ans).
- Données clients et fournisseurs : pendant la durée de la relation + délais légaux de prescription.
- Données commerciales non contractuelles : maximum 2 ans.

8.2. Suppression

Les données seront supprimées lorsqu'elles ne seront plus nécessaires, ou conservées sous forme bloquée en cas d'obligation légale de conservation.

9. Formation et sensibilisation minimales

Le Compliance Officer organisera :

- Une formation initiale de base pour les nouvelles recrues.
- Un bref rappel annuel pour l'ensemble du personnel.
- Des communications simples sur les bonnes pratiques (courriel, document bref).

10. Révision périodique de l'Annexe

Le Compliance Officer révisera cette Annexe tous les trois ans, sauf changements législatifs ou nouvelles activités le nécessitant.