PROCEDURE

Traitement des données personnelles : RGPD

Référence :

Rédigé par : Adrien Martin
Validé par : Stéphane Toullieux
Date de création : 21/08/2023

Services et collaborateurs concernés : Tous les collaborateurs d'ATHYMIS GESTION

Emplacement fichier : admin/RCCI/procédures

Diffusion de la procédure

La diffusion des procédures, en interne ou à l'externe, est du ressort du RCCI.
Les opérationnels rédigent les procédures dites « opérationnelles » assistée dans cette tâche par le contrôle interne.
Les procédures sont ensuite validées par les dirigeants.

Mises à jour

La procédure est mise à jour en cas de changements majeurs de l'activité d'Athymis Gestion ou de l'environnement réglementaire.
Les mises à jour de cette procédure se font à l'initiative du Secrétaire Général et du RCCI. Les opérationnels pourront être sollicités dans le cadre de ces mises à jour.
Toute mise à jour doit être validée par les dirigeants.
Les mises à jour sont matérialisées dans le corps de la procédure en tant que tel ; la référence de la procédure portant la date de modification de la procédure ainsi que la date de mise à jour.
Les versions précédentes portant des références antérieures sont conservées électroniquement et archivées.

Référence réglementaire

- Loi "Informatique et Libertés" du 6 janvier 1978 modifiée en 2004
- Article L533- 10 5°du Code Monétaire et Financier
- Règlement (UE 2016/679 du Parlement Européen et du Conseil du 19 avril 2016) Général sur la Protection des Données

Préambule

Athymis Gestion est une société de gestion agréée par l'AMF (08000035) depuis le 25/09/2008 et qui gère des OPCVM (fonds de la société de gestion) destinée à une clientèle professionnelle et institutionnelle.

I. Objectif et champ d'application de la procédure

1. Objectif de la procédure

La procédure a pour objet d'organiser le traitement des données informatiques collectées et stockées par la société de gestion, conformément au Règlement Général sur la Protection des Données (RGPD), qui s'applique à toute entreprise établie sur le territoire de l'Union Européenne.

2. Champ d'application

Cette procédure s'applique à l'ensemble des opérations réalisées dans le cadre de l'activité de la société de gestion. Tous les collaborateurs sont donc concernés, chacun à leur niveau et dans leurs fonctions.
Le RGPD a trait aux personnes physiques. Il porte sur les données des collaborateurs, des clients, des prospects, et sur toutes les autres données à caractère personnel traitées par l'établissement (sous-traitants, prestataires, fondateurs, membres d'organes de gouvernance, etc.).

La société de gestion met en place et tient à jour un registre de traitements tel que défini au point II.3 recensant tous les traitements réalisés par les collaborateurs.

II. Dispositif mis en place

1. Données concernées : données à caractère personnel

Les données à caractère personnel sont définies à l'article 4 du RGPD comme « toute information se rapportant à une personne physique identifiée ou identifiable » (ci-après dénommée "personne concernée").
Est réputée " personne physique identifiable" une personne physique qui peut être identifiée, directement (par exemple par son nom) ou indirectement (par son numéro de téléphone, un identifiant en ligne, etc.).

Deux types de données relèvent principalement du RGPD. Il s'agit :

- Données personnelles se rapportant à une personne physique identifiée ou identifiable :

  - État civil, identité, données d'identification, photos, etc.
  - Vie personnelle (situation familiale, etc.)
  - Informations d'ordre économique et financier (revenus, situation financière, situation fiscale, coordonnées bancaires, etc.)
  - Données de connexion (adresse IP, logs, etc.)
  - Données de localisation
  - Des données personnelles dites "sensibles" :

Par principe, la collecte et le traitement des données sensibles sont interdits. Cependant, dans la mesure où la finalité du traitement l'exige, l'interdiction peut être levée si les traitements pour lesquels

la personne concernée a donné son consentement exprès ou si les traitements sont justifiés par un intérêt public après autorisation de l'autorité nationale compétente (CNIL en France) ou décret en Conseil d'État. La collecte et le traitement de ces données doivent être justifiés au cas par cas au regard des objectifs recherchés.

- Les données révélant l'origine raciale ou ethnique, les opinions politiques, les convictions religieuses ou philosophiques, l'appartenance syndicale → **interdit pour Athymis ;**
- Les données génétiques ou biométriques aux fins d'identifier une personne physique de manière unique / les données concernant la santé **→ interdit pour Athymis ;**
- Les données concernant la vie sexuelle ou l'orientation sexuelle **→ interdit pour Athymis ;**
- Le numéro d'identification national unique (NIR soit le n° Sécu pour la France) : **→ autorisé pour Athymis, pour son personnel ;**
- Les données relatives à des condamnations pénales ou infractions **→ autorisé pour Athymis** pour son personnel, membre des organes de gouvernance (obligation réglementaire, ex AMF pour les responsables dirigeants, chargés d'affaires ou le RCCI).

2. Traitements concernés

Ils sont définis à l'article 4.2 du RGPD comme « *Toute opération ou tout ensemble d'opérations effectuées ou non à l'aide de procédés automatisés et appliqués à des données ou des ensembles de données à caractère personnel, telles que la collecte, l'enregistrement, l'organisation, la structuration, la conservation, l'adaptation ou la modification, l'extraction, la consultation, l'utilisation, la communication par transmission, la diffusion ou toute autre forme de mise à disposition, le rapprochement ou l'interconnexion, la limitation, l'effacement ou la destruction*.»

3. Registre des traitements

La tenue d'un registre des traitements est une obligation pour Athymis Gestion. Celui-ci doit pouvoir être communiqué à la CNIL lorsqu'elle le demande.

Ce registre doit recenser et analyser les traitements. Il doit permettre d'identifier précisément :

- Les parties prenantes qui interviennent dans le traitement des données (sous-traitant, co-responsable, représentant…)
- Les catégories des données traitées
- A quoi servent les données
- Qui accède aux données et à qui elles sont communiquées
- Combien de temps elles sont conservées

Par dérogation, Athymis Gestion étant une société de moins de 250 salariés, elle est autorisée à n'inscrire dans son registre que les traitements suivants :

- Traitements récurrents (gestion paie, gestion clients, prospects, fournisseurs…)

Le registre doit être mis à jour sur évènements par Athymis Gestion pour suivre les évolutions des activités et des traitements de données. Toute modification apportée aux conditions de mise en œuvre d'un traitement doit être mentionnée dans le registre (ex nouvelle catégorie de données collectées).

4. Sécurité des données

a) Mesures de sécurité

La société de gestion applique des mesures afin de garantir l'intégrité des données et la sécurité des systèmes.
Sur les données « papier » :

- Accès aux locaux sécurisés par la porte d'entrée des bureaux qui ne peut être ouverte que par les personnes ayant la clef.
- Placard fermant à clefs dans lequel sont placés les documents papiers concernant le personnel.

Sur les données « numériques » :

- Authentification / identification : l'ouverture de poste de travail nécessite une identification par nom d'utilisateur et un mot de passe confidentiel propre à chaque collaborateur. Les mots de passe des salariés sont changés tous les 90 jours
- Gestion des droits : les droits d'accès et/ou de modification des données de l'entreprise sont définies en fonction des besoins liés au poste de chaque collaborateur
- L'ensemble des ordinateurs d'Athymis est protégé par l'antivirus Avast Business Security
- Le réseau d'Athymis est protégé par un Firewall dont les fonctionnalités sont énoncées dans le PCA
- Réseau sécurisé par le stockage sur le serveur d'Athymis (présent physiquement dans les locaux et sous clé)

Le plan de continuité de l'activité et de sauvegarde des données traite en détail du dispositif dédié au maintien de l'activité. Ainsi, l'ensemble des informations relatives à la société de gestion est hébergé de manière à pouvoir mettre en œuvre le PCA à tout moment.

b) Les mesures de prévention

La direction de la société de gestion sensibilise les collaborateurs sur la protection et la confidentialité des données.
A ce titre, les bonnes pratiques sont à noter :

- Ne pas communiquer les codes d'accès à un tiers (même s'il s'agit d'un autre collaborateur)
- Ne pas laisser de documents confidentiels ou important sur son poste de travail en cas d'absence
- Ne pas laisser de documents confidentiels ou important lors de l'impression
- Verrouiller sa session de travail en cas d'absence à son poste de travail
- Vérifier la provenance d'un mail avant d'ouvrir une pièce jointe
- Prévenir immédiatement la direction en cas de doute.

5. Protection des données

a) Les principes

La société de gestion a nommé de Délégué à la Protection des Données (Data Protection Officers ou DPO). Il s'agit du Président Directeur Général de la société, Stéphane TOULLIEUX.
Le responsable du traitement est le Secrétaire Général, Adrien MARTIN.

L'entreprise se conforme également aux obligations d'informations et de notification relative à l'utilisation des informations transmises par le client au travers des supports papiers, électroniques ou

téléphonique ou tout autre support durable. Pour rappel la société de gestion peut traiter des données personnelles si le traitement relève du champ d'application des bases juridiques suivantes :

- Exécution d'un contrat : le traitement est nécessaire à l'exécution d'un contrat auquel la personne concernée est partie ou afin de prendre des mesures à la demande de la personne concernée avant la conclusion d'un contrat.
- Obligation légale : le traitement est nécessaire au respect d'une obligation légale à laquelle le responsable du traitement est soumis.
- Intérêts vitaux : le traitement est nécessaire afin de protéger les intérêts vitaux de la personne concernée ou d'une autre personne physique.
- Fonctions publiques : le traitement est nécessaire à l'exécution d'une tâche réalisée dans l'intérêt public ou dans l'exercice de l'autorité officielle du responsable du traitement.
- Intérêts légitimes : le traitement est nécessaire aux fins des intérêts légitimes poursuivis par le responsable du traitement ou par un tiers, sauf si ces intérêts sont supplantés par des intérêts supérieurs ou les droits et libertés fondamentales de la personne concernée qui requièrent la protection des données personnelles.
- Consentement : la personne concernée a donné son consentement au traitement de ses données personnelles pour une ou plusieurs finalités spécifiques.

La société de gestion applique le principe de minimisation des données, les données personnelles doivent être adéquates, pertinentes et limitées à celles qui sont nécessaires aux finalités pour lesquelles elles sont collectées et/ou traitées.

Le RGPD impose que les données personnelles ne soient conservées sous une forme qui permet l'identification des personnes concernées que pendant la période nécessaire aux finalités pour lesquelles elles ont été collectées ou pour lesquelles elles sont traitées. Au-delà, les données doivent être effacées ou anonymisées.

Le principe de limitation de la conservation des données s'applique aux supports papier, électroniques et à toute autre méthode utilisée pour le stockage des données personnelles.
La société de gestion, par l'intermédiaire de son responsable du traitement, tient à jour un registre de traitement des données répertoriant l'intégralité des données personnelles de ses clients ainsi que leur finalité.

b) Les droits et leur exercice

La société de gestion accorde une importance toute particulière au respect des droits octroyés aux personnes physiques (clients, collaborateurs...) par le RGPD et s'engage à respecter toutes ces dispositions tout en veillant à leur bonne application.
Le client ou prospect ou collaborateur peut à tout moment exercer ses droits indiqués ci- dessous (sauf obligations légales) et adresser sa demande, en indiquant ses coordonnées complètes au responsable de traitements :

- Accès
- Retrait de votre consentement
- Rectification ou effacement de vos données personnelles
- Limitation du traitement de vos données personnelles
- Opposition au traitement pour motif légitime
- Introduction d'une réclamation auprès de la CNIL
- Portabilité de vos données personnelles dans un format conforme, structuré et lisible en machine

- Définition des directives relatives à la conservation, à l'effacement et à la communication de vos données personnelles après votre décès.

Ces droits peuvent être soumis à certaines conditions, limitations et exceptions légales.
Dès la réception d'une demande d'exercice, le responsable de traitement la consigne dans le registre d'exercice des droits et la traite pour y répondre.

c) Réaction en cas d'exercice de ce droit

À la réception d'une demande de droit d'accès, Athymis Gestion, doit fournir une copie des données concernant l'intéressé ainsi que les informations suivantes : finalité du traitement, catégorie des données concernées, durée conservation, existence des différents droits, origine de données si collecte indirecte, existence éventuelle d'une prise de décision automatisée (profilage ?), droit d'introduire une réclamation auprès d'une autorité de contrôle, destinataires auxquels les données ont été communiquées.

À la réception d'une demande d'effacement par une personne physique, la personne en charge, devra considérer le fondement du traitement concerné :

- Si le traitement est fondé exclusivement sur le consentement de la personne, l'effacement devra être réalisé "dans les meilleurs délais"
- Si le traitement est soumis à une obligation légale sur la conservation de ces données, la société de gestion est tenue de respecter les durées minimales ou maximales de conservation de documents édictées par la réglementation. Cela concerne :

  - La conservation de tous types de contrats ;
  - La conservation des données pour contrôle des abus de marché ;
  - La conservation des données pour justifier des contrôles pour la lutte contre le blanchiment et le financement du terrorisme ;
  - KYC MIF, contraintes fiscales...

La suppression des données de la personne physique ne pourra donc être réalisée qu'après l'écoulement du délai légal.

La personne responsable doit répondre aux demandes d'effacement (positivement ou négativement) de façon motivée, dans les meilleurs délais, en tout état de cause dans un délai d'un mois à compter de la réception de la demande.

La personne responsable devra avertir, dès identification du délai de conservation (selon consentement/obligation légale), l'opérationnel impacté par cette demande d'effacement des données, pour qu'il puisse mettre à jour ses fichiers contenant les données à supprimer.

d) Le transfert des données

Le transfert de données personnelles est au sens de la CNIL « toute communication, copie ou déplacement de données personnelles ayant vocation à être traitées dans un pays tiers à l'Union européenne ».
Par principe, la société de gestion ne transfère pas de données personnelles à un tiers en dehors de l'Union Européenne. Si elle devait le faire, le responsable du traitement analyserait les restrictions

éventuelles et si le pays fait l'objet d'une décision d'adéquation ou non, et mettrait en place des mesures de sécurité appropriées.
Dans le cas d'un transfert de données personnelles à un tiers, seules les données strictement nécessaires à la finalité du traitement faisant l'objet du transfert sont transférées. Si le destinataire n'a pas besoin de recevoir les données identifiantes pour exécuter sa mission, ces données doivent être anonymisées.
Dans le cas de la sous-traitance de données personnelles, des clauses contractuelles sont prévues avec le prestataire. La société de gestion met en place toutes les mesures de sécurité appropriées avant de transférer les données personnelles notamment sur la base de la sensibilité des informations.

e) La gestion des violations des données

Une violation de données personnelles est une violation de sécurité qui entraîne la destruction, la perte, l'altération fortuite ou illicite, la divulgation ou un accès non autorisé aux données personnelles.
Les risques résultant pour la société de gestion d'un incident de sécurité ou de la violation des données personnelles sont significatifs : atteinte à la réputation de l'entreprise, réclamations, litiges et sanctions éventuelles prononcées par l'Autorité de contrôle.
Les violations des données personnelles sont soumises à un régime de notification auprès de l'Autorité de contrôle et/ou aux personnes concernées dans certains cas.
Tout collaborateur de la société de gestion ayant connaissance d'une telle violation de données, doit la remonter au responsable du traitement et au DPO sans délai.
Le responsable du traitement instruit la violation de données (étendue, impacts, etc.), l'inscrit dans le registre et avertie l'Autorité de contrôle et/ou aux personnes concernées le cas échéant. Des mesures de remédiation sont décidées et mises en place le cas échéant.

f) La protection des données dès la conception ou par défaut (Privacy by Design and by Default).

Athymis a mis en œuvre les mesures techniques et organisationnelles appropriées pour garantir que, par défaut, seules les données personnelles qui sont nécessaires au regard de chaque finalité spécifique du traitement sont traitées. Il s'agit en particulier de limiter la quantité de données collectées, l'étendue de leur traitement, leur durée de conservation et leur accessibilité. Un registre des données personnelles essentielles collectées se trouve en annexe de ce document.
Le traitement des données est limité à ce qui est nécessaire aux finalités pour lesquelles les données ont été collectées ; et seules les personnes ayant besoin d'avoir accès aux données personnelles peuvent y avoir accès.

III. Contrôles

Les contrôles de 1er niveau sont assurés par les unités opérationnelles intervenant dans ces activités.
Le contrôle de 2nd niveau est assuré par le RCCI, qui peut déléguer cette fonction à un prestataire externe, qui s'assure :
Du respect de la procédure et de sa mise à jour ;
De la sécurité, de l'intégrité et de la confidentialité des données ;

IV. Sanctions encourues en cas de non-conformité

Le règlement RGPD prévoit deux niveaux de sanctions, pour les entreprises, en cas de non-respect :
Des amendes administratives pourront s'appliquer pour un montant allant de 10 000 à 20 000 000€,

Ou bien 2 à 4 % du chiffre d'affaires annuel mondial total de l'exercice précédent (le montant le plus élevé étant retenu).

La CNIL peut également adopter des sanctions non administratives telles que rappel à l'ordre, injonction de mise en conformité, limitation d'un traitement, suspension de flux de données, exécution forcée de satisfaire demande d'une personne, retrait d'une certification….

V. Archivages et conservation des données

L'ensemble des documents liés au Règlement Général de la Protection des Données est conservé conformément à la réglementation en vigueur, pendant un délai minimum de 5 ans à partir de la fin de la relation, de l'opération ou de l'évènement.

Annexe 1 : registre des documents personnelles nécessaires au bon fonctionnement des activités de la société. Les durées de conservation sont à compter de la clôture de la relation.

	Type de documents	Justification	Mode de conservation	Accessibilité	Durée de conservation
Actionnaires	Document identité	Identification	Numérique sur le serveur	Ensemble des salariés en CDI	5 ans
	Justificatif de domicile	Identification	Numérique sur le serveur	Ensemble des salariés en CDI	5 ans
	Casier judiciaire	Vérification de l'honorabilité	Numérique sur le serveur	Ensemble des salariés en CDI	3 mois (durée de validité)
Salariés	Document Identité	Identification et demande externe	Numérique sur le serveur	Le PDG et le SG	5 ans
	Justificatif de domicile	Identification	Numérique sur le serveur	Le PDG et le SG	5 ans
	Casier judiciaire	Vérification de l'honorabilité	Numérique sur le serveur	Le PDG et le SG	3 mois (durée de validité)
	Attestation de droit à la sécurité sociale	Inscription à la mutuelle	Numérique sur le serveur Et papier dans le classeur RH Sous clef conservé par le SG	Le PDG et le SG	5 ans
	Détention du compte titre et PEA	Suivi des transactions personnelles	Numérique sur le serveur Et papier dans le classeur RH Sous clef conservé par le SG	Le PDG et le SG	5 ans
Clients	Document identité	Identification	Numérique sur le serveur physique dans des pochettes sous clefs	Ensemble des salariés en CDI	5 ans
	Justificatif de domicile	Identification	Numérique sur le serveur physique dans des pochettes sous clefs	Ensemble des salariés en CDI	5 ans
	Contrat / mandat		Numérique sur le serveur physique dans des pochettes sous clefs	Ensemble des salariés en CDI	5 ans
	Documents justifiant de l'origine des fonds	LCB FT	Numérique sur le serveur physique dans des pochettes sous clefs	Ensemble des salariés en CDI	5 ans
	KYC Athymis ou partenaire CGP	Classification client	Numérique sur le serveur physique dans des pochettes sous clefs	Ensemble des salariés en CDI	5 ans