POLITIQUE PROTECTION DES DONNEES A CARACTERE PERSONNEL

Date d'entrée en vigueur	25 mai 2018
Dates de mise à jour	
Références	Règlement n° 2016/679 du Parlement européen et du Conseil du 27 avril 2016

Athos Patrimoine a élaboré une politique en matière de protection des données à caractère personnel, afin de se conformer à la réglementation applicable, et notamment au règlement n° 2016/679 du Parlement européen et du Conseil 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 des données (règlement général sur la protection des données – RGPD).

1. Périmètre

1.1 Objet

Les données auxquelles Athos Patrimoine a accès dans l'exercice de ses activités sont susceptibles de relever de la vie privée de leurs clients : données relatives au patrimoine, situation familiale, etc...

Le respect par Athos Patrimoine de la réglementation relative à la protection des données à caractère personnel est un facteur de transparence et de confiance à l'égard de ses clients.

1.2 Glossaire

Données à caractère personnel : toute information se rapportant à une **personne physique** identifiée ou identifiable ; 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.

Destinataire : la 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.

Responsable du traitement : la personne physique ou morale, l'autorité publique, le service ou un autre organisme qui, seul ou conjointement avec d'autres, détermine les finalités et les moyens du traitement.

Traitement : toute opération ou tout ensemble d'opérations effectuées ou non à l'aide de procédés automatisés et appliquées 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.

Sous-traitant : la personne physique ou morale, l'autorité publique, le service ou un autre organisme qui traite des données à caractère personnel pour le compte du responsable du traitement.

2. Principes généraux applicables

Athos Patrimoine applique les principes suivants :

2.1 Principe de finalité

Athos Patrimoine recueille et traite les données à caractère personnel pour une finalité déterminée explicite et légitime, correspondant aux objectifs poursuivis (exemple : gestion de la clientèle : passation et gestion des contrats, suivi clientèle, traitement des réclamations, exécution d'obligations légales, gestion du personnel : recrutement, formation, mise à disposition d'outils informatiques…).

2.2 Principe de proportionnalité

Athos Patrimoine ne recueille et traite que les seules informations adéquates, pertinentes et nécessaires à la finalité du traitement peuvent faire l'objet d'un traitement de données à caractère personnel.

Par exemple, il n'est pas utile d'enregistrer des informations sur l'entourage familial d'une personne lorsque, au regard des finalité d'un traitement et de la nature de la prestation, seuls sont nécessaires des éléments relatifs à la composition de son patrimoine.

2.3 Principe de minimisation des données

En application des principes issus du RGPD, Athos Patrimoine se conforme au principe de minimisation des données, selon lequel des données à caractère personnel ne peuvent faire l'objet d'un traitement que si les finalités du traitement ne peuvent être atteintes par le traitement d'informations ne contenant pas de données à caractère personnel.

Dans ce cadre Athos Patrimoine s'engage à :

- s'interroger sur la nécessité de traiter des données à caractère personnel pour atteindre les finalités recherchées par le traitement ;
- s'interroger sur la question de savoir si le traitement de données à caractère personnel s'avère nécessaire, limiter le traitement des données au minimum, en ce qui concerne :
- identifier les catégories de données traitées ;
- identifier le volume ou la quantité de données traitées ;
- s'interroger sur la question de savoir si les données collectées sont plus ou moins nécessaires au traitement.

2.4 Durée de conservation limitée des données

Athos Patrimoine ne conserve pas indéfiniment les informations figurant dans un fichier. Il établit une durée de conservation en fonction de la finalité de chaque fichier.

2.5 Droit à l'oubli

L'article 17 du RGPD prévoit le droit à l'effacement ou droit à l'oubli : les personnes concernées ont le droit d'obtenir du responsable du traitement, dans les meilleurs délais, l'effacement des données à caractère personnel les concernant.

Athos Patrimoine ne mettra pas en œuvre le droit à l'effacement irréversible des données avant l'expiration de la durée de prescription de la responsabilité civile professionnelle du CGP. Par ailleurs, le droit à l'oubli ne prévaut pas sur certaines obligations d'archivage de données pendant des périodes déterminées, notamment pour des raisons de conformité aux obligations fiscales.

2.6 Principes de sécurité et de confidentialité

Les données contenues dans les fichiers ne peuvent être consultées que par les personnes habilitées à y accéder en raison de leurs fonctions (ex : personnel en charge des activités d'intermédiation).

Athos Patrimoine est astreint à une obligation de sécurité. Il doit ainsi prendre toutes les mesures nécessaires pour en garantir la confidentialité et éviter toute divulgation d'information.

Athos Patrimoine veille à ce que chaque personne habilitée à accéder aux informations dispose d'un mot de passe individuel (composé, si l'authentification repose uniquement sur un identifiant et un mot de passe, de 12

caractères minimum et de majuscules, minuscules, chiffres et caractères spéciaux et renouvelé régulièrement) et que les droits d'accès soient précisément définis en fonction des besoins réels.

2.7 Respect du droit des personnes

En application de l'article 13 du RGPD, Athos Patrimoine communique les informations suivantes lorsque les données sont collectées auprès de la personne concernée :

- les coordonnées du responsable du traitement et, le cas échéant, celles du représentant du responsable du traitement ;
- le cas échéant, les coordonnées du délégué à la protection des données ;
- les finalités du traitement auquel sont destinées les données à caractère personnel ;
- la base juridique du traitement ;
- les intérêts légitimes poursuivis par le responsable du traitement ou par un tiers lorsque ces intérêts légitimes sont la condition de licéité du traitement ;
- le fait que le responsable de traitement a l'intention d'effectuer un transfert de données à caractère personnel vers un pays tiers ;
- le cas échéant, l'existence ou l'absence d'une décision d'adéquation rendue par la CNIL, 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 à caractère personnel ou, lorsque ce n'est pas possible, les 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 ;
- lorsque le traitement est fondé sur le consentement de la personne concernée, l'existence du droit de retirer son consentement à tout moment, sans porter atteinte à la licéité du traitement fondé sur le consentement effectué avant le retrait de celui-ci ;
- le droit d'introduire une réclamation auprès d'une autorité de contrôle ;
- des informations sur la question de savoir si l'exigence de fourniture de données à caractère personnel a un caractère réglementaire ou contractuel ou si elle conditionne la conclusion d'un contrat et si la personne concernée est tenue de fournir les données à caractère personnel, ainsi que sur les conséquences éventuelles de la non-fourniture de ces données ;
- l'existence d'une prise de décision automatisée, y compris un profilage et, au moins en pareil cas, des informations utiles concernant la logique sous-jacente, ainsi que l'importance et les conséquences prévues de ce traitement pour la personne concernée.

Toute personne a le droit de s'opposer, pour un motif légitime, à ce que des données la concernant soient traitées, sauf si le traitement concerné présente un caractère obligatoire.

Par ailleurs, toute personne physique justifiant de son identité a le droit d'interroger le responsable d'un traitement de données à caractère personnel notamment pour :

- savoir si des données qui la concernent y figurent ou non ;
- obtenir la communication des données qui la concernent sous une forme compréhensible, d'une part, et de toutes les informations disponibles quant à leurs origines, d'autre part ;
- obtenir des informations sur la finalité du traitement, les données collectées et les destinataires.

2.8 Portabilité des données

Athos Patrimoine se conforme au droit à la portabilité des données permettant aux personnes concernées d'exiger des responsables de traitement la transmission de leurs données à caractère personnel à un autre responsable de traitement, sans que le responsable de traitement ayant initialement collecté les données ne puisse s'y opposer.

Dans ce cadre, les personnes concernées ont (i) 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 de les transmettre à un autre responsable de traitement et (ii) le droit d'obtenir que les données soient transmises directement d'un responsable de traitement à un autre lorsque cela est techniquement possible.

Athos Patrimoine qui a initialement traité les données à caractère personnel, est tenu de communiquer les données à caractère personnel relatives à son client ou à un confrère, lorsque le traitement initial repose sur l'un des fondements suivants :

- le client a exprimé son consentement au traitement de ses données à caractère personnel ou le traitement est nécessaire à l'exécution d'un contrat auquel le client est parti ou à l'exécution de mesures précontractuelles prises à la demande du client ;

- et le traitement est effectué à l'aide de procédés automatisés.

Athos Patrimoine devra donc faire droit à la demande de son client si celui-ci demande la transmission de ses données à caractère personnel à un confrère et les transmettre dans un format structuré, couramment utilisé et lisible par machine.

Selon le G29, le droit à la portabilité des données s'applique uniquement si le traitement des données est effectué à l'aide de procédés automatisés et, par conséquent, ne couvre pas la plupart des dossiers papier.

2.9 Analyses d'impact

En vertu de l'article 35 du RGPD, lorsqu'un type de traitement est susceptible d'engendrer un risque élevé pour les droits et libertés des personnes physiques, notamment le traitement à grande échelle de catégories particulières de données, le responsable du traitement doit effectuer, avant toute mise en œuvre, une analyse d'impact.

Athos Patrimoine doit apprécier s'il doit mettre en place une analyse d'impact dans le cadre du traitement des données. Il pourrait avoir à mettre en œuvre une analyse d'impact :

- si Athos Patrimoine effectue un traitement de données à grande échelle (considérant 91 : opérations de traitement à grande échelle qui visent à traiter un volume considérable de données à caractère personnel au niveau régional, national ou supranational, qui peuvent affecter un nombre important de personnes concernée) ;
- quand bien même il ne traiterait pas des données à « grande échelle » si les traitements mis en œuvre répondent à certaines caractéristiques.

En effet, dès lors qu'il répondra à plus de deux des neuf critères déterminés par la CNIL et par le G29 (évaluation/scoring, décision automatique avec effet légal ou similaire ; surveillance systématique ; collecte de données sensibles ; collecte de données à caractère personnel à large échelle ; croisement de données ; personnes vulnérables ; usage innovant ; exclusion du bénéfice d'un droit / contrat), le traitement sera, par principe, soumis à analyse d'impact.

Sur ce point, Athos Patrimoine prend connaissance des « lignes directrices » sur les DPIA et les traitements susceptibles d'engendrer des risques : https://www.cnil.fr/sites/default/files/atoms/files/wp248_rev.01_fr.pdf

S'il met en place une analyse d'impact, Athos Patrimoine utilise le logiciel open source PIA facilitant la conduite et la formalisation d'analyses d'impact sur la protection des données telles prévues par le RGPD : https://www.cnil.fr/fr/outil-pia-nouvelle-version-beta-du-logiciel

2.10 Tenue d'un registre des activités de traitement

Athos Patrimoine doit tenir un registre des catégories de traitement de données à caractère personnel mises en œuvre sous sa responsabilité, s'il compote plus de 250 salariés ou si le traitement qu'il effectue est susceptible de comporter un risque au regard des droits et des libertés des personnes concernées, **s'il n'est pas occasionnel** ou s'il porte notamment sur des données sensibles, ou sur des données se rapportant à des condamnations et des infractions pénales.

Le registre doit, conformément à l'article 30 du RGPD, comporter les informations suivantes :

- Le nom et les coordonnées du responsable du traitement et, le cas échéant, du responsable conjoint du traitement, du représentant du responsable du traitement et du délégué à la protection des données ;
- Les finalités du traitement ;
- Une description des catégories de données traitées, ainsi que les catégories de personnes concernées par le traitement ;
- Les catégories de destinataires auxquels les données à caractère personnel ont été ou seront communiquées, y compris les destinataires dans des pays tiers ou des organisations internationales ;
- Le cas échéant, les transferts de données à caractère personnel vers un pays tiers ou vers une organisation internationale, y compris l'identification de ce pays tiers ou de cette organisation internationale, et les documents attestant de l'existence de garanties appropriées ;
- Dans la mesure du possible, les délais prévus pour l'effacement des différentes catégories de données ;
- Dans la mesure du possible, une description générale des mesures de sécurité techniques et organisationnelles mises en œuvre.

2.11 Capacité à suivre les destinataires de données à caractère personnel

Athos Patrimoine doit être en mesure de suivre et d'identifier les destinataires des données à caractère personnel qu'il traite.

2.12 Nomination d'un délégué à la protection des données (DPO)

Athos Patrimoine doit obligatoirement désigner un DPO :

- S'il appartient au secteur public ;
- Si ses activités de base (principales) l'amènent à réaliser un suivi régulier et systématique des personnes à grande échelle ;
- Si ses activités de base (principales) l'amènent à traiter (toujours à grande échelle) des catégories particulières de données, dites « sensibles », et des données relatives à des condamnations pénales et à des infractions.

Athos Patrimoine apprécie si en fonction notamment du nombre de personnes concernées par les traitements de données à caractère personnel, du volume des données traitées, de la durée ou de la permanence des activités de traitement, de l'étendue géographique de l'activité de traitement, il doit nommer un DPO. La nomination d'un DPO peut également se faire de façon volontaire.

Le DPO est chargé :

- d'informer et de conseiller le responsable de traitement ou le sous-traitant, ainsi que leurs employés ;
- de s'assurer du respect du règlement et du droit national en matière de protection des données ;
- de conseiller l'organisme sur la réalisation d'études d'impact sur la protection des données et d'en vérifier l'exécution ;
- de coopérer avec l'autorité de contrôle et d'être le point de contact de celle-ci.

Le DPO peut être nommé en interne ou être externalisé.

3. Traitement des données personnelles et gestion des clients et prospects de [Nom du Cabinet]

3.1 Principes généraux

Dans le cadre de ces activités, les données à caractère personnel relatives à la clientèle correspondent à toutes les données à caractère personnel nécessaires dans la constitution du dossier du client, dans la prestation de conseil et/ou d'intermédiation, puis dans le suivi de ce dernier dans la durée.

Ces données peuvent concerner des données relatives tant à la vie personnelle qu'à la vie professionnelle, dès lors que Athos Patrimoine est amené à conseiller le client au regard des éléments de connaissance qu'il aura recueillie : situation patrimoniale, financière, professionnelle, connaissances et expériences, tolérance au risque, capacité à supporter les pertes, objectifs, besoins…

Athos Patrimoine ne traite pas des informations sensibles relatives aux condamnations pénales, aux infractions ou aux mesures de sûreté connexes, à l'origine raciale ou ethnique, les opinions politiques, les convictions religieuses ou philosophiques ou l'appartenance syndicale, ainsi que le traitement des données génétiques, des données biométriques aux fins d'identifier une personne physique de manière unique, des données concernant la santé ou des données concernant la vie sexuelle ou l'orientation sexuelle d'une personne physique, dans le cadre de ces activités .

En effet, l'article 9, al.1, du RGPD prévoit l'interdiction de principe du traitement de telles données et, conformément à l'article 5 du RGPD, Athos Patrimoine ne doit collecter que des données adéquates, pertinentes et strictement nécessaires à la finalité du traitement.

3.2 Dispositif de traitement des données

<u>Registre de traitement des données</u>

Athos Patrimoine doit tenir un registre des activités de traitement dans la mesure où il traite de manière non occasionnelle des données à caractère personnel.

Le registre des activités de traitement doit contenir une fiche dédiée à la gestion des ressources humaines qui doit comporter les éléments suivants :

- Identité et coordonnées du responsable de traitement ;
- Finalités ;
- Catégories de personnes concernées ;
- Catégories de données à caractère personnel ;
- Catégories de destinataires ;

- Transferts vers un pays tiers ou une organisation internationale ;
- Délais prévus pour l'effacement ;
- Description générale des mesures de sécurité techniques et organisationnelles.

Information des clients

Les clients et prospects de Athos Patrimoine doivent être informés :

- De l'identité et des coordonnées du responsable de traitement (le cabinet) ;
- Des coordonnées du délégué à la protection des données lorsqu'il y en a un ;
- De l'objectif poursuivi (gestion et suivi des dossiers de ses clients) ;
- De la base juridique du traitement (exécution contractuelle ou précontractuelle à la demande du client) ;
- De l'intérêt légitime s'il s'agit de la base légale du traitement ;
- Des destinataires des données (des sous-traitants, des huissiers, etc.) ;
- Des flux transfrontières ;
- De la durée de conservation ;
- Des droits dont ils disposent ;
- Des conditions d'exercice de ces droits ;
- Du droit de retirer son consentement s'il s'agit de la base légale du traitement ;
- Du droit d'introduire une réclamation auprès d'une autorité de contrôle ;
- Des informations sur le caractère réglementaire ou contractuel du traitement lorsqu'il s'agit de la base légale du traitement.

Ces informations peuvent figurer au sein du DER ou des documents contractuels. Ces informations peuvent également faire l'objet d'une communication par courriel ou par document distinct, notamment pour régulariser la situation auprès des clients qui n'ont pas été correctement informés.

Conservation des données

Les données à caractère personnel ne peuvent être conservées que le temps nécessaire à l'accomplissement de l'objectif poursuivi lors de leur collecte.

Les données relatives aux clients peuvent être conservées le temps de la relation contractuelle entre Athos Patrimoine et son client. Elles ne doivent pas être conservées au-delà d'un an à l'issue de la relation contractuelle **au sein des dossiers courants.**

Au-delà, les données devraient être archivées pour la période où la responsabilité de Athos Patrimoine pourrait être mise en cause et afin de respecter les dispositions relatives à la lutte anti-blanchiment et le financement du terrorisme, avant suppression définitive des données :

- Dossier client ayant souscrit à un investissement : durée de l'investissement/prêt + 5 ans,
- Dossier client conseillé mais n'ayant pas souscrit à un investissement : 5 ans à compter de la fin de la relation contractuelle.

En particulier et dans le cadre de la lutte anti-blanchiment, Athos Patrimoine conserve les documents et informations, quel qu'en soit le support, relatifs à l'identité des clients habituels ou occasionnels pendant cinq ans à compter de la cessation des relations avec eux (art. L. 561-12 CMF).

Les données à caractère personnel relatives à un prospect non client peuvent être conservées pendant un délai de trois ans à compter de leur collecte par le responsable de traitement ou du dernier contact émanant du prospect (par exemple, une demande de documentation ou un clic sur un lien hypertexte contenu dans un

courriel ; en revanche, l'ouverture d'un courriel ne peut être considérée comme un contact émanant du prospect).

Le choix du mode d'archivage est laissé à l'appréciation du responsable du fichier. Des données peuvent ainsi être archivées :

- dans une base d'archive spécifique, distincte de la base active, avec des accès restreints aux seules personnes ayant un intérêt à en connaitre en raison de leurs fonctions (par exemple, le service du contentieux) ;

- ou dans la base active, à condition de procéder à un isolement des données archivées au moyen d'une séparation logique (gestion des droits d'accès et des habilitations) pour les rendre inaccessibles aux personnes n'ayant plus d'intérêt à les traiter.

Lorsque cet archivage est réalisé sous forme électronique, il convient de respecter la recommandation n° 2005-213 de la CNIL du 11 octobre 2005 relative à l'archivage électronique de données à caractère personnel dans le secteur privé.

Sécurité des données

L'accès aux locaux dans lesquels sont stockés les dossiers est suffisamment sécurisé (bureaux fermés à clefs, accès par badge, etc.), ainsi que la sécurité du système d'information sur lequel sont stockés les dossiers sous format numérique (pare- feu, mots de passe, habilitations, etc.).

4. Traitement des données personnelles et ressources humaines de [Nom du Cabinet]

Dans le cadre du recrutement d'un employé ayant des activités d'intermédiation et de conseil auprès de la clientèle, ou encore de personnel support, Athos Patrimoine est amené à effectuer des traitements de données à caractère personnel, dans le respect des principes du RGPD.

Athos Patrimoine prend connaissance de la Norme simplifiée CNIL NS-046 en matière de .gestion du personnel : https://www.cnil.fr/fr/declaration/ns-046-gestion-du-personnel

4.1 Données recueillies

Principe général de respect de la minimisation

Athos Patrimoine ne doit collecter que des données adéquates, pertinentes et strictement nécessaires à la finalité du traitement.

Recrutement :

Les données ne doivent servir qu'à évaluer la capacité du candidat à occuper l'emploi proposé.

Seules des données relatives à la qualification et à l'expérience du collaborateur peuvent être collectées (exemples : diplômes, emplois précédents, etc.)

Il est donc interdit de :

- Demander à un candidat son numéro de sécurité sociale ;
- Collecter des données sur la famille du candidat ;
- Collecter des données sur les opinions politiques ou l'appartenance syndicale du candidat.

Gestion du personnel :

Dans le cadre de la gestion de son personnel, Athos Patrimoine peut collecter principalement deux types de données :

- Des données nécessaires au respect d'une obligation légale.
- Des données utiles à la (i) gestion administrative du personnel, (ii) à l'organisation du travail et (iii) à l'action sociale.

Contrôle de l'activité :

Athos Patrimoine peut mettre en place des outils de contrôle des activités du personnel :

- encadrement des conditions d'utilisation d'internet sur le lieu de travail ;
- dispositif de contrôle des horaires et d'accès du personnel.

Athos Patrimoine prend connaissance de la Norme simplifiée CNIL n°42 portant sur les badges dans les lieux de travail : https://www.cnil.fr/fr/declaration/ns-042-badges-sur-le-lieu-de-travail

4.2 Dispositif de traitement des données en matière RH

Registre de traitement des données

Athos Patrimoine doit tenir un registre des activités de traitement dans la mesure où il traite de manière non occasionnelle des données à caractère personnel.

Le registre des activités de traitement doit contenir une fiche dédiée à la gestion des ressources humaines qui doit comporter les éléments suivants :

- Identité et coordonnées du responsable de traitement ;
- Finalités ;
- Catégories de personnes concernées ;
- Catégories de données à caractère personnel ;
- Catégories de destinataires ;
- Transferts vers un pays tiers ou une organisation internationale ;
- Délais prévus pour l'effacement ;
- Description générale des mesures de sécurité techniques et organisationnelles.

Informations du personnel

Le personnel de Athos Patrimoine doit être informé :

- De l'identité et des coordonnées du responsable de traitement ;
- Des coordonnées du délégué à la protection des données lorsqu'il y en a un ;
- De l'objectif poursuivi (gestion administrative du personnel et du recrutement) ;
- De la base juridique du traitement ;
- De l'intérêt légitime s'il s'agit de la base légale du traitement ;

- Des destinataires des données (des sous-traitants de la gestion de paie, etc.) ;
- Des flux transfrontières ;
- De la durée de conservation ;
- Des conditions d'exercice de leurs droits d'opposition, d'accès, de rectification et de limitation, etc. ;
- Du droit de retirer son consentement s'il s'agit de la base légale du traitement ;
- Du droit d'introduire une réclamation auprès d'une autorité de contrôle ;
- Des informations sur le caractère réglementaire ou contractuel du traitement lorsqu'il s'agit de la base légale du traitement.

Ces informations peuvent figurer sur le contrat de collaboration ou sur le contrat de travail. Ces informations peuvent également faire l'objet d'un affichage ou d'une communication par courriel, notamment pour régulariser la situation auprès des collaborateurs qui n'ont pas été correctement informés.

Conservation

Athos Patrimoine conserve ces élements dans les dossiers courant durant le temps de la période d'emploi de la personne concernée (sauf dispositions législatives ou réglementaires contraires).

Au-delà, ces données peuvent être archivées pendant les durées de prescriptions légales,sur un support informatique distinct et à accès très limité, conformément aux règles applicables en matière d'archives publiques et d'archives privées.

5. Fournisseurs et prestataires

5.1 Notion de sous-traitant

Le sous-traitant est « la personne physique ou morale, l'autorité publique, le service ou un autre organisme qui traite des données à caractère personnel pour le compte du responsable de traitement ». Il peut s'agir notamment d'un comptable, un éditeur de logiciel, un hébergeur, etc.

5.2 Obligations en matière de traitement des données personnelles

Le contrat liant Athos Patrimoine au sous-traitant doit comporter :

- l'objet ;
- la durée ;
- la nature ;
- la finalité ;
- le type de données à caractère personnel ;
- les catégories de personnes concernées ;
- les droits et obligations du responsable de traitement ;
- les mesures de sécurité mises en œuvre concernant le traitement de données à caractère personnel qui sera réalisé.
- la possibilité de ne traiter les données que sur instruction documentée du responsable du traitement, même en ce qui concerne les flux transfrontières ;
- la confidentialité des données ;
- l'exercice des droits des personnes concernées ;
- l'aide qu'il doit fournir au responsable de traitement par des mesures techniques et organisationnelles appropriées, dans toute la mesure du possible, pour s'acquitter de l'obligation de donner suite aux demandes des personnes concernées ;
- l'aide fournie au responsable de traitement pour garantir le respect de ses obligations compte tenu de la nature du traitement et des informations à la disposition du sous-traitant ;

- la suppression des données concernées à l'issue du traitement, ou leur renvoi au responsable de traitement ou leur conservation s'il en est tenu par une disposition nationale ou européenne ;
- la mise à disposition du responsable du traitement de toutes les informations nécessaires pour démontrer le respect de ces obligations et pour permettre la réalisation d'audits, y compris des inspections, par le responsable du traitement ou un autre auditeur qu'il a mandaté, et contribuer à ces audits ;
- l'éventuel recrutement par le sous-traitant d'un sous-traitant ultérieur, d'un nouveau sous-traitant, et l'obtention de l'autorisation préalable écrite du responsable de traitement relative à ce recrutement qui doit être formalisé par un contrat mentionnant l'ensemble des obligations ci-dessus énumérées.

Athos Patrimoine a l'obligation de ne recourir qu'à « des sous-traitants qui présentent des garanties suffisantes quant à la mise en œuvre de mesures techniques et organisationnelles appropriées de manière à ce que le traitement réponde aux exigences du RGPD et garantisse la protection des droits de la personne concernée »

Athos Patrimoine doit interroger ses sous-traitants sur les garanties qu'ils ont mises en place afin de garantir leur conformité au RGPD. Dans le cas où Athos Patrimoine identifie des lacunes dans les mesures mises en place par le sous-traitant, ils devront conclure un avenant au contrat afin de combler lesdites lacunes.

6. Sites internet

6.1 Registre des traitements

Le registre des activités de traitement doit contenir une fiche dédiée au site internet de [Nom du CGP] qui doit comporter les éléments suivants :

- Identité et coordonnées du responsable de traitement ;
- Finalités ;
- Catégories de personnes concernées ;
- Catégories de données à caractère personnel ;
- Catégories de destinataires ;
- Transferts vers un pays tiers ou une organisation internationale ;
- Délais prévus pour l'effacement ;
- Description générale des mesures de sécurité techniques et organisationnelles.

6.2 Mentions du site internet

MENTIONS LEGALES	**Dénomination et raison sociale**	
	Adresse	
	Numéro d'inscription au registre du commerce et des sociétés	
	Coordonnées postales, téléphoniques et électroniques	
	Nom et coordonnées du directeur de publication du site	
	Nom, raison sociale, adresse et numéro de téléphone de l'hébergeur du site	
MENTIONS REGLEMENTAIRES	CIF	Conseiller en investissements financiers, numéro ORIAS, adhésion CNCIF Traitement des réclamations
	Intermédiaire en assurance	Courtier en assurance, (ou autre catégorie), numéro ORIAS Traitement des réclamations
	IOBSP	Courtier en opérations de banque et service de paiement (ou autre catégorie), numéro ORIAS Traitement des réclamations
	Carte T	Activité de transaction sur immeubles et fonds de commerce, carte

		professionnelle n°……. délivrée par …….. Garantie financière
MENTIONS RGPD	L'identité et les coordonnées du responsable du fichier	
	Les coordonnées du délégué à la protection des données	
	La finalité et la base juridique du traitement	
	Les intérêts légitimes poursuivis s'il s'agit de la base légale du traitement	
	Les destinataires ou les catégories de destinataires	
	La durée de conservation des données	
	Les éventuels transferts de données vers des pays hors UE	
	Les droits des personnes concernées (droit d'accès, de rectification, d'effacement, d'opposition, de limitation, etc.)	
	Le droit de retirer son consentement à tout moment s'il s'agit de la base légale du traitement	
	Le droit d'introduire une réclamation auprès d'une autorité de contrôle	
	Les informations sur le caractère réglementaire ou contractuel du traitement s'il s'agit de la base légale du traitement	
MENTIONS COOKIES	Les finalités des cookies	
	Le recueil du consentement des utilisateurs via « les bandeaux de consentement »	
	Les possibilités de refus des cookies	

7. Politique de sécurité des données

7.1 Mesures générales

Athos Patrimoine met en place des mesures générales de sécurité des données personnelles :

- limiter accès aux locaux ;
- ne pas stocker ou archiver les données personnelles dans des locaux accessibles à tous ;
- installer des alarmes, …

7.2 Mesures de sécurité informatiques

Athos Patrimoine met en place des mesures de sécurité informatiques des données personnelles :

- authentifier les utilisateurs (mot de passe de minimum 8 caractères contenant une majuscule, une minuscule, un chiffre et un caractère spécial)
- déterminer les personnes qui sont habilitées à accéder aux données à caractère personnel ; supprimer les permissions d'accès obsolètes ;
- sécuriser l'informatique mobile ;
- mettre en place des sauvegardes régulières, stocker les supports de sauvegarde dans un endroit sûr, etc.

8. Procédure en cas de violation des données

La violation de données à caractère personnel est une 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.

Sauf dans les cas où la violation n'est pas susceptible d'engendrer un risque pour les droits et libertés des personnes physiques, Athos Patrimoine la notifie à la CNIL dans les meilleurs délais et si possible, au plus tard dans les 72 heures après en avoir pris connaissance.

Un formulaire de notification de violation de données à caractère personnel est à la disposition du responsable de traitement sur le site de la CNIL :
https://www.cnil.fr/sites/default/files/typo/document/CNIL_Formulaire_ Notification_de_Violations.pdf

Si Athos Patrimoine a un sous-traitant, celui-ci devra également notifier au responsable de traitement toute violation de données à caractère personnel dans les meilleurs délais après en avoir pris connaissance.

Athos Patrimoine informera directement la personne concernée de la violation, sauf dans les cas où la violation n'est pas susceptible d'engendrer un risque élevé pour les droits et libertés d'une personne physique, d'informer directement la personne concernée de la violation.