Politique Interne de Confidentialité

1. INTERPRÉTATION

DÉFINITIONS

Pays de protection adéquate : un pays reconnu par la Commission européenne comme ayant des niveaux adéquats de protection des droits et libertés des personnes concernées, étant à la date de cette Politique, Andorre, Argentine, Canada, Îles Féroé, Guernesey, Israël, Île de Man, Jersey, Nouvelle-Zélande, Suisse et Uruguay.

Prise de Décision Automatisée (PDA) : lorsqu'une décision est prise sur la seule base du traitement automatisé (y compris le profilage) qui produit des effets juridiques ou affecte de manière significative un individu. Le RGPD interdit la prise de Prise de Décision Automatisée (sauf si certaines conditions sont remplies) mais pas le Traitement Automatisé.

Traitement Automatisé : toute forme de traitement automatisé d'Informations Personnelles Identifiables (IPI) consistant en l'utilisation de données personnelles pour évaluer certains aspects personnels relatifs à un individu, en particulier pour analyser ou prédire des aspects concernant sa performance au travail, sa situation économique, sa santé, ses préférences personnelles, ses intérêts, sa fiabilité, son comportement, sa localisation ou ses mouvements. Le profilage est un exemple de traitement automatisé.

Nom de l'entreprise : PUBLICATIONS AGORA FRANCE.

Personnel de l'entreprise : tous les Salariés, Freelances, Mandataires, et autres intervenants de l'entreprise.

Consentement : accord qui doit être librement donné, spécifique, informé et qui soit une indication non équivoque des souhaits de la personne concernée par laquelle, à travers une déclaration ou une action positive claire, elle donne un accord concernant le Traitement des informations personnellement identifiables la concernant.

Contrôleur de données : la personne ou l'organisation qui détermine quand, pourquoi et comment traiter les informations personnellement identifiables. Le Contrôleur des Données est responsable de l'établissement de pratiques et des politiques conformes au RGPD. PAF est le contrôleur de données de toutes les données personnelles relatives au Personnel de notre Société et aux données personnelles utilisées dans notre entreprise à des fins commerciales.

Le Sujet des Données : une personne vivante, identifiée ou identifiable à propos de laquelle nous détenons des données personnelles. Les personnes concernées peuvent être des ressortissants ou des résidents de n'importe quel pays et peuvent avoir des droits légaux concernant leurs données personnelles.

Analyse d'impact relative à la protection des données : outils et évaluations utilisés pour identifier et réduire les risques d'une activité de Traitement de données. L'analyse d'impact relative à la protection des données peut être réalisée dans le cadre de *Privacy by Design* (« protection des données dès la conception ») et devrait être réalisée pour tous les principaux programmes de changement de système ou d'entreprise impliquant le Traitement de données personnelles.

Data Protection Manager (DPM) : le Data Protection Manager de l'entreprise est le responsable de la conformité de la protection des données au niveau international. Ce poste est tenu par Paul Xu et Helen Hunsperger.

Espace économique européen (EEE) : les 28 pays de l'UE, ainsi que l'Islande, le Liechtenstein et la Norvège.

Consentement explicite : consentement qui nécessite une déclaration très claire et précise (qui ne se limite pas seulement à une action).

Règlement général sur la protection des données (RGPD) : le Règlement général sur la protection des données (*(UE) 2016/679*). Les données personnelles sont soumises aux garanties légales spécifiées dans le RGPD.

OneTrust : l'application en ligne que la Société et le groupe Agora dans son ensemble utilisent dans le cadre de ses processus de sécurité des données personnelles.

Données personnelles : toute information identifiant une personne concernée ou des informations relatives à une personne concernée que nous pouvons identifier (directement ou indirectement) à partir de ces données seules ou en combinaison avec d'autres identifiants que nous possédons ou auxquels nous pouvons raisonnablement accéder. Les données personnelles comprennent des données sensibles et des données personnelles pseudonymisées, mais excluent les données anonymes ou les données dont l'identité d'un individu a été définitivement supprimée. Les données personnelles peuvent être factuelles (par exemple, un nom, une adresse électronique, des détails de paiement, un lieu ou une date de naissance) ou une opinion sur les actions ou le comportement de cette personne.

Violation de données à caractère personnel : tout acte ou omission compromettant la sécurité, la confidentialité, l'intégrité ou la disponibilité des données personnelles ou les garanties physiques, techniques, administratives ou organisationnelles que nous ou nos fournisseurs de services tiers mettons en place pour les protéger. La perte, ou l'accès non autorisé, la divulgation ou l'acquisition, de données personnelles est une violation de données à caractère personnel.

Protection de la vie privée dès la conception (Privacy by Design) : mise en œuvre efficace des mesures techniques et organisationnelles appropriées pour assurer la conformité avec le RGPD.

Privacy Manager (PM) : personne responsable en premier chef du respect de la protection des données par la Société, étant à la date de ce règlement, Catherine Dourthe, concernant toutes les données personnelles.

Règles/Directives de confidentialité : les règles relatives à la confidentialité des données de la Société, directives fournies pour vous aider à interpréter et à mettre en œuvre cette Politique Interne de Confidentialité et ses procédures annexes.

Avis ou Politiques de Confidentialité : avis distincts définissant les informations pouvant être fournies aux personnes concernées lorsque la Société recueille des informations à leur sujet. Ces avis peuvent prendre la forme de Note générale applicable par un groupe spécifique de personnes (par exemple, la présente Politique Interne de Confidentialité du Personnel de la Société ou la Politique de Confidentialité du site) ou peuvent être des Avis de Confidentialité ponctuelles couvrant un Traitement lié à un objectif spécifique.

Traitement ou processus : toute activité impliquant l'utilisation d'informations personnelles identifiables. Cela comprend l'obtention, l'enregistrement ou la conservation des données, ou l'exécution de toute opération ou ensemble d'opérations sur les données personnelles, y compris l'organisation, la modification, la récupération, l'utilisation, la divulgation, l'effacement ou la destruction. Le traitement comprend également la transmission ou le transfert de données personnelles à des tiers.

Pseudonymisation ou pseudonymisé : remplacement d'informations qui identifient directement ou indirectement un individu avec un ou plusieurs identifiants ou pseudonymes fictifs, de sorte que la personne à laquelle les données se rapportent ne puisse être identifiée sans l'utilisation d'informations supplémentaires censées être conservées séparément et sécurisées.

Notes annexes : les Politiques, les Directives ou les Procédures de la Société liées à la présente Politique sur les

normes de confidentialité et conçues pour protéger les données personnelles, y compris les Lignes Directrices sur la sécurité des données personnelles.

Catégories de données personnelles sensibles : informations révélant l'origine raciale ou ethnique, opinions politiques, croyances religieuses ou similaires, appartenance syndicale, conditions de santé physique ou mentale, vie sexuelle, orientation sexuelle, données biométriques ou génétiques, et données personnelles relatives à des infractions pénales et convictions.

2. INTRODUCTION

2.1 Cette Politique Interne de Confidentialité définit comment PUBLICATIONS AGORA (« **PAF** », « **Nous** », « **notre** », « **nous** », la « **Société** ») traite les données personnelles de nos Clients, Fournisseurs, Salariés, Free-lances et autres tiers.

2.2 Cette Politique Interne de Confidentialité s'applique à toutes les données personnelles que nous traitons, quel que soit le support sur lequel ces données sont stockées ou concernant des Salariés passés ou présents, des Freelances, des Clients ou des Fournisseurs, des utilisateurs de sites Web ou toute autre personne concernée.

2.3 Cette Politique Interne de Confidentialité s'applique à tout le Personnel de l'entreprise (« **vous** », « **votre** »). Vous devez lire, comprendre et respecter cette Politique Interne de Confidentialité lors du traitement des données personnelles en notre nom et suivre une formation sur ses exigences. Cette Politique Interne de Confidentialité définit ce que nous attendons de vous pour que la Société se conforme à la loi applicable. Votre conformité à cette Politique Interne de Confidentialité est obligatoire. Les Directives et Notes annexes sont disponibles pour vous aider à interpréter et à agir conformément à cette Politique Interne de Confidentialité. Vous devez également vous conformer à toutes ces politiques et règles de confidentialité. Toute violation de cette Politique Interne de Confidentialité peut entraîner des mesures disciplinaires.

2.4 Cette Politique Interne de Confidentialité (avec les Notes annexes) est un document interne et ne peut être partagée avec des tiers, des clients ou des organismes de réglementation sans l'autorisation préalable du DPM.

3. PORTÉE

3.1 Nous sommes conscients que le traitement correct et légal des données personnelles maintiendra la confiance dans l'organisation et assurera le succès des opérations commerciales. Protéger la confidentialité et l'intégrité des données personnelles est une responsabilité critique que nous prenons au sérieux en permanence. La Société est exposée à des amendes pouvant aller jusqu'à 20 millions EUR ou 4% du chiffre d'affaires annuel mondial, selon le montant le plus élevé et en fonction de la violation, pour non-respect des dispositions du RGPD.

3.2 Tous les directeurs et les managers sont responsables de s'assurer que tout le Personnel de l'entreprise se conforme à cette Politique de Confidentialité et doivent mettre en œuvre des pratiques, des processus, des contrôles et une formation appropriés pour assurer cette conformité.

3.3 Le DPM est responsable de la supervision de cette norme de confidentialité au niveau international et, le cas échéant, de l'élaboration de Notes annexes. Le Privacy Manager (PM) est responsable de la supervision de cette norme de confidentialité au niveau de la Société.

3.4 Veuillez contacter le PM pour toute question concernant le fonctionnement de cette Politique Interne de Confidentialité ou le RGPD ou si vous craignez que cette Politique de Confidentialité ne soit pas respectée ou non. Vous devez notamment les contacter dans les cas suivants :

3.4.1 si vous n'êtes pas sûr de la base légale sur laquelle vous vous fondez pour traiter les données personnelles (y compris les intérêts légitimes utilisés par la Société) (voir section 5 ci-dessous);

3.4.2 si vous devez rédiger des Avis de Confidentialité (voir la section 5 ci-dessous) ;

3.4.3 si vous n'êtes pas sûr de la période de conservation pour les informations personnelles identifiables en cours de Traitement (voir la section 9 ci-dessous) ;

3.4.4 si vous n'êtes pas certain des mesures de sécurité ou autres que vous devez mettre en œuvre pour protéger les données personnelles (voir la section 0 ci-dessous) (dans ce cas, vous devez également contacter le PM) ;

3.4.5 s'il y a eu violation de données personnelles (section 0 ci-dessous). Dans ce cas, vous devez également contacter le PM ;

3.4.6 si vous ne savez pas sur quelle base juridique transférer des données personnelles en dehors de l'EEE (voir la section 11ci-dessous) ;

3.4.7 si vous avez besoin d'aide concernant les droits invoqués par une personne concernée (voir la section 12) ;

3.4.8 chaque fois que vous initiez, ou changez de façon significative, un Traitement important de données personnelles qui nécessitera probablement une analyse d'impact relative à la protection des données (voir la section 13 13ci-dessous) ou prévoyez d'utiliser des données personnelles à des fins autres que celles pour lesquelles elles ont été collectées ;

3.4.9 si vous prévoyez d'entreprendre des activités impliquant un Traitement automatisé, y compris le profilage ou la prise de décision automatisée (voir la section 13.12 ci-dessous) ;

3.4.10 si vous traitez des données personnelles sensibles ;

3.4.11 si vous avez besoin d'aide pour vous conformer à la loi applicable dans le cadre d'activités de marketing direct (voir la section 13 ci-dessous) ; ou

3.4.12 si vous avez besoin d'aide pour des contrats ou d'autres domaines relatifs au partage de renseignements personnels avec des tiers (y compris nos fournisseurs) (voir la section 13 ci-dessous).

4. PRINCIPES DE PROTECTION DES DONNÉES

4.1 Nous adhérons aux principes relatifs aux traitements des données personnelles définies dans le RGPD qui exigent que les données personnelles soient :

4.1.1 Traitées légalement, équitablement et de manière transparente (légalité, équité et transparence).

4.1.2 Recueillies uniquement à des fins précises, explicites et légitimes (limitation de la finalité).

4.1.3 Adéquates, pertinentes et limitées à ce qui est nécessaire par rapport aux fins pour lesquelles elles sont traitées (minimisation des données).

4.1.4 Précises et si nécessaire mises à jour (précision).

4.1.5 Non conservées sous une forme permettant l'identification des Sujets des données plus longtemps que nécessaire aux fins pour lesquelles les données sont traitées (limite de stockage).

4.1.6 Traitées de manière à assurer sa sécurité en utilisant des mesures techniques et organisationnelles appropriées pour se protéger contre tout traitement non autorisé ou illégal et contre la perte, la destruction ou les dommages accidentels (sécurité, intégrité et confidentialité).

4.1.7 Non transférées dans un autre pays sans protection appropriée (limitation de transfert).

4.1.8 Mises à la disposition des personnes concernées et des personnes concernées autorisées à exercer certains droits relatifs à leurs données personnelles (droits et demandes des personnes concernées).

4.2 Nous sommes responsables et devons être en mesure de démontrer la conformité aux principes de protection des données énumérés ci-dessus (responsabilité).

5. LÉGALITÉ, ÉQUITÉ, TRANSPARENCE

Légalité et équité

5.1 Les données personnelles doivent être traitées de manière légale, équitable et transparente à l'égard de la personne concernée.

5.2 Vous ne pouvez collecter, traiter et partager les données personnelles que de manière juste et légale et à des fins spécifiques. Le RGPD limite nos actions concernant les données personnelles à des fins légales spécifiées. Ces restrictions ne sont pas destinées à empêcher le traitement, mais à garantir que nous traitons les données personnelles de manière équitable et sans affecter le Sujet des Données.

5.3 Le RGPD permet le traitement à des fins spécifiques, dont les plus pertinentes pour la Société sont :

5.3.1 la personne concernée a donné son **consentement** ;

5.3.2 le traitement est **nécessaire pour l'exécution d'un contrat** avec la personne concernée ;

5.3.3 de poursuivre nos **intérêts légitimes** sauf s'ils prévalent les intérêts ou les libertés et droits fondamentaux des personnes concernées (les finalités pour lesquelles nous traitons les données

personnelles pour des intérêts légitimes doivent être précisées dans les Politiques de Confidentialité applicables) ; et

5.3.4 pour **répondre à nos obligations légales et de conformité**.

5.4 Vous devez identifier et documenter la base juridique invoquée pour chaque activité de Traitement. Les fondements juridiques doivent être enregistrés conformément aux règles de confidentialité.

Consentement

5.5 Un contrôleur de données ne doit traiter les informations personnelles que sur la base d'au moins une des bases légales énoncées dans le RGPD, qui comprennent le consentement.

5.6 Les Sujets des Données consentent au traitement de leurs données personnelles s'ils indiquent clairement un accord soit par une déclaration, soit par une action positive au Traitement. Le consentement nécessite une action positive, de sorte qu'il est peu probable que le silence, les cases pré-cochées ou l'inactivité soient suffisants. Si le consentement est donné dans un document qui traite d'autres questions, alors le consentement doit être séparé de ces autres questions.

5.7 Les Sujets des Données doivent être facilement en mesure de retirer le consentement au Traitement à tout moment et le retrait doit être promptement respecté. Le consentement peut avoir besoin d'être actualisé si vous avez l'intention de traiter des données personnelles pour un but différent et incompatible avec ce qui a été mentionné lorsque le Sujet des Données a donné son consentement initial.

5.8 À moins de pouvoir compter sur une autre base légale de Traitement, le consentement explicite est généralement requis pour le traitement des données personnelles sensibles et pour la prise de décision automatisée. Principalement, nous nous baserons sur une autre base légale (et n'exigerons pas de consentement explicite) pour traiter la plupart des données personnelles, mais lorsque le consentement explicite est requis, vous devez envoyer un Avis de Confidentialité aux Sujets des Données pour capturer leur consentement explicite.

5.9 Vous devrez prouver que le consentement a été recueilli et conserver les preuves de tous les consentements afin que la Société puisse démontrer qu'elle se conforme aux exigences du consentement.

Transparence (notifier les personnes concernées)

5.10 Le RGPD exige que les contrôleurs de données fournissent des informations spécifiques et détaillées aux Sujets des Données selon que les informations ont été collectées directement auprès des Sujets des Données ou ailleurs. De telles informations doivent être fournies au moyen d'Avis de Confidentialité appropriés, qui doivent être concis, transparents, intelligibles, facilement accessibles et rédigés dans un langage clair et simple afin qu'un Sujet des Données concerné puisse facilement les comprendre.

5.11 Chaque fois que nous collectons des données personnelles directement auprès des Sujets des Données, notamment à des fins de ressources humaines ou de recrutement, nous devons lui fournir toutes les informations requises par le RGPD, y compris l'identité du Contrôleur des Données et du PM, divulguer, protéger et conserver ces renseignements personnels selon un Avis de Confidentialité qui doit être présenté lorsque le Sujet des Données fournit ses données personnelles pour la première fois.

5.12 Lorsque les données personnelles sont collectées indirectement (par exemple, à partir d'une source tierce ou publiquement disponible), vous devez fournir au Sujet des Données toutes les informations requises par le RGPD le plus rapidement possible après la collecte / la réception des données. Vous devez également vérifier que les données personnelles ont été collectées par le tiers conformément au RGPD et sur une base qui est compatible avec notre traitement de ces données personnelles.

6. LIMITATION DE L'OBJECTIF

6.1 Les données personnelles sont recueillies uniquement à des fins précises, explicites et légitimes (limitation de la finalité). Elles ne doivent pas être traitées d'une manière incompatible avec ces objectifs.

6.2 Vous ne pouvez pas utiliser les données personnelles à des fins nouvelles, différentes ou incompatibles comparées à celles indiquées lors de leur première obtention, sauf si vous avez informé le Sujet des Données des nouveaux objectifs et qu'il y a consenti si nécessaire.

7. MINIMISATION DE DONNÉES

7.1 Les données personnelles doivent être adéquates, pertinentes et limitées à ce qui est nécessaire par rapport aux fins pour lesquelles elles sont traitées (minimisation des données).

7.2 Vous ne pouvez traiter les données personnelles que dans le cadre de votre travail. Vous ne pouvez pas traiter les données personnelles pour une raison indépendante de votre travail.

7.3 Vous ne pouvez collecter que les données personnelles dont vous avez besoin pour votre travail : ne collectez pas de données excessives. Assurez-vous que toutes les données personnelles recueillies sont adéquates et pertinentes aux fins prévues.

7.4 Vous devez vous assurer que lorsque les données personnelles ne sont plus nécessaires à des fins spécifiques, elles sont supprimées ou rendues anonymes conformément aux directives de conservation des données de la Société.

8. PRÉCISION

8.1 Les données personnelles doivent être précises et si nécessaire mises à jour (précision). Elles doivent être corrigées ou supprimées sans délai si elles sont inexactes.

8.2 Vous vous assurerez que les données personnelles que nous utilisons et conservons sont exactes, complètes, tenues à jour et pertinentes aux fins pour lesquelles nous les avons recueillies. Dans la mesure du possible, vous devez vérifier l'exactitude des données personnelles au moment de la collecte et à intervalles réguliers par la suite. Vous devez prendre toutes les mesures raisonnables pour détruire ou modifier les données personnelles inexactes ou périmées.

9. LIMITATION DE L'OBJECTIF

9.1 Les données personnelles ne doivent pas être conservées sous une forme permettant l'identification des Sujets des Données plus longtemps que nécessaire aux fins pour lesquelles les données sont traitées (limite de stockage).

9.2 Vous ne devez pas conserver les données personnelles sous une forme permettant l'identification des Sujets des Données plus longtemps que nécessaire aux fins commerciales légitimes pour lesquelles nous les avons initialement collectées, y compris pour satisfaire aux exigences légales, comptables ou autres exigences réglementaires.

9.3 La Société maintiendra des politiques et des lignes directrices sur la conservation des données afin de s'assurer que les données personnelles soient supprimées après un délai raisonnable aux fins pour lesquelles elles étaient détenues, à moins qu'une loi n'exige que ces données soient conservées pendant une période minimale.

9.4 Vous prendrez toutes les mesures raisonnables pour détruire ou effacer de nos systèmes toutes les données personnelles dont nous n'avons plus besoin conformément à tous les délais et politiques de conservation des documents applicables de la Société. Cela inclut d'exiger des tiers de supprimer ces données le cas échéant.

9.5 Vous vous assurerez que les Sujets des Données sont informées de la période pour laquelle les données sont stockées et de la façon dont cette période est déterminée dans tout Avis ou Politique de Confidentialité applicable.

10. INTÉGRITÉ DE SÉCURITÉ ET CONFIDENTIALITÉ

Protéger les données personnelles

10.1 Les données personnelles doivent être protégées par des mesures techniques et organisationnelles appropriées contre tout traitement non autorisé ou illicite, ainsi que contre la perte accidentelle, la destruction ou l'endommagement.

10.2 Nous développerons, mettrons en œuvre et maintiendrons des sauvegardes adaptées à notre taille, portée et activité, nos ressources disponibles, la quantité de données personnelles que nous possédons ou conservons pour le compte d'autrui et les risques identifiés (y compris le cryptage et la pseudonymisation le cas échéant). Nous évaluerons et testerons régulièrement l'efficacité de ces mesures de protection afin d'assurer la sécurité de notre traitement des données personnelles. Vous êtes responsable de la protection des données personnelles que nous détenons. Vous devez mettre en œuvre des mesures de sécurité raisonnables et appropriées contre le traitement illégal ou non autorisé des données personnelles et contre la perte accidentelle ou les dommages causés aux données personnelles. Vous devez faire particulièrement attention à la protection des données personnelles sensibles, notamment à la perte et à l'accès non autorisé, l'utilisation ou la divulgation.

10.3 Vous devez suivre toutes les directives, procédures et technologies que nous avons mises en place pour maintenir la sécurité de toutes les données personnelles du point de collecte au point de destruction.

10.4 Vous devez maintenir la sécurité des données en protégeant la confidentialité, l'intégrité et la disponibilité des données personnelles, définies comme suit :

10.4.1 La confidentialité signifie que seules les personnes qui en ont besoin sont autorisées à accéder et à utiliser les données personnelles.

10.4.2 L'intégrité signifie que les données personnelles sont exactes et appropriées aux fins pour lesquelles elles sont traitées.

10.4.3 La disponibilité signifie que les utilisateurs autorisés peuvent accéder aux données personnelles lorsqu'ils en ont besoin à des fins autorisées.

10.5 Les transferts à des tiers fournisseurs doivent respecter les dispositions de la présente section ainsi que la clause 13.22.

10.6 Vous devez respecter nos Lignes Directrices de Confidentialité et ne pas tenter de contourner les mesures de protection administratives, physiques et techniques que nous mettons en œuvre et maintenons conformément au RGPD et aux normes pertinentes pour protéger les renseignements personnels.

Signaler une atteinte à la protection des données

10.7 Le RGPD exige que les contrôleurs de données notifient toute violation de données personnelles à l'organisme de réglementation compétent et, dans certains cas, au(x) Sujet(s) des Données concerné(s).

10.8 Nous avons mis en place des Lignes Directrices pour traiter toute violation présumée des données personnelles et aviser les Sujets des Données ou tout organisme de réglementation pertinent lorsque nous sommes légalement tenus de le faire.

10.9 Si vous savez ou soupçonnez qu'une violation de données personnelles a eu lieu, n'essayez pas d'enquêter vous-même. Contactez immédiatement le PM, le DPM et le service informatique et suivez le processus de réponse aux incidents de données. Vous devez conserver toutes les preuves relatives à l'atteinte potentielle aux données personnelles.

11. LIMITATION DU TRANSFERT

11.1 Le RGPD limite les transferts de données à des pays en dehors de l'EEE afin de garantir que le niveau de protection des données accordé aux individus par le RGPD ne soit pas compromis. Vous transférez des données personnelles provenant d'un pays au-delà des frontières lorsque vous transmettez, envoyez, consultez ou accédez à ces données dans un pays différent.

11.2 Vous ne pouvez transférer des données personnelles en dehors de l'EEE que si l'une des conditions suivantes s'applique :

11.2.1 le transfert est à un pays de protection adéquat ;

11.2.2 des garanties appropriées sont en place avant le transfert, y compris la présence d'une clause contractuelle type approuvée par la Commission européenne, dont une copie peut être obtenue auprès du PM et du DPM :

11.2.3 le Sujet des Données a fourni un consentement explicite au transfert proposé après avoir été informé de tout risque potentiel ; ou

11.2.4 le transfert est nécessaire pour l'une des autres raisons énoncées dans le RGPD, y compris l'exécution d'un contrat entre nous et le Sujet des Données, pour établir, exercer ou défendre des réclamations juridiques et, dans certains cas limités, pour nos intérêts légitimes.

11.3 Vous devez vous conformer aux Directives de la Société sur les transferts de données transfrontaliers énoncées dans les Directives de sécurité des données.

12. DROITS ET DEMANDES DU PERSONNES CONCERNEES

12.1 Les Sujets des Données ont des droits quand il s'agit de la façon dont nous gérons leurs données personnelles. Ceux-ci comprennent les droits suivants :

12.1.1 les Sujets des Données doivent être facilement en mesure de retirer le consentement au traitement à tout moment et le retrait doit être promptement respecté ;

12.1.2 recevoir certaines informations sur les activités de Traitement du Contrôleur des Données ;

12.1.3 demander l'accès à leurs données personnelles que nous détenons ;

12.1.4 limiter notre utilisation de leurs données personnelles à des fins de marketing direct ;

12.1.5 nous demander d'effacer leurs données personnelles si elles ne sont plus nécessaires par rapport aux finalités pour lesquelles elles ont été collectées ou traitées, ou pour rectifier des données inexactes ou pour compléter des données incomplètes ;

12.1.6 restreindre le traitement dans des circonstances particulières ;

12.1.7 contester le traitement des Données qui a été justifié sur la base de nos intérêts légitimes ;

12.1.8 demander une copie d'un accord en vertu duquel les données personnelles sont transférées en dehors de l'EEE ;

12.1.9 s'opposer aux décisions basées uniquement sur le traitement automatisé, y compris le profilage ;

12.1.10 empêcher tout traitement susceptible de causer des dommages ou toute détresse à un Sujet des Données ou à toute autre personne ;

12.1.11 être informé d'une infraction aux données personnelles susceptible d'entraîner un risque élevé pour ses droits et libertés ;

12.1.12 déposer une plainte auprès de l'autorité de surveillance (CNIL en France) ; et

12.1.13 dans des circonstances limitées, recevoir ou demander que leurs renseignements personnels soient transférés à un tiers dans un format structuré, communément utilisé (portabilité).

12.2 Vous devez vérifier l'identité d'une personne qui demande des données sous l'un des droits énumérés ci-dessus (ne

vous laissez pas persuader de divulguer des données personnelles sans autorisation appropriée).

12.3 Vous devez immédiatement transmettre toute demande de Sujet des Données que vous avez reçue au PM.

13. RESPONSABILITÉ

Mesures techniques et organisationnelles

13.1 Le Contrôleur des Données doit mettre en œuvre de manière efficace les mesures techniques et organisationnelles appropriées afin de garantir le respect des principes de protection des données. Il est responsable du respect des principes de protection des données et doit être en mesure d'en démontrer le respect.

13.2 La Société doit disposer de ressources et de contrôles adéquats pour assurer et documenter la conformité au RGPD, notamment :

13.2.1 la mise en œuvre de la protection de la vie privée dès la conception lors du traitement des données personnelles et de la réalisation de l'analyse d'impact relative à la protection des données lorsque le Traitement présente un risque élevé pour les droits et libertés des Sujets des Données ;

13.2.2 intégrer la protection des données dans les documents internes, y compris la présente Politique Interne de Confidentialité et les Notes annexes ;

13.2.3 former régulièrement le Personnel de l'entreprise sur le RGPD, la présente Politique Interne de Confidentialité et les Notes Annexes, ainsi que sur les questions de protection des données personnelles. La Société doit tenir un registre des présences aux formations du Personnel de la Société ; et

13.2.4 tester régulièrement les mesures de protection de la vie privée mises en œuvre et effectuer des audits et des vérifications périodiques pour évaluer la conformité, notamment en utilisant les résultats des tests pour démontrer l'effort d'amélioration de la conformité.

Tenue des registres

13.3 Le RGPD nous oblige à tenir des registres complets et précis de toutes nos activités de Traitement des données.

13.4 Vous devez conserver et tenir à jour des registres précis reflétant nos Traitements, y compris des enregistrements des consentements des Sujets des Données et des bases légales pour l'obtention de consentements. Cela signifie maintenir les archives des promotions, des bons de commande, des pages d'inscription (Sign-ups), des Notes de Confidentialité, etc. Cela signifie également que vous devez utiliser OneTrust et le maintenir à jour à tout moment.

13.5 Ces enregistrements doivent inclure, au minimum, le nom et les coordonnées du Contrôleur des Données, du DPM et du PM, des descriptions claires des types d'informations, des types de données, des Traitements, des destinataires tiers des informations personnelles, les emplacements de stockage des données personnelles, les transferts de données personnelles, la période de rétention des données personnelles et une description des mesures de sécurité en place.

Formation et audit

13.6 Nous sommes tenus de veiller à ce que tout le Personnel de l'entreprise ait suivi une formation adéquate pour lui permettre de se conformer aux lois sur la confidentialité des données. Nous devons également tester régulièrement nos systèmes et processus pour évaluer la conformité.

13.7 Vous devez suivre toutes les formations obligatoires sur la confidentialité des données et vous assurer que votre équipe suit une formation similaire.

13.8 Vous devez examiner régulièrement tous les systèmes et processus sous votre contrôle pour vous assurer qu'ils sont conformes à la présente Politique Interne de Confidentialité et vérifier que des contrôles et des ressources adéquats sont en place pour garantir une utilisation et une protection adéquates des données personnelles.

« Privacy by design » et analyse d'impact relative à la protection des données

13.9 Nous sommes tenus de mettre en œuvre des mesures de protection dès la conception pour tout Traitement de données personnelles, en mettant en œuvre, de manière efficace, des mesures techniques et organisationnelles appropriées (comme la pseudonymisation), afin de garantir le respect des principes de confidentialité des données.

13.10 Vous devez évaluer quelles mesures de protection intégrées peuvent être mises en œuvre sur tous les programmes / systèmes / processus qui traitent les données personnelles en tenant compte des éléments suivants :

13.10.1 être à la pointe ;

13.10.2 le coût de la mise en œuvre ;

13.10.3 la nature, la portée, le contexte et les objectifs du traitement ; et

13.10.4 les risques de variation de la probabilité et de la gravité des droits et libertés des Sujets des Données posés par le traitement.

13.11 Les Contrôleurs des Données doivent également effectuer des analyses d'impact relatives à la protection des données concernant le traitement à haut risque. Ces analyses doivent être complétées sur OneTrust.

13.12 Vous devriez mener une analyse d'impact relative à la protection des données (et discuter de vos conclusions avec le PM) lors de la mise en œuvre de grands programmes de changement de système ou de procédure impliquant le traitement des données personnelles, y compris :

13.12.1 l'utilisation de nouvelles technologies (programmes, systèmes ou processus) ou l'évolution des technologies (programmes, systèmes ou processus) ;

13.12.2 traitement automatisé comprenant le profilage et la prise de décision automatisée ; et

13.12.3 une surveillance à grande échelle et systématique d'une audience/public (cela ne couvre pas l'utilisation de cookies, etc.).

13.13 Une analyse d'impact relative à la protection des données doit inclure :

13.13.1 une description du Traitement, de ses objectifs et des intérêts légitimes du Contrôleur des Données, le cas échéant ;

13.13.2 une évaluation de la nécessité et de la proportionnalité du Traitement par rapport à son objectif;

13.13.3 une évaluation du risque pour les individus ; et

13.13.4 les mesures d'atténuation des risques en place et la démonstration de conformité.

Marketing direct

13.14 Nous sommes soumis à certaines règles et lois sur la protection de la vie privée lors de la commercialisation auprès de nos clients.

13.15 Par exemple, le consentement préalable d'une personne concernée est requis pour le marketing direct (que ce soit par courrier électronique, poste ou téléphoniques) lorsque les règles de l' « opt-in » ne s'appliquent pas. Pour les clients existants, la règle de l'« opt in » permet aux organisations d'envoyer du marketing si elles ont obtenu des coordonnées lors d'une vente à cette personne, si elles commercialisent leurs propres produits ou services similaires, et si elles ont donné à la personne la possibilité de s'opposer au marketing direct (lors de la première collecte des données et dans chaque message ultérieur).

13.16 Le droit de s'opposer au marketing direct doit être explicitement offert au Sujet des Données de manière intelligible, de sorte qu'il se distingue clairement des autres informations. Cela inclut un lien de désabonnement dans les e-mails.

13.17 L'objection d'un Sujet des Données au marketing direct doit être promptement respectée. A tout moment, si un client s'y oppose, ses coordonnées doivent être supprimées dès que possible. La suppression consiste à conserver juste assez d'informations pour s'assurer que ses préférences en matière de marketing soient respectées dans le futur.

13.18 Vous devez vous conformer aux lignes directrices de la Société sur le marketing direct auprès des clients, énoncées dans le document *Astuces pour les marqueteurs concernant le RGPD (GDPR Tips for Marketers)*.

Partage de données personnelles et fournisseurs tiers

13.19 En règle générale, nous ne sommes pas autorisés à partager des renseignements personnels avec des tiers à moins que certaines garanties et certains arrangements contractuels aient été mis en place.

13.20 Vous ne pouvez partager les données personnelles que nous détenons avec un autre salarié, sous-traitant ou autre intervenant d'Agora que si le destinataire en a besoin dans le cadre de son travail et en vous assurant que le transfert respecte les restrictions de transfert transfrontalières applicables énoncées à la clause 11.

13.21 Vous ne pouvez partager les données personnelles que nous détenons avec des tiers, tels que nos sous-traitants que si :

13.21.1 ils ont besoin de connaître l'information aux fins de fournir les services sous contrat ;

13.21.2 le partage des données personnelles est conforme à l'Avis de Confidentialité fourni à la personne concernée et, si nécessaire, le consentement du Sujet des Données a été obtenu ;

13.21.3 le tiers a accepté de se conformer aux normes, politiques et directives de sécurité des données requises et a mis en place des mesures de sécurité adéquates ;

13.21.4 le transfert est sécurisé et respecte toutes les restrictions de transfert transfrontalières applicables ;

13.21.5 le tiers a rempli les questionnaires adéquats sur OneTrust ; et

13.21.6 un contrat écrit et signé contenant des clauses types approuvées dans le cadre du RGPD a été obtenu.

13.22 Vous devez vous conformer aux Directives de la Société sur les transferts de données transfrontaliers énoncées dans les Lignes Directives.

MODIFICATIONS APPORTÉES À CETTE POLITIQUE INTERNE DE CONFIDENTIALITÉ

13.23 Nous nous réservons le droit de modifier cette Politique Interne de Confidentialité à tout moment sans préavis. Veuillez donc vérifier régulièrement que vous disposez de la dernière version de cette Politique Interne de Confidentialité.

13.24 Nous avons révisé cette Politique Interne de Confidentialité pour la dernière fois le 25 Mai 2018.

13.25 Cette Politique Interne de Confidentialité ne remplace pas les lois et réglementations nationales applicables en matière de confidentialité des données dans les pays où la Société est active.

13.26 Certains pays peuvent avoir des variantes locales de cette Politique Interne de Confidentialité, disponibles sur demande auprès du DPM.

ACCUSÉ DE RÉCEPTION ET D'EXAMEN DE LA POLITIQUE INTERNE DE CONFIDENTIALITE ET DES NOTICES ANNEXES

Je sous-signé [NOM DU SALARIE]

Déclare, par la présente, avoir reçu et lu une copie de la Politique Interne de Confidentialité de PUBLICATIONS AGORA France (datée du 25 mai 2018), ainsi que les notices Lignes Directrices annexes.

Je déclare avoir compris cette Politique Interne de Confidentialité et m'engage à la respecter.

Fait à
Le

Signature précédée de la mention « Lu et approuvé »