



Politique synthétique de gestion des données à caractère personnel

1. Préambule et définitions principales	1
2. Champ d'application	2
3. Engagements en matière de protection des Données personnelles	2
4. Collecte de données personnelles : objectifs, destinataires et principes	2
5. Droits des personnes concernées	3
6. Mesures de sécurisation des Données personnelles	4
7. Registre et archivage	4
8. Coopération avec les autorités	4
9. Audit	5
10. Violations des Données personnelles	5

1. Préambule et définitions principales

Cette politique vise à décrire le processus de gestion des données personnelles (données personnelles) au sein du Groupe ABC arbitrage conformément à la réglementation européenne et française sur les données personnelles.

« **Données à Caractère Personnel** » ou « **Données personnelles** » : désignent toute information se rapportant à une personne physique identifiée ou identifiable; 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 ;

« **Données sensibles** » : désigne 3 types de données, à savoir : (i) les donnée(s) révélant une origine raciale ou ethnique, des opinions politiques, des croyances religieuses ou philosophiques ou l'adhésion à un syndicat, (ii) les donnée(s) sur la santé ou la sexualité, (iii) les donnée(s) lié(es) à des délits, des condamnations ou des mesures de sécurité, N° d'identification national unique (NIR pour la France) ;

« **Personne concernée** » : désigne toute personne à laquelle se rapportent des données personnelles, identifiée ou identifiable directement ou indirectement ;

« **Traitement des Données personnelles** » signifie toute opération ou groupe d'opérations appliqué aux Données personnelles, quel que soit le support de service en ligne en question et le procédé utilisé.

2. Champ d'application

Cette politique s'applique à toute personne concernée et à toute société du Groupe directement responsable du traitement de données personnelles pour son compte ou pour le compte de tout client ou de toute autre société du Groupe. Cette politique et les bonnes pratiques qui y sont détaillées servent également de référence pour les sociétés du groupe qui ne sont pas formellement soumises aux obligations découlant du règlement général de l'UE sur la protection des données (RGPD).

Le groupe met en application toutes les spécificités locales éventuelles résultant de contraintes locales existantes.

3. Engagements en matière de protection des Données personnelles

ABC ARBITRAGE, Société Anonyme à Conseil d'administration, immatriculée au RCS de Paris sous le numéro 400 343 182, dont le siège social est situé 18, rue du Quatre Septembre 75002 Paris, est le responsable du traitement.

En tant que responsable de traitement des Données personnelles, le Groupe veille à la protection, la confidentialité, la non altération, la disponibilité et la sécurité des Données personnelles qui lui sont confiées. Il prend l'ensemble des mesures nécessaires afin de fournir une information claire et transparente sur la collecte et le traitement de ces données et veille à la mise en place de mesures techniques et organisationnelles nécessaires pour les protéger et assurer que leur traitement est conforme à la réglementation applicable.

Les données personnelles contenant des Données sensibles feront l'objet d'un traitement dans des cas très limités, et sous conditions strictes (consentement de la personne, données déjà dans le domaine public, traitement essentiel à une action en justice ou explicitement autorisé par la législation nationale).

4. Collecte de données personnelles : objectifs, destinataires et principes

Dans le cadre de la prestation de service ou du respect de ses obligations légales, le Groupe est amené à collecter des Données personnelles, pour, par exemple, la gestion d'une relation contractuelle, de candidatures, des contentieux, le respect de ses obligations légales et réglementaires, la prévention de la fraude, le suivi de l'actionnariat, l'accès aux locaux et aux systèmes d'informations, etc. Dans certains cas, la suppression des Données personnelles pourra avoir comme conséquence l'impossibilité pour le Groupe de poursuivre l'exécution du contrat ou de satisfaire à ses obligations légales.

Les destinataires des Données personnelles sont les sociétés du Groupe, ses partenaires et les autorités de contrôles.

Les Données personnelles sont traitées conformément aux principes essentiels suivants :

- **Finalité** : avant tout traitement de données personnelles, une finalité doit être déterminée.
- **Fondement juridique** : le traitement de données personnelles doit reposer sur un fondement juridique (application d'une obligation légale ou d'un contrat). Dans le cas contraire, il doit présenter un intérêt légitime, qui ne porte pas préjudice à la vie privée.
- **Minimiser les données personnelles** : la collecte des données personnelles doit être strictement nécessaire à la finalité déterminée.
- **Qualité des données personnelles** : les données personnelles doivent être exactes et actualisées pendant tout leur cycle de vie.
- **Durée de conservation des données personnelles** : les données personnelles ne doivent pas être conservées plus longtemps que nécessaire au regard de la finalité. Ces durées sont établies en amont et pour tout le groupe en fonction des différents types de données et finalités.
- **Mesures de sécurité** : des mesures de sécurité sont mises en place afin de protéger les données personnelles, notamment via le Système d'Information.
- **Sous-traitance**. Afin d'assurer la protection des Données personnelles et du respect des droits pour les opérations avec un tiers destinataire, le Groupe met en place les sécurités nécessaires avec ses sous-traitants éventuels, notamment via un contrat écrit et un accord de confidentialité spécifique. Le sous-traitant devra présenter des garanties techniques et organisationnelles appropriées et traiter les données conformément aux principes listés ci-dessus.

5. Droits des personnes concernées

Dans l'objectif de permettre un contrôle des usages des Données personnelles, les personnes concernées disposent des droits suivants :

- **droit d'opposition** aux traitements des Données personnelles ;
- **droit d'information** sur les usages des Données personnelles ;
- **droit d'accès et d'information** sur les données détenues et leur traitement ;
- **droit de rectification** si les données personnelles sont inexactes ou incomplètes ;
- **droit à l'effacement** des données personnelles dans certaines circonstances ;
- **droit à la portabilité** : dans certaines circonstances et uniquement aux données personnelles fournies directement à toute société du Groupe ;
- **droit à la limitation** du traitement de Données personnelles ;
- **droit de définir des directives** relatives à la conservation, l'effacement et la communication des Données personnelles après la mort de la personne concernée ;
- **droit de déposer une réclamation** auprès de l'autorité de contrôle nationale ;
- **droit de retrait du consentement** au traitement de données personnelles.

Ces droits peuvent être exercés par email accompagné d'une copie d'une pièce d'identité (carte nationale d'identité ou passeport) à l'adresse gdpr@abc-arbitrage.com. Des

précisions sur le contenu de ces droits peuvent également être obtenues en contactant la même adresse. Des éléments de réponse sont fournis dans les meilleurs délais.

6. Mesures de sécurisation des Données personnelles

Chaque société du Groupe met en place des mesures de sécurité organisationnelles et techniques adaptées pour protéger les Données personnelles contre toute intrusion malveillante, perte, altération ou divulgation à des tiers non autorisés.

L'accès aux données personnelles est limité aux collaborateurs du Groupe ou prestataires agissant pour son compte, qui en ont besoin dans le cadre de l'exécution de leurs missions. Ceux-ci sont liés par un devoir de confidentialité et s'exposent à des mesures disciplinaires prévues par le règlement intérieur (du blâme au licenciement pour faute) si elles ne respectent pas les obligations et principes décrits dans cette politique. Chacun est encouragé à faire preuve de prudence pour empêcher tout accès non autorisé à ses Données personnelles, y compris sur les équipements numériques, conformément à la charte d'usage du système d'information, annexée au règlement intérieur. Une présentation sur la gestion des données personnelles est partagée à l'ensemble des collaborateurs tous les ans et des rappels leur sont régulièrement envoyés.

Les transferts de données personnelles dans ou en dehors de l'Espace économique européen sont soumis aux mêmes dispositions.

7. Registre et archivage

Le Groupe, ou ses sous-traitants éventuels, s'engage à tenir à jour un Registre et aura la responsabilité de s'assurer que tout nouveau traitement de Données personnelles soit consigné avec les informations pertinentes (nom et les coordonnées du responsable du traitement, finalités du traitement, catégories de personnes concernées et des données personnelles, destinataires des données personnelles, garanties appropriées, délais prévus pour l'effacement des données, description générale des mesures de sécurité techniques et organisationnelles).

Le processus d'archivage des données personnelles stockées au sein du Groupe fait l'objet d'une procédure spécifique dont l'accès est restreint aux administrateurs réseaux, afin d'être en conformité avec la réglementation européenne et française sur les données personnelles.

8. Coopération avec les autorités

Le Groupe s'engage à maintenir de bonnes relations avec la Commission nationale de l'informatique et des libertés (CNIL) ou toute autre autorité de protection des données personnelles. À cet effet, il coopérera avec et acceptera d'être audité par la CNIL et de suivre ses conseils sur des affaires dont celle-ci pourrait avoir connaissance.

9. Audit

Les risques liés au traitement des données personnelles sont identifiés et formalisés dans la cartographie des risques du groupe.

Le Groupe a intégré dans son programme de contrôle de deuxième niveau l'évaluation de conformité vis-à-vis de l'archivage et du respect des contraintes relatives à la gestion des données personnelles. Le contrôle périodique sur les systèmes d'informations peut également inclure ces points.

10. Violations des Données personnelles

Si une violation de Données personnelles est constatée, une procédure spécifique sera appliquée, avec les étapes suivantes :

1. Identification d'une éventuelle violation de Données personnelles
2. Constitution d'une « fiche de remontée d'incident » et information de la direction générale
3. Analyse de l'incident pour évaluer ses impacts
4. Communication de l'incident aux parties prenantes
5. Gestion de la communication à l'égard des personnes impactées
6. Notification de l'autorité de contrôle dans les 72h suivant la détection de la faille
7. Confirmation de la prise en compte de la demande de suppression des données divulguées
8. Clôture de la « fiche de remontée d'incident »
9. Rédaction d'un rapport d'incident et identification des actions de remédiation