Procédure : Protection de données personnelles et confidentielles en AFS

1 Contexte 2

2 Data Privacy Liaison Officer de la région AFS 2

3 Formation du personnel 2

4 Collecte, gestion et destruction de données personnelles 3

5 Délais de conservation des données personnelles 3

6 Déclaration d'incidents 3

7 Historique, révision et approbation du document 4

1 Contexte

Cette politique a été conçue dans le but de se conformer aux prescriptions du chapitre 15 du Global Quality Risk Management Manual, notamment les politiques 15.1 à 15.3.6 relatives à la gestion et la protection de données personnelles et confidentielles.

Par la même occasion, elle permettra au cabinet d'offrir à nos clients, prospects, partenaires et employés, un cadre sécurisé pour la gestion de leurs données personnelles et confidentielles collectées uniquement dans le cadre de la réalisation de nos missions.

Cette politique a été définie suivant les normes internationales, doit également demeurer conforme à la règlementation en vigueur dans les bureaux au sein desquels elle sera diffusée. Elle explique ainsi les principes de la protection des données personnelles, mais aussi toutes les actions à mettre en œuvre.

2 Data Privacy Liaison Officer de la région AFS

Le Data Privacy Liaison Officer de la région est **Joseph Siba**. Il sera assisté d'un Data Privacy Delegate Officer, **Armand Nkembe**. Il aura pour rôles le suivi de l'implémentation de la présente procédure au sein de la région, mais surtout servira de point focal entre l'international et la région pour toute question et/ou incident relatif à la gestion des données personnelles.

3 Formation du personnel

Chaque cabinet de la région devra procéder à la formation annuelle de l'ensemble de son personnel dans un délai de trois (03) mois après le début de la saison. Les nouveaux entrants devront impérativement suivre la formation dans un délai d'un mois suivant son entrée au cabinet et impérativement avant toute intervention chez un client.

Le support de formation à utiliser sera celui développé par l'international (GITSG). Lorsque qu'une législation en matière de protection des données personnelles existe dans le pays du cabinet il conviendra de s'assurer que le support de formation de l'international recouvre toutes les dispositions de la législation locale. Dans le cas où il existe des divergences entre la politique de KPMG en matière de protection des données personnelles et la législation locale, le cabinet devra appliquer la législation locale.

En l'absence de diffusion de nouveaux supports de formation par GITSG, le bureau devra utiliser le support de l'année précédente.

4 Collecte, gestion et destruction de données personnelles

La collecte de données personnelles ne doit être effectuée que pour un but précis et légal. La collecte de données pour un usage futur est proscrite. Le titulaire desdites données devra préalablement être informé du but de la collecte, du destinataire, mais aussi des délais de conservation, par tout moyen légal laissant trace. Cette collecte ne devra se limiter qu'aux informations nécessaires à la réalisation de la mission objet de la requête. Les données collectées doivent être exactes et actualisées en cas de besoin. En cas de requête et de réception d'une pléthore d'informations personnelles et pas nécessaires, ne retenir que celles requises et procéder à un renvoi au titulaire par tout moyen légal, ou à leur destruction pure et simple suivant son accord.

Des mesures adéquates doivent être prises afin de conserver toutes données personnelles collectées et éviter leur perte, altération, destruction, transmission accidentelle à et/ou par un tiers. La collecte se faisant par le biais de supports (Clés USB ; disques amovibles ; Ordinateurs ; papiers…), les données devront systématiquement être déposées sur un serveur sécurisé.

Les titulaires d'informations collectées pourront y avoir accès sur autorisation du Data Privacy Liaison Officer en vue de leur mise à jour. Le transfert de toute donnée personnelle au sein et en dehors du Cluster Afrique Francophone Subsaharienne devra être fait sous réserve de l'assurance d'une mise en place d'une procédure de collecte et gestion de données personnelles et confidentielles auprès de l'utilisateur de ces données. La transmission de données personnelles à des tiers est sujette à l'accord préalable du titulaire. Aussitôt les informations utilisées dans le but exclusif de leur collecte, elles devront être retournées au titulaire ou détruites dans les délais règlementaires. La mise en œuvre de toutes les actions citées ci-dessus est soumise à l'approbation du Data Privay Liaison Officer.

5 Délais de conservation des données personnelles

Le délai moyen de conservation des données personnelles au sein de la région Afrique Francophone Subsaharienne est de deux (02) ans, sous réserve d'un délai plus long instruit par la règlementation en vigueur.

6 Déclaration d'incidents

Tout incident relatif à la perte de données personnelles devra être immédiatement déclaré à sa hiérarchie qui à son tour informera le Liaison Data Privacy Officer de la

région AFS (Joseph Siba et Armand Nkembe à l'adresse ci-fmafsdpo@kpmg.ci), dans un délai maximal de 12 (douze) heures à compter de la survenance dudit incident.

Le Data Privacy Liaison Officer devra à son tour :

- requérir de l'équipe concernée des informations complémentaires ;
- remonter dans un délai de 24 (vingt-quatre) heures l'incident au Risk Management Partner et aux associés du bureau qui décideront de la nécessité d'informer le client ou pas, mais aussi de toute action à entreprendre.

Sont considérés comme incident :

- la perte de tout matériel ou support contenant des données personnelles de clients, fournisseurs, (Clé USB ; disque amovible ; Ordinateur ; dossier de travail),
- la transmission de données ou informations personnelles à tout tiers autre que le destinataire,
- la destruction accidentelle de toute donnée personnelle. Cette liste n'est point exhaustive.

Cette politique devra être lue de manière conjointe avec la procédure mise en place par KPMG International et disponible via le lien suivant :

https://goazrweb026.kworld.kpmg.com/ReportServer/Pages/ReportViewer.aspx?/IPG%2fGlobal%20Privacy%20Policies&LibraryID=983522D3-3741-4924-A6B6-7A65075F184A&rc:stylesheet=IPGHtmlViewer

7 Historique, révision et approbation du document

Version	Auteur	Date	Révision
1	Armand Nkembe	11-déc-17	01 Fév. 2018

Révision

Nombre	Auteur	Dates
1	Toussaint de Souza	01 Fév. 2018
2	Lucie Caro	09 Fév. 2018

	3	Papys Agniezska	09 Fév. 2018
	4	Toussaint de Souza	26 Fév. 2018
	5	Toussaint de Souza	01-mars-18
	6	Reine Diby	27 Fév. 2019

Approbation	Nom	Expert	Signature
	Toussaint de Souza		01-mars-18
	Reine Diby		27 Fév. 2019