MESURES TECHNIQUES ET ORGANISATIONNELLES PRÉVUES PAR LE RGPD
DOCUMENT DE SYNTHÈSE

HISTORIQUE DU DOCUMENT			
RÉVISION	**DATE**	**NOM ET QUALITE**	**DESCRIPTION**
0.1	01/08/2018	Gustave Noukagué, DPO	Initialisation
0.2	06/09/2018	Xavier LE FLOCH	1ere révision
0.3	10/10/2018	Gustave Noukagué, DPO	2eme révision
0.4	15/11/2018	Xavier LE FLOCH	3eme révision
1.0	12/12/2018	Gustave Noukagué, DPO	Version 1.0
1.1	06/10/2020	Xavier LE FLOCH	Version 1.1

GOUVERNANCE DU DOCUMENT	
Classification	Non confidentiel
Diffusion	Interne
	Aux clients qui le demanderont
Publication sur le web	Non
Prochaine révision	Dès que nécessaire

RAPPEL DES DISPOSITIONS DU RGDP CONCERNANT LES MESURES TECHNIQUES ET ORGANISATIONNELLES

Le Règlement européen n° 2016/679 du 27 avril 2016 sur la protection des données à caractère personnel (ci-après le « Règlement » ou « RGPD ») fait obligation au responsable du traitement (en l'occurrence ALWAYSDATA) de mettre en œuvre des **mesures techniques et organisationnelles** appropriées pour s'assurer et être en mesure de démontrer que le traitement de telles données est effectué conformément audit Règlement.

Ces mesures techniques et organisationnelles doivent tenir compte de la nature, de la portée, du contexte et des finalités du traitement ainsi que des risques, dont le degré de probabilité et de gravité varie, pour les droits et libertés des personnes physiques (art. 24 du RGPD).

Au titre de la **protection des données dès la conception et par défaut** (art. 25), le RGPD oblige le responsable de traitement à :

a) mettre en œuvre, tant au moment de la détermination des moyens du traitement qu'au moment du traitement lui-même, des **mesures techniques et organisationnelles** appropriées, telles que la pseudonymisation, qui sont destinées à mettre en œuvre les principes relatifs à la protection des données, par exemple la minimisation des données, de façon effective et à assortir le traitement des garanties nécessaires afin de répondre aux exigences dudit Règlement et de protéger les droits de la personne concernée. Ces mesures techniques et organisationnelles doivent tenir compte de l'état des connaissances, des coûts de mise en œuvre et de la nature, de la portée, du contexte et des finalités du traitement ainsi que des risques, dont le degré de probabilité et de gravité varie, que présente le traitement pour les droits et libertés des personnes physiques.

b) mettre en œuvre les **mesures techniques et organisationnelles** appropriées pour garantir que, par défaut, seules les données à caractère personnel qui sont nécessaires au regard de chaque finalité spécifique du traitement sont traitées. Cela s'applique à la quantité de données à caractère personnel collectées, à l'étendue de leur traitement, à leur durée de conservation et à leur accessibilité. En particulier, ces mesures garantissent que, par défaut, les données à caractère personnel ne sont pas rendues accessibles à un nombre indéterminé de personnes physiques sans l'intervention de la personne physique concernée.

S'agissant de la **sous-traitance**, le RGPD précise que lorsqu'un traitement doit être effectué pour le compte d'un responsable du traitement, celui-ci fait uniquement appel 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 dudit Règlement et garantisse la protection des droits de la personne concernée (art. 28 du RGPD).

Au titre de la **sécurité du traitement**, le RGPD prévoit que le responsable du traitement et le sous-traitant mettent en œuvre les **mesures techniques et organisationnelles** appropriées afin de garantir un niveau de sécurité adapté au risque, y compris entre autres, selon les besoins :

a) la pseudonymisation et le chiffrement des données à caractère personnel;
b) des moyens permettant de garantir la confidentialité, l'intégrité, la disponibilité et la résilience constantes des systèmes et des services de traitement;

c) des moyens permettant de rétablir la disponibilité des données à caractère personnel et l'accès à celles-ci dans des délais appropriés en cas d'incident physique ou technique;
d) une procédure visant à tester, à analyser et à évaluer régulièrement l'efficacité des mesures techniques et organisationnelles pour assurer la sécurité du traitement (art. 32-1 du RGPD).

Lors de l'évaluation du niveau de sécurité approprié, il est tenu compte en particulier des risques que présente le traitement, résultant notamment de la destruction, de la perte, de l'altération, de la divulgation non autorisée de données à caractère personnel transmises, conservées ou traitées d'une autre manière, ou de l'accès non autorisé à de telles données, de manière accidentelle ou illicite (art. 32-2 du RGPD).

Le responsable du traitement et le sous-traitant prennent des mesures afin de garantir que toute personne physique agissant sous l'autorité du responsable du traitement ou sous celle du sous-traitant, qui a accès à des données à caractère personnel, ne les traite pas, excepté sur instruction du responsable du traitement, à moins d'y être obligée par le droit de l'Union ou le droit d'un État membre (art. 32-4 du RGPD).

Les mesures techniques et organisationnelles prévues ci-dessous doivent tenir compte de l'état des connaissances, des coûts de mise en œuvre et de la nature, de la portée, du contexte et des finalités du traitement ainsi que des risques, dont le degré de probabilité et de gravité varie, pour les droits et libertés des personnes physiques (art. 24, 25 et 32 du RGPD).

Ces mesures techniques et organisationnelles sont réexaminées et actualisées si nécessaire (art. 24-1, *in fine*).

L'application d'un code de conduite approuvé comme le prévoit l'article 40 du RGPD ou d'un mécanisme de certification approuvé comme le prévoit l'article 42 du RGPD peut servir d'élément pour démontrer le respect des exigences prévues dans les dispositions précitées (art. 24-3 ; 25-3 ; 28-5 et 32-3 du RGPD).

Avec l'entrée en vigueur du RGPD le 25 mai 2018 et en l'absence actuellement d'un code de conduite approuvé comme le prévoit l'article 40 du RGPD ou d'un mécanisme de certification approuvé comme le prévoit l'article 42 du RGPD, nous avons synthétisé et formalisé dans le présent document les mesures techniques et organisationnelles que nous avons mises en place pour assurer la protection et la sécurité des données à caractère personnel ainsi que la conformité de leur traitement au RGPD (ci-après le « **Document de synthèse** »).

Pour l'essentiel et en l'état, ces mesures techniques et organisationnelles sont résumées dans le Tableau ci-après.

SYNTHÈSE DES MESURES TECHNIQUES ET ORGANISATIONNELLES MISES EN PLACE PAR ALWAYSDATA		
REF.	ITEM	MESURE
1	Acteurs de la mise en œuvre et du contrôle permanent de la conformité RGPD	Désignation d'un DPO externe, rattaché directement à la Direction de ALWAYSDATA
		Désignation d'un interlocuteur du DPO en interne chez ALWAYSDATA
2	Outils de pilotage de la conformité RGPD	Elaboration et tenue d'un Registre des activités de traitement
		Elaboration d'une procédure de Notification à l'autorité de contrôle d'une violation de données à caractère personnel
		Elaboration d'une procédure de Communication à la personne concernée d'une violation de données à caractère personnel
3	Moyens permettant de garantir la confidentialité des données (empêcher l'accès à des tiers non autorisés)	Identification par login et mot de passe. Double authentification et filtrage par IP possible sur l'administration cliente. Connexion serveur par clé SSH + filtrage par IP. VPN interne pour que les employés autorisés puissent accéder aux serveurs en dehors des IP autorisées (IP bureau et domiciles).
		Elaboration de Conditions générales de Prestations de Services (CGPS) et de Conditions Particulières à chaque type de services (hébergement dédié; hébergement mutualisé; hébergement sur VPS et Parrainage) ; Clauses de sous-traitance; Politique de protection des données contenant des obligations de confidentialité forte à la charge des clients
		Charte informatique ayant une force contraignante pour les salariés et contenant des obligations fortes de confidentialité à leur charge (voir notre Charte informatique)
		Accord de confidentialité – NDA à faire signer par tout intervenant extérieur à ALWAYSDATA susceptible d'avoir connaissance ou accès aux données à caractère personnel (voir notre NDA)
4	Moyens permettant de garantir l'intégrité des données	Infrastructure redondée (deux sources électriques distinctes et réseaux, doublement des switchs, circuit primaire et secondaire) et accessible physiquement par identification (Poste de sécurité

		avec vérification d'identité + reconnaissance par empreinte à plusieurs niveaux).
		Backup journalier avec rétention sur 30 jours côté client sur des infrastructures différentes, backups de notre base référentielle toutes les 15mn sur des serveurs différents.
		Les disques durs sont tous en RAID1 (duplication temps réelle) serveurs de productions et backups.
5	Moyens permettant de garantir la disponibilité et la résilience constantes des systèmes et des services de traitement	Voir les Réponses à la Question/Rubrique n° 4.
		Gestion de spare matériel et serveur pour chaque baie.
6	Moyens permettant de rétablir la disponibilité des données à caractère personnel et l'accès à celles-ci dans des délais appropriés en cas d'incident physique ou technique	Concernant les données hébergées par nos clients, nous partirons des backups ; ces procédures sont maîtrisées par nos soins. Concernant notre base référentielle (tous les objets manipulés depuis l'administration alwaysdata), le serveur est redondé ; si le master tombe, le slave prendra la suite automatiquement. Un backup de cette base est effectué toutes les 30mn et conservé pendant 11 jours.
7	Procédure visant à tester, à analyser et à évaluer régulièrement l'efficacité des mesures techniques et organisationnelles pour assurer la sécurité du traitement	Nous utilisons en interne un outil d'audit (OpenVAS) permettant de scanner nos serveurs à la recherche de vulnérabilités. De plus, nous prévoyons de déployer prochainement un système automatisé de remise en disponibilité des données de nos clients en cas d'incident grave (réinstallation de serveurs + copie des données depuis les backups), l'objectif étant que ce système soit testé et exécuté chaque trimestre sur un serveur de test.
8	Procédure permettant de détecter une violation de données personnelles	Nous utilisons un outil (rkhunter) permettant de contrôler quotidiennement l'intégrité de fichiers critiques (cas de piratage direct du serveur). Nous proposons depuis l'administration de nos clients l'activation d'un firewall applicatif, de même que sur chaque serveur sont installés un outil (fail2ban) de bannissement les IPs qui effectueraient des échecs de connexion à répétition et un autre permettant, en fonction de règles définies, de bannir des IP effectuant des requêtes HTTP suspectes (attaques, tentatives d'infections..).
9	Outils qui nous permettraient, en cas de besoin, d'anonymiser les données	Compte tenu de la nature, de la portée, du contexte et des finalités du traitement ainsi que des risques (dont le degré de probabilité et de gravité varie d'un organisme à l'autre) pour les

		droits et libertés des personnes physiques, et sachant que l'anonymisation des données représenterait un surcoût significatif pour le client, cette mesure ne nous parait pas « appropriée » au sens du RGPD.
10	Outils qui nous permettraient, en cas de besoin, de pseudonymiser les données personnelles	Compte tenu de la nature, de la portée, du contexte et des finalités du traitement ainsi que des risques (dont le degré de probabilité et de gravité varie d'un organisme à l'autre) pour les droits et libertés des personnes physiques, et sachant que la pseudonymisation des données représenterait un surcoût significatif pour le client, cette mesure ne nous parait pas « appropriée » au sens du RGPD.
11	Outils qui nous permettraient, en cas de besoin, de chiffrer les données personnelles	Compte tenu de la nature, de la portée, du contexte et des finalités du traitement ainsi que des risques (dont le degré de probabilité et de gravité varie d'un organisme à l'autre) pour les droits et libertés des personnes physiques, et sachant que le chiffrement des données représenterait un surcoût significatif pour le client, cette mesure ne nous parait pas « appropriée » au sens du RGPD.
12	Moyens permettant de sensibiliser le personnel ayant accès à des données personnelles	Réunion mensuelle avec l'ensemble du personnel, sur les travaux en cours et rappels.
		Wiki interne permettant notamment de sensibiliser le personnel ayant accès à des données personnelles.
13	Gestion des habilitations	Les accès sont définis par groupes d'utilisateurs, avec des droits différents et des autorisations par IP de connexion.
		L'accès aux données des clients est limité aux seules personnes autorisées.
		Les permissions d'accès sont supprimées lorsqu'elles ne sont plus justifiées (départ de la personne concernée) ou lorsqu'elles sont obsolètes.
		Les habilitations sont revues, vérifiées et actualisées. Il n'y a pas de périodicité particulière pour ces opérations, mais une personne les contrôle régulièrement.
14	Moyens permettant de tracer les accès et gérer les incidents	Il y a une journalisation de tous les services installés par nos soins sur les serveurs et entrant dans le cadre de notre infogérance (Systèmes de base de données, serveurs HTTP, emails, contrôles d'accès, etc.).
		Dans un premier temps, les utilisateurs n'ont pas été formellement informés de la mise en place du système de journalisation. Mais à force de le demander régulièrement, ils en sont désormais quasiment tous informés. Cette information sera de toute façon

		formellement effectuée lors de la prochaine mise à jour de notre Charte informatique.
		Les équipements de journalisation et les informations journalisées sont protégés ; seuls les administrateurs ont accès à ces logs (clé SSH, restriction par IP).
		Des procédures sont prévues pour les notifications en cas de violation de données à caractère personnel
15	Sécurisation des postes de travail	La procédure de verrouillage automatique de session est paramétrée sur chaque poste de travail
		Les antivirus utilisés sont régulièrement mis à jour
		Les « pare-feux » (*firewalls*) logiciels sont régulièrement mis à jour
		Sauf circonstance exceptionnelle, l'accord de l'utilisateur est systématiquement obtenu avant toute intervention sur son poste
16	Sécurisation de l'informatique mobile	L'accès aux serveurs, référentiels, etc. ne peut se faire qu'en passant par notre VPN (authentification par clé)
17	Protection du reseau informatique interne	Les accès distants aux appareils informatiques nomades par VPN sont sécurisés
		Les réseaux Wi-Fi sont sécurisés par des protocoles régulièrement mis à jour (WPA2)
18	Sécurisation des serveurs	L'accès aux outils et interfaces d'administration est limité aux seules personnes habilitées
		Les mises à jour sont régulièrement installées
19	Sécurisation des sites web	Le protocole SSL est utilisé pour l'authentification et le chiffrement des données, avec vérification régulière de la mise en œuvre dudit protocole.
		Nous vérifions régulièrement qu'aucun mot de passe ou identifiant ne passe dans les url, la plus importante étant développée par nous-mêmes. Mise en place d'un programme de bug bounty.
20	Moyens permettant de sauvegarder et d'assurer la continuité d'activité	Des sauvegardes sont effectuées régulièrement et stockées dans un endroit sûr
		Des tests de continuité d'activité sont réalisés régulièrement, selon une fréquence mensuelle au niveau du datacenter (tests électriques et réseau)

21	Archivage sécurisé	Nous avons mis en œuvre des modalités d'accès spécifiques aux données archivées qui nous sont propres, sachant que chaque client est invité à réaliser le plus souvent possible une sauvegarde de ses données et à les récupérer intégralement avant le terme du contrat, au vu des alertes que nous lui enverrons à cette fin.
		Les archives obsolètes sont détruites de manière sécurisée, sans aucun risque qu'elles se retrouvent dans la nature ou entre les mains de tiers
22	Maintenance et destruction des données	Les interventions de maintenance sont tracées et enregistrées
		ALWAYSDATA ne fait pas appel à des tiers pour intervenir sur les données à caractère personnel en son sein
		Les données sont effacées de tout matériel avant sa mise au rebut
23	Gestion de la sous-traitance	Nous avons intégré dans nos Conditions Générales de Prestations de Services des Clauses de sous-traitance avec nos clients Responsables de traitement et dont nous sommes Sous-traitants
		Nous avons interrogé la conformité RGPD de nos propres sous-traitants via un "Questionnaire de conformité RGPD pour sous-traitance"
24	Sécurisation des échanges avec d'autres organismes	En l'absence de mécanisme de chiffrement des données, nous nous assurons, avant leur envoi, qu'il s'agit bien du bon destinataire
		Lorsque les données sont transmises codées, les éléments de décodage font l'objet d'un envoi distinct et via un canal différent
25	Protection des locaux	Afin de contrôler et de surveiller l'accès aux datacentres, ces derniers sont dotés d'équipements de sécurité de pointe assortis de techniques et de procédures de sécurité avancées. L'accès à la zone d'hébergement des infrastructures nécessite en général de franchir cinq contrôles de sécurité, constitués de personnel de sécurité, de sas de sécurité et de lecteurs biométriques.
		Des alarmes anti-intrusion sont installées, et vérifiées périodiquement Des agents de sécurité sont présents sur site H24.
26	Moyens permettant d'encadrer les développements Informatiques	Les développements informatiques et mises à jour à venir se feront en conformité avec les principes du "Privacy by design" et du "Privacy by default".
27	Utilisation des fonctions cryptographiques	Nous privilégions l'utilisation des algorithmes, des logiciels et des bibliothèques reconnues
		Les secrets et les clés cryptographiques sont conservés de manière

		sécurisée