CONDITIONS SPECIFIQUES DONNEES PERSONNELLES

Les présentes Conditions Spécifiques Données Personnelles (« **DPA** ») a pour objet de garantir la conformité avec l'article 28, paragraphes 3 et 4, du règlement (UE) 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 de ces données, et abrogeant la directive 95/46/CE (« **RGPD** »).
SUEZ a désigné un Délégué à la protection des données à caractère personnel, joignable à l'adresse privacy@suez.com.

1. DEFINITIONS

Sauf définition contraire dans les présentes Conditions Spécifiques Données Personnelles, les termes débutant par une majuscule ont la signification qui leur est donnée dans le Contrat. Les termes débutant par une majuscule, utilisés au singulier ou au pluriel, auront la signification qui leur est donnée ci-après :

Réglementation sur les données personnelles : désigne le RGPD y compris notamment toutes dispositions, directives, recommandations ou réglementations actualisées, additionnelles, modifiées ou autres dispositions de remplacement, en vigueur à la date d'effet du Contrat et toute loi nationale d'application ou équivalente, ainsi que toute autre loi relative à la vie privée, à la sécurité ou à la protection des données personnelles, telle qu'applicable dans toutes les juridictions concernées.
Les termes et expressions « **Données à caractère personnel** », « **Traitement** », « **Responsable de traitement** », « **Sous-traitant** », « **Personne concernée** », « **Violation de données** » et « **Autorité de contrôle** » auront la signification qui leur est donnée dans le RGPD.
Données Personnelles du Client : désigne les Données à caractère personnel fournies ou rendues accessibles par le Client et traitées par SUEZ pour la fourniture des Services.
Sous-traitants Ultérieurs : désignent les Sous-traitants recrutés par SUEZ pour mener des activités de Traitement spécifiques pour le compte du Client.

2. OBLIGATIONS DE SUEZ EN QUALITE DE SOUS-TRAITANT

2.1 Description du/des Traitement(s)

Les détails des Traitement, et notamment les catégories de Données à caractère personnel et les finalités du traitement pour lesquelles les Données Personnelles du Client sont traitées, sont précisés à l'annexe 1-1 du DPA.

2.2 Instructions

SUEZ traite les Données Personnelles du Client en qualité de Sous-traitant, uniquement selon les instructions et pour les finalités documentées à l'annexe 1-1 du DPA par le Client en qualité de Responsable du traitement, à moins que SUEZ ne soit tenu d'y procéder en vertu du droit de l'Union européenne ou du droit de l'État membre auquel il est soumis. Dans ce cas, SUEZ informe le Client de cette obligation juridique avant le Traitement, sauf si la loi le lui interdit pour des motifs importants d'intérêt public. Si SUEZ considère qu'une instruction du Client constitue une violation de la Réglementation sur les données personnelles, elle s'engage à l'informer.

2.3 Sécurité du traitement

SUEZ met en œuvre les mesures techniques et organisationnelles appropriées pour assurer la sécurité des Données Personnelles du Client et notamment empêcher toute Violation de données. Les mesures mises en œuvre par SUEZ sont précisées à l'Annexe 1-2 du DPA.

SUEZ veille à ce que les personnes autorisées à traiter les Données Personnelles du Client s'engagent à respecter la confidentialité ou soient soumises à une obligation légale de confidentialité appropriée.

2.4 Sous-traitants ultérieurs

SUEZ est autorisée à recourir à des Sous-traitants Ultérieurs figurant sur la liste de l'Annexe 1-3 du DPA.

SUEZ informe le Client de tout ajout ou remplacement de Sous-traitants Ultérieurs. Le Client peut formuler une objection au recrutement d'un Sous-traitant Ultérieur dans les quinze (15) jours suivant la réception de l'information, pour des raisons liées à la Réglementation sur les données personnelles, sans affecter le droit de SUEZ de recourir au(x) nouveau(x) Sous-traitant(s) Ultérieur(s) après le délai de préavis indiqué ci-dessus.

En cas d'objection du Client, les Parties s'engagent à discuter de bonne foi d'une résolution de l'objection. SUEZ peut alors décider de :

- prendre des mesures raisonnables pour répondre à l'objection du Client en recourant aux services du Sous-traitant Ultérieur ;
- ne pas recourir au Sous-traitant Ultérieur ; ou
- recourir au Sous-traitant Ultérieur.

Suez notifie sans délai sa décision au Client. Dans le délai de quinze (15) jours suivant la réception de la notification de SUEZ, si le Client maintient son objection pour des raisons liées à la Réglementation sur les données personnelles, SUEZ peut résilier le service recourant au nouveau Sous-traitant Ultérieur dans le respect des conditions de résiliation prévues par le Contrat. Le Client accepte le recours au Sous-traitant Ultérieur proposé jusqu'à la date effective de résiliation.

Lorsqu'un remplacement rapide est requis pour des raisons de sécurité ou d'urgence, un Sous-traitant Ultérieur peut être remplacé sans préavis par SUEZ. SUEZ informe le Client du remplacement du Sous-traitant Ultérieur le plus rapidement possible dans la suite de sa nomination.

Lorsque SUEZ recrute un Sous-traitant Ultérieur pour mener des activités de traitement spécifiques pour le compte du Client, elle le fait au moyen d'un contrat qui impose au Sous-traitant Ultérieur, en substance, les mêmes obligations en matière de protection des données à caractère personnel que celles imposées à SUEZ en vertu du présent DPA. SUEZ veille à ce que le Sous-traitant Ultérieur respecte les obligations auxquelles elle est elle-même soumise en vertu du présent DPA et de la Règlementation sur les données personnelles.

2.5 Transferts Internationaux

SUEZ ne transfère des Données Personnelles du Client hors de l'Union Européenne que sur la base d'instructions documentées du Client ou afin de satisfaire à une obligation légale ou réglementaire spécifique à laquelle SUEZ est soumise. Si SUEZ ou l'un des Sous-traitants Ultérieurs transfère des Données Personnelles du Client hors de l'Union Européenne tel que décrit aux Annexes 1-2 et 1-3, SUEZ s'engage à respecter les exigences du chapitre V du RGPD.

3. ASSISTANCE AU CLIENT – RESPONSABLE DE TRAITEMENT

3.1 Réponses aux demandes des personnes concernées d'exercer leurs droits

Lorsque SUEZ reçoit une demande d'une Personne concernée d'exercer ses droits, SUEZ informe sans délai le Client de cette demande. SUEZ ne donne pas elle-même suite à cette demande, sauf instructions contraires données par le Client. SUEZ assiste le Client pour remplir l'obligation qui lui incombe de répondre aux demandes des Personnes concernées d'exercer leurs droits.

3.2 Respect des obligations du Client

SUEZ aide le Client à garantir le respect des obligations suivantes, compte tenu de la nature du Traitement et des informations dont dispose SUEZ :

- l'obligation de procéder à une analyse d'impact relative à la protection des données lorsque celle-ci est requise dans la limite d'un jour ouvré de prestation ;
- l'obligation de consulter l'Autorité de contrôle compétente lorsque celle-ci est requise dans la suite de l'analyse d'impact relative à la protection des données ;
- l'obligation de veiller à ce que les Données Personnelles du Client soient exactes et à jour, en informant sans délai le Client si SUEZ apprend que les Données Personnelles du Client qu'il traite sont inexactes ou sont devenues obsolètes ;
- les obligations prévues à l'article 32 et suivants du RGPD.

4. NOTIFICATION DES VIOLATIONS DE DONNEES

En cas de Violation de données traitées par SUEZ pour le compte du Client, SUEZ en informe le Client dans les meilleurs délais après en avoir pris connaissance. Cette notification contient :

- une description de la nature de la Violation de données constatée ;
- les coordonnées d'un point de contact auprès duquel des informations supplémentaires peuvent être obtenues au sujet de la Violation de données ;

- ses conséquences probables et les mesures prises ou les mesures qu'il est proposé de prendre pour remédier à la Violation, y compris pour en atténuer les éventuelles conséquences négatives.

Lorsqu'il n'est pas possible de fournir toutes les informations en même temps, la notification initiale contient les informations disponibles à ce moment-là et, à mesure qu'elles deviennent disponibles, des informations supplémentaires sont communiquées par la suite dans les meilleurs délais.

5. INFORMATION ET AUDIT

SUEZ met à la disposition du Client, à sa demande, toutes les informations nécessaires pour démontrer le respect des obligations énoncées dans le DPA, y compris tout rapport d'audit ou de certification tel que SOC, ISO, NIST, PCI DSS, HIPAA ou tout autre document équivalent émis par un auditeur ou certificateur tiers qualifié au cours des 12 derniers mois.

Si le Client considère que les informations fournies par SUEZ sont insuffisantes pour démontrer le respect des obligations énoncées dans le DPA, le Client en informe SUEZ par écrit en précisant les motifs pour lesquels les informations fournies sont insuffisantes. SUEZ met alors à la disposition du Client les informations complémentaires pertinentes.

Si le Client estime les informations complémentaires fournies par SUEZ insuffisantes, le Client peut procéder ou faire procéder à un audit des Traitements couverts par le DPA, dans la limite d'une fois par an sauf en cas de Violation de données traitées par SUEZ.

Le Client informe SUEZ par écrit de son intention de procéder à un audit en respectant un préavis de (vingt) 20 jours ouvrés, sauf période plus courte en cas de Violation de données traitées par SUEZ. Le calendrier et la portée de tout audit sont convenus entre les Parties agissant raisonnablement et de bonne foi. Le Client supportera les coûts de tout audit initié.

Le Client désigne l'auditeur tiers, non-concurrent de SUEZ, sous réserve de l'accord écrit et spécifique de SUEZ.

6. SUSPENSION ET RESILIATION

6.1 Suspension et Résiliation par le Client

En cas de manquement de SUEZ aux obligations qui lui incombent en vertu du DPA, le Client peut donner instruction à SUEZ de suspendre le Traitement jusqu'à ce que ce dernier se soit conformé au DPA.

Le Client est en droit de résilier le Contrat dans le respect des conditions de résiliation prévues par le Contrat, si :

- le Traitement par SUEZ a été suspendu par le Client en application du présent article 6.1 et le respect du DPA n'est pas rétabli dans un délai d'un mois à compter de la suspension ;
- SUEZ est en violation grave ou persistante du présent DPA ou des obligations qui lui incombent en vertu de la Réglementation sur les données personnelles ;
- SUEZ ne se conforme pas à une décision contraignante d'une juridiction compétente ou de l'Autorité de contrôle compétente concernant les obligations qui lui incombent en vertu du DPA ou de la Réglementation sur les données personnelles.

6.2 Résiliation par SUEZ

SUEZ est en droit de résilier le Contrat dans le respect des conditions de résiliation prévues par le Contrat, si après avoir informé le Client que ses instructions enfreignent la Réglementation sur les données personnelles, le Client maintient ses instructions dans les mêmes termes.

7. RESTITUTION ET DESTRUCTION DES DONNEES

A l'expiration ou après la résiliation du Contrat ou sur demande du Client, SUEZ s'engage à détruire ou restituer au Client, au choix de ce dernier, dans le délai convenu entre les Parties, toutes les Données Personnelles du Client, y

compris toutes copies qui en auraient été faites sur quelque support que ce soit, sauf en cas de nécessité de conservation requise par une loi applicable.

***

ANNEXE 1-1 – DESCRIPTION DES TRAITEMENTS

Finalité du Traitement	Nature du Traitement	Catégories de données traitées	Catégories de Personnes concernées	Lieu du traitement	Durée du traitement	Durée de conservation des données	Sous-traitant Ultérieur
Fourniture du Service ON'connect™ metering: - Suivi de la consommation - Suivi de la métrologie du compteur (alerte batterie de l'émetteur, suivi des associations compteur/émetteur, maintenance évolutive des assets) - Gestion des alertes (alertes fuite, alerte surconsommation)	Collecte, stockage, enregistrement, mise à disposition, archivage	**Données relatives à la vie personnelle :** index de consommation courante, index de consommation journalière, volume de nuit, index retours d'eau **Données relatives à la télérelève** : index télé-relevés (15m, 1h, 6h, 24h), index interpolé minuit, informations sur débit minimum et maximum, débit maximum instantané, volume de fuite, alarmes des transmetteurs (gel, batterie, fixation, accès, sur-débit, retours d'eau, fuite d'eau, risque de compteur bloqué) **Données de localisation** : coordonnées GPS du point de service **Caractéristiques point de service** : ID point de service, adresse postale du point de service, code INSEE, diamètre	Abonnés aux contrats de distribution d'eau	France	Durée d'exécution de l'Accord	**Données relatives à la vie personnelle :** 5 ans **Données relatives à la télérelève** : 5 ans **Données de localisation** : durée de vie de l'équipement **Caractéristiques point de service** : durée de vie de l'équipement	**Cloud temple** (hébergement) **Accenture** (Tierce Maintenance d'exploitation applicative)

		compteur, matricule compteur, matricule émetteur, poids d'impulsion du compteur, niveau batterie émetteur, température de l'émetteur					

Fourniture du Service ON'connect™ coach : Suivi de la consommation par l'abonné et conseils de consommation	Collecte, stockage, enregistrement, mise à disposition, archivage	**Données relatives à la vie personnelle :** index de consommation courante, index de consommation journalière, volume de nuit, index retours d'eau **Données relatives à la télérelève** : index télé-relevés (15m, 1h, 6h, 24h), index interpolé minuit, informations sur débit minimum et maximum, débit maximum instantané, volume de fuite, alarmes des transmetteurs (gel, batterie, fixation, accès, sur-débit, retours d'eau, fuite d'eau, risque de compteur bloqué) **Données de localisation** : coordonnées GPS du point de service **Caractéristiques point de service** : ID point de service, adresse postale du point de service, code INSEE, diamètre compteur, matricule compteur, matricule émetteur, poids d'impulsion du compteur, niveau batterie émetteur, température de l'émetteur	Abonnés aux contrats de distribution d'eau	France, Irlande	Durée d'exécution de l'Accord	**Données relatives à la vie personnelle :** 5 ans **Données relatives à la télérelève** : 5 ans **Données de localisation** : durée de vie de l'équipement **Caractéristiques point de service** : durée de vie de l'équipement	**Cloud temple** (hébergement) **Microsoft Azure** (hébergement)

Fourniture du service Opti'Revenue : Gestion du parc de compteurs d'eau (surveillance de l'état technique et analyses des consommations)	Collecte, stockage, enregistrement, mise à disposition, archivage	**Données relatives au compteur** : relevés quotidiens, alarmes quotidiennes des compteurs, alarmes quotidiennes des transmetteurs **Données clients** : coordonnées / adresse postale, identification du client, matricule du client et numéro du point de service **Données financières** : coûts de remplacement et d'installation des compteurs	Abonnés aux contrats de distribution d'eau	Espagne	Durée d'exécution de l'Accord	**Données quotidiennes** : 2 ans. **Données mensuelles** : 5 ans	**Siemens** (prestataire Saas pour la gestion compteurs d'eau)

ANNEXE 1-2 – Descriptions des Mesures techniques et organisationnelles de sécurité

MESURES DE SECURITE TECHNIQUES ET ORGANISATIONNELLES			SERVICES		
			ON'connect ™ metering	ON'connect ™ coach	Opti' Revenue
1	**Piloter la sécurité des données**	Faire de la sécurité un enjeu partagé et porté par l'équipe dirigeante	X	X	X
		Prévoir une politique de sécurité de l'information ainsi que des politiques thématiques de sécurité	X	X	X
		Prévoir une organisation de sécurité de l'information où les fonctions et responsabilités sont définies	X	X	X
		Prévoir une politique de classification et de marquage des données	X	X	X
		Prévoir une politique de protection des données personnelles	X	X	X
		Recenser les traitements des données personnelles (registre)	X	-	X
		Évaluer régulièrement l'efficacité des mesures de sécurité mises en œuvre et adopter une démarche d'amélioration continue	X	X	X
2	**Définir un cadre pour les utilisateurs**	Rédiger une charte informatique comprenant les modalités d'utilisation des systèmes informatiques, les règles de sécurité et les moyens d'administration en place	X	X	X
		Donner une force contraignante à la charte et y rappeler les sanctions encourues en cas de non-respect	-	-	-
3	**Impliquer et former les utilisateurs**	Sensibiliser les personnes manipulant les données et plus particulièrement les données personnelles	X	X	X
		Documenter les procédures d'exploitation	X	X	X
4	**Authentifier les utilisateurs**	Octroyer un identifiant (« login ») unique à chaque utilisateur	X	X	X
		Adopter la politique de mot de passe SUEZ	X	X	X
		Obliger l'utilisateur à changer le mot de passe attribué automatiquement ou par un administrateur	X	X	X
5	**Gérer les habilitations**	Définir des profils d'habilitation	X	X	X
		Faire valider toute demande d'habilitation	X	X	X

		Supprimer les permissions d'accès des utilisateurs dès qu'ils ne sont plus habilités à accéder à un local ou une ressource, ainsi qu'à la fin de leur contrat	X	X	X
		Réaliser une revue annuelle des habilitations	X	X	X
6	**Sécuriser les postes de travail**	Prévoir une procédure de verrouillage automatique de session	-	-	X
		Installer et configurer un proxy de filtrage Internet	X	X	X
		Utiliser des antivirus régulièrement mis à jour	X	X	X
		Déployer les mises à jour de sécurité au plus tôt	X	X	X
		Limiter les droits des utilisateurs au strict minimum en fonction de leurs besoins	X	X	X
		Favoriser le stockage des données des utilisateurs sur un espace régulièrement sauvegardé accessible via le réseau interne	X	X	X
		Effacer de façon sécurisée les données présentes sur un poste préalablement à sa réaffectation	X	X	X
		Recueillir l'accord de l'utilisateur avant toute intervention sur son poste	X	X	X
7	**Sécuriser l'informatique mobile**	Sensibiliser les utilisateurs aux risques spécifiques du nomadisme	X	X	X
		Prévoir des moyens de chiffrement des équipements mobiles	X	X	X
		Exiger un secret pour le déverrouillage des smartphones	X	X	X
8	**Protéger le réseau informatique**	Limiter les flux réseau au strict nécessaire	X	X	X
		Sécuriser les réseaux Wi-Fi, notamment en mettant en œuvre le protocole WPA3	X	X	X
		Sécuriser les accès distants des appareils informatiques nomades par VPN	X	X	X
		Cloisonner le réseau, entre autres en mettant en place une DMZ (zone démilitarisée)	X	X	X
9	**Sécuriser les serveurs**	Limiter l'accès aux outils et interfaces d'administration aux seules personnes habilitées	X	X	X
		Installer sans délai les mises à jour critiques après les avoir testées le cas échéant	X	X	X
		Utiliser des logiciels de détection et de suppression de programmes malveillants	X	X	X
		Effectuer des sauvegardes et vérifier régulièrement leur intégrité et la capacité de les restaurer	X	X	X
		Mettre en place un système de journalisation des évènements	X	X	X

10	**Sécuriser les sites Web**	Sécuriser les flux d'échange de données par l'obtention de certificats adaptés et l'utilisation obligatoire de TLS	X	X	X
		Limiter les ports de communication strictement nécessaires au bon fonctionnement de l'application	X	X	X
		Limiter l'accès aux outils et interfaces d'administration aux seules personnes habilitées	X	X	X
		Si des cookies non-nécessaires au service sont utilisés, recueillir le consentement de l'internaute	X	X	X
		Vérifier qu'aucun secret ou donnée personnelle ne passe par les URL	X	X	X
		Limiter les informations renvoyées lors de la création d'un compte utilisateur ou lors de réinitialisation d'un mot de passe	X	X	X
		Adopter les bonnes pratiques pour le développement informatique (Top 10 OWASP, …)	X	X	X
11	**Encadrer les développements informatiques**	Intégrer la protection des données, y compris ses exigences en termes de sécurité des données personnelles, dès la conception	X	X	X
		Utiliser des composants et outils sécurisés reconnus par la communauté	X	X	X
		Mettre en œuvre des mesures contre les attaques courantes qui visent les bases de données (injection code SQL, …)	X	X	X
		Pour tout développement à destination du grand public, mener une réflexion sur les paramètres influant sur le respect de la vie privée	X	X	X
		Eviter le recours à des zones de texte libre ou de commentaires	-	-	-
		Réaliser des tests complets avant la mise à disposition ou la mise à jour d'un produit	X	-	X
		Effectuer les développements informatiques et les tests dans un environnement informatique distinct de celui de la production	X	X	X
		Veiller à l'absence de secrets (d'authentification ou de chiffrement) lors du dépôt de code dans un outil de gestion de versions	X	X	X
		Utiliser des données fictives ou anonymisées pour le développement et les tests	X	X	X
		Effectuer un test de non-régression et/ou une revue de code avant tout passage en production d'une mise à jour	-	-	X
12	**Protéger les locaux**	Restreindre les accès aux locaux	X	X	X
		Installer des alarmes anti-intrusion et les vérifier périodiquement	X	X	X

		Mettre en place des détecteurs de fumée ainsi que des moyens de lutte contre les incendies et les inspecter annuellement	X	X	X
		Etablir les règles et moyens de contrôle d'accès des visiteurs, au minimum en faisant accompagner les visiteurs en dehors des zones d'accueil du public	X	X	X
		Protéger physiquement les matériels informatiques par des moyens spécifiques	X	X	X
13	**Sécuriser les échanges avec l'extérieur**	Chiffrer les données avant leur enregistrement sur un support physique à transmettre à un tiers	X	X	X
		Lors d'un envoi via un réseau : chiffrer les pièces sensibles à transmettre, utiliser un protocole sécurisé (SFTP, HTTPS, …) et assurer la confidentialité des secrets	X	X	X
		Transmettre le secret lors d'un envoi distinct et via un canal différent	X	X	X
		Ouvrir un fichier venant de l'extérieur seulement si l'expéditeur est connu et après soumission à une analyse antivirus	X	X	X
14	**Gérer la sous-traitance**	Faire appel uniquement à des sous-traitants présentant des garanties suffisantes	X	X	X
		Prévoir des clauses spécifiques de sécurité dans les contrats des sous-traitants	X	X	X
		S'assurer de l'effectivité des garanties prévues (ex. : audits de sécurité, PAS, visites)	X	X	-
15	**Encadrer la maintenance et la fin de vie des matériels et logiciels**	Insérer des clauses de sécurité dans les contrats de maintenance effectuée par des prestataires pour encadrer leurs accès aux SI	X	X	X
		Encadrer les interventions de tiers par un responsable de l'organisme	X	X	X
		Supprimer de façon sécurisée les données des matériels avant leur mise au rebut, leur envoi en réparation chez un tiers ou en fin de contrat de location	X	X	X
16	**Tracer les opérations**	Prévoir un système de journalisation	X	X	X
		Informer les utilisateurs de la mise en place du système de journalisation	X	X	X
		Protéger les équipements de journalisation et les informations journalisées	-	-	X
		Analyser de manière active, en temps réel ou à court terme, les traces collectées pour être en mesure de détecter la survenue d'un incident	X	X	X
17	**Sauvegarder**	Effectuer des sauvegardes fréquentes des données	X	X	X
		Stocker au moins une sauvegarde sur un site géographiquement distinct du site d'exploitation	X	X	X
		Protéger les sauvegardes, autant pendant leur stockage que leur convoyage	X	X	X
		Tester régulièrement la restauration des sauvegardes et leur intégrité	X	X	X

18	**Prévoir la continuité et la reprise d'activité**	Prévoir un plan de continuité (PCA) et de reprise (PRA) d'activité informatique	-	-	X
		S'assurer que les utilisateurs, prestataires et sous-traitants savent qui alerter en cas d'incident	-	-	X
		Effectuer régulièrement des exercices d'application du plan de continuité ou de reprise de l'activité	X	X	X
19	**Gérer les incidents et les violations**	Analyser régulièrement les traces collectées et traiter les alertes remontées par le système de journalisation	-	-	X
		Etablir une(des) procédure(s) détaillant le processus de gestion des incidents incluant(s) la gestion des violations de données et définir les critères de qualification d'une violation	X	X	X
		Evaluer le risque, pour les personnes, engendré par la violation	X	X	X
		Tenir un registre interne de toutes les violations de données personnelles	X	X	X
		Notifier à la CNIL, dans les 72 heures (tel que prévu par le RGPD), les violations présentant un risque pour les droits et libertés des personnes et informer les personnes concernées	X	X	X
20	**Analyse de risques**	Mener une analyse de risques, même minimale, sur les traitements de données envisagés	X	X	X
		Identifier les traitements de données personnelles pour lesquels une analyse d'impact relative à la protection des données (AIPD) doit être obligatoirement menée selon le RGPD	X	X	X
		Suivre au cours du temps l'avancement du plan d'action décidé à l'issue de l'analyse de risques	X	X	X
21	**Chiffrement, hachage, signature**	Utiliser des algorithmes, des logiciels et des bibliothèques reconnues et sécurisées	X	X	X
		Utiliser des tailles de clés suffisantes	X	X	X
		Conserver les secrets et les clés cryptographiques de manière sécurisée	X	X	X
22	**Cloud : Informatique en nuage**	Cartographier les données et les traitements dans le Cloud	X	X	X
		Inclure les services Cloud dans l'analyse de risques	X	X	X
		Configurer les outils de sécurité mis à disposition par le fournisseur le cas échéant	X	X	X
		Assurer le même niveau de sécurité dans le cloud que sur site	X	X	X
23	**Applications mobiles : Conception et développement**	Prendre en compte les spécificités de l'environnement mobile pour réduire les données personnelles collectées et limiter les permissions demandées (authentification incluse)	X	X	X
		Sécuriser les communications (TLS) et stocker les secrets cryptographiques par empaquetage	X	-	X

		Prendre en compte la possibilité que le système d'exploitation effectue des sauvegardes automatiques des données personnelles	X	-	X
		Recourir à un moyen d'authentification correspondant au niveau de sécurité recherché	X	-	X
24	**Intelligence artificielle : Conception et apprentissage**	Constituer une équipe de développement aux compétences pluridisciplinaires, veiller à sa formation sur les bonnes pratiques de sécurité et sensibiliser aux vulnérabilités propres à l'IA	X	-	X
		Mettre en œuvre une procédure obligatoire pour le développement et l'intégration continus notamment pour les modifications apportées au code de production	X	X	X
		Vérifier la qualité des données et annotations, la présence de biais, la fiabilité des sources de données	X	X	X
		Eviter les copies, partielles ou totales, des bases de données et recourir à des données fictives ou de synthèse	X	X	X
		Documenter le fonctionnement et les limitations du système	-	-	X
		Vérifier la légitimité des utilisateurs du système lorsque celui-ci est rendu disponible en tant que service	X	X	X
		Prévoir un plan d'audit du système portant sur les éléments logiciels, matériels et sur les mesures organisationnelles telles que les procédures de supervision humaine du système d'IA	X	X	-
25	**API : Interfaces de programmation applicative**	Organiser et documenter la sécurité des accès aux API et aux données	-	-	X
		Limiter le partage des données uniquement aux personnes et aux finalités prévues	X	X	X

ANNEXE 1-3 – Liste des Sous-traitants Ultérieurs

Sous-traitant intervenant pour le compte du Prestataire Dénomination sociale, Adresse postale, pays Adresse électronique d'un représentant et du DPO	**Pays dans lesquels les Traitements sont réalisés**	**Description du Traitement sous-traité**	**Outils d'adéquation utilisé en cas de transferts de Données (et mesures de sécurité techniques et organisationnelles additionnelles, le cas échéant)**
Cloud Temple Le Belvédère, 1-7 Cr Valmy, 92800 Puteaux – SPACES	France	Hébergement	N/A
Accenture – 118, avenue de France, 75013 Paris **DPO :** dataprivacy@accenture.com	France, île Maurice, Vietnam	Tierce Maintenance d'exploitation applicative (service ON'connect™ metering)	Clauses contractuelles types
Microsoft Ireland Operations Limited – One Microsoft Place, South Country Business Park, Leopardstown, Dubin 18, D18 P521 – Ireland **Microsoft France SAS** - 39 quai du Président Roosevelt, Issy les Moulineaux, 92130, France **DPO** : Microsoft EU Data Protection Officer in Ireland, +353 (1) 706-3117	Irlande, États-Unis	Hébergement	Décision d'adéquation (Data privacy framework)
Siemens Industry Software SAS – 107 Avenue de la République, 92320 Hauts-de-Seine, France **Siemens Industry Software, S.L.U. -** Tres Cantos - Madrid (Espagne) - Ronda de Europa 5, 28760 Tres Cantos, Madrid, Espagne **DPO**: dataprivacy@siemens.com	Espagne, Allemagne	Fourniture d'une solution en mode Saas pour gestion du parc de compteur d'eau	N/A