



Attribution d'une Concession de Service Public relative au Réseau de Chaleur Urbain de la Ville de Sucy-en-Brie

**Pièce E – Base 25 ans :
Protection des données personnelles**

Partie E – Protection des données à caractère personnel

Offre finale – 31/07/2024



SOMMAIRE

PREAMBULE.....

1

1 LA PROTECTION DES DONNEES A CARACTERE PERSONNEL AU SEIN D'ENGIE ENERGIE SERVICES – ENGIE SOLUTIONS.....

2

1.1 LA POLITIQUE D'ENGIE SOLUTIONS EN MATIERE DE DONNEES A CARACTERE PERSONNEL.....

2

1.2 LA GOUVERNANCE

3

1.3 LES ACTIONS DE FORMATION ET DE SENSIBILISATION.....

4

1.4 UN DISPOSITIF D'AUDIT

5

2 LES ENGAGEMENTS DU CONCESSIONNAIRE DANS LE CADRE DU CONTRAT DE CONCESSION

6

2.1 COLLABORATION.....

6

2.2 FINALITES DES TRAITEMENTS DE DONNEES PERSONNELLES

6

2.3 STATUT DES PARTIES.....

7

2.4 DONNEES TRAITEES

10

2.5 MISE A JOUR ET DUREES DE CONSERVATION DES DONNEES COLLECTEES.....

11

2.6 DESTINATAIRES DES DONNEES COLLECTEES – SOUS-TRAITANCE

12

2.7 INFORMATION ET DROITS DES PERSONNES CONCERNEES

12

2.8 MESURES DE SECURITE ET DE CONFIDENTIALITE

13

2.9 ANALYSE D'IMPACT SUR LA PROTECTION DES DONNEES (AIPD)

14

2.10 AUTRES ENGAGEMENTS

14

Dans le cadre de l'offre finale, le présent livrable n'a pas été modifié.

Préambule

Dans le cadre de l'exécution du Contrat de Concession, le Concessionnaire s'engage à respecter la réglementation applicable en matière de protection des données personnelles, en particulier le Règlement européen sur la protection des données (RGPD) et toute loi ou réglementation le transposant, le mettant en œuvre ou le complétant, ainsi que les règles, recommandations ou code de conduite adoptés par les autorités chargées de la protection des données, en particulier la CNIL en France.

Dans ce cadre, la présente annexe expose :

1. l'organisation et les principaux outils de conformité au RGPD mis en place chez ENGIE Solutions et qui seront appliqués par la Société dédiée (le Concessionnaire) ;
2. les engagements que cette dernière propose de mettre en œuvre dans le cadre de la future concession, si son offre est retenue.



1 LA PROTECTION DES DONNEES A CARACTERE PERSONNEL AU SEIN D'ENGIE ENERGIE SERVICES – ENGIE SOLUTIONS

Le Règlement Général sur la Protection des Données (« RGPD ») est un règlement européen (UE 2016/679) sur la protection des données qui vise à protéger les données personnelles des citoyens. Il est entré en vigueur à compter du 25 mai 2018 et s'applique à l'ensemble des organismes, privés comme publics, de l'Union Européenne.

ENGIE Energie Services – ENGIE Solutions attache la plus grande importance à la protection des données personnelles dans ses relations commerciales. Le Concessionnaire veille à traiter ces données de manière éthique, responsable et transparente conformément aux dispositions du RGPD et plus généralement à la réglementation applicable en matière de protection des données personnelles.

La mise en place d'une gouvernance et de procédures articulées autour de nombreux relais chargés de veiller à la conformité des traitements font d'ENGIE Solutions un acteur de confiance.

À ce titre, ENGIE Solutions a adopté diverses mesures et déployé différents outils visant à assurer la conformité au RGPD, mesures et outils qui seront déclinés et mis en œuvre à l'occasion de l'exécution du Contrat de concession par le Concessionnaire.

La conformité d'ENGIE Solutions repose sur plusieurs éléments, notamment l'adoption d'une Politique de Protection des Données à Caractère Personnel, une gouvernance souple et réactive face aux événements Data Privacy, un dispositif d'audit et de contrôle interne exigeant ainsi qu'une démarche de sensibilisation et de formation continue aux enjeux Privacy.

Par ailleurs, ENGIE Solutions s'est dotée de plusieurs procédures visant à intégrer dès l'origine d'un projet la protection des données personnelles et à en assurer la sécurité by design and by default. Par exemple, toute relation contractuelle avec un prestataire pressenti donne lieu, au préalable, à une évaluation de son niveau de conformité, afin de s'assurer que la chaîne de sous-traitance est conforme aux engagements de sa Politique de Protection des Données personnelles. De même, au stade de la contractualisation, un Plan d'Assurance Sécurité (PAS) décrit les exigences de sécurité et Privacy du Concessionnaire et les dispositions que le prestataire s'engage à mettre en place pour le projet donné.

1.1 La politique d'ENGIE Solutions en matière de Données à Caractère Personnel

Dès le 16 janvier 2017, afin d'anticiper l'entrée en vigueur du Règlement Général sur la protection des données à caractère personnel (RGPD) 2016/679, le Groupe ENGIE a mis en place une politique sur la protection des données à caractère personnel et s'est doté des outils et de la gouvernance nécessaire à son implémentation. Cette politique Groupe a été révisée



en 2022 pour tenir compte de la nouvelle organisation du groupe ENGIE et des évolutions réglementaires survenues dans le domaine de la protection des données.

S'inscrivant dans les orientations données par la Politique de protection des données à caractère personnel du Groupe ENGIE, afin de maîtriser les risques réglementaires et opérationnels, ENGIE Solutions s'est dotée très rapidement à son tour d'une Politique de Protection des Données à Caractère Personnel ainsi que d'une organisation et des moyens appropriés à assurer la conformité de l'entreprises, à toute échelle (filiales, territoires et agences). Cette politique ENGIE Solutions a été mise à jour en avril 2023.

1.2 La gouvernance

Conformément à la Politique de Protection des données du Groupe ENGIE et à sa propre politique, ENGIE Solutions a désigné un Data Privacy Manager (« DPM ») qui est en charge d'assurer la mise en œuvre effective de la Politique de Protection des Données Personnelles et veiller à son application au sein d'ENGIE Solutions et donc de la future société dédiée.

Ses principales missions sont les suivantes :

- Assurer l'« accountability », notamment par l'établissement et le déploiement des procédures, chartes et autres documents appropriés (i.e. procédure privacy by design et default, procédure de gestion des demandes d'exercice des droits des personnes, procédure de gestion des failles de sécurité, etc.) et rassembler les preuves de l'accountability de l'Entreprise ;
- Prendre part aux analyses d'impact sur la vie privée (lorsqu'un traitement est susceptible d'engendrer un risque élevé pour les droits et libertés des personnes concernées) ;
- Tenir et maintenir à jour les registres d'activités de traitements d'ENGIE Solutions et de ses filiales, dont le Concessionnaire, agissant en qualité de responsable de traitement et/ou de sous-traitant (au sens du RGPD) de l'Autorité concédante ;
- Vérification du respect des finalités par les métiers ;
- Vérification de l'implémentation des politiques de conservation des données personnelles ;
- Piloter les incidents et violations de données selon la procédure mise en place et effectuer, si nécessaire, les notifications auprès des autorités compétentes, ainsi que cas échéant, auprès des personnes concernées ;
- Assurer un niveau d'alerte continu sur la conformité à la protection des données ;
- Etablir un rapport annuel des activités de protection des Données implémentée sur son périmètre et le communiquer au Data Privacy Manager du Groupe ENGIE et au Codir d'ENGIE Solutions ;
- Informer, conseiller et, si nécessaire, alerter les responsables de traitement sur les questions relatives à la protection des données à caractère personnel.

En complément de l'organisation mise en place au niveau du Groupe ENGIE, le DPM d'ENGIE Solutions mobilise et anime un réseau composé par tous les métiers afin de garantir la conformité au RGPD. Cette équipe dédiée au pilotage de la mise en conformité est composée par des représentants des différents métiers, appelés Correspondants Data Privacy Manager



(CDPM). Ces acteurs sont les relais du DPM au sein des directions, filières et entités opérationnelles d'ENGIE Solutions (DSI, DRH, ...)

Leurs principales missions sont les suivantes :

- Informer, conseiller et si besoin alerter le DPM d'ENGIE Solutions,
- Contribuer aux actions de sensibilisation du personnel dépendant du périmètre d'intervention,
- Collaborer aux actions du DPM, notamment pour la négociation, la conclusion et la mise à jour contractuelle de façon à garantir la conformité au RGPD à travers les directives d'ENGIE Solutions en tant que responsable de traitement.
- Faire connaître et respecter les principes et modalités de la politique d'ENGIE Solutions en matière de protection des données personnelles,
- Contribuer à la mise à jour de la documentation servant à démontrer la conformité sur le périmètre, notamment par des actions de purge et de limitation des données traitées ;
- Conseiller les responsables de traitements en amont des projets ou lors des évolutions des applications sur les analyses à réaliser et les mesures de protection des données personnelles à prendre en compte dès l'origine de ces projets ;
- Déclarer au DPM et à l'Ethics Officer d'ENGIE Solutions des usages inappropriés de données personnelles dont ils auraient été informés,
- Alerter le DPM et apporter leur soutien en cas de contrôle de la CNIL.

Ainsi, en sus de leurs activités opérationnelles, leurs principales missions sont d'organiser la remontée des informations relatives à tous nouveaux projets impliquant le traitement de données personnelles et collaborer avec le DPM à la tenue du Registre des activités de traitement tant pour les activités pour lesquelles l'entreprise est responsable de traitement que pour celles pour lesquelles elle a le rôle de sous-traitant.

1.3 Les actions de formation et de sensibilisation

Le Concessionnaire diffuse une culture de protection des données auprès de l'ensemble de ses collaborateurs et intègre les principes de la protection des données dès l'origine des projets.

A cet effet, le DPM et son équipe mobilisent plusieurs moyens d'information, de sensibilisation et de formation, notamment :

- **Des vidéos et supports d'information** destinés à l'ensemble des collaborateurs accessibles dans l'intranet de l'entreprise à tout moment à l'ensemble des collaborateurs (e-learning) ;
- **Des formations spécifiques et approfondies** sont mises en place au profit de certaines catégories d'acteurs plus spécialement concernés (Service Achats et Approvisionnements, RH, commerciaux, chefs de projets...).
- **Une veille réglementaire hebdomadaire** en matière de Privacy et cybersécurité.



1.4 Un dispositif d'audit

La conformité aux dispositions inscrites dans la Politique de Protection des Données Personnelles du Concessionnaire est contrôlée annuellement dans le cadre d'un programme d'audit interne, nommé INCOME. Le périmètre de l'audit couvre l'ensemble des filiales d'ENGIE Solutions.

Ce programme d'audit est fondé sur un référentiel de contrôle interne, dit le « COR7 » relatif à la protection des données à caractère personnel. Ce référentiel comporte 11 contrôles visant à maîtriser l'ensemble des risques liés à la mise en œuvre de la réglementation applicable. Il a été conçu pour répondre aux nouvelles exigences réglementaires liées à la protection des données à caractère personnel, en Europe et hors Europe.



2 LES ENGAGEMENTS DU CONCESSIONNAIRE DANS LE CADRE DU CONTRAT DE CONCESSION

2.1 Collaboration

Le Concessionnaire s'engage à collaborer pleinement avec l'Autorité Concédante, et tout particulièrement avec le DPO de cette dernière, pour toute question relative au traitement des données et à la protection des données à caractère personnel intéressant l'exécution du contrat de concession.

Les coordonnées du Data Privacy Manager d'ENGIE Solutions, sont les suivantes :

ENGIE Solutions - A l'attention du Data Privacy Manager (DPM), T1, Case courrier 13.12 - 1 place Samuel de Champlain – Faubourg de l'Arche, 92930 Paris La Défense Cedex, ou: dpm.engie-solutions@engie.com.

Les coordonnées du Délégué à la Protection des Données de l'Autorité Concédante sont les suivantes :

DPO XXXX **[Insérer les coordonnées du DPO de l'Autorité Concédante]**

2.2 Finalités des traitements de données personnelles

Les principales données à caractère personnel traitées seront celles des personnes morales ou physiques, propriétaires ou gestionnaires de l'immeuble ou du bâtiment raccordé, ayant souscrit une police d'abonnement au service public de chaleur pour les besoins d'un immeuble dont elles sont propriétaires ou gestionnaires désignées ci-après par le terme « Abonnés », et celles des « Usagers », terme désignant toute personne, physique ou morale, bénéficiaire final du Service.

Le Concessionnaire collectera des données à caractère personnel pour des finalités déterminées, explicites et légitimes, à savoir notamment :

- **mise en place des abonnements ;**
- **gestion de la relation avec les Abonnés et Usagers** (i.e. encaissement des droits de raccordement, des redevances ; communication aux Abonnés et/ou Usagers concernant l'état du réseau, concernant les travaux menés sur les installations, notamment ceux devant affecter la continuité ou la qualité de la fourniture, les pannes ou d'interruptions du service ; le coût du service et la facturation; mise à disposition des Abonnés et/ou Usagers du suivi des consommations ; mise en place d'actions de pédagogie et d'un moyen visant à permettre aux Abonnés de détecter de façon la plus réactive possible d'éventuelles dérives destinée à aider à réaliser des économies d'énergie ; répondre aux demandes formulées par les Abonnés et/ou Usagers et en faire communication à l'Autorité Concédante si besoin)
- **Transmission annuelle de la base Abonnés telle** que prévue à **l'article 69.5 du Contrat de concession;**
- **Prospection** : mise en place d'un dispositif de prospection basé sur un inventaire et une cartographie des bâtiments existants potentiellement raccordables au réseau,



référençant les énergies en place, les puissances, l'âge des équipements ; réalisation d'enquêtes de satisfaction auprès des Abonnés ;

- **Développement du service** : opérations d'extension, densification, optimisation, interconnexion du réseau

2.3 Statut des Parties

Pour rappel, le Sous-traitant est celui qui traite de données personnelles « *pour le compte, sur instruction et sous l'autorité d'un responsable de traitement* », lui-même défini au sein de l'article 4 du RGPD comme « *la personne physique ou morale, l'autorité publique, le service ou un autre organisme qui, seul ou conjointement avec d'autres, détermine les finalités et les moyens du traitement.* ».

Dans le même ordre d'idées, une coresponsabilité naît lorsque plusieurs parties déterminent, pour certaines opérations de traitement :

- soit les finalités,
- soit les éléments essentiels des moyens.

Il en dérive que dans le cadre d'une coresponsabilité, la participation des parties à la détermination conjointe peut revêtir différentes formes et n'est pas nécessairement partagée de façon égale.

Afin de définir avec exactitude le statut des parties, les [Lignes directrices 07/2020 concernant les notions de responsable du traitement et de sous-traitant dans le RGPD](#) de l'EDPB précisent que la répartition des rôles devrait généralement résulter d'une analyse des éléments factuels ou des circonstances de l'espèce et, en tant que telle, elle n'est pas négociable (§ 12).

Dans son guide « [La responsabilité des acteurs dans le cadre de la commande publique](#) » (2022), la CNIL précise également que l'identification des acteurs doit, sauf disposition légale encadrant le traitement et procédant à une désignation directe ou indirecte, résulter d'une analyse des circonstances juridiques et factuelles dans lesquelles il intervient. La CNIL précise notamment que « *C'est la nature du service sollicité dans le marché ou la concession et le fait que les principales composantes d'un ou plusieurs traitements de données y ont été encadrées qui vont déterminer si les opérations de traitement en cause ont été suffisamment décidées par l'administration et relèvent, à ce titre, de sa responsabilité.* »

L'analyse ci-dessous doit permettre de déterminer les statuts de chaque entité juridique en fonction des différentes finalités des traitements qui seront mis en œuvre dans le cadre de la Concession. **Elle pourra être complétée/adaptée au cours des phases de la consultation.**



| Finalités | Niveau d'autonomie du Concessionnaire | Qualifications |
|---|---|--|
| Mise en place des abonnements | Les finalité et les conditions sont fixées par l'Autorité Concédante de commun accord avec le Concessionnaire dans le Contrat. | Autorités Concédante et Concessionnaire : RT conjoints |
| Gestion de la relation avec les Abonnés : Sous-finalité : Encaissement des droits de raccordement, des redevances | Activité dans laquelle l'Autorité Concédante n'intervient pas. Les finalités et les moyens sont déterminées par le Concessionnaire qui supporte les risques. | Concessionnaire : RT |
| Gestion de la relation avec les Abonnés et les Usagers : Sous-finalités : 1. Communication aux Abonnés et/Usager concernant l'état du réseau (i.e. les travaux menés sur les installations, notamment ceux devant affecter la continuité ou la qualité de la fourniture, les pannes ou d'interruptions du service, ...), le coût du service et la facturation; 2. Répondre aux demandes formulées par le Abonnés et/ou Usagers et en faire communication à l'Autorité Concédante (telles que les demandes d'intervention ou réclamations). | Contrôle de l'Autorité Concédante. Le Concessionnaire devra mettre en place un ensemble d'outils de communication grâce auxquels les abonnés pourront faire connaître leurs éventuels problèmes vis-à-vis du service. | Autorité Concédante et Concessionnaire : RT conjoints |



| | | |
|---|---|--|
| <p>Gestion de la relation avec les Abonnés :</p> <p>Sous-finalités :</p> <p>1. Mise à disposition des Abonnées et/usagers du suivi des consommations.</p> <p>2. Mise en place pour le suivi d'un moyen permettant aux Abonnés de détecter de façon la plus réactive possible d'éventuelles dérives destinée à aider à réaliser des économies d'énergie</p> <p>3. Mise à disposition annuelle à l'Autorité Concédante d'une base de données Abonnés</p> | <p>Finalité définie par l'Autorité Concédante, mais moyens essentiels et non essentiels définis par le Concessionnaire.</p> | <p>Autorité Concédante et Concessionnaire : RT conjoints</p> |
| <p>Développement du service / prospection :</p> <p>Le Concessionnaire assure à ses frais, risques et périls, la commercialisation du Service à l'intérieur du périmètre concédé.</p> <p>Mise en place d'un dispositif de prospection basé sur un inventaire et une cartographie des bâtiments existants potentiellement raccordables au réseau</p> | <p>. Finalités définies par l'Autorité Concédante ; Moyens essentiels à déterminer par le Concessionnaire</p> | <p>Autorité Concédante et Concessionnaire : Responsables conjoints</p> |



Conclusion et observations :

Compte tenu de l'analyse, le Concessionnaire préconise de retenir la qualification de responsable de traitement ou de responsable de traitement conjoint, en fonction des finalités ou sous-finalités identifiées.

Une telle approche mérite d'être approfondie et discutée avec l'Autorité Concédante. En fonction de la qualification retenue, le Contrat de concession devra comporter un dispositif contractuel adapté visant à régir les droits et obligations des Parties. Le Concessionnaire attire l'attention de l'Autorité Concédante sur le fait que le schéma retenu aura un impact, notamment, sur le clausier à mettre en place, sur les obligations d'information à l'égard des personnes concernées, etc..

2.4 Données traitées

Dans le cadre du Contrat de concession, le Concessionnaire sera amené à traiter à l'occasion des finalités présentées au 2.2 du présent document, les données listées ci-dessous et figurant dans la Base Abonné telle que définie dans **l'article 69.5 du Contrat de Concession**.

Il est précisé que les données listées ci-après ne sauraient être qualifiées de données à caractère personnel que si elle sont rattachées, directement ou indirectement, à une personne physique (représentant de l'Abonné et/ou Usager).

- Référence et adresse du Poste de Livraison de l'Abonné ;
- Identification du type d'usage (chauffage, ECS, vapeur, froid, chaleur process) avec indication des puissances souscrites ;
- Réseau (en cas de pluralité de réseau)
- Identification de l'Abonné
 - personnes physiques : nom, prénom, adresse, n° de téléphone et courriel de l'Abonné ;
 - personnes morales : raison sociale ou dénomination, adresse du siège social, numéro RCS ou registre des métiers, nom du mandataire social
- type d'Abonné (bailleur social, syndicat de copropriété, collectivité, hôpital, promoteur privé, ...)
- Identification du destinataire de la facture, si ce dernier est différent de l'Abonné ;
- Référence au type d'abonnement / tarifs appliqué ;
- Référence du compteur : date de pose et de dernière vérification du compteur selon **l'ARTICLE 38.4 – Mesure des fournitures** ;
- Divers :
 - Les informations relatives aux réclamations, aux incidents de paiement, y compris les pièces relatives au recouvrement contentieux en cours, le cas échéant ;
 - L'historique des contacts, demandes de renseignement et courrier clientèle et des interventions techniques ou commerciales avec l'Abonné.



Parmi les données personnelles susceptibles d'être collectées dans le cadre du Contrat, le candidat n'identifie, a priori, aucune donnée susceptible d'être qualifiée de sensible¹.

2.5 Mise à jour et durées de conservation des données collectées

Conservation des données pendant l'exécution du Contrat de concession

Les données seront conservées pendant la durée de l'exécution du Contrat de concession.

Le candidat s'engage à ce que :

- toute Donnée à caractère personnel de l'Abonné/Usager soit maintenue exacte et à jour pour toute la durée de l'exécution du Contrat de concession ;
- une durée de conservation des Données à caractère personnel de l'Abonné/Usager soit définie en fonction des finalités poursuivies ;
- ne soient collectées que les données légitimes au regard de la finalité du traitement et de la nature des données à caractère personnel de l'Abonné/Usager.

Les données traitées aux fins de la gestion de la relation avec les Abonnés/Usagers sont conservées par le Concessionnaire pendant toute la durée de la police d'abonnement, majorée des durées de conservation légales applicables au Concessionnaire (i.e. prescription en matière comptable, etc.).

Concernant les données conservées au-delà de la date de fin de la police d'abonnement, le Concessionnaire met en place un niveau d'archivage intermédiaire permettant de conserver ces données de manière sécurisée et d'accès restreint afin de respecter les obligations légales de conservation et de se prémunir en cas d'éventuels contentieux.

Les données personnelles des Abonnés/Usagers recueillies aux fins de prospection commerciale, seront conservées par le Concessionnaire trois (3) ans maximum après le dernier contact commercial.

Sort des données en fin de Concession

A l'expiration des durées de conservation définies ci-dessus, sur demande de l'Autorité Concédante, le Concessionnaire détruira intégralement les copies de Données Personnelles détenues dans ses systèmes d'information et en apportera la preuve (ex : attestation sur l'honneur ou/et procès-verbal du RSSI, impressions d'écrans etc.), concomitamment à la signature du procès-verbal de restitution du fichier d'Abonnés.

¹ Désignées « catégories particulières de données à caractère personnel » par l'art 9 RGPD, à savoir les informations qui révèlent la prétendue origine raciale ou ethnique, les opinions politiques, les convictions religieuses ou philosophiques ou l'appartenance syndicale, ainsi que le traitement des données génétiques, des données biométriques aux fins d'identifier une personne physique de manière unique, des données concernant la santé ou des données concernant la vie sexuelle ou l'orientation sexuelle d'une personne physique.



2.6 Destinataires des données collectées – Sous-traitance

Les données personnelles ne seront communiquées qu'aux seules personnes concernées par ces informations ainsi qu'aux tiers autorisés ayant qualité pour les recevoir de façon ponctuelle et motivée.

Les données à caractère personnel pourront être partagées ou sous-traitées s'agissant d'une partie des traitements réalisés aux fins de fournitures des prestations prévues par le Contrat de concession.

Le Concessionnaire mettra en œuvre ou s'appuiera sur des documents pertinents afin de s'assurer que son sous-traitant garantit un niveau de protection des données à caractère personnel équivalent aux dispositions prévues par le Contrat de concession.

Sur demande expresse, le Concessionnaire fournira à l'autorité Concédante une liste de ses sous-traitants intervenants dans la fourniture des prestations.

2.7 Information et droits des personnes concernées

Le candidat s'engage à ce que :

- Une information complète, claire et exacte sera dispensée aux Personnes Concernées dont les Données à caractère personnel sont traitées, conformément aux articles 13 et 14 du RGPD ;

Cette information sera notamment déployée :

- Dans une clause dédiée des règlements de services et des polices d'abonnement
- Sur le site internet dédié qui sera mis en place par le Concessionnaire : à cet effet, ENGIE Solutions a notamment élaboré un pack de conformité de ses sites Internet, intégrant des modèles de mentions légales, conditions générales d'utilisation, notices Privacy et cookies conformes aux exigences réglementaires et de la CNIL.

En fonction de la qualification des Parties qui sera retenue, les obligations d'information à l'égard des personnes concernées seront à la charge de l'une et/ou l'autre Partie ;

- Des moyens appropriés et effectifs seront garantis aux Personnes Concernées dont les Données à caractère personnel seront traitées en vertu du Contrat de concession afin d'exercer leurs droits concernant le traitement de leurs données à caractère personnel conformément à la législation en vigueur (accès, rectification, mise à jour, suppression, etc.) ;
- Lorsqu'une demande émanant d'une Personne Concernée sera directement adressée au Concessionnaire, ce dernier répondra à la demande de la Personne Concernée dans sa totalité, correctement, et dans un délai raisonnable ;
- Le Concessionnaire informera l'Autorité Concédante, selon des modalités à convenir, de la demande ainsi que de la réponse apportée à l'Abonné/Usager.



2.8 Mesures de sécurité et de confidentialité

Le Concessionnaire s'engage à mettre en place et à maintenir pendant toute la durée du Contrat de concession toutes les mesures techniques et organisationnelles, notamment les mesures matérielles et logiques éprouvées au sein du Groupe ENGIE, et adaptées à la nature des Données Personnelles traitées et aux risques présentés par les traitements qu'elle effectuera, y compris, entre autres :

- l'application de mesures de sécurité et de confidentialité techniques et organisationnelles ayant pour objectif d'empêcher la destruction, la perte, l'altération ou la communication ou l'accès non-autorisé, de manière accidentelle ou illicite, des/aux données à caractère personnel ;
- le chiffrement des flux de données ;
- la gestion, le suivi et la revue régulière des habilitations du personnel du Concessionnaire accédant aux données personnelles traitées ;
- les moyens permettant de garantir la confidentialité, l'intégrité, la disponibilité et la résilience constantes des systèmes et des services de traitement ;
- la mise en œuvre de sauvegarde (back-up) des données traitées ;
- le cloisonnement des données personnelles traitées dans le cadre du Contrat de concession ;
- l'hébergement des données capable de satisfaire les exigences de sécurité physique (contrôles des accès physiques, alarme anti intrusion...) ;
- les moyens permettant de rétablir la disponibilité des données et l'accès à celles-ci dans des délais appropriés en cas d'incident physique ou technique ;
- la mise en place de procédures visant à tester, à analyser et à évaluer régulièrement l'efficacité des mesures techniques et organisationnelles pour assurer la sécurité du traitement ;
- la mise en place d'une protection contre les cyber attaques pour protéger les données personnelles traitées dans le cadre du Contrat (ex : politique antivirus).

Le Concessionnaire déclare, pour ce faire, disposer d'un système d'information sécurisé conformément aux standards Internationaux ISO 27001. Le Concessionnaire dispose d'une procédure et d'outils internes destinés à régir les éventuels cas de violation de données personnelles de manière efficace. La procédure décrit les rôles, les moyens et les obligations des parties prenantes internes et externes.

Si de telles menaces ou vulnérabilités étaient constatées, le Concessionnaire informera sans délai l'Autorité Concédante de ladite menace ou vulnérabilité. Le Concessionnaire mettra par ailleurs en place un plan d'action ou de remise en état afin de supprimer, atténuer ou limiter l'impact de la menace ou de la vulnérabilité. En effet, Le Concessionnaire s'est dotée d'une organisation de la sécurité qui évolue et s'adapte continuellement afin d'être performante, réactive, capable de détecter et de pallier les menaces et les risques de violation.



2.9 Analyse d'Impact sur la Protection des Données (AIPD)

L'analyse d'impact sur la protection des données (AIPD) est une analyse qui doit être obligatoirement réalisée par le responsable de traitement préalablement à la mise en œuvre d'un traitement de données à caractère personnel, lorsque ledit traitement est « susceptible d'engendrer un risque élevé pour les droits et libertés des personnes concernées ».

- soit le traitement envisagé figure dans la liste des types d'opérations de traitement pour lesquelles la CNIL a estimé obligatoire de réaliser une analyse d'impact relative à la protection des données (<https://www.cnil.fr/sites/default/files/atoms/files/liste-traitements-aipd-requise.pdf>)
- Soit le traitement remplit au moins deux des neuf critères issus des lignes directrices du G29 :
 - évaluation/scoring (y compris le profilage) ;
 - décision automatique avec effet légal ou similaire ;
 - surveillance systématique ;
 - collecte de données sensibles ou données à caractère hautement personnel ;
 - collecte de données personnelles à large échelle ;
 - croisement de données ;
 - personnes vulnérables (patients, personnes âgées, enfants, etc.) ;
 - usage innovant (utilisation d'une nouvelle technologie) ;
 - exclusion du bénéfice d'un droit/contrat

Dans le cadre de la Concession, seul le critère lié à une collecte de données « à large échelle » devrait être rempli. En conséquence, sous réserve d'une analyse ultérieure plus poussée, le candidat estime à ce stade qu'une AIPD n'est pas requise dans le cadre de la Concession.

Toutefois, le candidat attire l'attention de l'autorité Concédante qu'il entend mettre en place une démarche *privacy by design*, ce qui pourra permettre d'identifier de manière efficace et dans les plus brefs délais les principaux risques liés au traitement et d'adopter les mesures techniques et organisationnelles adaptées aux risques d'atteinte à la vie privée des personnes concernées.

En outre, en cas de demande expresse, Le Concessionnaire pourra diligenter des analyses d'impact par finalité. Elle dispose à cet effet d'une procédure et d'outils dédiés à ce type d'exercice.

2.10 Autres engagements

Le Concessionnaire s'assurera que toute Donnée à caractère personnel traitée aux fins du Contrat de concession soit traitée conformément à la réglementation en vigueur.

Le Concessionnaire s'engage notamment à ce que :

- toute donnée à caractère personnel traitée dans le cadre du Contrat de concession sera traitée sur le fondement d'une base juridique appropriée autorisée par la réglementation en vigueur en matière de protection des données ;



- toute donnée à caractère personnel sera traitée pour une finalité définie, explicite et légitime ;
- toute donnée à caractère personnel sera pertinente et non excessive au regard de la ou des finalités poursuivies ;
- le cas échéant, toutes les formalités nécessaires et appropriées, ou la documentation interne exigé(es) conformément à la Législation Applicable en matière de Protection des Données, seront accomplies et conservées en interne ;
- un registre des activités de traitement de données personnelles traitées sera tenu ;
- le personnel chargé du traitement des données à caractère personnel dans le cadre du Contrat de concession sera formé et soumis à une obligation de confidentialité appropriée concernant le traitement de Données à caractère personnel.

