# Rapport sur les obligations issues du Règlement Général sur la Protection des Données

**Projet SMILE, Chantier SEN1 – phase POC**

Tableau de suivi des versions

| | | | | |
|---|---|---|---|---|
| Version | 1 | | | |
| Auteurs | CGE, JXM, GHU | | | |
| Date | 25/06/19 | | | |
| Commentaires | Version initiale | | | |


Diffusion : illimitée
Contact : pro _@_ consometers.org

# TABLE DES MATIÈRES

# 1 Avant-propos

Le présent rapport est structuré en trois parties. Tout d'abord l'avant-propos précise le cadre et les références de l'étude. Ensuite la partie contexte reprend les éléments saillants des lois étudiées et le contexte dans lequel elles s'inscrivent. Enfin, l'analyse que nous en faisons, ainsi que les recommandations à en tirer pour le projet SEN1 sont regroupées en troisième partie. N'étant pas juristes, cette extrapolation est donc issue de notre lecture et compréhension des deux lois.

Il ne sera fait état ici que des prescriptions concernant un protocole fédéré d'échange de donnée énergétique, conformément aux objectifs du projet SEN1 dans sa phase de préfiguration (Proof-of-Concept ou POC). Ainsi il a été omis toute information concernant des données dites sensibles (données concernant la santé, le domaine public, le domaine juridique...).

De même, les modalités de l'échange de données entre membres, et leurs implications spécifiques.

## 1.1 Textes étudiés

Dans le présent rapport, nous avons analysé dans le détail les deux textes de loi suivants :

- le Règlement Général pour la Protection des Données ou règlement (UE) 2016/679 du 27 avril 2016, désigné par la suite « le RGPD », qui définit le cadre au niveau Européen, qui se compose de 173 considérants et 99 articles, https://www.cnil.fr/fr/reglement-europeen-protection-donnees,
- l'ordonnance n° 2018-1125 du 12 décembre 2018, appelé par la suite « l'Ordonnance », qui précise l'application du RGPD dans la loi française, https://www.cnil.fr/fr/publication-de-lordonnance-de-reecriture-de-la-loi-informatique-et-libertes .

## 1.2 Zone géographique

Nous nous sommes cantonnés dans ce premier travail à l'étude des chapitres du RGPD traitant des transferts intra-européens. Nous avons également étudié sa retranscription dans le droit français jusqu'au début de l'année 2019.

Ainsi, dans le cadre de notre POC et vraisemblablement pour les premières versions de la fédération, le Responsable de Traitement devra être situé en Europe et l'utilisateur devra résider en France. En effet, même si le RGPD est un règlement européen permettant l'uniformisation des règles en termes de gestion des données personnelles, une cinquantaine de point laissent des marges de manœuvre laissés au libre arbitre des Etats membres (ex : âge légal de consentement). Il faudra donc, en tout état de cause, se référer au droit de chaque pays pour contrôler que nous respectons bien ces conditions particulières. Il n'a pas été traité non plus les échanges avec des Responsables de Traitement hors Union Européenne, soumis à un régime distinct.

Cependant, il pourra être envisagé à l'avenir de répliquer cette étude sur l'ensemble des retranscriptions dans les autres Etats membres de l'Union afin de mettre en lumière chacune de ces particularités.

## 1.3 Définitions

Dans le présent rapport, les termes débutant par une majuscule ont la signification suivante (issue des textes de loi étudiés) :

- **Donnée personnelle** : information se rapportant à une personne qui peut être identifiée, directement ou indirectement, notamment par référence à un identifiant (numéro, données de géolocalisation, identifiant en ligne, élément d'identité).
- **Traitement** : opération appliquée à des données, telles que la collecte, l'enregistrement, l'organisation, la structuration, la conservation, l'adaptation ou la modification, l'extraction, la consultation, l'utilisation, la communication par transmission, la diffusion ou toute autre forme de mise à disposition, le rapprochement ou l'interconnexion, la limitation, l'effacement ou la destruction.
- **Pseudonymisation** : le traitement de données de telle façon que celles-ci ne puissent plus être attribuées à une personne concernée précise, sans avoir recours à des informations supplémentaires (séparées de manière technique et organisationnelle).
- **Fichier** : tout ensemble structuré de données à caractère personnel accessibles selon des critères déterminés, que cet ensemble soit centralisé, décentralisé ou réparti de manière fonctionnelle ou géographique.
- **Responsable du traitement (RT)** : 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.
- **Sous-traitant** : qui traite des données à caractère personnel pour le compte du responsable du traitement.
- **Destinataire** : personne physique ou morale, l'autorité publique, le service ou tout autre organisme qui reçoit communication de données à caractère personnel.
- **Consentement de la personne concernée** : toute manifestation de volonté, libre, spécifique, éclairée et univoque par laquelle la personne concernée accepte, par une déclaration ou par un acte positif clair, que des données à caractère personnel la concernant fassent l'objet d'un traitement.
- **Délégué à la protection des données** : Personne assistant le Responsable de Traitement dans ses obligations, avec pour mission (au moins) : l'information du RT sur ses obligations, le contrôle du respect de celles-ci, le conseil sur les analyses d'impact, la coopération et le point de contact avec les autorités de contrôle.

# 2 Contexte et extraits-clés

Cette partie reprend le contexte récent de l'évolution réglementaire autour de la protection des données personnelles, et présente un certain nombre d'articles de loi et d'extraits des textes étudiés. Cela compose la base documentaire sur laquelle nous avons bâti notre analyse, à la fois les références et les liens entre elles.

## 2.1 Contexte

Le Règlement Général sur la Protection des Données (règlement (UE) 2016/679) a été adopté le 14 avril 2016 par le parlement européen. Il résulte d'un travail de quatre ans, pour permettre la protection des données des citoyens au sein des 28 États membres de l'Union Européenne. Il unifie et renforce la protection des données à caractère personnel. Contrairement aux directives européennes, le règlement est d'application directe, et ne nécessite pas de loi de transposition nationale. Cependant, des marges d'adaptation sont laissées à la discrétion de chaque État membre.

Le RGPD est entré en application au 25 mai 2018, laissant ainsi deux ans à chaque État membre pour adapter au besoin son droit national, et aux Responsables de Traitement de s'y conformer.

Fait nouveau, le RGPD prévoit entre autres de lourdes peines pour les Responsables de Traitement ne s'y conformant pas. Il prévoit également que tout RT, indépendamment de sa localisation, doit respecter le RGPD dès lors que les données qu'il traite relèvent d'un résident de l'UE. Cela concrétise ainsi une extra-territorialité des règles européennes à l'échelle mondiale.

Trois grands principes régissent ce règlement :

- Accountability : obligation pour les entreprises de démontrer le respect des dispositions du RGPD (contrôle à posteriori plutôt qu'a priori),
- Privacy by design : la protection des données personnelles doit être prise en compte dès la conception de produit et de service,
- Privacy by default : la protection des données personnelles n'est plus une option mais une obligation appliquée par défaut.

Dans le contexte législatif français, depuis 1978, la France possédait déjà un ensemble de lois, couramment appelé « Loi Informatique et Liberté » (Loi n° 78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés), instaurant notamment la Commission Nationale Informatique et Libertés (CNIL) mais sans véritable pouvoir de sanction.

En vue d'adapter le droit français au RGPD, deux textes techniques ont tout d'abord été adoptés : la LOI n° 2018-493 du 20 juin 2018 « relative à la protection des données personnelles », et le décret (Décret n° 2018-687 du 1er août 2018). Ces deux textes contiennent uniquement de modifications de références, une prise en compte factuelle du RGPD par les autres codes, et des ajouts temporaires, en attendant la véritable adaptation, prévue par l'Ordonnance. Le RGPD définit en effet une cinquantaine de points des marges de manœuvre pour les États membres (pouvoir des

régulateurs nationaux, renforcement du mécanisme d'action de groupe, âge limite de consentement, élargissement des données sensible aux données juridiques, directive en cas de décès ...).

Après consultation de la CNIL sur le projet de loi visant à transposer le règlement européen, celle-ci a rendu un rapport en novembre 2017 dans lequel, elle appelait à l'adoption d'une ordonnance visant à simplifier et rendre plus lisible le nouveau cadre législatif pour les professionnels et les citoyens. Cette recommandation a été entendue par l'état, qui a promulgué l'Ordonnance du 12 décembre 2018 (Ordonnance n° 2018-1125) : ce texte est une refonte complète de la loi Informatique et Libertés.

Avant d'en livrer l'analyse, nous détaillons dans la partie ci-après les dispositions principales de ces deux textes, à la fois en termes de droits des usagers et d'obligations pour les Responsables de Traitement.

## 2.2 Consentement et autorisation de traitement

Une des conditions majeures de licéité de l'utilisation d'information à caractère personnel est d'obtenir le consentement de la personne concernée, tel que défini aux articles 4 à 11 du RGPD. Ce consentement doit être une manifestation de volonté, libre, spécifique, éclairée et univoque. Il devra faire l'objet d'une acceptation par un acte positif clair. Il est également précisé que l'utilisateur doit donner son consentement pour l'éventuelle transmission et le traitement de ses données à caractère personnel par un sous-traitant.

Les conditions de consentement des personnes mineures, et notamment leur âge, fait partie des marges de manœuvre laissées aux États membres. Le RGPD fixe l'âge minimum pour considérer qu'une personne peut consentir seule à 13 ans (limite en dessous de laquelle le consentement sera soumis à son tuteur légal). La France a fait le choix à l'article 45 de l'Ordonnance de relever cette limite à 15 ans. De plus, elle ajoute que le consentement devra se faire conjointement par le mineur concerné et le ou les détenteurs de l'autorité parentale.

## 2.3 Les droits des personnes concernées

### 2.3.1 Droit d'accès et d'information

L'article 15 du RGPD dispose que le Responsable de Traitement doit fournir à l'utilisateur un accès aux données traitées. Son article 13 détaille les informations complémentaires que les personnes concernées peuvent demander au RT pour chaque traitement. Il est fait la distinction entre une collecte directe par le RT effectuant le traitement, et une collecte effectuée via à un autre Responsable de Traitement.

#### 2.3.1.1 Donnée collectée directement auprès de l'utilisateur

Le Responsable de Traitement qui collecte auprès d'une personne des données à caractère personnel devra être en mesure de lui fournir les informations suivantes :

- l'identité et les coordonnées du Responsable de Traitement et le cas échéant les coordonnées du délégué à la protection des données
- les finalités du traitement
- les destinataires des données s'ils existent
- la durée de conservation
- l'existence du droit de demander :
  - le retrait du consentement
  - l'accès aux données
  - la rectification
  - l'effacement
  - la limitation ou l'opposition de traitement
  - le portabilité des données
- l'existence du droit d'introduire une réclamation auprès de l'autorité de contrôle
- si les données à caractère personnel ont un caractère contractuel ou réglementaire. Si la personne concernée est tenue de fournir les données à caractère personnel, elle doit être également informée sur les conséquences de la non-fourniture.

Le droit français (art. 48 de l'Ordonnance) ajoute que le Responsable de Traitement est tenu d'informer la personne concernée qu'elle peut définir des directives quant au sort de ses données après sa mort.

Si les finalités de traitement de ces données changent, il a également l'obligation d'en informer la personne concernée.

En cas de rectification, d'effacement ou de limitation de traitement de données à caractère personnel, le RT se doit de notifier chaque destinataire auquel les données à caractère personnel ont été envoyées dans la mesure où cela ne se révèle pas impossible ou exige des efforts disproportionnés. Si l'utilisateur en fait la demande, il recevra également des informations sur les destinataires (art. 19 du RGPD).

#### 2.3.1.2 Donnée reçue d'un autre Responsable de Traitement

Lorsque le Responsable de Traitement ne collecte pas directement les données à caractère personnel, il possède les mêmes devoirs que celui qui les collecte, précisés aux articles 14-1 et 14-2 du RGPD, auxquels s'ajoutent deux éléments :

- les catégories de données à caractère personnel concernées par ce transfert,
- la source d'où proviennent les données à caractère personnel.

Le Responsable de Traitement ne collectant pas les données directement, il se peut dans certains cas qu'il ne puisse pas communiquer ces informations aussitôt à la personne concernée, faute d'avoir un contact direct. Cependant l'article 14-3 fait état d'un délai ne dépassant pas un mois pour

effectuer ce devoir. Ce même article précise qu'avant de pouvoir à son tour communiquer ces données à un autre destinataire, il devra s'acquitter de fournir à la personne concernée les informations précédentes.

### 2.3.2 Droit de rectification et d'effacement des données

Chaque Responsable de Traitement (RT) doit laisser à ses utilisateurs le droit de rectification (art. 16 du RGPD) de ses données à caractère personnel, qui ne sont plus à jour ou tout simplement erronées. L'Ordonnance ajoute que si celles-ci ne sont plus à jour, elles doivent être rectifiées ou supprimées sans tarder (art. 4-4). Pour finir, l'article 19 du RGPD oblige, dans la mesure du possible, à notifier chaque destinataire auquel les données à caractère personnel ont été communiquées, qu'elles ont été mises à jour.

Le Responsable de Traitement a l'obligation d'effacer les données à caractère personnel dans les meilleurs délais (art. 17 du RGPD), dans les cas suivants :

- les données à caractère personnel ne sont plus nécessaires au regard des finalités pour lesquelles elles ont été collectées ou traitées d'une autre manière
- la personne concernée retire le consentement sur lequel est fondé le traitement
- la personne concernée s'oppose au traitement
- les données à caractère personnel ont fait l'objet d'un traitement illicite
- les données à caractère personnel doivent être effacées pour respecter une obligation légale auquel le responsable du traitement est soumis.

Lorsque la donnée a été rendue publique et que le RT est tenu de les effacer, il est stipulé à l'article 17-2 du RGPD que

> *« Le responsable du traitement, compte tenu des technologies disponibles et des coûts de mise en œuvre, prend des mesures raisonnables, pour informer les RT qui traitent ces données à caractère personnel que la personne concernée a demandé l'effacement, par ces responsables du traitement, de tout lien vers ces données à caractère personnel, ou de toute copie ou reproduction de celles-ci. »*

L'Ordonnance précise à son article 51 la disposition pour les personnes mineures au moment de la collecte.

### 2.3.3 Droit à la limitation et à l'opposition de traitement

L'article 21 du RGPD précise que la personne concernée a le droit de s'opposer au traitement de ses données à caractère personnel, à moins que le RT ne démontre qu'il existe des motifs légitimes pour ce traitement (qui prévalent alors sur les intérêts et les droits). Chaque Responsable de Traitement (RT) doit laisser à ses utilisateurs le droit de rectification (art. 16 du RGPD) de ses données à caractère personnel, qui ne sont plus à jour ou tout simplement erronées. L'Ordonnance ajoute que si celles-ci ne sont plus à jour, elles doivent être rectifiées ou supprimées sans tarder (art. 4-4). Pour finir, l'article 19 du RGPD oblige, dans la mesure du possible, à notifier chaque destinataire auquel les données à caractère personnel ont été communiquées, qu'elles ont été mises à jour.

Le Responsable de Traitement a l'obligation d'effacer les données à caractère personnel dans les meilleurs délais (art. 17 du RGPD), dans les cas suivants :

- les données à caractère personnel ne sont plus nécessaires au regard des finalités pour lesquelles elles ont été collectées ou traitées d'une autre manière
- la personne concernée retire le consentement sur lequel est fondé le traitement
- la personne concernée s'oppose au traitement
- les données à caractère personnel ont fait l'objet d'un traitement illicite
- les données à caractère personnel doivent être effacées pour respecter une obligation légale auquel le responsable du traitement est soumis.

Lorsque la donnée a été rendue publique et que le RT est tenu de les effacer, il est stipulé à l'article 17-2 du RGPD que :

> *« Le responsable du traitement, compte tenu des technologies disponibles et des coûts de mise en œuvre, prend des mesures raisonnables, pour informer les RT qui traitent ces données à caractère personnel que la personne concernée a demandé l'effacement, par ces responsables du traitement, de tout lien vers ces données à caractère personnel, ou de toute copie ou reproduction de celles-ci. »*

L'Ordonnance précise à son article 51 la disposition pour les personnes mineures au moment de la collecte.

### 2.3.4 Droit à la limitation et à l'opposition de traitement

L'article 21 du RGPD précise que la personne concernée a le droit de s'opposer au traitement de ses données à caractère personnel, à moins que le RT ne démontre qu'il existe des motifs légitimes pour ce traitement (qui prévalent alors sur les intérêts et les droits et libertés de la personne concernée), ou que ces données sont nécessaires pour la constatation, l'exercice ou la défense de droits en justice.

Le RT devra, au plus tard au moment de la première communication avec la personne concernée, présenter clairement et séparément de toute autre information ses droits à l'opposition de traitement.

Il est également exprimé à l'article 18 du RGPD un droit à la limitation de traitement, permettant alors à ces données à caractère personnel de n'être, à l'exception de la conservation, traitées qu'avec le consentement de la personne concernée, ou pour :

- la constatation, l'exercice ou la défense de droits en justice
- pour la protection des droits d'une autre personne physique ou morale
- pour des motifs importants d'intérêt public de l'Union ou d'un État membre.

Cette limitation peut s'exercer uniquement quand :

- l'exactitude des données à caractère personnel est contestée par la personne concernée. Dans ce cas elle s'applique pendant une durée permettant au Responsable du Traitement de vérifier l'exactitude des données à caractère personnel,

- le traitement est illicite et la personne concernée s'oppose à leur effacement et exige à la place la limitation de leur utilisation,
- le Responsable du Traitement n'a plus besoin des données à caractère personnel aux fins du traitement mais celles-ci sont encore nécessaires à la personne concernée pour la constatation, l'exercice ou la défense de droits en justice,
- la personne concernée s'est opposée au traitement en vertu de l'article 21. Pendant la vérification portant sur le point, les données seront alors limitées jusqu'à ce qu'il soit démontré que les motifs légitimes poursuivis par le Responsable du Traitement prévalent sur ceux de la personne concernée au titre de son droit d'opposition.

Il est également précisé qu'en cas de levée de la limitation, le RT devra en informer la personne concernée.

### 2.3.5 Droit à la portabilité des données

Conformément à l'article 20 du RGPD, la personne concernée a le droit d'exercer un droit de portabilité de ses données à caractère personnel, selon les dispositions suivantes :

1. Les personnes concernées ont le droit de recevoir les données à caractère personnel les concernant qu'elles ont fournies à un responsable du traitement, dans un format structuré, couramment utilisé et lisible par machine, et ont le droit de transmettre ces données à un autre responsable du traitement sans que le responsable du traitement auquel les données à caractère personnel ont été communiquées y fasse obstacle, lorsque:
    a. le traitement est fondé sur le consentement en application de l'article 6, paragraphe 1, point a), ou de l'article 9, paragraphe 2, point a), ou sur un contrat en application de l'article 6, paragraphe 1, point b);
    b. le traitement est effectué à l'aide de procédés automatisés.
2. Lorsque la personne concernée exerce son droit à la portabilité des données en application du paragraphe 1, elle a le droit d'obtenir que les données à caractère personnel soient transmises directement d'un responsable du traitement à un autre, lorsque cela est techniquement possible.
3. L'exercice du droit, visé au paragraphe 1 du présent article s'entend sans préjudice de l'article 17. Ce droit ne s'applique pas au traitement nécessaire à l'exécution d'une mission d'intérêt public ou relevant de l'exercice de l'autorité publique dont est investi le responsable du traitement.
4. Le droit visé au paragraphe 1 ne porte pas atteinte aux droits et libertés de tiers.

## 2.4 La pseudonymisation et l'anonymisation

Le RGPD définit la pseudonymisation dans son article 4 §5 comme « *le traitement de données à caractère personnel de telle façon que celles-ci ne puissent plus être attribuées à une personne concernée précise sans avoir recours à des informations supplémentaires, pour autant que ces*

*informations supplémentaires soient conservées séparément et soumises à des mesures techniques et organisationnelles afin de garantir que les données à caractère personnel ne sont pas attribuées à une personne physique identifiée ou identifiable. »*

Le considérant 28 précise que la pseudonymisation est un outil mais ne constitue pas une mesure de protection complète :

*« La pseudonymisation des données à caractère personnel peut réduire les risques pour les personnes concernées et aider les responsables du traitement et les sous-traitants à remplir leurs obligations en matière de protection des données. L'introduction explicite de la pseudonymisation dans le présent règlement ne vise pas à exclure toute autre mesure de protection des données. »*

Enfin le considérant 26 précise :

*« Il y a lieu d'appliquer les principes relatifs à la protection des données à toute information concernant une personne physique identifiée ou identifiable. Les données à caractère personnel qui ont fait l'objet d'une pseudonymisation et qui pourraient être attribuées à une personne physique par le recours à des informations supplémentaires devraient être considérées comme des informations concernant une personne physique identifiable. Il convient de prendre en considération l'ensemble des moyens raisonnablement susceptibles d'être utilisés par le responsable du traitement ou par toute autre personne pour identifier la personne physique directement ou indirectement, tels que le ciblage. Pour établir si des moyens sont raisonnablement susceptibles d'être utilisés pour identifier une personne physique, il convient de prendre en considération l'ensemble des facteurs objectifs, tels que le coût de l'identification et le temps nécessaire à celle-ci, en tenant compte des technologies disponibles au moment du traitement et de l'évolution de celles-ci. ».*

Ainsi le considérant expose qu'à l'inverse, il n'y a pas lieu d'appliquer les principes de protection à des données où la personne concernée n'est plus identifiable (ce qui relève alors de l'anonymisation des données).

## 2.5 Sous-traitance / co-traitance entre Responsables de Traitement

Ce sujet est particulièrement important pour notre étude dans le cadre du projet SEN1, en ce qu'il définit les rôles et les obligations relatives des différents participants à la fédération.

### 2.5.1 Lien entre RT et sous-traitant

Selon les articles 28 et 29 du RGPD, une application ou un service est considéré comme un sous-traitant au titre du RGPD lorsqu'il effectue un traitement de donnée à caractère personnel pour le compte d'un autre RT. Le Responsable de Traitement final doit alors répondre aux exigences normales du RGPD, tout en étant soumis à des règles strictes le liant à son RT donneur d'ordre.

L'Ordonnance prévoit également que :

- il est formellement interdit à tout sous-traitant et toute personne agissant sous l'autorité du Responsable du Traitement ou sous celle du sous-traitant, de traiter des données à caractère personnelle sans l'accord du Responsable de Traitement (article 61),
- ce traitement sous-traité devra faire l'objet d'un contrat écrit entre le RT et le sous-traitant, y compris en format électronique (article 60). Il est toutefois précisé à l'article 40-2 du RGPD

que ce contrat peut prendre la forme d'un code de conduite (voir : 2.6 Les codes de conduite),

- le sous-traitant ne peut pas recruter un autre sous-traitant sans l'autorisation écrite préalable, spécifique ou générale, du Responsable du Traitement.

### 2.5.2 Lien entre les RT conjoints

Conformément à l'article 26 du RGPD, les Responsables conjoints du Traitement (ci-après « RcT ») sont définis ainsi :

- Lorsque deux Responsables du Traitement, ou plus, déterminent conjointement les finalités et les moyens du traitement, ils sont les Responsables conjoints du Traitement.
- Ils se doivent de définir de manière transparente leurs obligations respectives par voie d'accord entre eux afin de respecter le RGPD. Dans cet accord, les rôles respectifs de chaque RcT y sont précisés, ainsi que leurs liens respectifs avec la personne concernée par l'usage de ses données personnelles. Il pourra cependant être désigné un point de contact unique pour celle-ci. Il est aussi précisé que les grandes lignes de l'accord doivent être mises à la disposition de la personne concernée.
- Enfin, la personne concernée pourra faire valoir les droits que lui confère le RGPD auprès de l'un quelconque des RcT.

## 2.6 Les codes de conduite

Le RGPD prévoit à son article 40 la possibilité, pour des catégories de Responsables de Traitement aux besoins spécifiques (notamment les PME), de mettre en place des règles qui viennent préciser ou compléter les modalités d'application du Règlement. De telles règles sont appelées Codes de Conduite, une fois validées par le régulateur. Les considérants 99, 77 et 81 ainsi que les articles 41 à 43 du RGPD définissent la procédure de validation et de certification concernant ces codes de conduite. Ils deviennent ainsi des pièces supplémentaires dans l'évaluation juridique des « garanties suffisantes » au titre du RGPD, pour tous les Responsables de Traitement qui s'engagent à les respecter.

# 3 Analyse et recommandations

Cette partie contient les analyses que nous faisons du corpus de textes disponibles, éclairé par les premières actualités sur le sujet. Les recommandations sont condensées dans une forme spécifique, pour faciliter une utilisation opérationnelle pour de prochains projets.

## 3.1 Consentement

Le cadre du RGPD renverse les positions de pouvoir dans l'utilisation des données personnelles : les RT ayant un pouvoir de fait (par leur contrôle des infrastructures techniques permettant de rendre les services), le RGPD construit alors une régulation en mettant l'usager au centre et en libérant ses choix. Il est par exemple interdit de conditionner l'accès à un service (site web, prestation...) à la fourniture de données qui ne sont pas indispensables à la fourniture dudit service (données d'identité ou comportement de navigation, par exemple).

La présente étude ne formule pas de recommandation quant à la collecte du consentement pour chaque application pour ses propres usages. Ce cas standard est déjà traité par la littérature disponible.

Le cas considéré ici est celui du transfert de données demandé par une application « initiale » (l'application depuis laquelle l'usager demande l'accès à des données issues de la fédération) à une application « secondaire ». Dans cette optique, la fédération n'a pas de rôle juridique entre ces deux applications.

RECOMMANDATION 1

Dans le cadre de la fédération, le recueil du consentement peut s'envisager selon deux modalités :

1. Le consentement est laissé à la charge de l'application « initiale » qui en transfère une preuve à l'application « secondaire », et assume l'ensemble de la responsabilité de traitement.
2. La demande de consentement est transmise à l'application « secondaire » qui le recueille selon ses propres modalités, puis transmet les données concernées à l'application « initiale ».

Dans les deux cas, il sera opportun de disposer d'un parcours d'inscription harmonisé, qui garantisse la validité du consentement exprimé dans chaque outil de la fédération. Pour cela, il pourra être fait appel à un design d'interface graphique (UI designer) et d'expérience utilisateur (UX designer).

## 3.2 Exercice des droits des personnes

### 3.2.1 Droit d'accès et d'information

Le RGPD pose des exigences de transparence dans les procédures liées aux données traitées. La régulation s'exerce désormais a posteriori, avec une obligation davantage de résultats que de moyens. Comme toute structure utilisant des données personnelles, chaque application fédérée devra répondre à ces obligations.

> RECOMMANDATION 2
>
> Dans le cadre de la fédération, il peut être défini une procédure commune de diffusion des données utilisées et de l'information sur le traitement. Ainsi, les nouveaux entrants dans la fédération auraient un cadre clair (modèles et procédures approuvées) leur permettant de mettre en place leur service de manière rapide et contrôlée.

### 3.2.2 Droit de rectification et d'effacement

L'article 19 du RGPD encadre le devoir du RT en cas de demande d'effacement par la personne concernée, lorsque celui-ci a communiqué (en accord avec la personne concernée) ces données à des RT destinataires. Ainsi il a le devoir de notifier les destinataires de tout effacement, sauf si cela se révèle impossible ou exige des efforts disproportionnés. Cet article ouvre par ailleurs le droit à la personne concernée d'obtenir des informations sur ces destinataires.

Le droit à l'effacement s'applique également en lien direct avec la durée de conservation des données à caractère personnel. En effet, le Responsable de Traitement est tenu d'informer la personne qui consent au partage de ses données à caractère personnel, qu'il les conservera pour une durée limitée au regard du traitement envisagé. Une fois ce délai écoulé, il a l'obligation de les effacer.

Enfin, l'Ordonnance vient préciser (art. 4-4) que les données doivent être tenues à jour : si celles-ci se révèlent inexactes, elles doivent être effacées ou rectifiées sans tarder.

On voit donc à nouveau la nécessité de clarifier la notion de sous-traitance ou de co-traitance dans les liens de la fédération. En effet, dans les deux cas, la notification par le RT « source » est obligatoire (RGPD-Art.19), cependant, dans le cas d'une relation entre un Responsable de Traitement et un sous-traitant, celui-ci n'aura certainement pas d'autre choix que de suivre les prescriptions du RT. En effet, l'article 60 de l'Ordonnance restreint le droit au traitement par un sous-traitant à l'accord du RT. Celui-ci n'ayant lui-même plus l'accord de la personne concernée, il ne peut donner son accord à son sous-traitant.

Cependant, dans une relation entre deux co-traitants s'échangeant des données, la question reste ouverte à ce stade. L'article 19 n'est pas aussi catégorique que l'article 17-2, quant au devenir des copies de ces données en possession du RT destinataire. L'Ordonnance ajoute à l'article 51-II une précision, mais uniquement concernant les personnes mineures au moment de la collecte.

La durée de conservation est une information importante et devra faire l'objet dans notre fédération d'une attention particulière. Elle devra certainement se transmettre au Responsable de Traitement (sous-traitant ou co-traitant) réceptionnant ces données pour qu'il sache sur quelle durée maximale d'engagement le RT collecteur a obtenu l'accord de son l'utilisateur. Dès lors, peut-on considérer qu'à partir du moment où un co-traitant informe l'utilisateur, dans le cadre de l'obligation d'information à l'article 14-2 du RGPD, d'un délai différent, il ne soit plus tenu de suivre le délai émis par le Responsable de Traitement collecteur ? Ou bien s'agit-il d'un délai maximal auquel le RT destinataire ne pourra être qu'inférieur ?

Même si, dans l'Ordonnance comme dans le RGPD, il est ajouté systématiquement des notions relativisant ces actions à des mesures « raisonnables » ou « des efforts disproportionnés », l'application juridique de ces notions devra être éclairé par des jurisprudences adaptées. Il paraît cependant éthiquement difficile de ne pas en tenir compte dans le projet SEN1, compte-tenu du fait que le cœur même de notre développement est justement la communication entre applications via le protocole d'échange fédéré.

RECOMMANDATION 3

Pour chaque application, une attention particulière devra être portée sur la provenance des données. A minima, chaque donnée transférée devra s'accompagner d'une durée de conservation maximale, qui s'imposera aux applications la recevant.

A défaut de pouvoir prouver via le protocole de fédération que les données obtenues auprès d'un Responsable de Traitement ont été collectées directement par lui-même (et qu'il a bien respecté ses devoirs au titre du RGPD), il devra être envisagé de s'en assurer au travers d'un Code de Conduite (voir 2.6 Les codes de conduite), et ce avant toute utilisation de donnée à caractère personnel.

### 3.2.3 Droit à la limitation et l'opposition de traitement

Tout comme le droit à l'effacement, le RT est tenu d'informer les RT auxquelles les données à caractère personnel ont été communiquées, que celles-ci sont soumises à une limitation de traitement. Ainsi la limitation s'appliquera pour les co-traitants et les sous-traitants, à moins que cette communication ne se relève impossible ou exige des efforts disproportionnés (RGPD-Art.19).

RECOMMANDATION 4

En cas d'exercice du droit d'opposition, les données d'un traitement qui consiste en la transmission d'information à un tiers cesseront d'être transmises.

1- Dans le cas d'un sous-traitant, il n'aura plus aucune justification de conserver les données déjà transmises, et devra donc les supprimer.

2- Dans le cas de co-traitance, le RT étant en communication directe avec la personne concernée (par son obligation d'information), il n'y a pas d'obligation explicite d'arrêt du traitement des données déjà transmises.

### 3.2.4 Droit à la portabilité des données

Conformément à l'article 20 du RGPD, la personne concernée a le droit d'exercer la portabilité de ses données à caractère personnel. En d'autres mots, elle peut faire la demande pour recevoir l'ensemble des données qu'un RT possède sur elle, et ce, dans un format structuré et lisible par une machine. Elle pourra alors les transmettre à un autre Responsable de Traitement sans que le RT source ne puisse y faire opposition. C'est la « liberté de déménager » d'un service à un autre.

> RECOMMANDATION 5
> La portabilité peut être encouragée par la définition d'un format d'export de données commun à toute la fédération.

## 3.3 La pseudonymisation et l'anonymisation

Au vu des définitions et implications prévues dans le RGPD, nous formulons la recommandation suivante concernant la technique de pseudonymisation.

> RECOMMANDATION 6
> La pseudonymisation peut être une méthode de gestion des données pour la fédération. Cependant il faut mettre en place une procédure explicite de traitement de pseudonymisation, qui désigne les informations supplémentaires ayant été retirées, ainsi que leurs modalités de séparation (technique et organisationnelle), afin de se prémunir contre la levée d'anonymat.

## 3.4 Sous-traitance / co-traitance entre Responsables de Traitement

La collecte d'information ou même sa transmission est vue par le RGPD comme un traitement. Or, dans le cas d'une collecte effectuée par un RT de la fédération puis transmise à autre RT, il pourrait être postulé que la collecte est un traitement effectué pour le compte d'un tiers, ou bien a contrario, en définissant l'ensemble dans une vision plus large, qu'il s'agit d'un traitement effectué conjointement par les RT. La vision hiérarchique ne correspondant pas à l'idéologie horizontale d'une fédération, et les obligations contractuelles de la relation de sous-traitance étant extrêmement contraignantes sur le plan administratif, il semble opportun d'éclaircir cette notion et de lever rapidement cette interrogation.

#### 3.4.1.1 Cas de la relation entre Responsable de Traitement et sous-traitance

L'Ordonnance précise à son article 60 que la qualité de sous-traitant n'exonère en rien du respect des dispositions applicables. Ainsi lors d'échange entre Responsable de Traitement à l'intérieur de la fédération, toutes les dispositions du RGPD restent applicables.

RECOMMANDATION 7

Dans le cadre des échanges entre applications via le protocole technique de fédération, il est nécessaire de définir juridiquement la nature de la relation entre les Responsables de Traitement ainsi fédérés.

Cette démarche pourrait s'enrichir d'un modèle de document juridique pour la sous-traitance et pour la cotraitance.

## 3.5 Les codes de conduites sectoriels

Suite à la publication du RGPD et avant même son entrée en vigueur en mai 2018, plusieurs initiatives de codes de conduite ont vu le jour pour divers secteurs d'activités. Parmi elles, les entreprises de l'infrastructure informatique en nuage (IaaS), qui ont constitué dès 2016 une association pan-européenne : CISPE (Cloud Infrastructure Service Providers Europe, https://cispe.cloud). Celle-ci a pour but de porter la rédaction d'un code de conduite, son évaluation par le régulateur, et par la suite la labellisation des acteurs souhaitant se réclamer de l'application dudit code (plus de 70 certifiés en 2019, et 130 volontaires). Le code devient ainsi un outil technique autant que marketing, permettant l'identification d'une marque et des parties prenantes. Des entreprises souhaitant afficher leur engagement au respect du RGPD peuvent afficher les logos et labels du CISPE, après une candidature et une adhésion payante, selon la procédure définie dans le Code de Conduite.

Ce dispositif réglementaire permet aux acteurs techniques d'apporter des précisions à la législation, avec une flexibilité accrue, et une validation a postériori par les régulateurs officiels. C'est une démarche idéale dans un cadre d'innovation, où le processus juridique peut être long à rattraper la technique. Ainsi, CISPE a initié en 2018 la rédaction d'un nouveau code de conduite, spécifique aux opérations de « portabilité des données personnelles ». Ce nouveau droit, défini dans le RGPD, a en effet besoin d'être éclairé techniquement afin que les usagers puissent le mettre en œuvre de manière pratique et rapide.

RECOMMANDATION 8

Les opérateurs de services (applications) de la fédération pourront co-rédiger un code de conduite tel que défini dans le RGPD, afin de clarifier la mise en œuvre du RGPD dans le cadre de la fédération de données d'énergie.

À court terme, ce code servira de charte entre les acteurs de la fédération naissante, ainsi que du document explicatif de la philosophie du projet.

À moyen terme, le code pourra être soumis à la CNIL pour une approbation juridique, devenant ainsi une marque de sérieux pour les interlocuteurs.

# 4 Conclusion

Ce travail préliminaire dans le cadre du POC-SEN1 nous a permis de confirmer que d'une part, les interactions basiques entre une application et ses utilisateurs relevaient bien de l'application normale du RGPD, et que d'autre part, certains points de la réglementation laissaient dans l'ombre les implications liées à une fédération.

En effet, le cadre que nous proposons pour les échanges de données entre acteurs fédérés n'est pas clairement identifié dans les textes. Il est donc nécessaire de repréciser à la fois le principe de la fédération, et la manière dont ce principe peut être traité par la réglementation.

Enfin, il faut souligner que les auteurs du présent rapport n'ont pas de formation ou de qualification juridique spécifique. Pour aller plus loin dans l'analyse et consolider les recommandations actuelles, une assistance plus qualifiée sera nécessaire.