RAPPORT N° 14
DU COORDINATEUR CONFIDENTIALITE

Article 17, alinéa 2, de l'arrêté du 21 mars 2002 relatif aux gestionnaires de réseaux et article 7, alinéa 2, de l'arrêté du 16 octobre 2003 relatif aux gestionnaires de réseaux gaziers

TABLE DES MATIERES

Chapitre I

Préambule

L'article 17 de l'arrêté du 21 mars 2002 relatif aux gestionnaires de réseaux stipule que : « *le gestionnaire de réseau veille à recueillir et à consigner les informations personnelles et commerciales dont il a connaissance dans l'exécution de ses tâches sous une forme et dans des conditions propres à en préserver la confidentialité. Il garantit la séparation systématique entre ces données et celles qui sont susceptibles de connaître une publicité.*

Le gestionnaire du réseau désigne une personne, indépendante des producteurs, fournisseurs aux clients éligibles et intermédiaires, spécialement chargée de la coordination des mesures adoptées en application du présent article. La CWaPE peut solliciter à tout moment de la personne ainsi désignée un rapport sur l'application de ces mesures. »

L'article 7 de l'arrêté du 16 octobre 2003 relatif aux gestionnaires de réseaux gaziers contient des dispositions identiques.

ORES SCRL est chargée de la coordination des mesures adoptées en application des articles 17 et 7 précités.

Le présent rapport couvre les activités d'ORES Assets sur l'ensemble du territoire desservi, tant pour l'électricité que pour le gaz naturel.
Il a pour objet d'exposer les mesures prises ou poursuivies au cours de l'année 2017 pour répondre mieux encore à l'objectif de préserver la confidentialité des informations dont ORES a connaissance dans l'accomplissement des tâches qui lui sont confiées.

Le présent rapport du coordinateur confidentialité était jusqu'à présent approuvé par le Comité d'éthique d'ORES SCRL lequel est devenu caduque suite aux modifications des statuts intervenues lors de l'Assemblée générale du 22 juin 2017.

Le présent rapport a dès lors été arrêté par le Comité de direction d'ORES SCRL en date du 23 mars 2018.

Chapitre II

Confidentialité et protection des données

I. Confidentialité des informations personnelles et commerciales

Sur la base des dispositions décrétales, les administrateurs, le personnel d'ORES et ses sous-traitants doivent respecter les règles relatives à la confidentialité des informations personnelles et commerciales. Tel que le précisent l'article 16 bis, § 1er, du décret électricité et l'article 17 bis, § 1er, du décret gaz, ces données personnelles et commerciales sont considérées comme relevant du secret professionnel et sont celles reprises aux articles 12, § 2, et 16, § 1er, du décret électricité et aux articles 13, § 2, et 17, § 1er, du décret gaz.

Cette notion de « données » est à resituer dans le cadre des missions exercées par le Gestionnaire de Réseaux de Distribution et par sa filiale ORES, conformément aux articles 12 et 16 du décret électricité et aux articles 13 et 17 du décret gaz tels que repris ci-après.

Pour paraphraser l'article 12, § 1er, 4°, et § 1bis, du décret électricité et l'article 13, § 1er, 4°, et § 1bis, du décret gaz, les données sont :
- personnelles : en ce qu'elles touchent directement à la personne physique ou morale ici considérée comme utilisateur de réseau ou comme appartenant à une catégorie d'utilisateurs du réseau ;
- commerciales : en ce que l'utilisation des données relatives à cette personne afférentes à son alimentation ou sa consommation de gaz et de l'électricité pourrait donner un avantage concurrentiel à un opérateur censé ne pas les détenir ou autrement dit, il convient d'éviter toute « *discrimination (notamment) en faveur des associés du gestionnaire de réseau ainsi que des entreprises liées à ces associés ou au gestionnaire de réseau* » (article 12, § 1er, 4°, et § 1bis, du décret électricité et article 13, § 1er, 4°, et § 1bis, du décret gaz).

Enfin, il convient de préciser que ces notions ne sont pas à confondre avec la notion de « secret des affaires » à laquelle le personnel d'ORES est tenu dans le cadre de l'examen des dossiers de marchés publics, notamment.

II. Précautions prises vis-à-vis du personnel par rapport à la confidentialité de certaines données

Les contrats de travail des membres du personnel prévoient des clauses qui imposent une obligation de confidentialité dans leur chef.

Ainsi ces clauses définissent ce qui doit notamment être considéré comme des données confidentielles : les procédés utilisés et les méthodes de production, les listes de clients, les listes et les données du personnel, les renseignements techniques, commerciaux et financiers, et tous autres renseignements de quelque nature qu'ils soient, qui sont directement ou indirectement en rapport avec ORES dont les membres du personnel ont eu connaissance du fait de leur fonction.

Les membres du personnel s'engagent dans leur contrat de travail à ne pas communiquer ces données, à les utiliser dans le cadre de l'exécution de leur contrat de travail, à ne les copier ou les reproduire sans autorisation préalable écrite et expresse d'ORES, à restituer à ORES les données qui, au moment de la cessation du contrat de travail, sont encore en leur possession et ce, immédiatement après la cessation du contrat de travail.

III. Protection des données à caractère personnel - RGPD

Faisant suite à l'entrée en vigueur du règlement général sur la protection des données (RGPD)[1], un projet a été mis en place en ORES afin que l'implémentation des obligations découlant de ce règlement puisse être effective à la date où celui-ci entre en application, à savoir le 25 mai 2018.
Un plan d'actions a de ce fait été établi afin qu'ORES puisse se conformer au RGPD dans les délais requis.

Dans le courant de l'année 2017, le projet a donné lieu à plusieurs réalisations qui sont décrites dans le chapitre IV du présent rapport.

L'exécution de ce plan d'actions se poursuivra en 2018 en vue de mettre ORES en conformité avec les impositions du RGPD au plus tard pour le 25 mai 2018 (mise en place d'un registre des traitements, rédaction et publication d'une privacy notice, désignation d'un délégué à la protection des données (DPO), revue des contrats avec les sous-traitants…).

[1] 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,

Chapitre III

Les services Access&Transit et Relevé et Validation Comptage – Services internes à ORES

1. Description des activités

Les services Access&Transit et Relevé et Validation Comptage font partie du département Gestion du Marché & Clientèle. Ce département gère d'une part, tous les processus du marché libéralisé et d'autre part, les obligations de service public sociales.

Le service Access&Transit gère le registre d'accès. Le registre d'accès est la pièce maîtresse du marché libéralisé. Il s'agit de la base de données à partir de laquelle s'organisent les relations et les échanges entre les différents acteurs du marché et le GRD. C'est en fait l'instrument qui garantit la mise à jour et les flux d'informations. Chaque point d'accès (appelé aussi point de fourniture) y est répertorié via son code EAN. Derrière ce code, on retrouve principalement les données du client, celles de son fournisseur et quelques autres informations utiles. Couplé à MDM/Mercure - la base de données répertoriant les consommations de chaque point de fourniture -, le registre d'accès donne une image complète du marché.

Le service Relevé et Validation Comptage regroupe entre autres les releveurs et les valideurs. Leur rôle est de relever les données de consommation chez les clients pour tout le territoire couvert par ORES et de les valider, c'est-à-dire de vérifier si les relevés sont cohérents au regard des statistiques et historiques de consommation ou des critères climatiques. Le service gère à la fois la relève annuelle des compteurs des clients résidentiels et petits professionnels (une visite tous les deux ans et l'envoi d'une carte l'autre année), la relève mensuelle (une visite tous les mois) et la relève à distance à intervalles réguliers pour les gros consommateurs (quart-horaire pour l'électricité et horaire pour le gaz).

La gestion journalière des applications informatiques utilisées par les deux services susmentionnés - le registre d'accès pour Access&Transit et MDM/Mercure pour le service Relevé et Validation Comptage – est assurée en collaboration avec EANDIS.

2. Mesures spécifiques adoptées au sein des services examinés

- **Service Access&Transit**

  L'infrastructure informatique est sécurisée et l'accès à l'application est individualisé et réservé aux membres de l'équipe Access&Transit. Toute nouvelle demande d'accès est soumise à l'approbation du cadre responsable du service.

  Les fournisseurs ont également accès à l'application mais chaque fournisseur ne peut disposer que des données des clients pour lesquels il a reçu une acceptation d'enregistrement sur le point d'accès de la part du registre d'accès. Les règles de sécurité et d'accès de l'application informatique gèrent cette mise à disposition limitée de l'information liée au point d'accès.

Outre cette sécurisation via l'application informatique, le service Access&Transit même ne communique des renseignements par mail ou par téléphone sur le point d'accès qu'au fournisseur reconnu sur ce point d'accès. Il va de même pour l'historique du point d'accès.

Si un fournisseur lance un scénario de marché *drop* ou pose d'un compteur à budget - ce qui sous-entend que le client a des difficultés de paiement -, un autre fournisseur qui lancerait un *switch* (changement de fournisseur) sur le point d'accès ne recevra pas comme message de retour qu'un *drop* ou une pose d'un compteur à budget sont en cours mais qu'un scénario de fin de contrat est en cours. De ce fait, le nouveau fournisseur ne pourra pas prendre connaissance des difficultés de paiement du client.

Access&Transit ne communique des renseignements par téléphone, par courrier ou par mail qu'au client (ou à une personne mandatée par ce dernier) qui se trouve sur le point d'accès et seulement durant la période d'occupation de ce client. Le client final n'a pas accès à l'application informatique même.

Une traçabilité est possible de toutes les transactions du marché ainsi que des envois de données. Une traçabilité est également possible des actions de chaque personne ayant accès à la base de données.

Les documents du service Access&Transit portent tous le logo de confidentialité. Les procédures et instructions du service sont uniquement accessibles par le service même.

- **Service Relevé et Validation Comptage**

L'infrastructure informatique est sécurisée et l'accès à l'application est individualisé et réservé aux membres du département Gestion du Marché et Clientèle. Toute nouvelle demande d'accès est soumise à l'approbation d'un *application owner*. Le *call center* a un accès aux applications via une interface Web sécurisée par un mot de passe. Les accès à l'application Mercure sont quant à eux approuvés par une personne du service de la gestion des processus *Measure*.

Les fournisseurs ont également accès à l'application via une interface web mais chaque fournisseur ne peut disposer que des consommations des clients pour lesquels il a reçu une acceptation d'enregistrement sur le point d'accès de la part du registre d'accès. Les règles de sécurité et d'accès de l'application informatique gèrent cette mise à disposition limitée de l'information liée aux consommations du point d'accès.

Un client qui souhaite connaître son historique de consommation peut le consulter par le biais du site d'ORES via une identification sécurisée. Il peut être envoyé à une autre personne ou à un fournisseur mais ceux-ci doivent avoir un mandat écrit et signé du client du point d'accès concerné.
Une traçabilité est possible de toutes les transactions du marché ainsi que des envois de données. Une traçabilité est également possible des actions de chaque personne ayant accès à la base de données.

Les PDA (*Personal Digital Assistant)* des agents releveurs qui permettent l'introduction de l'index sur place sont sécurisés par un mot de passe.

Chapitre IV

Le service de Sécurité Informatique d'ORES

1. Description des activités

Le service « Information Security Office » a été créé suite à la réorganisation du département IT. Il est placé sous la responsabilité du Chief Information Security Officer (CISO) qui rapporte directement au Chief Information Officer (CIO). Sa mission est de définir et mettre en œuvre la politique de sécurité de l'entreprise et d'évaluer la **vulnérabilité du système d'information**. Il valide les solutions et leur implémentation pour garantir la **sécurité** et l'**intégrité** du système d'information et des données.

- **Politique et normes** : définir et faire évoluer la **politique de sécurité** des systèmes d'information (PSSI) et les **normes de sécurité** (chartes).
- **Plans** : établir un **plan de prévention** des risques informatiques et un **plan de continuité d'activité / plan de maintien** en conditions opérationnelles du SI.
- **Dispositifs techniques** : choisir les dispositifs les plus **appropriés aux besoins** de l'entreprise en se basant sur **une analyse de risque** de sécurité.
- **Bonnes pratiques et référentiel** : définir des **« bonnes pratiques » de sécurité IT** et implémenter le **référentiel de gouvernance** de sécurité IT, les actualiser, en assurer la diffusion et **veiller à leur application**.
- **Projets** : valider l'**adhérence des projets** aux **principes de sécurité IT**.
- **Incidents** : gérer les incidents de sécurité IT en coordonnant les différents acteurs et proposer des solutions pour **rétablir rapidement les services**.
- **Testing** : **tester régulièrement le bon fonctionnement des mesures** de sécurité mises en place et le respect des « bonnes pratiques ».
- **Conscientisation** : conscientiser le personnel d'ORES sur les risques liés à la sécurité au travers de **formations** et d'**actions de communication**.
- **Audit** : réaliser des **audits du système** de sécurité et **analyser les risques** (incluant les sous-traitants) et dysfonctionnements.
- **Dashboard** : élaborer et suivre des **tableaux de bord** des incidents de sécurité IT.
- **Innovation** : suivre les **évolutions technologiques et réglementaires**.

2. Mesures et plans d'actions

Dans le cadre du programme de sécurité IT 2017, les actions suivantes ont été réalisées :

Projets informatiques de gestion

- **Analyse de la criticité pour les applications d'ORES**
    - L'équipe « Information Security Office » a analysé 50 applications critiques pour ORES au niveau de la confidentialité, l'intégrité et la disponibilité pour évaluer leur criticité. Ces données ont permis de créer un fichier Excel BCP (Business Continuity Plan) afin de servir de point

d'entrée à la revue des SLA et l'écriture en 2018 du document DRP (Disaster Recovery Plan) par l'équipe I&O (IT Infrastructures & Operations).

- **Implémentation de SAP Identity Manager (SAP IDM) pour l'application ENERGIS**

    - **ENERGIS** (application - basée sur AutoCAD - qui permet la réalisation des plans, cartes et schémas as-built de nos installations électriques, gaz et télécoms).

        - ENERGIS est la 1ère application .NET dont la gestion des utilisateurs et de leurs accès est entièrement pilotée par SAP IDM via l'AD (Active Directory) : soit automatiquement pour le personnel interne (sur la base des données RH), soit par traitement manuel pour le personnel externe (données d'ITIM).

        - Suppression automatique des accès informatiques (de-provisioning) d'ENERGIS sur la base des données RH (internes) / ITIM (externes).

- **Implémentation de SAP IDM pour les applications SAP suivantes :**

    - SAP Solution Manager

        - SAP WP0 : automatisation de la gestion des utilisateurs internes et externes avec assignation manuelle des accès via l'interface web de SAP IDM sur la base du suivi d'une formation.
        - SAP WD0 : automatisation de la gestion des utilisateurs internes et externes avec assignation manuelle des accès via l'interface web de SAP IDM.
        - Suppression automatique des accès informatiques sur ces 2 environnements sur la base des données RH/ITIM.

    - SAP – ERP Development (ATRIAS)

        - SAP WD4 100/600 : automatisation de la gestion des utilisateurs internes et externes avec assignation manuelle des accès via l'interface web de SAP IDM.
        - Suppression automatique des accès informatiques sur ces 2 environnements sur la base des données RH/ITIM.

    - SAP – ERP Integration (Uniwall)

        - SAP WI2 : automatisation de la gestion des utilisateurs internes et externes avec assignation manuelle des accès via l'interface web de SAP IDM.
        - Suppression automatique des accès informatiques sur cet environnement sur la base des données RH/ITIM.

- **Gestion des Personal Accounts (PA) ORES dans l'Active Directory (AD) USER ORES via SAP IDM :**

    - Tout le personnel d'ORES interne et externe (PA - Personal Accounts) est piloté par SAP IDM. Le provisioning des groupes Active Directory pour les PA était quant à lui déjà piloté par SAP IDM.

- **Gestion des Personal Admin Accounts (PAA) ORES dans l'Active Directory (AD) USER ORES via SAP IDM :**

    - Les comptes avec accès privilégiés (PAA) sont complètement pilotés par SAP IDM.
      Le provisioning des groupes Active Directory pour les PAA est manuel et réalisé directement dans l'Active Directory.

- **Nouvelle organisation du département IT**

    - Création du service « Information Security Office » qui travaille au niveau gouvernance de la sécurité et création du service I&O (IT Infrastructures & Operations) qui prend en charge la partie opérationnelle de la sécurité.

    - Un nouveau découpage des tâches s'est mis en place.

    - Des réunions de « coordination de la sécurité opérationnelle » sont mises en place tous les mois pour aligner la partie gouvernance avec la partie opérationnelle.

- **Mise en conformité de la sécurité informatique d'ORES par rapport à la norme ISO27001:2013**

    - Un projet sur 4 ans a été défini pour la mise en conformité de la sécurité informatique par rapport à la norme **ISO27001:2013**.
    - En 2017, nous avons réalisé :
        - Revue et correction de la Directive Sécurité IT ;
        - Réévaluation de la situation sécurité IT et centralisation des bonnes pratiques actuelles ;
        - Création et suivi du plan d'implémentation de sécurité IT ;
        - Création de la procédure gestion des risques IT :
            - Rédaction de la procédure générale de gestion des risques
            - Rédaction des instructions de travail pour l'évaluation et le traitement des risques
        - Création de la procédure de gestion de la continuité ;
        - Création de la procédure de gestion des identités et des accès ;

- Création de la procédure de gestion des incidents de sécurité ;
- Création de la procédure de gestion des exceptions (gestion des dérogations temporaires aux règles des politiques) ;
- Vérification et évolution de la politique de crypto (écriture d'une nouvelle version) ;
- Descriptions des sections de gestion des risques IT au niveau des phases projet : pré-cadrage et cadrage ;
- Vérification politique de bureau propre écran propre ainsi que sa mise en application ;
- Vérification des contrats-types employés ORES ;
- Vérification définition des rôles et responsabilités en sécurité physique (logistique et bâtiments) ;
- Evaluation de la situation et aperçu des projets en matière de sécurité physique (logistique et bâtiments) ;
- Vérification et amendement de la politique de gestion des appareils mobiles ;
- Documentation des fiches BCP IT pour les services IT / applications critiques ;
- Alignement continu avec le projet RGPD (Règlement Général de Protection des Données).

- **Analyse de la sécurité Microsoft Office 365**

  - L'analyse de sécurité Microsoft Office 365 a été réalisée mais l'écriture des règles de sécurité dans le document de politique de sécurité IT sera effectuée en 2018, en même temps que les premiers tests sur Microsoft Office 365.

- **Renforcement du Chinese Walls**

  - Sécurisation du MicroCosme : mise en place de deux couches de Firewalling Nextgen en haute disponibilité afin de protéger Lumiweb et les services réseaux et téléphoniques.

  - Silo ORES@Engie-Electrabel : étude pour avoir un proxy internet dédié à ORES (autorisation d'accès à internet).

  - SaaS Spécifiques : mise en place d'une fédération d'accès au niveau de l'application TalentSoft (application en SaaS) pour les utilisateurs d'ORES.

- **Sécurisation de l'environnement Smart Meter**

  - Au niveau sécurité, l'équipe « Information Security Office » a effectué les actions suivantes :

- Participation à l'écriture du cahier des charges, partie sécurité, pour le compteur Linky ;
- Etude de la solution HSM (Hardware Security Module) pour l'encryption des échanges au niveau de la chaîne communicante ;
- Etude de la solution PKI (Public Key Infrastructure) pour la gestion des certificats ;
- Etude des risques de sécurité sur la chaîne communicante avec la méthode EBIOS ;
- Ecriture de la politique de sécurité Smart Meter.

Projet d'informatique Industrielle OT (Operational Technology)

- **Déploiement *firewalls* OT (Operational Technology)**

  - Déploiement des firewalls pour la protection des appareillages de coupure dans les postes haute-tension ;
  - Mise en place des liens ICCP avec Eandis ;
  - Documentation des procédures de support.

Projet Règlement Général de Protection des Données (RGPD)

- **Récupération des informations**

  - Un fichier Excel a été établi pour récupérer auprès des différents services concernés les informations pertinentes afin d'élaborer le registre des traitements.
  - Une analyse des réponses a été faite en recoupant les informations.

- **Plan d'actions**

  - La récupération des informations sur l'utilisation des données à caractère personnel d'ORES a permis l'élaboration d'un plan d'actions RGPD.
  - Le plan d'actions a reçu l'aval du Comité de direction.

- **Démarrage du projet**

  - Suite à la validation du plan d'actions RGPD par le Comité de direction, une équipe projet a été mise en place.

- **Cyber Assurance pour 2018**
  - ORES a souscrit une police d'assurance pour couvrir les risques cyber consécutifs à ses activités pour lesquelles elle utilise des systèmes de gestion informatique de données.
  - Cette police couvre les dommages aux tiers et les dommages propres dans les cas suivants :

- atteinte aux données (aussi bien à caractère personnel que les données de l'entreprise), que ce soit un simple accès à ces données ou bien une réelle divulgation/utilisation de celles-ci.
- extorsion (menace à l'encontre d'ORES dans le but de l'exposer à un problème de sécurité).
- vol cybernétique (la perte d'argent ou de biens matériels résultant d'un accès non autorisé dans le système).
- piratage du système téléphonique.
- interruption de réseau et du système informatique (due à une défaillance de sécurité).
- défaillance ou intrusion dans le système informatique qui apporte un problème de sécurité du réseau.
- « cyber terrorisme » (c'est-à-dire une utilisation préméditée d'activités perturbatrices contre le système informatique dans le but de provoquer un dommage pour des raisons sociales et idéologiques).

Chapitre V

Gestion des interactions avec la clientèle

I. Gestion par ORES

Lorsqu'ORES se charge des relations avec la clientèle, tout est mis en place, que ce soit au niveau du personnel, des sous-traitants, de la sécurité informatique…, afin de préserver la confidentialité des informations personnelles et commerciales mises à sa disposition.
Nous renvoyons à ce propos aux autres chapitres du présent rapport.

II. Délégation partielle de la gestion par ORES

ORES confie une partie de la gestion de ses relations avec la clientèle à la société N-Allo. Les appels téléphoniques et les courriels échangés entre ORES et sa clientèle sont traités par une première ligne d'agents N-Allo.
N-Allo s'engage à répondre selon des objectifs définis en accord avec ORES. Les demandes et problèmes plus complexes sont transférés depuis N-Allo vers une seconde ligne constitués d'agents ORES.

Les agents N-Allo disposent des connaissances et des outils nécessaires au traitement des données clients d'ORES. Une séparation stricte entre les outils de communication et de gestion des différents donneurs d'ordre de N-Allo est exigée et contrôlée par ceux-ci.

Les agents N-Allo disposent d'une application nommée « coupole ». Celle-ci doit être vue comme une application assurant un certain niveau de convergence entre les différentes applications sous-jacentes, au sein desquelles les opérateurs sont appelés à travailler.

La gestion des interactions téléphoniques est réalisée à travers une infrastructure téléphonique de type centre d'appels qui est mutualisée. Cette technologie permet une distribution automatique des appels en fonction du sujet de l'appel, des compétences des agents, de leur charge et de leur disponibilité.
Un trust établi entre les *Active Directory* d'ORES et de N-Allo permet à N-Allo de contrôler de façon plus fine et en temps réel les personnes ayant accès aux outils de communication.
Une gestion de profils permet de différencier les utilisateurs de la plateforme et d'attribuer des droits d'accès correspondant à leurs rôles et compétences.

Un contact center tel que N-Allo est dès lors composé de cinq éléments constitutifs : la plateforme de communication, une application centrale (la coupole), les applications des clients du contact center, le reporting/monitoring et les réseaux.

Pour chacun de ces éléments, des mesures ont effectivement été prises par ORES et N-Allo afin de garantir la confidentialité des données personnelles et commerciales qui transitent par le contact center.

1. La plateforme de communication

La plateforme de communication englobe l'ensemble des moyens qui sont mis en œuvre pour assurer les traitements en amont de la distribution de tous les types d'interactions ([2]) pour leur traitement : mise en attente et diffusion de message (pour les appels), routage et distribution (pour toutes les interactions)…

La plateforme de communication est une infrastructure partagée, en ce sens qu'elle est unique pour l'ensemble du contact center et de ses clients.

De par son organisation, son architecture et sa gestion, l'ensemble de la plateforme de N-Allo est mise à la disposition des différents sites opérationnels de N-Allo et des différents donneurs d'ordre selon un modèle de type SaaS (Software as a Service). Les éléments actifs sont hébergés au sein du *Data Center* de Crealys avec, pour les applications critiques, une redondance dans le *Local Data* du site de Gosselies.

Mesures garantissant la confidentialité

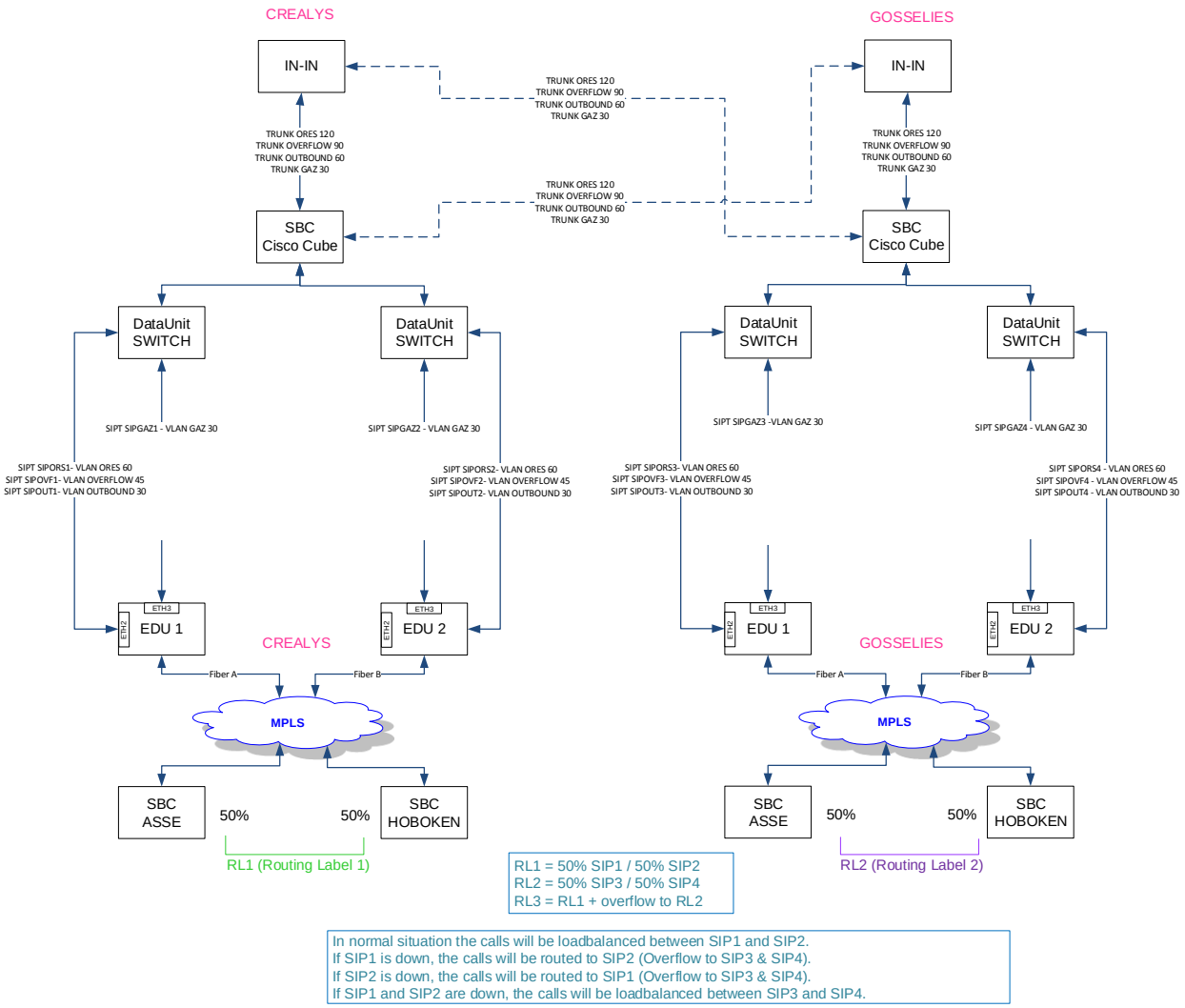
Au sein de la plate-forme, ont été définis les cloisonnements suivants :

- ✓ Pour chaque donneur d'ordre de N-Allo, un *cluster* étanche est défini. On retrouve au sein de ces *clusters* les différents points d'entrée de chacun des donneurs d'ordre (DDI : ce sont les numéros d'entrée propres à chacun des donneurs d'ordre, les *« functional mailboxes »*...).
- ✓ Pour chacun de ces points d'entrée, des règles de routage propres ont été définies. Par règle de routage propre, il faut entendre que chaque interaction reste dans le *cluster* au sein duquel elle est entrée.

De façon presque systématique à présent, les solutions logicielles sont construites pour permettre le fonctionnement dans un modèle de type SaaS (Software as a Service). Elles offrent donc les mécanismes de cloisonnement entre les activités supportées.

L'isolement des activités est visible sur le schéma suivant :

[2] Il y a lieu en effet de ne plus considérer que les interactions téléphoniques. L'évolution des modes de communication amène effectivement N-Allo à traiter également les mails, et t les interactions supportées sur le web (*chat)*



2. La coupole

La coupole est l'application centrale du contact center. Elle est l'espace principal de travail pour les opérateurs. C'est là que l'opérateur reçoit et ensuite traite les interactions.

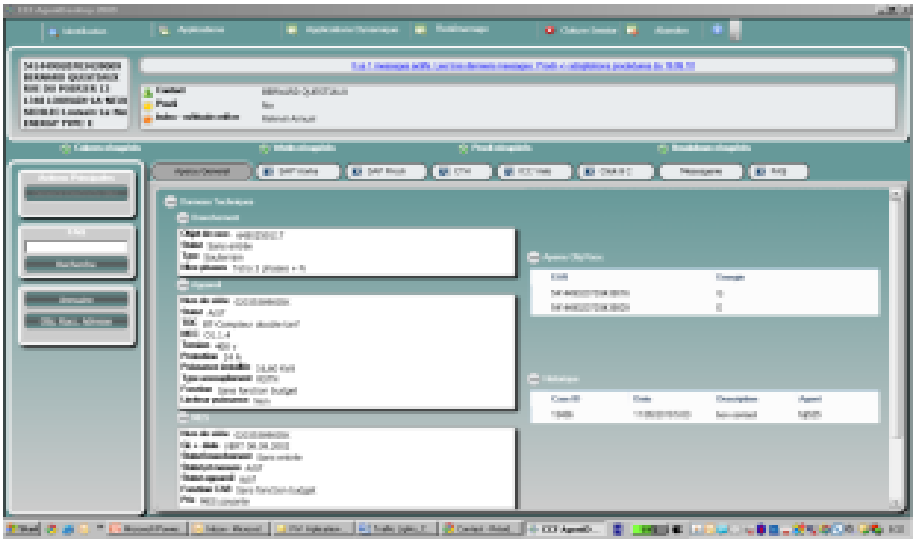
Pour ce faire, il dispose de trois grands types de données au sein de la coupole :

- ✓ toutes les données permettant d'identifier le client si cette identification n'a pu se faire en amont dans le traitement auquel cas cette fonctionnalité est automatisée ([3]) ;
- ✓ les cases (tickets) associées à ce client, une fois qu'il est identifié ;
- ✓ les processus de travail qui permettent de traiter les interactions avec les clients : il s'agit là d'un catalogue de procédures propres à ORES et qui sont mises à la disposition des opérateurs pour assurer dans les meilleures conditions de qualité et de traçabilité le traitement des interactions.

<u>Mesures garantissant la confidentialité</u>

[3] Fonction *Screen Pop Up* qui assure l'ouverture automatique du dossier du client sur base d'informations collectées préalablement.

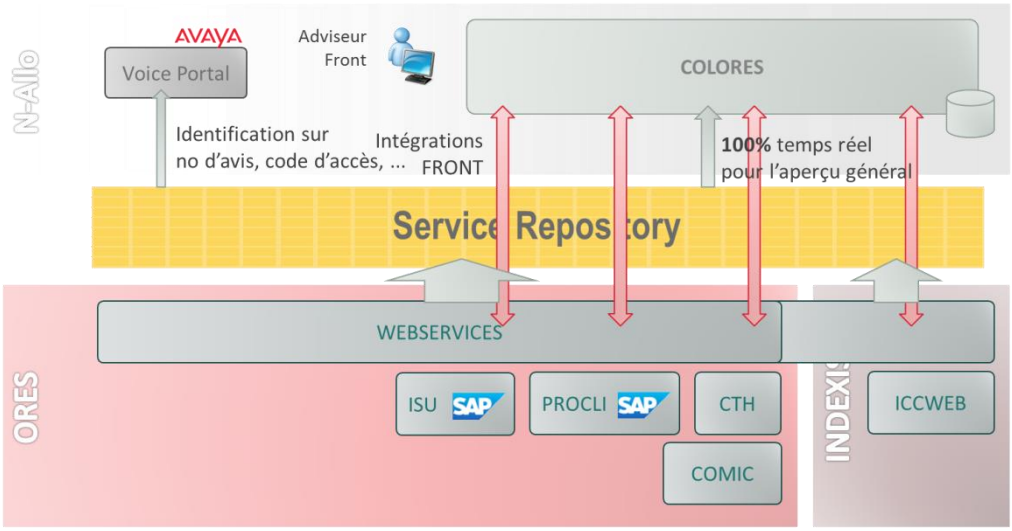
Les collaborateurs de N-Allo traitant les interactions d'ORES disposent de leur environnement propre totalement séparé de tout autre environnement opérationnel.



En d'autres termes, c'est exclusivement les collaborateurs travaillant pour ORES qui ont accès à cette application.

Techniquement, les données sont dans une base indépendante totalement et physiquement séparée de toute autre donnée au sein de N-Allo.

En effet, grâce à la publication par ORES de *web services* (à ce stade, avec un périmètre fonctionnel réduit), N-Allo a mis en place un *Service Repository* permettant d'assurer des services à valeur ajoutée sur les IVR (interactive voice response), ainsi qu'au sein de la coupole. Ces services ont été repris dans le cadre du projet Accessibilité en partenariat avec ORES et portent principalement sur l'identification du client ainsi que sur la qualification de la raison de l'appel.



L'accès aux *services web* publiés par ORES est strictement protégé par l'utilisation du protocole https ainsi que l'échange de certificats.

3. Les applications d'ORES

Dans le cadre des procédures de travail, l'opérateur peut être appelé à consulter ou à effectuer des transactions dans les applications d'ORES. L'accès à ces différentes applications est géré par une « *password policy »* ou un mécanisme sécurisé de SSO *(Single Sign On)* qui a été défini avec ORES.

Mesures garantissant la confidentialité

Les droits d'accès à l'application ainsi qu'aux applications de gestion d'ORES (Lopex, Procli, Mercure) sont attribués sur la base de profils (*Active Directory*) « trustés » par ORES (seules les personnes autorisées par ORES à accéder à ses systèmes ont effectivement les droits nécessaires pour avoir ces accès).

4. Le *reporting/monitoring*

Le *reporting* est l'ensemble des moyens qui permettent de mesurer l'activité réalisée au sein du contact center.

Le *monitoring* permet de remonter les mêmes informations mais en temps réel afin de pouvoir intervenir directement sur les opérations.

Mesures garantissant la confidentialité

Ces deux activités se font sur des bases qui garantissent la totale indépendance entre les différents donneurs d'ordre du contact center.
Il s'agit :

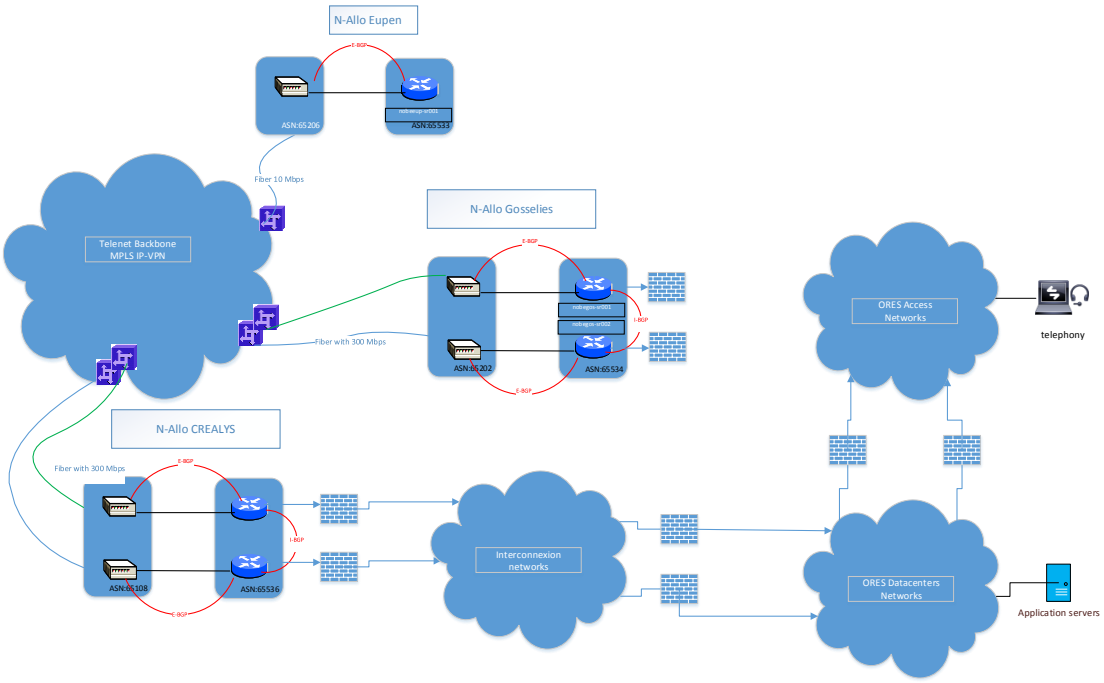
- ✓ des points d'entrée (lignes d'appels, *mailboxes*...) : ils sont propres à chacun des donneurs d'ordre ;
- ✓ des *skills* (compétences) des opérateurs : elles sont spécifiques aux activités des différents donneurs d'ordre, ce qui garantit la totale indépendance de celles-ci.

5. Les réseaux

L'ensemble des systèmes est relié par des réseaux IP. N-Allo a également une connectivité avec plusieurs donneurs d'ordre extérieurs à l'organisation.

Le schéma ci-dessous donne un aperçu de la connectivité des réseaux d'ORES et N-Allo :

Schema 1: IP-VPN network (layer 3)



Mesures garantissant la confidentialité

Prenant en compte que l'ensemble des applications sont extrêmement critiques en matière de sécurité, de disponibilité et de continuité, les différents réseaux sont sécurisés et redondés. En particulier, les mesures suivantes sont mises en œuvre :

- ✓ pas d'entrée du monde extérieur en dehors d'un protocole de sécurisation extrêmement sévère supporté par des *firewalls* ;
- ✓ pas d'accès au réseau sans une identification préalable et personnelle de l'opérateur ;
- ✓ *monitoring* permanent de l'activité sur le réseau ;
- ✓ *tracing* de l'ensemble des actions réalisées au sein des différents systèmes.

En matière de sécurisation et d'isolement, N-Allo a mis en œuvre une structure en *sous-réseau*, chacun des donneurs d'ordre se trouvant ainsi isolé sur son propre *sous-réseau*.

Il faut noter par ailleurs que ces mesures de sécurisation peuvent régulièrement faire l'objet d'audits de la part d'ORES qui se doit de préserver, d'une part, l'accès à ses systèmes d'information et, d'autre part, la confidentialité des informations disponibles chez N-Allo.

A côté de ces cinq éléments constitutifs, l'organisation opérationnelle du contact center doit également être prise en compte afin de garantir au mieux la confidentialité des données échangées.

Les activités gérées par N-Allo pour le compte d'ORES sont organisées sous la direction du Responsable Opérationnel en charge des clients traités sur les sites de Gosselies/Eupen. Dans le cadre du plan DRP de N-Allo, des positions opérationnelles sont également disponibles sur d'autres sites permettant de

reprendre les activités sur ces sites en cas d'indisponibilité prolongée du site de Gosselies.

N-Allo est appelée pour nombre de ses donneurs d'ordre (dont ORES) à mettre en œuvre une gestion étanche dans le traitement de leur clientèle respective. Ces « *Chinese walls* » font l'objet d'audits.

Chapitre VI

Gestion des comptages d'énergie

Depuis le 1er juin 2015, les activités de relève, de calcul de la consommation et de validation des données de comptage sont gérées au sein d'ORES via une application dénommée Mercure.

En décembre 2015, la sécurité liée à l'encodage des données d'index via le portail web a été modifiée pour éviter le piratage informatique.

Indexis continue, pour sa part, à gérer l'envoi des données de comptage au marché, les processus de *settlement* (*infeed*, allocation et réconciliation), le calcul du *gridfee* ainsi que le registre d'accès et les processus de *structuring* (changement de fournisseur, déménagement, etc.).

Les activités restant en Indexis seront reprises par Atrias à la date de son go-live.

Les mesures de sécurité en vigueur pour toutes les applications d'ORES sont également applicables à l'application relative à la gestion des données de comptage (cf. chapitre IV « Le service de Sécurité Informatique d'ORES »).

Chapitre VII

Relation avec les producteurs

La procédure de raccordement à la haute tension qui est mise en place en ORES respecte strictement les dispositions actuelles pertinentes du règlement technique.

Cette procédure, toujours d'application en 2017, devra être adaptée afin de tenir compte de l'Arrêté du Gouvernement wallon du 10 novembre 2016[4] (et de sa transposition dans le règlement technique), ainsi que du retour d'expérience - à discuter avec la CWaPE - suite aux premières études qui ont été réalisées selon la nouvelle méthodologie de cet AGW.

La procédure repose actuellement sur les principes suivants :

- un système de file d'attente est mis en place sur la base du principe « Premier arrivé – premier servi » ;

- le producteur prend contact avec le GRD afin d'obtenir un avis préalable sur les possibilités d'accueillir une production décentralisée sur le réseau. Cet avis gratuit est indicatif et n'engage nullement ni le GRD, ni le candidat producteur ;

- réalisation d'une étude facultative d'orientation afin d'établir un ordre de grandeur du coût de raccordement et afin que le producteur puisse évaluer la rentabilité de son projet. A cette fin, le producteur prend contact avec le GRD. Le paiement des frais d'étude conditionne l'initiation de cette étude ;

- Dans les 15 jours ouvrables[5] de l'enregistrement du paiement, le GRD communique au demandeur un rapport qui précise :
  - l'ordre de grandeur du coût de raccordement ;
  - diverses informations technico-administratives utiles pour la réalisation du projet ;

- Réalisation d'une étude détaillée. Le paiement des frais de cette étude et sa recevabilité conditionnent l'initiation de l'étude et la réservation de capacité d'accueil. Dès la réception en comptabilité du paiement des frais d'études, le GRD examine si le réseau est capable d'accepter la production demandée. Pour ce faire, il se coordonne avec le GRT/GRTL.

    1. Dans l'affirmative, le GRD fait, endéans 30 jours ouvrables (40 si P> 1 MW), une Proposition Technique et Financière (dénommée « PTF » dans la suite du texte), rédige un projet de contrat de raccordement en 2 exemplaires et demande au producteur de payer un acompte sur le montant de la PTF. Lorsqu'une demande ne peut être traitée dans le délai de 30 jours ouvrables en raison d'études de capacité qui doivent être effectuées, sur le réseau de transport ou de transport local, dans le cadre de cette demande, ce délai est porté à 70 jours ouvrables. Une réservation

[4] Arrêté du Gouvernement wallon du 10 novembre 2016 relatif à l'analyse coût-bénéfice et aux modalités de calcul et de mise en œuvre de la compensation financière

[5] Ce délai peut être porté à 30 jours ouvrables, voire à 70 jours ouvrables selon le cas.

de capacité correspondant à la demande du candidat producteur lui est attribuée. Elle prend cours soit à la date d'envoi de l'accusé de réception de la recevabilité de sa demande soit à la date de paiement de la demande d'étude détaillée (seule la date la plus tardive est prise en compte). Dès l'envoi des documents, le producteur dispose d'un délai de 30 jours ouvrables (40 si P> 1 MW) pour marquer son accord sur la proposition en renvoyant un exemplaire dûment signé du contrat de raccordement et en payant l'acompte susmentionné. Si une demande de raccordement ne conduit pas à la conclusion d'un contrat de raccordement endéans ce délai, la procédure de demande de raccordement est considérée comme caduque. Le GRD avertit le demandeur 10 jours ouvrables avant l'expiration de ce délai et informe la CWaPE en cas de caducité. Sur demandes motivées, le demandeur peut obtenir des prolongations de ce délai, de maximum 20 jours ouvrables chacune, avec maintien de la réservation de puissance tant qu'aucune autre demande n'a été introduite. A contrario, dès réception du contrat de raccordement signé et du paiement de l'acompte, la capacité d'accueil réservée est définitivement acquise au producteur sauf désistement écrit de sa part ou si les travaux de raccordement n'ont pas été commandés dans un délai de 1 an (paiement de la totalité des termes A, B, C et D de la PTF). Dans ce dernier cas, il est possible pour le producteur de demander un délai supplémentaire de maximum 1 an pour la réalisation du raccordement pour autant qu'il apporte la preuve par une attestation d'une autorité communale ou régionale compétente que la demande de permis est bien introduite et suit son cours normal. Dans ce cas, si le délai est prolongé au-delà de 1 an, l'offre est réactualisée. A défaut de produire cette attestation ou si le producteur a confirmé l'abandon de son projet, le dossier introduit et la capacité d'accueil qui s'y rattache deviennent caducs. En cas de désistement du producteur ou d'annulation du contrat pour dépassement du délai, le paiement effectué, lié à la signature du contrat de raccordement, est remboursé après déduction d'un forfait approuvé par la CREG.

2. Si le réseau ne peut accepter qu'une partie de la production, le GRD contacte, dans un délai n'excédant pas 30 jours ouvrables, le producteur pour voir s'il est intéressé par cette capacité d'accueil limitée. Si OUI, le GRD poursuit comme au point 1. pour la capacité d'accueil disponible et comme au point 3. pour la partie non disponible pour autant que le producteur ait confirmé par écrit la poursuite de son intérêt pour cette partie non disponible immédiatement. Si NON, le GRD poursuit comme au point 3. si la demande du producteur ne peut être scindée.

3. Dans la négative, le GRD signale au producteur que sa demande ne peut être acceptée dans l'immédiat et l'informe du motif et si possible du délai approximatif dans lequel sa demande pourrait être acceptée soit par désistement de projets en cours et/ou investissements réalisés par le gestionnaire dans ses réseaux. Sa demande est actée - dans un ordre de priorité selon la date de l'accusé de réception de la recevabilité de la demande - dans un fichier en attendant qu'une capacité d'accueil se libère. Cette liste reprend, sur la base du critère chronologique défini, les demandes partiellement satisfaites, les nouveaux projets et les extensions

de projets existants. Dès que la possibilité de capacité apparaît, le GRD reprend contact, par ordre de priorité, avec les producteurs en attente pour voir s'ils restent intéressés par leurs demandes initiales. Si OUI, la procédure reprend conformément au point 1. ou 2.. En cas d'application du 2., le candidat garde son ordre de priorité pour la partie non encore complètement satisfaite. Si NON, la demande du producteur devient caduque et est retirée de la liste d'attente.

- Le projet est radié de la file d'attente si un producteur modifie notablement, en cours de procédure, les données de son installation.

Il convient de noter que la procédure ainsi mise en place n'a donné lieu à aucun litige.

Chapitre VIII

Processus « Travaux clients » - Procédure d'application dans les services internes à ORES

La gestion du processus « travaux clients » est sous la responsabilité du département Infrastructures.
Ce processus traite l'ensemble des demandes de travaux tant externes qu'internes portant sur les branchements et compteurs électricité et/ou gaz naturel.
Les demandes externes peuvent être émises par un client (personne physique ou morale) ou par un tiers mandaté, par un organisme étatique ou par un fournisseur.
Les demandes internes sont émises par les services internes à ORES (Relevé et Validation Comptage, Access&Transit, *Metering*…).

Le processus couvre les modules suivants :

- La **CAPTATION** : collecte et enregistrement des informations nécessaires au traitement d'une demande ;
- L'**ETUDE** : étude des travaux de réseau nécessaires pour permettre la réalisation du raccordement ;
- L'**OFFRE** : établissement et envoi de l'offre pour les travaux et frais d'étude éventuelle ainsi que l'enregistrement de l'accord du client ;
- La **PREPARATION** : préparation administrative et technique d'une demande de travail et planification ;
- L'**EXECUTION** : exécution technique du travail ;
- La **POST ADMINISTRATION** : tâches administratives à remplir pour toute demande après l'exécution d'un travail (encodage, facturation).

Toutes les demandes sont enregistrées et traitées en SAP CS *(Customer Service)* par l'intermédiaire de l'outil informatique LOPEX.
Les données captées auprès du demandeur permettent de définir la prestation à réaliser par le GRD et de dimensionner le nouveau raccordement ou de modifier celui-ci (puissance mise à disposition, type d'alimentation, type de compteur…).

Les données personnelles recueillies auprès du demandeur se limitent aux informations nécessaires à l'établissement de l'offre et à la facturation des prestations (coordonnées du demandeur, adresse de facturation, taux de TVA…).

Dès l'exécution des travaux, les données techniques *(assets)* relatives au nouveau raccordement ou à sa modification sont enregistrées lors de la post administration en SAP ISU.

En matière de données personnelles, cette *database* ne contient que le nom de l'utilisateur du réseau de distribution (URD selon le règlement technique) et la date d'effet de son contrat de fourniture, établi avec le fournisseur. Ces informations sont transférées automatiquement à partir du registre d'accès d'A&T. Il est à noter que l'identifiant repris en SAP ISU sous l'URD n'est pas nécessairement le même que celui qui a fait la demande de travaux.
Seuls les intervenants d'ORES spécifiquement dédicacés ont accès aux outils SAP CS ET SAP ISU.

L’accès est en outre sécurisé. Ces outils ne sont donc pas accessibles aux tiers.

Les clients sont informés du respect de la confidentialité des données lors du traitement de celles-ci. Les documents suivants reprennent ces engagements :

- les conditions générales de raccordement ;
- le contrat de raccordement (si d’application).

L’infrastructure informatique est sécurisée et l’accès à l’application est individualisé et réservé aux agents ORES en charge de ces prestations.

Chapitre IX

Le Programme « *Smart Metering & Users* »

ORES est concernée par le respect de la confidentialité des informations dont elle a connaissance, également dans le Programme « *Smart Metering & Users* » qu'elle développe.

Pour rappel, différentes procédures ont été mises en place pour respecter ces principes de confidentialité dans les projets pilotes qui ont été lancés.
Dans le cadre des études et des projets pilotes relatifs à la mise en place d'un système de comptage intelligent et de son déploiement, ORES a contacté la Commission de protection de la vie privée (ci-après la « *CPVP* ») en vue de se mettre en conformité avec la recommandation qu'elle avait émise sur les principes à respecter pour les réseaux et le comptage intelligents (CO-AR-2011-004).

Une déclaration de traitement a été introduite par ORES et publiée par la CPVP dès septembre 2013.

Cette déclaration précise les précautions prises par ORES dans la gestion des données personnelles.

Le principe de proportionnalité, établi à l'article 4 de la loi sur la protection de la vie privée, impose au responsable du traitement de collecter exclusivement des données adéquates, pertinentes et non excessives, pour réaliser les finalités envisagées.
La transparence est absolument nécessaire. C'est dans cette perspective que des informations sur le traitement envisagé des données ont été transmises aux utilisateurs de réseau qui pourraient participer aux études projetées.

Les clients concernés qui acceptent de participer aux études ont reçu également tous les renseignements leur permettant d'exercer leur droit d'accès aux informations et de rectification le cas échant : un point de contact leur a été désigné.

Dans la suite des études et des projets pilotes, le Programme *Smart Metering & Users* a mis en place des ateliers de travail sur le thème « Sécurité et *Data Privacy* ».

ORES a présenté à la CWaPE dès 2015 les actions réalisées pour la protection des données et les orientations prises pour un déploiement à grande échelle.

En concertation avec la CWaPE, et dans la suite de la recommandation européenne (Recommandation de la Commission du 10 octobre 2014 concernant le modèle d'analyse d'impact sur la protection des données des réseaux intelligents et des systèmes intelligents de mesure (2014/724/UE)), ORES a collaboré avec les GRD wallons pour établir une première analyse des risques relatifs à la protection des données des compteurs intelligents selon le modèle du DPIA (*Data Protection Impact Assessment*).

Dans le cadre de cette collaboration, les GRD wallons et la CWaPE ont rencontré ensemble la CPVP afin d'échanger sur les compteurs intelligents et leur utilisation et ce, dans une volonté de complète transparence.

ORES a ensuite rédigé une analyse d'impact sur la protection de la vie privée (DPIA) comprenant d'une part, un socle commun aux GRD wallons qui reprend les principes généraux pour l'application du DPIA dans le cadre du déploiement de compteurs intelligents en Wallonie et, d'autre part, une analyse relative aux spécificités d'ORES qui tient compte de ses choix technologiques et opérationnels.

Ces deux documents ont été adressés à la CWaPE en date du 23 décembre 2015.

Il est à relever que le RGPD (Règlement Général sur la Protection des Données (ci-après le « *RGPD* ») requiert à partir du 25 mai 2018 la réalisation d'un DPIA lorsqu'un traitement *« est susceptible d'engendrer un risque élevé pour les droits et libertés des personnes physiques »*.
Il devra être vérifié si le DPIA existant ne doit pas être revu sur la base des normes et recommandations implémentant cette obligation de réaliser des DPIA.

Ces études et projets relatifs au comptage intelligents ont pour objectif de préparer le plus efficacement possible le plan de déploiement des compteurs intelligents qui devra être mis en place dans les prochaines années conformément à la règlementation applicable.