RAPPORT N° 15
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 tel que modifié par l'arrêté du 6 décembre 2018 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.*
Parmi les membres de son personnel, le gestionnaire du réseau désigne une personne 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 tel que modifié par l'arrêté du 6 décembre 2018 contient des dispositions identiques.

Vu l'article 16, § 1er, du décret du 12 avril 2001 relatif à l'organisation du marché régional de l'électricité (ci-après « décret électricité ») et l'article 17, § 1er, du décret du 19 décembre 2002 relatif à l'organisation du marché régional du gaz (ci-après « décret gaz ») qui permettent au GRD de confier tout ou partie de l'exploitation journalière de ses activités à une filiale disposant d'un personnel propre, un membre du personnel d'ORES SCRL, filiale d'ORES Assets, a été désigné coordinateur confidentialité par le Comité de direction du 1er février 2019, à savoir Audrey Réveillon.

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 2018 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.

Ce rapport a été arrêté par le Comité de direction d'ORES SCRL en date du 22 mars 2019.

Chapitre II

Confidentialité et protection des données

1. 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 16bis, § 1er, du décret électricité et l'article 17bis, § 1er, du décret gaz, ces données personnelles et commerciales sont considérées comme relevant du secret professionnel et sont celles reprises à l'article 12, § 2, du décret électricité et à l'article 13, § 2, du décret gaz.

Cette notion de « données » est à resituer dans le cadre des missions exercées par le gestionnaire de réseaux de distribution (ci-après « GRD ») et par sa filiale ORES, conformément aux articles 12 et 16 du décret électricité et aux articles 13 et 17 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 la consommation de gaz et d'électricité pourrait donner un avantage concurrentiel à un opérateur censé ne pas les détenir.

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 notamment dans le cadre de l'examen des dossiers de marchés publics.

2. 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.

Dans leur contrat de travail, les membres du personnel s'engagent ainsi notamment à ne pas communiquer les données confidentielles, 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.

En outre, un Code de conduite éthique applicable à l'ensemble des membres du personnel reprend l'engagement des collaborateurs d'ORES de respecter un ensemble de règles en matière d'éthique, notamment l'obligation de faire preuve de bon sens et de prudence en matière d'information concernant leur activité professionnelle.

Dans le cadre du contrôle réalisé par la CWaPE en 2018 concernant le respect des règles d'*unbundling*, ces dispositions des contrats de travail des membres du personnel d'ORES ont été examinées.
Ces dispositions reprenaient bien les obligations en matière de confidentialité des données. A la demande de la CWaPE, elles ont été légèrement revues afin de viser également expressément les données à caractère personnel, les informations commercialement sensibles et toute information qui pourrait offrir de façon injustifiée un avantage concurrentiel à un producteur, fournisseur ou intermédiaire.
Ces dispositions sont bien prévues comme telles à présent dans les nouveaux contrats de travail.
En ce qui concerne les collaborateurs actifs, les dispositions du Code de conduite éthique ont également été adaptées en ce sens afin que ces dispositions complètes soient opposables à l'ensemble des membres du personnel d'ORES SCRL.

3. Protection des données à caractère personnel - RGPD

Faisant suite à l'entrée en vigueur du règlement général sur la protection des données (RGPD)[1], ORES a poursuivi ses efforts dans l'implémentation des principes du règlement.

Le plan d'actions établi en 2018 a été affiné et un délégué à la protection des données a été nommé.

Durant l'année 2018, les effort ont été concentrés sur le « *privacy by design* » avec la mise en œuvre d'un processus d'analyse d'impact et la réalisation d'études d'impact sur les processus existants et sur la pseudonymisation des données de test.

Voir le chapitre IV « Le service de Sécurité Informatique d'ORES » pour plus de détails.

L'exécution du plan d'actions se poursuivra en 2019 . Un accent sera mis sur la sensibilisation de l'organisation à tous ses niveaux.

[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

Le service *Structuring* et *Measure* – Service interne à ORES

1. Description des activités

Le service *Structuring* et *Measure* fait 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 *Structuring* 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 au 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 *Measure* 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 le service *Structuring* et MDM/Mercure pour le service *Measure* – est assurée en collaboration avec Fluvius.

2. Mesures spécifiques adoptées

- **Service *Structuring***

  L'infrastructure informatique est sécurisée et l'accès à l'application est individualisé et réservé aux membres de l'équipe *Structuring*. 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 *Structuring* 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.

Le service *Structuring* 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 *Structuring* portent tous le logo de confidentialité. Les procédures et instructions du service sont uniquement accessibles par le service même.

- **Service *Measure***

  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

- **Analyse de la directive européenne *network* et infrastructure de sécurité (NIS)**

  La directive européenne, adoptée le 6 juillet 2016, a pour objectif d'assurer un niveau de sécurité élevé et commun pour les réseaux et les systèmes d'information de l'Union européenne. Cette directive doit être transposée en droit belge.

  - **Rédaction en collaboration avec Synergrid d'un « *position paper* »**
    Rédaction d'un « *position paper* » relatif à la transcription en droit belge de la directive dans le cadre de la participation d'ORES à Synergrid ;

  - **Analyse de la proposition de loi écrite par le Centre de CyberSécurité belge**
    Analyse du projet de loi écrit par le Centre de CyberSécurité belge dans le cadre de Synergrid. Plusieurs remarques ont été faites pour aboutir à un nouveau projet de loi ;

  - **Analyse des impacts de cette directive sur ORES**
    Analyse des impacts de cette directive sur ORES, définition des actions pour 2019, élaboration d'un budget 2019 avec comme objectif l'écriture de la « Politique des Systèmes d'Information » ;

  - **Présentation de la directive au Comité de direction d'ORES**
    La directive « NIS » a été présentée en Comité de direction d'ORES et le budget du projet validé pour 2019.

- **Analyse de vulnérabilité**

  - **Plusieurs analyses de vulnérabilité ont été réalisées en 2018**
    - sur notre environnement industriel : postes et cabines ainsi que sur notre système SCADA ;
    - sur l'application « *Connect My Home*" dans Azure ;
    - sur notre site web partie « Relevé Validation Comptage ».

- **Recrutement en interne**

  - **Recrutement en interne au service Sécurité**
    - Nous avons recruté une nouvelle personne dans le service sécurité pour prendre en charge :
      - les analyses des risques de sécurité de l'information ;
      - la mise en conformité aux lois et aux normes comme par exemple : la future loi NIS, la norme ISO27001,… ;
      - la rédaction des documents de gouvernance en sécurité.

- **<u>Projet de mise en conformité au règlement européen RGPD</u>**

  ORES travaille depuis 2017 à la mise en conformité au règlement européen RGPD via une collaboration étroite des départements IT, Juridique et des différents métiers. En 2018, les principales activités dans ce domaine étaient les suivantes :

  - **Implémentation du processus de *Data Protection by Design***
    Le processus *data protection by design* vise à maintenir la conformité ORES au cours du cycle de vie des projets et les améliorations apportées à nos systèmes. Il comprend une évaluation de base du traitement considéré ou de sa modification ainsi qu'une analyse approfondie si le niveau de risque le nécessite (DPIA – *Data Protection Impact Assessment*) ;

  - **Listing, planification et début d'implémentation des points d'amélioration sur les traitements existants**
    L'analyse des activités de traitement des données à caractère personnel réalisée en 2017 et début 2018 a révélé des points d'amélioration pour la conformité des traitements existants au RGPD. Ceux-ci ont été évalués et placés dans les différentes *roadmaps* (IT et Business). L'implémentation de certains « *Quick Wins* » a déjà été faite en 2018 mais la majorité d'entre eux seront prévus en 2019 ;

  - **Listing et début de réalisation de DPIA *a posteriori***
    Le listing des activités de traitement des données à caractère personnel mentionné ci-dessus nous a également amenés à lister une série de traitements potentiellement à risque pour tous les clients et qui nécessitent une étude approfondie (DPIA). Ces études approfondies ont été listées et démarrées en 2018 ;

  - **Processus de réponse aux demandes de personnes concernées**
    Ce processus a été mis en place pour répondre à nos clients et tout autre type de personnes concernées lorsqu'ils ont des demandes concernant un de leurs droits conférés par le RGPD ;

  - **Processus de gestion des *data breaches* (inclusion dans le processus de gestion d'incidents de sécurité)**
    Le processus de gestion des incidents de sécurité a été modifié et doit être finalisé pour tenir compte des « *personal data breaches* » afin d'y inclure d'une part, les exigences légales de notifications et d'autre part, les actions à prendre pour limiter l'impact de celles-ci ;

  - **Achat d'une solution d'anonymisation de données dans le contexte SAP**
    Ce périmètre SAP ayant été jugé particulièrement risqué au niveau de la protection de la vie privée, nous avons décidé d'acquérir la solution « EPI-USE » et avons lancé son implémentation en 2018. De plus, cet outil nous permettra d'optimiser à terme la mise à jour des données de nos systèmes non productifs ;

- **Conscientisation du personnel ORES au RGPD**
  Des actions de conscientisation auprès du personnel ORES ont été menées. Un film explicatif a été réalisé et a ensuite été distribué à tous les membres du personnel. Pour les collaborateurs IT (tant internes qu'externes) impliqués tant en termes de détection d'incident qu'en termes d'impact des actions correctives à implémenter, des efforts de conscientisation supplémentaires ont été menés sous forme de conférences.

- **<u>Gouvernance de sécurité de l'information</u>**

  - **Création et validation d'un standard de gestion des environnements**
    Afin de soutenir une nouvelle méthodologie de gestion des tests, d'augmenter le niveau de sécurité des environnements de production et de non-production ainsi que d'éviter des traitements de données à caractère personnel abusif, nous avons établi un nouveau standard de sécurité pour la gestion des environnements de développement. Celui-ci a été validé par la Direction IT et sera appliqué dans les nouveaux développements.

  - **Réécriture de la directive de sécurité**
    Dans l'optique d'une simplification de la politique de sécurité actuelle et d'une certification ISO27001, la directive de sécurité a été simplifiée et réécrite afin d'être compréhensible par tout le personnel.

  - **Choix d'une nouvelle méthodologie d'analyse de risque**
    Afin de mieux prendre en compte le risque causé par les menaces intentionnelles malveillantes, nous avons opté pour l'utilisation de la nouvelle méthodologie de gestion du risque « Ebios Risk Manager 2018 ». Celle-ci est en effet plus en phase avec la menace actuelle. Un « *proof of concept* » a été lancé fin 2018 afin de pouvoir avoir une image objective du risque fin 2019.

- **<u>Implémentation de SAP *Identity Manager* (SAP IDM) pour l'application STRATEGIS</u>**

  - **STRATEGIS est l'application en charge de la gestion cartographique des stratégies, plans d'investissement et de la gestion des chantiers voiries**
    - STRATEGIS est la 1ère application dans l'espace AZURE dont la gestion des utilisateurs et de leurs accès est entièrement pilotée par SAP IDM via l'AD (*Active Directory*) « *on premises* » c'est-à-dire automatiquement pour le personnel interne (sur base des données RH) soit par traitement manuel pour le personnel externe (données d'ITIM) ;
    - Suppression automatique des accès informatiques (*de-provisionning*) STRATEGIS sur base des données RH (internes) / ITIM (externes) ;
    - Mise à jour de la documentation de type « Instructions et méthode de travail » liée à la politique de gestion des comptes et accès informatiques.

- **Gestion des « *Personal Admin Cloud* (PAC) » ORES dans l'*Active Directory* (AD) USER ORES via SAP IDM**

    - Les comptes avec accès privilégiés dédiés dans l'espace AZURE (PAC) sont complètement pilotés par SAP IDM ;
    - Le *provisioning* des groupes *Active Directory* pour les PAC est manuel et réalisé directement dans l'*Active Directory* ;
    - Mise à jour de la documentation de type « Instructions et méthode de travail » liée à la politique de gestion des comptes et accès informatiques.

- **Analyse de l'upgrade de SAP *Identity Management* 7.2 vers 8.0**

    - Mise en place de l'infrastructure d'hébergement de la nouvelle solution ;
    - Choix de la stratégie de migration des données ;
    - Réalisation de batteries de tests ;
    - Rédaction de la documentation.

- **Revue des accès informatiques sur base des nouvelles organisations des départements Informatique, *Finances & Controlling* et Gestion du Marché/Clientèle**

    - Les accès aux applications gérés par SAP IDM ont été alignés sur base des nouvelles organisations et d'une matrice métier adaptée.

- **Définition par métier des accès de l'application Mercure R2**

    - Les accès sont définis sur base d'une matrice métier dans l'*Active Directory* et gérés par SAP IDM.

- **Remplacement de l'application Wipass ORES (ENGIE-IT) par l'application ADSelfService Plus**

    - Tous les collaborateurs d'ORES internes et externes (PA - *Personal Accounts*) peut désormais activer, réinitialiser et débloquer son compte personnel en libre-service et de manière sécurisée via ADSelfService Plus.

- **Déploiement de l'application AD Audit Plus**

    - Accès aux rapports d'évènements de l'*Active Directory*.

- **Revue des accès suite de l'upgrade SAP *Solution Manager* 7.1 vers 7.2**

    - Redéfinition des accès de l'application SAP *Solution Manager*.

- **Mise en place des accès SAP ERP WP1 pour le projet « Revue du Système de Gestion »**

    - Intégration des nouveaux accès liés à ce projet dans nos métiers ORES.

- **<u>Collaboration de l'équipe sécurité au projet Microsoft Office 365</u>**

    - Configuration de la sécurité des outils inclus dans la solution Microsoft Office 365 (Intunes, Onedrive, Exchange Online, SharePoint Online, Skype) ;
    - Mise en place d'un monitoring de la sécurité via l'outil : « *Secure Score* » ;
    - Rédaction d'une documentation de type « *baseline* » de sécurité Office 365 reprenant les informations décrites dans le standard de Sécurité Cloud mais adaptée au contexte particulier de la solution Office 365.

- **<u>Cyber Assurance pour 2018-2019</u>**

  – 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) ;

  – Les capitaux couverts ont été augmentés de manière significative afin de couvrir adéquatement les risques consécutifs à l'entrée en vigueur du RGPD ;

  – Cette police d'assurance fera l'objet d'un replacement au 1er janvier 2020 qui nécessitera une nouvelle analyse du risque et d'adaptation de la garantie.

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

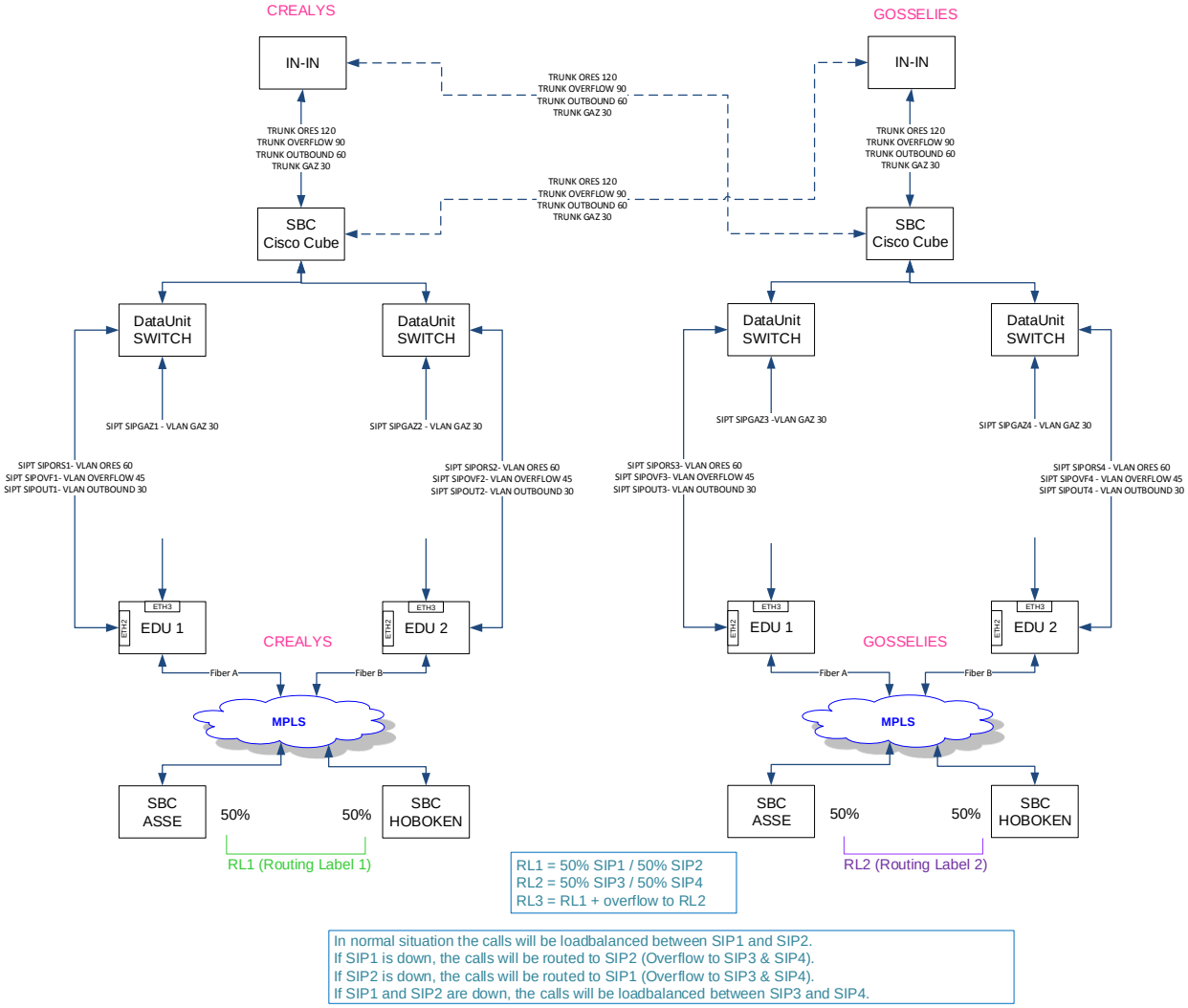
Au sein de la plate-forme, ont été définis les cloisonnements suivants :

- ✓ 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.

[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 les interactions supportées sur le web (*chat)*.

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



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.

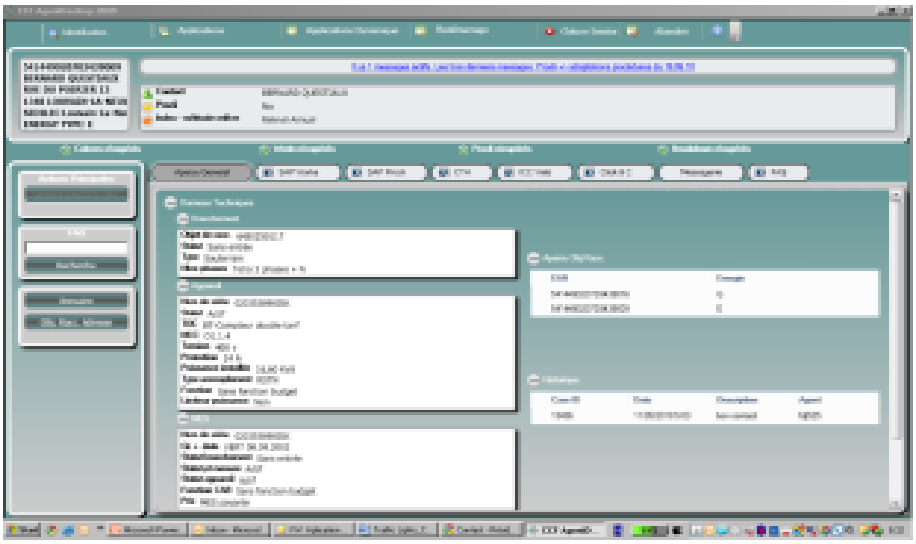
Pour ce faire, il dispose de trois grands types de données au sein de la coupole :

- ✓ 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.

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

Mesures garantissant la confidentialité

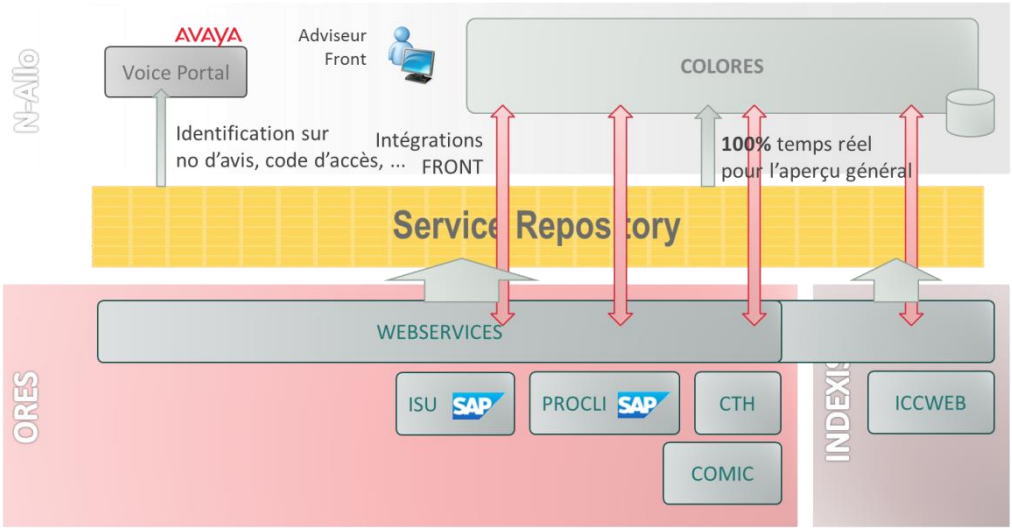
Les collaborateurs de N-Allo traitant les interactions d'ORES disposent de leur environnement propre totalement séparé de tout autre environnement opérationnel.



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

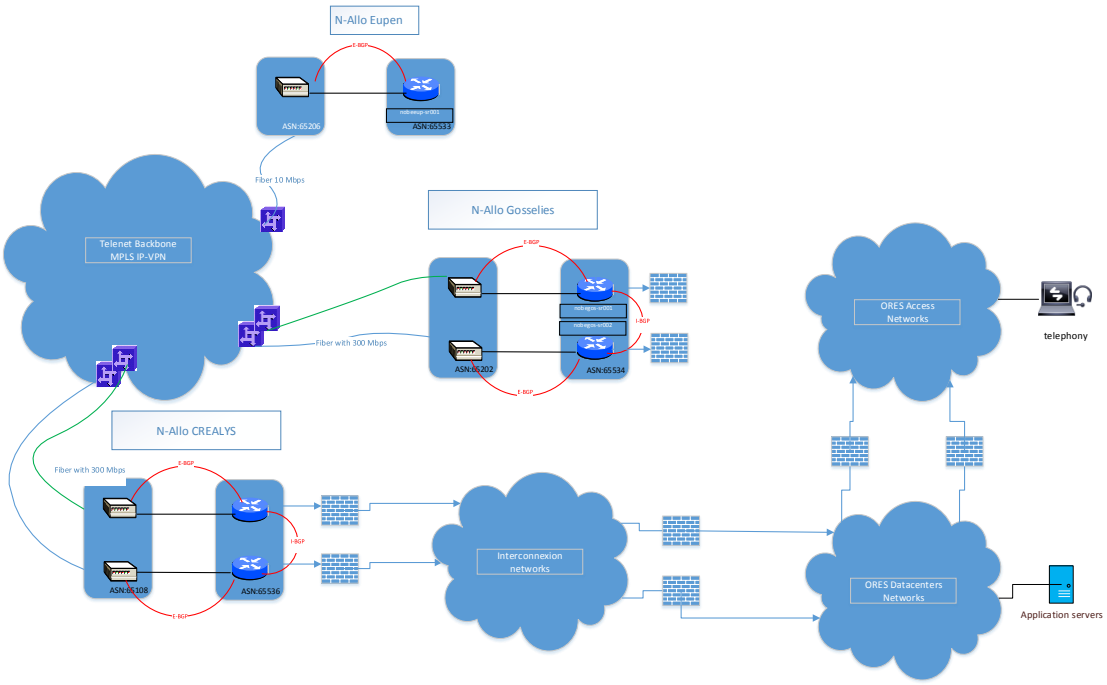
Ces deux activités se font sur des bases qui garantissent la totale indépendance entre les différents donneurs d'ordre du *contact center*.
Il s'agit :

- ✓ 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.

III. Futur *contact center*

Depuis les changements apportés aux décrets électricité et gaz dans le courant de l'année 2018, toutes les missions du GRD doivent à présent être exercées soit par du personnel du GRD, soit par du personnel d'une filiale juridiquement distincte de tout producteur, fournisseur ou intermédiaire.

De ce fait, une réflexion a eu lieu en vue de réorganiser le *contact center*, ORES ne pouvant plus déléguer cette mission à N-Allo à partir du 1er juin 2019.

Il en découle notamment que le développement des outils tels que la nouvelle Coupole et le Référentiel client seront pris en charge par ORES afin de garantir l'autonomie du nouveau *contact center* d'ORES Assets par rapport à N-Allo.

Parallèlement, un projet de constitution d'une nouvelle filiale a été lancé afin d'assurer la reprise dès le 1er juin 2019 des activités réalisées par N-Allo pour le compte d'ORES Assets. Cette filiale devra acquérir progressivement son autonomie afin de devenir totalement indépendante des activités de N-Allo. Des mesures seront bien évidemment également prises par ce nouveau *contact center* afin de garantir la confidentialité des données qu'il sera amené à gérer.

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.

Suite à la dissolution d'Indexis et à l'intégration de ses activités en Fluvius, cette dernière assure pour le compte d'ORES la gestion de 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.).
Fluvius exécute les mêmes mesures destinées à préserver la confidentialité des informations concernées que celles appliquées pour les données de ses propres clients.

Il est actuellement prévu que ces activités 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 2018, 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 en 2018.
Provisoirement, et dans l'attente de la transposition de l'AGW dans le règlement technique, une série de remarques incluant les effets de l'AGW ont été intégrées dans les principes existants ci-dessous.

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 ».

  Remarque : cette file d'attente s'est réduite suite aux études réalisées en 2018 selon la nouvelle méthodologie de l'AGW et disparaîtra définitivement début 2019.

- 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.

[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.

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 forfaitaire 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 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 CWaPE.

   Remarque : suite à la mise en place de la nouvelle méthodologie de l'AGW, une étape supplémentaire peut avoir lieu lors de l'étude détaillée.
   En effet, si une capacité permanente ne peut être octroyée pour l'ensemble de la demande, une étude préalable doit être réalisée. Il s'agit de l'évaluation par le GRD du caractère économiquement justifié d'un projet d'adaptation du réseau visant à octroyer au projet de production d'électricité verte une capacité d'injection supplémentaire par rapport à celle octroyée dans le cadre de la situation de référence. Cette étude préalable est envoyée à la CWaPE qui doit la valider. Cette étape

supplémentaire peut occasionner un délai complémentaire à la finalisation de l'étude détaillée.

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.

   Remarque : suite à la mise en place de la nouvelle méthodologie de l'AGW, ce cas de figure ne peut plus arriver puisqu'une proposition, plus ou moins flexible, est toujours réalisée pour l'ensemble de la demande du producteur.

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.

   Remarque : suite à la mise en place de la nouvelle méthodologie de l'AGW, ce cas de figure ne peut plus arriver puisqu'une proposition, plus ou moins flexible, est toujours réalisée pour l'ensemble de la demande du producteur.

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

  Remarque : suite à la mise en place de la nouvelle méthodologie de l'AGW, dans un tel cas, le projet ne sera pas radié mais sa date de recevabilité (et donc son ordre de priorité) sera revue en fonction de la complétude des nouvelles informations.

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 (*Measure*, *Structuring*, *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.

Projets pilotes

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 avait contacté à l'époque la Commission de protection de la vie privée (actuellement l'Autorité de Protection des Données) en vue de se mettre en conformité avec la recommandation qu'elle a émise sur les principes à respecter pour les réseaux et le comptage intelligents (CO-AR-2011-004).

Le principe de proportionnalité 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 échéant.

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

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

DPIA

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.

ORES avait 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.

Depuis l'entrée en vigueur du RGPD, un DPIA doit obligatoirement être réalisé lorsqu'un traitement *« est susceptible d'engendrer un risque élevé pour les droits et libertés des personnes physiques »*.

La réalisation d'un DPIA pour le projet Smart Metering a été initié. Une première analyse de haut vol a confirmé la nécessité de réaliser un DPIA poussé selon la gouvernance en place au sein d'ORES. L'exercice est coordonné par le département IT et le DPO.

<u>Déploiement des compteurs intelligents</u>

Dans le courant de l'année 2018, ORES a dû entreprendre une profonde réflexion quant au déploiement des compteurs et quant au choix de la technologie.

En effet, suite aux modifications apportées au décret électricité, les plans de déploiement doivent nécessairement être segmentés et ils doivent tenir compte des contraintes reprises dans les décrets.

La technologie privilégiée initialement a donc dû être remise en question et ORES a l'intention d'opter pour une approche commune avec RESA en matière de déploiement.

Quelle que soit la solution qui sera mise en œuvre, la question de la confidentialité des informations transitant par les compteurs intelligents fera l'objet d'une attention très particulière.