# RAPPORT N° 13
# 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.

Par acte du 5 décembre 2013, la société ORES s.c.r.l. est devenue filiale d'ORES Assets, intercommunale constituée le 31 décembre 2013 suite à la fusion des GRD IDEG, IEH, IGH, INTEREST, INTERLUX, INTERMOSANE, SEDILEC et SIMOGEL (M.B. du 10 janvier 2014). Elle 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 au cours de l'année 2016 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.

# Chapitre II

## ORES s.c.r.l. – Filiale d'ORES Assets en Wallonie – Comité d'Ethique

## Comité d'Ethique

ORES s.c.r.l., filiale d'ORES Assets, s'est dotée de structures propres parmi lesquelles, conformément à l'article 16, § 1er, 4ème alinéa, du décret du 12 avril 2001 relatif à l'organisation du marché régional de l'électricité et à l'article 17, § 1er, 4ème alinéa, du décret du 19 décembre 2002 relatif à l'organisation du marché régional du gaz, outre le Conseil d'Administration, un Comité d'Ethique.

### I. Le Comité d'Ethique en ORES

Le Comité d'Ethique est un Comité constitué au sein du Conseil d'Administration en application de l'article 14 des statuts.

La Charte de Gouvernement d'entreprise établit les principes applicables à ce Comité.

### II. Mission du Comité d'Ethique

Le Comité d'Ethique est chargé de contrôler le respect, par le personnel, des règles relatives à la confidentialité des informations personnelles et commerciales.

Pour ce faire :

1. Le Comité d'Ethique bénéficie d'un accès illimité à tous les processus et à toutes les procédures mises en place ainsi qu'au personnel de la société.

2. Le Comité d'Ethique aura à sa disposition le contenu actualisé de tous les processus traitant des informations personnelles et commerciales.

3. Le Comité d'Ethique pourra entendre n'importe quel membre du personnel ayant accès à pareilles données.

### III. Confidentialité des informations personnelles et commerciales

Sur base d'une lecture combinée des dispositions décrétales et du Règlement du Comité d'Ethique, 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.

Les données personnelles et commerciales sont à ce titre confidentielles et relèvent du secret professionnel. L'article 16, § 1er, du décret électricité et l'article 17, § 1er, du décret gaz ne précisent pas exactement à qui sont dévolues les tâches stratégiques ou confidentielles. Il n'en demeure pas moins que le Comité d'Ethique doit reprendre à son compte les données reprises à l'article 16, § 1er, du décret électricité, et à l'article 17, § 1er, du décret gaz en ce qu'elles revêtent un caractère confidentiel. Le Comité d'Ethique est strictement chargé de contrôler le respect, par les administrateurs, personnel et sous-traitants d'ORES, des règles relatives à la confidentialité des données visées aux articles 12, § 2, et 16, § 1, du décret électricité et aux articles 13, § 2, et 17, § 1, 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 considérées comme utilisateur de réseau ou catégories 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.

Le Comité d'Ethique examine depuis 2009, sur base des dispositions précitées, les processus ou procédures mis en place en ORES ou par les sous-traitants d'ORES établissant le respect des dispositions en matière de confidentialité des 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, celle 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 *Metering*.

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 de sécurité Informatique d'ORES fait partie du département Informatique. Il est placé sous la responsabilité du Chef de Service responsable de la Gouvernance IT.

La mission de la sécurité Informatique ORES se résume en cinq types d'actions génériques. Elle consiste à:

- définir le périmètre et les vulnérabilités liés à l'usage des technologies de l'information et de la communication;
- garantir la confidentialité, l'intégrité et la disponibilité des actifs informatiques, ainsi que la protection de la vie privée;
- mettre en œuvre et valider les architectures, les mesures, les outils et les procédures de sécurité;
- optimiser la performance du système d'information en fonction du niveau de sécurité requis;
- assurer les conditions d'évolution du système d'information et de sa sécurité en respectant les contraintes légales, règlementaires et contractuelles.

L'efficacité de la sécurité d'un système d'information ne repose pas uniquement sur les outils de sécurité, mais également sur une stratégie, une organisation et des procédures cohérentes. Cela nécessite une structure de gestion adéquate dont la mission est de gérer, mettre en place, valider, contrôler et conscientiser l'ensemble des acteurs de l'entreprise à l'importance de la sécurité Informatique. Cette structure a été mise en place en 2011 chez ORES.

### 2. Mesures et plans d'actions

Le département Informatique d'ORES a établi un rapport complet de l'activité sécurité Informatique ORES 2016 : « Rapport annuel du Comité de Sécurité : Décembre 2016 ».

Dans le cadre du programme de sécurité 2016, les actions suivantes ont été réalisées :

**Projets informatiques de gestion**

- **Déploiement de la gestion des risques IT : Analyse de la criticité pour les applications du paysage d'ORES**
    - L'équipe Sécurité IT a analysé 15 applications au niveau de la confidentialité, l'intégrité et la disponibilité pour évaluer leur criticité. Ces données serviront à l'écriture du *Business Continuity Planning* (BCP). L'objectif est de passer en revue toutes les applications d'ORES dans les deux ans.

- **Implémentation de SAP *Identity Manager* (SAP IDM) pour les applications Netgis et Proxxx[1]**
    - NETGIS (application ORES de type « *Geographic Information System »)* WALLP1
        - La gestion des utilisateurs et de leurs accès est entièrement pilotée par SAP IDM : soit automatiquement pour le personnel interne (sur base des données RH) soit par traitement manuel pour le personnel externe (donnée ITIM).
        - Suppression automatique des accès informatiques *(de-provisionning)* de NETGIS sur base des données RH (internes) / ITIM (externes).
    - Proxxx
        - L'intégration des applications Proxxx sera faite en 2017.

- **Implémentation de SAP IDM pour les applications SAP liées au projet Odicéa**
    - SAP EWM : *Enterprise Warehouse Management* (ODICEA – Magasin d'Aye) : 4 environnements (PRD / QA / 2xDEV)
        - SAP WP9 : automatisation complète de la gestion des utilisateurs internes et de leurs accès sur base de leur métier (mêmes règles que sur SAP ECC).
        - SAP WD9-100 et 600 + WA9 : assignation manuelle des accès via l'interface web de SAP IDM.
        - Suppression automatique des accès informatiques de tous ces nouveaux environnements sur base des données RH/ITIM.

- **Gestion des *users* ORES dans l'*Active Directory* (AD) USER ORES via SAP IDM**
    - Tout le personnel d'ORES est migré dans l'AD USER ORES. Les groupes liés à la migration sont supprimés
        - Nettoyage des groupes AD Locaux « métiers » et « casquettes » (groupes de populations de référence) devenus obsolètes dans le cadre de la migration AD CORP vers AD ORES (projet SKYNOTE).
        - Création de nouveaux groupes AD de référence (Direction, espace SharePoint : Plan Interne d'Urgence (PIU), Mon Vadémécum, Gestion de la demande, Journal de Bord SCADA,…).

- **Inventaire *Disaster Recovery Plan* (DRP) & BCP**
    - Une analyse des risques de sécurité IT sur 15 applications ORES a été réalisée en 2016. L'écriture du document commencera en 2017.

- **Sécurisation de l'environnement Azure[2] ORES**
    - Suite aux tests de vulnérabilité réalisés sur les deux sites Web d'ORES hébergés dans le *Cloud* Azure, l'importance de revoir la sécurité IT de notre environnement Azure est devenue une priorité.

[1] Proxxx : les applications Proele et Progaz.
[2] Azure : la solution *Cloud* de Microsoft qu'utilise ORES.

- L'équipe sécurité IT a redessiné une architecture de sécurité pour notre *Cloud* Azure en utilisant un WAF *(Web Application Firewall)*.
- *Web Application Firewall (WAF)* dans Azure : installation et configuration du WAF pour bloquer les failles de sécurité découvertes pendant les tests de vulnérabilité. Seul le WAF est visible d'Internet, les serveurs Web seront derrière le WAF.

- **Mise en place d'une gestion opérationnelle des logs de sécurité**
  - L'équipe sécurité IT s'est renforcée d'un expert en sécurité pour s'occuper de la mise en place de la sécurité opérationnelle pour tous les environnements utilisés par le département Informatique.

- **Analyse d'écart de la sécurité informatique d'ORES par rapport à l'ISO27001:2013**
  - L'analyse d'écart par rapport à ISO27001:2013 n'a pas pu être réalisée (contrainte priorités/ressources).
  - Le service Gouvernance a décidé de ne pas faire cette analyse d'écart mais de directement implémenter l'ISO27001:2013 en 2017.

- **Tests de vulnérabilité IT**
  - ORES.BE et PROMOGAZ.BE (http://bonplan.ores.be/)
    - L'équipe Sécurité IT a sélectionné une société externe (test en boîte noire) pour effectuer des tests de vulnérabilité sur ces sites Web en février et en septembre 2016 et suite aux résultats, nous avons mis en place un *Web Application Firewall* dans notre environnement Azure.
  - EMORES (*Energy Management* ORES)
    - ORES a choisi une solution du type SAAS *(Software as a Service)* pour permettre aux clients EMORES d'afficher les courbes de charges. Cette solution est aussi utilisée pour le pilote *Smart Meter* de Charleroi.
    - Des données sensibles appartenant à ORES vont être utilisées par cette solution SAAS. Un test de vulnérabilité a été réalisé et des correctifs ont été mis en place par le fournisseur avant la mise en production.

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

- Au niveau sécurité, l'équipe sécurité IT a analysé une solution d'*Advanced Metering Infrastructure* (AMI) pour la gestion des compteurs électriques
  - Etude des échanges de clés et de certificats entre les différents composants de la chaîne Linky.

**Projet d'informatique Industrielle (*Operational Technology*, OT)**

- **Déploiement des premiers *firewalls* OT**
  - L'équipe Sécurité IT a commencé la mise en place du plan de sécurité défini en 2015 par la création d'un laboratoire pour vérifier le bon paramétrage des différents *firewalls*.

- Installation des *firewalls* des *Celos*[3] : le service gaz va installer 600 Celos (Internet Of Things, IoT, permettant de remonter la pression gaz) qui communiqueront via Internet avec un serveur du dispatching.
- L'équipe Sécurité IT a découpé le projet en petite partie et étudié le moyen de les réaliser séquentiellement en production, le tout afin de diminuer le temps d'arrêt de service et de pérenniser les changements.

- **Déploiement de la console de sécurité OT**
  - Installation d'un produit de supervision qui permet de configurer à distance les *firewalls*.

**Réalisations 2016 qui s'ajoutent au programme initial**

- **Evolution de SAP IDM en 2016**
  - La gestion des utilisateurs et des accès à certaines applications de type Windows ont également été intégrées à SAP IDM via le connecteur *Microsoft Active Directory* (LDAP).
  - Des « *Self-Services* » (via interface Web SAP IDM) dédiés à certains métiers du département Informatique pour des demandes d'accès critiques SAP (mode '*debug'* – '*full* accès') avec notification vers les responsables et la sécurité IT.
  - Optimisation et simplification du processus de gestion des accès spécifiques de type « casquette » permettant dès lors une plus grande autonomie et un meilleur suivi de la part des responsables business.

- **SAP *Single Sign-On* (SSO)**
  - Activation du SSO sur l'ensemble des environnements SAP.

- **Audit externe des accès du département Finances & Controlling et du service Achats & Logistiques**
  - Une société d'audit a été mandatée pour analyser les accès SAP du département Finances & Controlling ainsi que ceux du service Achats & Logistiques du département Technique.
  - Les résultats ont permis de mettre en évidence la bonne gestion des accès au sein de ces deux services.
    En effet, il n'est ressorti lors de la phase d'analyse qu'un nombre minime de risques non identifiés ou non déjà mitigés, et cela tout aussi bien pour les risques provenant des accès critiques que pour ceux générés par le cumul des tâches.
  - Lors de la phase de remédiation, en accord avec les services impactés, et afin d'atténuer les risques existants, des accès critiques ont été supprimés et de nouveaux contrôles compensatoires ont vu le jour.

[3] *Celo* : équipement qui permet de transmettre la pression gaz au *Dispatching*.

- **CyberAssurance**
    - ORES a souscrit une police d'assurances 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 et peut sortir ses effets 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 bien matériels résultant d'un accès non autorisé au système),
        - piratage du système téléphonique,
        - interruption de réseau et du système informatique (due à une défaillance de sécurité),
        - défaillance ou d'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).

## 3. Objectifs 2017

### Projets informatiques de gestion

- Analyse de la criticité pour les applications plus importantes du paysage d'ORES : augmentation des licences Citicus : 60 applications.
- Ecriture du BCP pour les applications IT.
- Gouvernance de sécurité IT : adaptation des processus de sécurité IT à la norme ISO27001:2013.
- Sécurisation de l'environnement Azure ORES.
- Analyse de la sécurité Office 365.
- Fourniture d'une politique d'authentification.
- Mise en place d'une gestion opérationnelle des *logs* de sécurité.
- Tests de vulnérabilité IT (scope à déterminer sur base de la roadmap 2017).
- Implémentation de SAP IDM pour les systèmes SAP :
    - WD0 - ORES - SAP Sol. Man. 7.1 - Development
    - WP0 - ORES - SAP Sol. Man. 7.1 - Production
    - WD4 - ORES - ERP Development (Atrias)
    - WI2 - ORES - ERP Integration (Uniwall).
- Implémentation de SAP IDM pour les applications PROELE et PROGAZ via le connecteur ODBC – ORACLE.
- Implémentation de SAP IDM pour ENERGIS (application .NET) via le connecteur *Microsoft Active Directory*.
- Gestion des utilisateurs ORES dans l'AD USER ORES via SAP IDM.
- Mise à jour de la documentation SAP IDM.

**Projet *Smart Metering***

- Participation au projet sur le périmètre Sécurité Informatique lié au trajet AMI/MOC/SOC.

**Projets d'informatique Industrielle**

- Mise en *Demilitarized Zone* (DMZ, zone démilitarisée) des interconnexions avec les partenaires externes.
- Procédure d'incidents de sécurité informatique industrielle.
- Lancement de la campagne d'installation des *firewalls* dans les postes et cabines.
- Définition d'une gouvernance de la sécurité pour l'informatique industrielle.

# Chapitre V

## N-ALLO

*Les faits marquants :*

- En 2010, N-Allo a fait évoluer l'environnement de travail des collaborateurs de façon assez importante avec l'introduction de la Coupole en remplacement de Vantive.
  La Coupole 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.

- En 2012, la mise à disposition par ORES d'un certain nombre de *services web* permettant un dialogue plus facile avec les applications de gestion (SAP ISU, SAP PROCLI, CTH, ICCWeb…) a permis de mettre en place les premières fondations d'une architecture SOA (Architecture Orientée Service). Le catalogue de web services a continué à évoluer depuis.

- En 2014, un trust a été établi entre les *Active Directory* d'ORES et de N-Allo permettant à ORES de contrôler de façon plus fine et en temps réel les personnes ayant accès aux applications de gestion et aux données associées.

- Depuis 2015, chacun des collaborateurs des Back Offices Techniques Travaux Planifiés (BOT TP) est désormais à même de recevoir des appels clients directement routés par la plateforme de communication de N-Allo. Ceci permet d'éviter une interaction en première ligne où l'opérateur n'a que peu de valeur ajoutée quand un dossier est déjà en cours de traitement.

- Et en septembre-octobre 2015 encore, dans le cadre de la préparation aux éventuels plans de délestage, N-Allo a réalisé avec succès une campagne exceptionnelle de test des infrastructures, des procédures et des systèmes pour s'assurer de la continuité du service dans des conditions d'urgence.

- En 2016, le paysage applicatif a connu un double changement particulièrement important :
  - Tout d'abord, la plateforme de communication a été migrée vers une nouvelle technologie, *Interactive Intelligence*.
  - Ensuite, l'ensemble des infrastructures ont été transférées vers le site de Crealys.

### ○ UN MODELE PARTAGE : UN DEFI

En matière de technologie, les principes fondamentaux d'un *contact center* peuvent être à certains égards considérés comme antagonistes.

Il s'agit en effet et dans le même temps :

- de mutualiser certaines infrastructures qui sont partagées entre un nombre important de clients : en regard des coûts

associés à cette technologie mais aussi à sa complexité, la mutualisation est un objectif en tant que tel ;

- d'assurer dans le même temps l'indépendance nécessaire entre le traitement et les données associées à chacun de ces clients.

La rencontre de ces deux objectifs est donc un souci constant pour le management du *Contact Center* et se traduit par la mise en œuvre de solutions propres, d'infrastructures spécifiques.

## ○ LES ELEMENTS CONSTITUTIFS D'UN *CONTACT CENTER*

### 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 ([4]) pour son traitement : mise en attente et diffusion de message (pour les appels), routage et distribution (pour toutes les interactions),…

Les moyens mis en œuvre pour ce faire sont :

- les lignes téléphoniques qui apportent les appels au sein de l'organisation pour les interactions téléphoniques ;
- le lien IP qui apporte au sein de l'organisation les autres types d'interactions – mail, chat,… ;
- le cœur de la plateforme (CIC Serveur) qui assure la distribution des interactions de tout type vers les collaborateurs ;
- les autres serveurs qui assurent les traitements sur les autres interactions : serveur mail, serveur documentaire,...
- les applications en marge de ces applications assurant le *reporting* et le *monitoring* de chacun de ces canaux de communication.

### Le CRM

Le CRM est l'application centrale du *Contact Center*. Il 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 du CRM :

- 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 ([5]) ;

[4] 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, les SMS et bientôt les interactions supportées sur le web : *chat, co-browsing*,...

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

- 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 chacun des donneurs d'ordre et qui sont mises à la disposition des opérateurs pour assurer dans les meilleures conditions de qualité et de traçabilité le traitement des interactions. Ces processus sont de plus en plus accompagnés d'informations complémentaires dont les opérateurs peuvent avoir besoin dans le traitement.

Deux types d'application CRM existent au sein de N-Allo :

- les applications des donneurs d'ordre : de plus en plus de donneurs d'ordre disposent de leur propre application CRM ;
- une application CRM construite et maintenue par N-Allo : ce secteur connaît un développement particulièrement important tant la qualité et la vitesse de traitement des interactions par les opérateurs est fonction de la qualité, de la richesse et de la convivialité de cette solution. N-Allo a très largement investi dans ce domaine avec le développement de ce que l'on appelle de façon générale le UDA (*Unique Desktop Application*), et en particulier pour ORES, la Coupole. Les principes de ce type d'application sont les suivants :
  - une grande convivialité ;
  - une interface unique qui pilote toutes les autres applications de gestion ;
  - la volonté de plonger l'opérateur dans le contexte du client dès que l'interaction est proposée : au lieu d'attendre de l'opérateur qu'il parcoure différents menus dans les différentes applications de gestion afin de pouvoir répondre au client, c'est l'application qui va faire ce travail de façon automatisée et qui va de la sorte proposer à l'opérateur l'information nécessaire à la compréhension de la problématique de l'interlocuteur, voire même la réponse à sa question.

**Les applications clients**

Pour certaines procédures de travail, l'opérateur peut être appelé à consulter ou à effectuer des transactions dans les applications des donneurs d'ordre. Ces applications sont propres à chacun des donneurs d'ordre de N-Allo. L'accès à ces différentes applications est géré par une '*password policy*' ou un mécanisme sécurisé de SSO *(Single Sign On)* et est défini avec chacun des donneurs d'ordre.

## Le *reporting/monitoring*

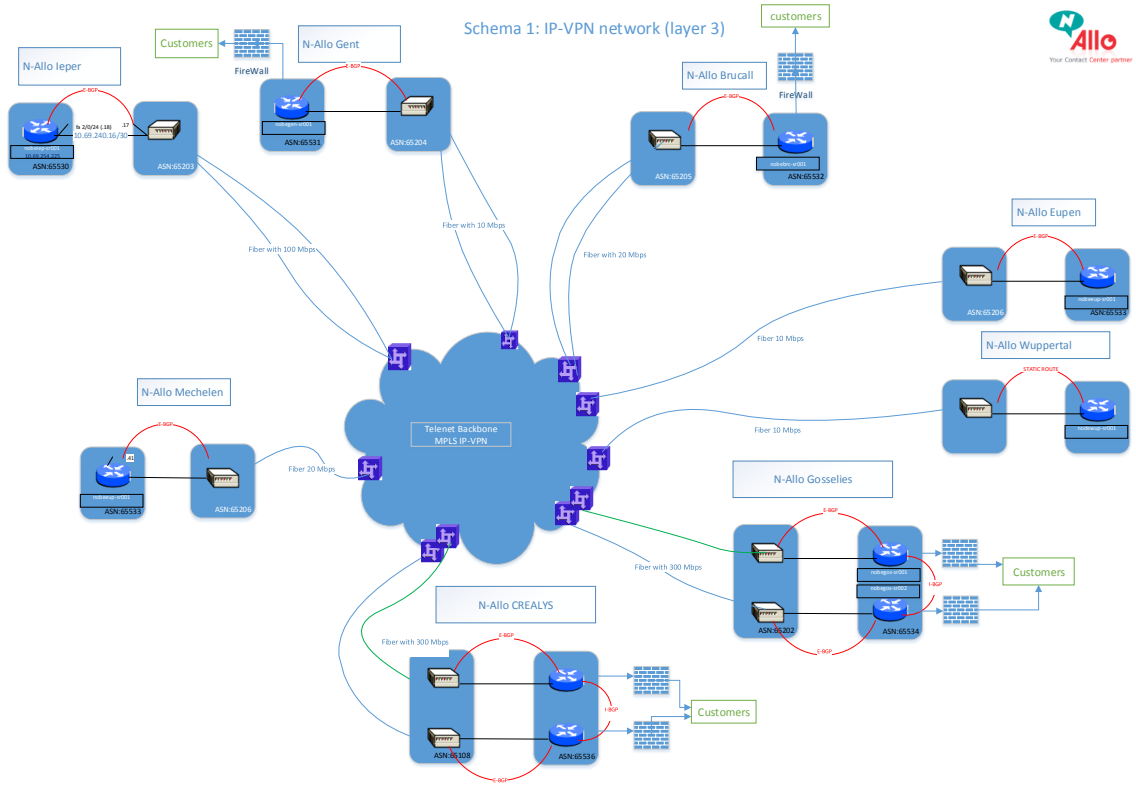
Le *reporting* est l'ensemble des moyens qui permettent de mesurer l'activité réalisée au sein du *Contact Center*. Le *monitoring* permet de remonter les mêmes informations mais en temps réel afin de pouvoir intervenir directement sur les opérations.Le *monitoring* est porté directement par les outils de la plateforme de communication, tandis que le *reporting* est généré à partir de bases de données externes de la plateforme au sein desquelles les différentes données opérationnelles sont collectées. On retrouve dans ces *reportings* les données relatives :

- à l'activité sur chacun des points d'entrée pour les différents types d'interaction : les points d'entrée sont propres à chacun des donneurs d'ordre. Il s'agit d'un numéro de téléphone, d'une adresse électronique, d'un numéro de SMS,...
- à l'activité des opérateurs ;
- à la durée de traitement des interactions.

Tant le *monitoring* que le *reporting* portent sur des données opérationnelles et non sur des données « client ».

## Les réseaux

L'ensemble des systèmes est relié par des réseaux IP depuis la migration complète de la plateforme. Ces réseaux sont particulièrement importants dans l'organisation N-Allo eu égard à sa structure sur 6 sites et au nombre de ses clients. N-Allo a également une connectivité importante avec plusieurs donneurs d'ordre extérieur à l'organisation. Le schéma ci-dessous donne un aperçu du réseau de N-Allo :



## LA MISE EN ŒUVRE AU SEIN DE N-ALLO

### ○ LE MODELE

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

L'évolution du marché vers ce type de modèle est une réalité mais est également importante pour N-Allo : en effet, de façon presque systématique maintenant, les solutions logicielles sont construites pour permettre le fonctionnement dans ce type d'architecture ; elles offrent donc les mécanismes de cloisonnement entre les activités supportées.

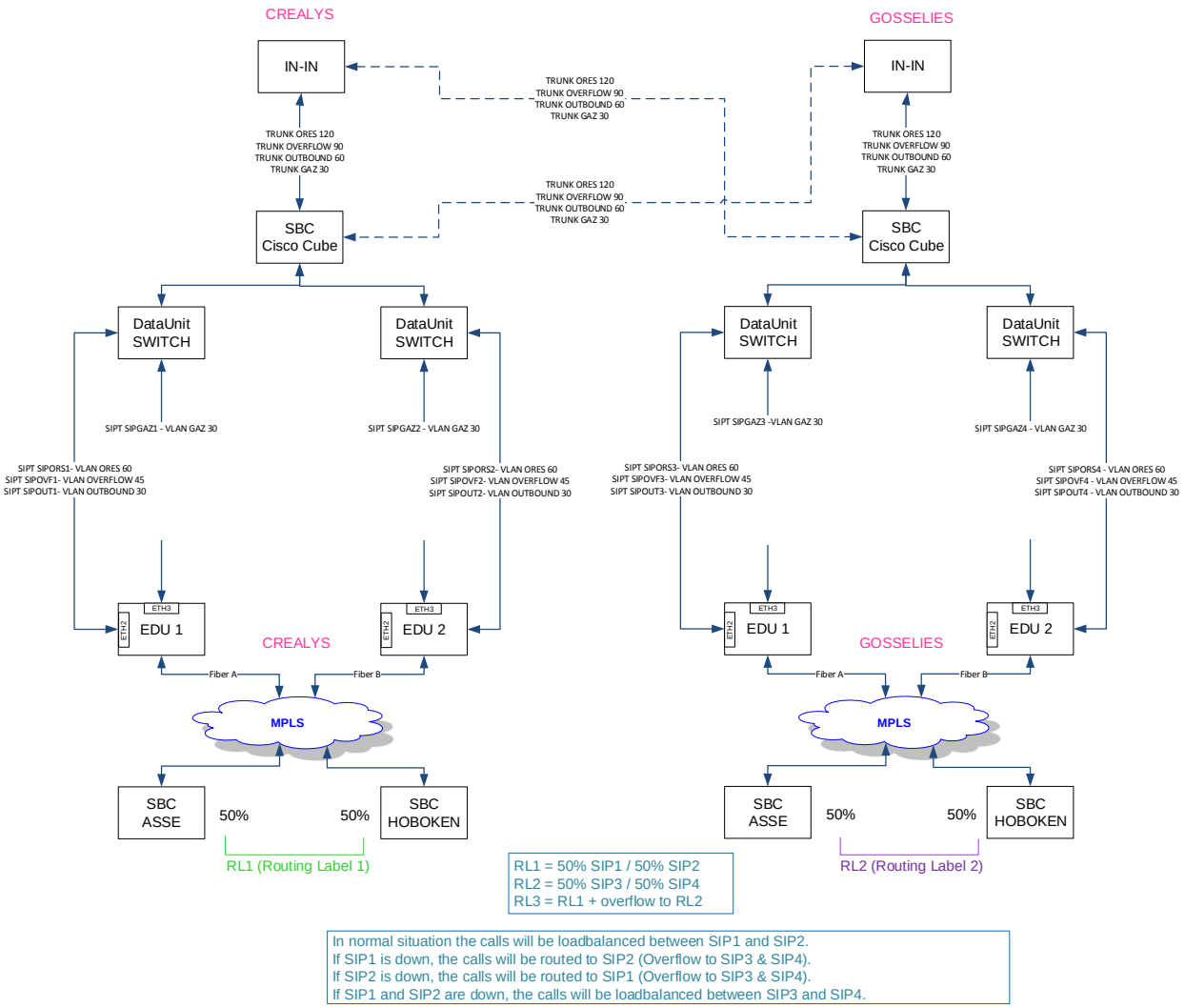
### ○ LA PLATEFORME DE COMMUNICATION

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

Cependant au sein de celle-ci, 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 rentrée.

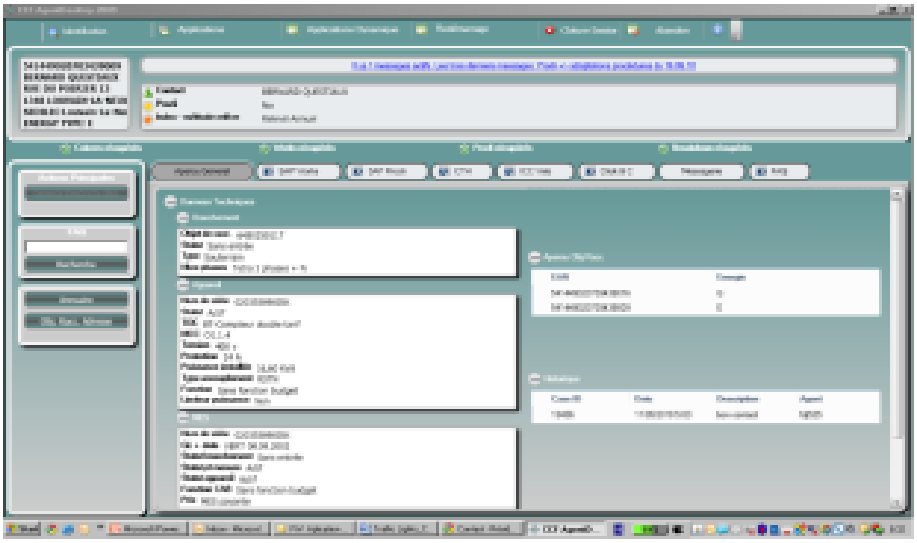
L'isolement des activités est visible sur le schéma suivant, où les routages affectés aux activités générales d'ORES, pour les odeurs gaz et pour les appels sortants, sont distincts. On notera qu'une disponibilité des services de très haut niveau est assurée comme le démontre également le descriptif.




## ○ L'ISOLEMENT DES ACTIVITES LES UNES PAR RAPPORT AUX AUTRES FAIT REGULIEREMENT L'OBJET DE TESTS. LE CRM – LA COUPOLE

ORES COUPOLE @ N-Allo

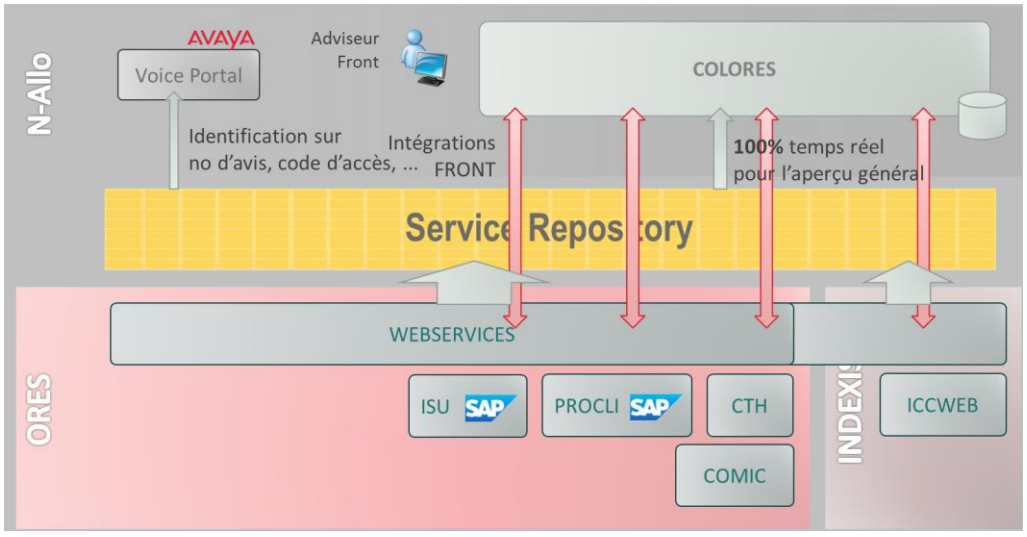
Avec le développement de l'application Colores, les collaborateurs de N-Allo traitant les interactions d'ORES disposent de leur environnement propre totalement séparé de tout autre environnement opérationnel.



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 dans l'environnement N-Allo.

L'architecture sous-jacente à cette application a en 2012 fondamentalement évolué. 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 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 la qualification de la raison d'appels.




Les droits d'accès à l'application ainsi qu'aux applications de gestion d'ORES (Lopex, Procli, Mercure) sont attribués sur 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).

Quant à l'accès aux *services web* publiés par ORES, ils sont strictement protégés par l'utilisation du protocole https ainsi que l'échange de certificats.

### ○ LE *REPORTING* ET LE *MONITORING*

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

1. des points d'entrée (lignes d'appels, *mailboxes*,...) : elles sont propres à chacun des donneurs d'ordre ;
2. des *skills* (compétences) des opérateurs : elles sont, pour ce qui est des activités Fournisseur et Gestionnaire de Réseaux, incompatibles.

### ○ LES RESEAUX

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 *subnetworks*, chacun des donneurs d'ordre se trouvant ainsi isolé sur son *subnetwork* propre. Cette nouvelle structure du réseau est opérationnelle depuis juillet 2007.

Il faut noter par ailleurs que ces mesures de sécurisation font régulièrement l'objet d'audit de la part de certains des donneurs d'ordre qui se doivent de préserver d'une part l'accès à leurs systèmes d'information et d'autre part la confidentialité des informations disponibles chez N-Allo.

### ○ SYNTHESE

En mettant ces différents moyens en œuvre, N-Allo peut ainsi garantir une totale étanchéité entre les activités liées aux différents donneurs d'ordre. Cette étanchéité est assurée tout au long du traitement comme suit :

- Au sein de la plateforme de communication : ce sont des numéros propres, des *mailboxes*,... pour chacun des donneurs d'ordre ;

- A chacun de ces points d'entrée sont associées des règles de routage qui amènent les appels vers des opérateurs propres à chacun des donneurs d'ordre ;
- Ceux-ci identifient le client :
  - soit au sein d'application qui sont spécifiques pour chacun des donneurs d'ordre et qui plongent dans des bases de données distinctes hébergées sur des machines distinctes ;
  - soit directement dans l'application propre au donneur d'ordre ;
- Les processus de traitement des interactions sont propres à chacun des donneurs d'ordre et ils sont accessibles dans les écrans qui sont eux-mêmes spécifiques ;
- Le stockage des interactions se fait dans les environnements propres ;
- Tout le suivi de l'activité se fait sur base de critères qui sont également propres à chaque donneurs d'ordre (ligne, compétences,…) ;
- Le réseau en œuvre au sein de l'organisation est particulièrement sécurisé afin d'empêcher toute intrusion externe ou toute indiscrétion par rapport aux données.

Remarque : la notion d'incompatibilité entre les *skills* des opérateurs est discutée avec chacun des donneurs d'ordre et tient donc compte de toute exigence particulière.

Ainsi dans le monde libéralisé, il y a stricte incompatibilité entre les opérateurs travaillant pour les activités du Gestionnaire de Réseau et les activités du Fournisseur tandis que des effets d'échelle entre les activités Fournisseur et celles d'autres donneurs d'ordre n'ayant rien à voir avec les marchés de l'énergie sont mis en œuvre afin d'optimiser la capacité de production de l'organisation.

## ORGANISATION OPERATIONNELLE

### ○ ORGANISATION GENERALE

Les activités gérées par N-Allo pour 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 le site de Bruxelles permettant de reprendre sans délai les activités de la permanence sur ce site en cas d'indisponibilité prolongée du site de Gosselies.

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

pour Affinion, dans le secteur de l'assurance, NIBC dans le secteur de la finance,…).

Cette organisation opérationnelle est le prolongement de l'infrastructure technique et permet d'assurer à ce niveau également une indépendance complète entre les différentes activités.

### ○ ORGANISATION PHYSIQUE

En fonction des besoins propres, une isolation physique peut également être assurée entre certaines activités. Les mesures en œuvre chez N-Allo sont par exemple les suivantes :

- Certains donneurs d'ordre disposent d'un local propre (avec ou sans contrôle d'accès) ;
- Certains donneurs d'ordre sont isolés sur des étages distincts ;
- Enfin, pour certains donneurs d'ordre seule une séparation physique simple est mise en œuvre (ilots propres).

# 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 modifié 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 (cfr. chapitre IV « Le service de Sécurité Informatique d'ORES »).

# Chapitre VII

## Relation avec les producteurs

La procédure respecte strictement les dispositions du règlement technique relatives à la procédure de raccordement à la haute tension.

Cette procédure repose sur les principes et étapes suivants :

- un système de file d'attente est mis en place sur 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[6] 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 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

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

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 où 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 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** : Etude des travaux de réseau nécessaires pour permettre la réalisation du raccordement ;
- L'**OFFRE** : Etablissement 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 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*)[7].

[7] Le modèle du DPIA est disponible sur le site de la Commission européenne : https://ec.europa.eu/energy/sites/ener/files/documents/2014_dpia_smart_grids_forces.pdf

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, jusqu'à présent, la réalisation d'un DPIA n'est toujours pas légalement requise mais a fait l'objet d'une phase de test initiée par la Commission européenne.
Toutefois, le règlement général sur la protection des données (ci-après le « *RGPD* ») voté par le Parlement européen et le Conseil en date du 27 avril 2016 requiert la réalisation d'un DPIA lorsqu'un traitement *« est susceptible d'engendrer un risque élevé pour les droits et libertés des personnes physiques »*. Ce règlement sera applicable à partir du 25 mai 2018. D'ici cette date, des précisions seront certainement apportées à la manière d'appliquer ces dispositions. Ainsi, il faut noter que le projet de recommandation de la CPVP sur la question est actuellement soumis à une consultation publique. Par la suite, ORES devra vérifier s'il n'est pas nécessaire de revoir les DPIA réalisés.
Plus généralement concernant le RGPD, ORES mettra en place un plan d'actions afin d'implémenter les nouvelles dispositions légales. Une réflexion est actuellement en cours au sein du secteur des gestionnaires de réseau de distribution.

En ce qui concerne l'acquisition du matériel nécessaire au déploiement des compteurs intelligents, il faut noter la collaboration avec ENEDIS (anciennement ERDF) afin de développer un compteur Linky adapté aux besoins des gestionnaires de réseau de distribution belges. Une procédure de marché public va être lancée en mars 2017 pour l'achat des compteurs et concentrateurs.
De même, une procédure est actuellement en cours afin de désigner le prestataire chargé de mettre à disposition d'ORES une solution informatique interopérable avec tout matériel Linky G3-PLC permettant de couvrir tous les besoins d'ORES.