RAPPORT N° 19
DU COORDINATEUR CONFIDENTIALITE D'ORES ASSETS

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

Chaque année depuis 2014, ORES Assets publie un rapport de confidentialité à l'attention de la CWaPE.
En vue de se conformer à la demande de la CWaPE adressée à ORES Assets[1], trois rapports distincts et spécifiques sont établis pour le Groupe ORES, soit un pour ORES Assets et deux autres pour chacune de ses filiales, à savoir ORES SC et Comnexio. Ces trois rapports sont établis sur la base de la même structure et détaillent les bonnes pratiques mises en place en matière de confidentialité. Ils visent à répondre au prescrit décrétal dont il est question ci-dessous.
Il convient de garder à l'esprit que la gestion opérationnelle et journalière des activités d'ORES Assets[2] en ce compris l'exercice des tâches stratégiques et confidentielles d'une part, et, la représentation d'ORES Assets dans le cadre de cette gestion, d'autre part, est confiée à ORES SC.
Les activités de *contact center* ont quant à elles été confiées à Comnexio à compter du 1er juin 2019.
Les modalités de ces gestions par lesdites filiales sont définies aux annexes 6 et 7 des statuts d'ORES Assets, et, par le Conseil d'administration, pour toute décision complémentaire.
La spécificité liée à la structure sociétale et à la réalité opérationnelle d'ORES Assets et ORES SC, où ORES Assets est le GRD et ORES SC[3] la société exploitante, a pour conséquence que le contenu de leur rapport est quasiment identique.

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 SC, filiale d'ORES Assets, a été désigné coordinateur confidentialité par le Comité de direction d'ORES SC du 1er février 2019, à savoir Audrey Réveillon.

[1] Conclusions provisoires du contrôle sur le niveau d'implémentation des règles de gouvernance, courrier de la CWaPE du 15 octobre 2019.
[2] Article 13 des statuts d'ORES Assets (voir aussi l'annexe 6 : modalités de l'exploitation opérationnelle et journalière réalisée par la société exploitante ORES).
[3] Article 3 des statuts d'ORES SC.

Depuis l'inventaire des bonnes pratiques en matière de confidentialité dressé par la CWaPE en 2019 dans le cadre de son contrôle des règles de gouvernance au sein des GRD et de leurs filiales, lesdits GRD et leurs filiales démontrent dans leur rapport confidentialité que l'ensemble de ces bonnes pratiques est effectivement mis en œuvre.

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 2022 pour répondre mieux encore à l'objectif de préserver la confidentialité des informations dont ORES Assets a connaissance dans l'accomplissement des tâches qui lui sont confiées.

Chapitre II – Obligations du personnel et des membres des organes de gestion en matière de confidentialité des données

1. Obligations du personnel en matière de confidentialité des données

Du fait qu'ORES Assets a confié à ORES SC l'exploitation journalière de ses activités conformément à l'article 16, § 1er, du décret électricité et à l'article 17, § 1er, du décret gaz, l'ensemble du personnel prestant pour le compte d'ORES Assets est sous contrat de travail avec ORES SC. Les dispositions qui suivent sont dès lors celles qui sont applicables en ORES SC.
Les contrats de travail des membres du personnel prévoient des clauses leur imposant une obligation de confidentialité.
Dans leur contrat de travail, les membres du personnel s'engagent ainsi notamment à ne pas communiquer les données confidentielles, à les utiliser exclusivement dans le cadre de l'exécution de leur contrat de travail, à ne pas les copier ou les reproduire sans autorisation préalable écrite et expresse d'ORES SC, à restituer à ORES SC 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 SC 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.

En conformité avec le règlement général sur la protection des données (ci-après « RGPD »), ORES SC a mis en place une série de processus et décrit les rôles et responsabilités de chacun. ORES SC poursuit, en outre, un effort constant dans l'amélioration de l'application des principes du règlement ainsi que dans la sensibilisation du personnel.
Une déclaration de politique générale a été écrite et publiée en interne en 2019. Elle donne au personnel d'ORES SC les lignes directrices que s'impose l'entreprise en matière de RGPD et est revue chaque année par le Comité de direction d'ORES SC. La dernière actualisation a eu lieu en date du 11 février 2022.
Des collaborateurs ont été formés dans chaque Direction afin de seconder le délégué à la protection des données (en abrégé « DPO » pour « *Data Protection Officer* ») sur le terrain.

Concrètement, la sensibilisation du personnel inclut :

- la diffusion d'une information de base sur les obligations en matière de confidentialité via la lecture et signature à l'engagement d'une clause de confidentialité ;
- la signature d'une fiche d'Engagement de confidentialité et de non divulgation à la remise du matériel informatique portable par la Direction Informatique ;
- l'imposition via le règlement de travail d'un nombre d'obligations en matière de confidentialité ;

- la transmission de la CCT TIC (technologies de l'information et de la communication) à tous les nouveaux employés d'ORES. Ce document fixe le cadre de l'utilisation des moyens de télécommunication par les travailleurs ;
- la mise à disposition d'un *Welcome Pack* pour chaque collaborateur dès son arrivée comprenant un volet cybersécurité ;
- la mise à disposition d'une courte vidéo expliquant l'importance de la sécurité et le rôle que chaque collaborateur doit jouer ;
- la réalisation d'une séance d'information comprenant des questions sur la cybersécurité. Cette séance faisait suite à une enquête de satisfaction « IT » ayant mis en avant une série de questions ou de difficultés de compréhension (par exemple : Pourquoi certains sites web sont bloqués ? Pourquoi ne peut-on pas installer tel logiciel ?,…). Cette séance était accessible en présentiel ou via vidéoconférence ;
- un *e-learning* obligatoire « RGPD » et divers modules d'*e-learning* en matière de sécurité de l'information ont été mis en place en 2020 pour l'ensemble des collaborateurs. Ces cours sont obligatoires pour tous les collaborateurs ORES ainsi que pour tout nouvel arrivant. Ces messages sont ensuite appuyés, depuis fin 2020 et de manière continue, par des campagnes de conscientisation sur divers sujets de sécurité en fonction des mesures de l'état de connaissance des collaborateurs ORES ainsi que des menaces principales pesant sur nos données. En 2022, comme en 2021, des campagnes ont eu pour objet de sensibiliser le personnel ORES au risque de phishing ;
- l'ouverture d'un espace collaboratif dédié au RGPD à disposition de l'ensemble des collaborateurs afin de faciliter l'accès à l'information pertinente et aux procédures à appliquer dès lors que des données à caractère personnel sont en jeu.

Pour mémoire, les informations ci-dessus ont déjà fait l'objet d'un rapport de la CWaPE dans le cadre de son contrôle sur l'implémentation des règles de gouvernance.
Le 6 décembre 2019, la CWaPE a confirmé à ORES qu'aucune recommandation n'était formulée pour ORES SC en ce qui concerne les obligations du personnel en matière de confidentialité des données.

2. Obligations des membres des organes de gestion en matière de confidentialité des données

Outre le devoir général de réserve imputable à tout administrateur de société, les administrateurs d'ORES Assets (GRD) mais également d'ORES SC et de Comnexio (filiales) sont conscientisés à leur obligation de confidentialité via les règles de gouvernance adoptées et appliquées en leur sein (en l'occurrence le Règlement d'ordre intérieur pour ORES Assets et les Chartes de gouvernance d'ORES SC et de Comnexio par ailleurs accessibles sur les sites internet).

Ils se sont également engagés individuellement à - notamment - observer les règles de déontologie, en particulier en matière de conflits d'intérêts, d'usage d'informations privilégiées, de loyauté, de discrétion et de bonne gestion des deniers publics, conformément à l'article L1532-1, § 1er, du Code de la Démocratie Locale et de la Décentralisation en signant une déclaration sur l'honneur à cet effet.

Par ailleurs, les administrateurs d'ORES Assets et d'ORES SC ont adopté un code de conduite MAR[4] et ont signé individuellement une déclaration en leur qualité de personne initiée.

[4] Règlement européen « Abus de marché » visant à améliorer l'intégrité des marchés et la protection des investisseurs.

Chapitre III – Mesures de sécurité quant à l'accès du personnel aux données à caractère personnel et aux données commerciales

Lorsqu'ORES SC traite, pour le compte d'ORES Assets, des données à caractère personnel en relation avec sa clientèle, tout est mis en place, que ce soit au niveau du personnel, des sous-traitants et de la sécurité informatique afin de préserver la confidentialité des informations personnelles et commerciales mises à sa disposition. Les données personnelles des utilisateurs du réseau recueillies auprès des divers interlocuteurs se limitent aux informations nécessaires à l'exécution des tâches liées aux missions légitimes d'ORES : raccordements, travaux planifiés comptages, OSP…

ORES a mis en place des procédures de protection des données dès la conception (« *Privacy by design* » et « *Security by design* ») de manière à ce que les aspects relatifs à la protection des données à caractère personnel de ses clients soient pris en compte dès le lancement de nouveaux projets ou à l'occasion modifications des traitements existants.

En parallèle, ORES SC réalise pour chaque nouveau traitement envisagé et chaque modification dans les processus des analyses RGPD appelées « questionnaire préalable ». En outre, des DPIA (*Data Protection Impact Assessments*) sont réalisés pour tout nouveau traitement susceptible *« d'engendrer un risque élevé pour les droits et libertés des personnes physiques »* clientes d'ORES. L'aspect « accès » aux données à caractère personnel est évalué dans chaque exercice. Des analyses de risque de sécurité sont également faites pour les nouveaux processus métiers.

Les mesures techniques et organisationnelles suivantes sont en place :

- la gestion des autorisations à nos applications informatiques est centralisée et automatisée au travers de l'outil « *SAP Identity Management* » (par exemple : Sap : lopex, procli ; *Active directory* : Mercure, registre national ; Oracle : netgis) ;
- la méthodologie appliquée pour la distribution des accès est le « contrôle d'accès basé sur les rôles » auquel ORES SC ajoute les deux principes suivants « *least privilege* » and « *need to know* » ;
- dans le cas d'accès privilégiés, ces derniers font l'objet d'un processus spécifique d'approbation ;
- le cycle de vie de nos identités informatiques est quant à lui automatiquement aligné sur la gestion du personnel ;
- les droits d'accès par métier sont validés par RH et les managers de chaque service ;
- les cahiers des charges concernant les nouvelles applications mentionnent spécifiquement le besoin d'intégration à notre système de gestion des identités et accès informatiques ;
- l'accès au registre national n'est donné qu'au personnel interne, après avoir signé un document expliquant pourquoi il a besoin d'accéder au registre. Ce document est validé par le supérieur hiérarchique et envoyé à la Direction RH pour être inséré dans le dossier personnel de l'employé. La liste des accès est revue par les managers tous les six mois. Un registre des consultations du numéro de registre national est tenu.

De manière générale, il convient de souligner que, dans le cadre de la loi du 7 avril 2019 établissant un cadre pour la sécurité des réseaux et des systèmes d'information d'intérêt général pour la sécurité publique (ci-après « NIS »), ORES Assets a été désignée Opérateur de Service Essentiel en date du 1er novembre 2022. ORES a en conséquence rédigé un document descriptif des systèmes soutenant ses services essentiels à destination du SPF Économie et du Centre pour la Cybersécurité en Belgique (CCB) et poursuit ses efforts en vue d'obtenir la certification ISO 27001.

Chapitre IV – Mesures de sécurité quant à l'accès des fournisseurs et des clients aux données confidentielles

1. Les services concernés d'ORES SC

Le Service *Structuring, Measure & Settlement (SMS)* fait partie de la Direction Clients. Cette Direction gère tous les processus liés au marché libéralisé (*Assets, structure, measure, settle et rectification*) ainsi que les obligations de service public à caractère social.
C'est l'équipe *Gestion du Registre d'Accès (GRA)* au sein du Service SMS qui gère le registre d'accès fédéral (CMS Atrias, *Central Market Design* dont le go live a eu lieu en décembre 2021) pour le portefeuille d'ORES ainsi que les contacts opérationnels avec les fournisseurs d'énergie.

Le CMS est la plateforme informatique fédérale qui permet de faciliter l'échange et le traitement de l'information entre tous les acteurs du marché belge de l'énergie sur base des MIGs (*Message Implementation Guide*).

Chaque point d'accès (*headpoint*) y est répertorié via son code EAN. Derrière ce code, on retrouve principalement les données du client, celles de son fournisseur et d'autres informations utiles. Derrière ce *headpoint*, on retrouve également les services component (par exemple pour un client prosumer, il y aura un service component pour le prélèvement et un pour l'injection).
Couplé – au niveau ORES – au MDM/Mercure (la base de données répertoriant les consommations de chaque point de fourniture) par le biais d'un grand orchestrateur (BPMS, *Business Process Management System*) mais également au backend SAP ISU (reprenant l'ensemble des informations techniques liées à un point de fourniture), le CMS donne une image complète du marché.

C'est l'équipe *Measure* du Service SMS - regroupant entre autres les releveurs et les valideurs - qui relève les données de consommation chez les clients toujours équipés de compteurs électromécaniques pour tout le territoire couvert par ORES et les valide, c'est-à-dire vérifie si les relevés sont cohérents au regard des statistiques et historiques de consommation ou des critères climatiques. L'équipe 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).

Depuis le go live d'Atrias, une nouvelle équipe a été mise en place pour suivre les dossiers bloqués soit parce que liés aux maladies de jeunesse du CMS soit parce que faisant partie du BaU (*Business as Usual*) des scénarios de marché. Il s'agit du *Market Service Center* (MSC).

Depuis le placement des compteurs communicants, une nouvelle plateforme de relève automatisée des index a été mise en place. Il s'agit de l'outil Prism (application permettant la collecte des données des compteurs communicants et gérant les téléopérations vers le HES, *Head-End System*), relié au MDM/Mercure

d'une part et à la chaine communicante des compteurs. Cette chaine de communication est supervisée par une nouvelle équipe – la *Smart Control Room (SCR)* – intégrée au sein du service SMS.

L'équipe *Gestion des Processus de Marché* (GPM) – Service Gestion Clients Marchés (GCM) de la Direction Clients – doit également accéder aux données reprises dans le CMS pour mener à bien les processus de *Drop*, *End-Of-Contract*, Initiate Leaving Customer (ILC) et Pose de compteur à prépaiement initiés par les fournisseurs d'énergie. Outre l'envoi de courriers, les agents sont amenés à contacter les clients (ex. d'une enquête sur un dossier ILC) et/ou les fournisseurs commerciaux (ex. d'une annulation sécurisée).

Enfin, notre *contact center* Comnexio, filiale d'ORES Assets, dispose également d'accès aux informations de la CMS ou encore de Mercure pour répondre aux appels de première ligne des clients.

La gestion des accès aux applications par ces différents agents et la manière dont des informations sont communiquées aux clients et/ou aux fournisseurs commerciaux sont expliquées au point suivant.

2. Mesures spécifiques adoptées

- **Le registre d'accès (CMS)**

  L'infrastructure informatique est sécurisée et l'accès à l'application est individualisé et réservé – par le biais notamment d'un outil de *reporting Business Object* (BO) – aux membres des équipes GRA, MSC et GPM (lecture et écriture).
  Toute nouvelle demande d'accès est soumise à l'approbation de l'application *owner Structuring*. Le gestionnaire des accès est informé – par le biais des fiches métier RH reprenant outre le descriptif des tâches, la liste des applications et transactions auxquelles chaque fonction donne droit – des accès spécifiques pour chacun.

  Les fournisseurs ont également accès à l'application (en consultation mais également pour initier/annuler des processus de marché) mais uniquement par le biais du portail de la CMS. Un fournisseur ne sait accéder qu'aux données des clients pour lesquels il a un contrat enregistré dans le registre d'accès. Les données client consultées seront celles qui auront été fournies par le fournisseur lui-même, par le biais des messages marché vers le GRD.
  Il peut également disposer des données techniques – liées aux points d'accès pour lesquels il est reconnu comme fournisseur. Ces données ne seront communiquées par le GRD que pour la durée de son contrat.
  Il n'aura donc aucun accès à des données client actif chez un autre fournisseur.
  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, les équipes GRA et GPM sont formées pour ne communiquer des renseignements par mail ou par téléphone qu'au seul fournisseur reconnu sur ce point d'accès.

Les équipes GRA, MSC et GPM ne communiquent des renseignements par téléphone, par courrier ou par mail qu'au client (ou à une personne mandatée par ce dernier) reconnu sur le point d'accès et seulement durant la période d'occupation de ce client, il lui sera demandé de communiquer son numéro de compteur pour vérification. Le client final n'a pas accès à l'application informatique même. Si un client demande au GRD quel fournisseur est lié au point d'accès, l'information lui sera envoyée par courrier à l'adresse d'installation.

La procédure appliquée par notre *contact center* Comnexio est également maitrisée. Si c'est un fournisseur commercial qui formule la demande, il sera d'office renvoyé vers le portail du CMS étant donné les accès dont il dispose.
S'il s'agit d'un client, ce n'est que contre la communication de son numéro de compteur que son EAN pourra lui être donné. L'information lui sera ensuite communiquée non pas oralement mais par le biais d'un SMS envoyé sur le numéro de GSM que le client aura dû nous communiquer. Si le client adresse sa demande par écrit ou s'il ne dispose pas d'un numéro de GSM, l'information lui sera transmise par courrier nominatif. S'il s'agit d'une demande concernant plus de deux EAN, il est demandé au client d'adresser sa demande par courrier/courriel avec la liste des adresses et numéros de compteurs concernés. Ces appels et communications sont tracés dans le système.

Le GRD fournit également des informations client aux CPAS. Le CPAS possède un numéro de contact spécifique pour solliciter des informations concernant ses administrés (état d'un dossier, fournisseur actif sur le point, historique de consommations,…) pour lesquels il dispose d'un mandat permanent. Il est demandé aux CPAS de ne jamais diffuser ce numéro d'appel.

Il existe une trace de toutes les transactions du marché ainsi que des envois de données.

Enfin, il est à noter que si un fournisseur lance un scénario de marché *drop* ou *pose d'un compteur à prépaiement* - 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 prépaiement* est en cours, mais seulement un message mentionnant 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. Il est à noter que, suite à la nouvelle procédure de défaut de paiement mise en place dans le cadre du décret appelé couramment « décret juge de paix », un fournisseur pourra toujours lancer une demande de Switch sur un EAN faisant l'objet d'une demande de pose de compteur à prépaiement sans qu'un rejet ne lui soit adressé.

- **Système Mercure**

  L'infrastructure informatique est sécurisée et l'accès à l'application est individualisé et réservé en mode 'modification' aux membres du service SMS.
  Toute nouvelle demande d'accès (en lecture ou en modification) est soumise à l'approbation de *l'application Owner Measure* qui dispose – par métier et fonction RH – des droits d'accès à l'application dont cet *application owner* est responsable.

  Le *contact center* Comnexio a également un accès à l'application mais uniquement via une interface web sécurisée par un mot de passe. Les accès à l'interface web sont également approuvés par *l'application owner*.

  Les fournisseurs ont accès à l'application via une interface web mais chaque fournisseur ne peut consulter que les données des clients/points d'accès pour lesquels il a reçu une acceptation d'enregistrement sur le point d'accès de la part du registre d'accès. De plus, la mise à disposition des données est limitée sur la base des données contractuelles entre le client et le fournisseur.

  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 disposer d'un mandat écrit et signé du client du point d'accès concerné.
  Il existe une trace de toutes les transactions du marché ainsi que des envois de données.

  Si le client appelle notre *contact center* Comnexio pour connaître son historique de consommation, la procédure en place lui indiquera que :
  - s'il s'agit d'un relevé à distance (hors compteur communicant), le client doit être invité à introduire sa demande via notre site web. Il recevra alors un historique portant sur les trois dernières années maximum ;
  - s'il s'agit d'un relevé annuel ou mensuel, il est d'abord rappelé aux conseillers-clientèle que les données de consommation sont des informations privées. Si un propriétaire souhaite connaître les consommations de ses locataires, il doit le demander directement à ses locataires ;
  - s'il s'agit d'un compteur communicant, le client peut accéder à ses historiques de consommation par le biais du portail mis à sa disposition et donc les accès sont également suivis strictement en matière de sécurité.

  Le client est ensuite invité à formuler sa demande par le biais de notre site web mais s'il ne le souhaite pas, la demande est prise en charge par le conseiller et un courrier reprenant au maximum les trois dernières années d'historique sera communiqué à l'adresse de consommation.
  Les clients étant dès le début de l'appel informés de son enregistrement, les équipes en charge des processus (*Process Owner*) peuvent faire des écoutes

téléphoniques d'appels enregistrés dans le but de vérifier l'application correcte des règles mises en place.

Les PDA (*Personal Digital Assistant*) des agents releveurs qui permettent l'introduction de l'index sur place sont également sécurisés par une identification personnelle sur la base d'un nom d'utilisateur et d'un mot de passe.

Enfin, dans le cadre des relevés de compteur, il est permis aux clients qui le souhaitent d'accéder à un espace digitalisé pour y communiquer leurs relevés. Après inscription sécurisée, le client peut recevoir ses courriers de demande de relève sous format digital. Ce processus est soumis à l'ensemble des règles du RGPD et en cas de changement de client, la fonctionnalité est automatiquement stoppée.

- **Le BPMS**

  Les équipes ayant accès à l'outil BPMS en mode « changement » sont uniquement les équipes informatiques habilitées. L'équipe MSC peut néanmoins y accéder en mode lecture pour les besoins d'analyse de cas bloqués. Les accès à cette application sont donnés par l'*application Owner* sur la base des fiches métier IT. Il n'y a pas d'autres équipes qui nécessitent l'accès à cette application.

- **Prism et le HES**

  Le HES n'est accessible que par le prestataire externe qui le met à disposition. S'agissant du Prism, il est accessible en lecture seule par l'équipe SCR mais également – toujours sur la base d'une fiche métier – à l'équipe Gestion des Prépaiements (GDP) qui gère depuis toujours les rechargements des compteurs à budget (Talexus) et à présent des compteurs communicants en mode prépaiement (via l'outil PPP 'hosté' au sein d'Atrias).
  Les téléopérations (ex. activation du port P1 ou demande de addIndex) sont exécutées au travers du Prism par le biais du système SAP CS (Outil nommé LoPex en ORES). Tous les accès à l'application Lopex sont contrôlés sur la base des fiches métiers RH.

Chapitre V – Mesures de sécurité quant à l'accès des sous-traitants aux données confidentielles

Mesures techniques et organisationnelles

Diverses mesures de sécurité adaptées au risque ont été mises en œuvre parmi lesquelles :

- l'utilisation d'identifiant unique pour les entrepreneurs et la limitation des droits d'accès aux chantiers ;
- la pseudonymisation des données rendues accessibles aux sociétés de développement informatique œuvrant pour ORES ;
- la ségrégation des accès aux données de production et aux données de test ;
- la limitation des accès aux données de production ;
- la limitation des accès aux données par les fournisseurs externes pour raison de maintenance ;
- la gestion des comptes d'administration et de support de prestataires externes via un système de « coffre-fort » (Produit CyberArk) ;
- la réalisation d'audits ;
- la minimisation des données fournies.

Mesures contractuelles

Lors de la conclusion de marchés ou de contrats avec ses partenaires, ORES insère systématiquement des clauses « RGPD » précisant l'ensemble des éléments prévus à l'article 28 du RGPD : durée, périmètre, finalité, instructions de traitement, autorisation préalable en cas de recours à un sous-traitant, mise à disposition de toute documentation apportant la preuve de la conformité, notification immédiate de toute violation de données. Un effort particulier a été réalisé afin de mettre en conformité nos contrats et marchés publics avec les nouvelles clauses contractuelles type publiées par la Commission européenne en juin 2021, ce, dès lors que ces marchés et contrats impliquaient un transfert possible des données à caractère personnel dont ORES SC est le responsable du traitement en dehors de l'espace Economique Européen.

Dès lors que des données sont partagées en dehors de l'Union européenne, les clauses contractuelles types sont appliquées.

Des clauses de confidentialité plus larges sont également prévues dans les contrats.

Chapitre VI – Traçabilité comme vecteur de confidentialité

ORES utilise les solutions « SAP » et a opté pour un paramétrage de la traçabilité plus poussé que le paramétrage standard recommandé par SAP. En ce qui concerne la traçabilité des activités des utilisateurs et des comptes techniques liés aux solutions tierces, ORES conserve dans la base de données SAP :

- une vue agrégée de l'utilisation journalière pendant 31 jours ;
- une vue agrégée de l'utilisation hebdomadaire pendant 20 semaines ;
- une vue agrégée de l'utilisation mensuelle pendant 20 mois.

Précisons que SAP garde la trace des transactions qu'une personne a initiées mais pas des données que cette transaction a permis de consulter. Le contexte n'est pas conservé. L'agrégation concerne le moment d'exécution de la transaction.

En ce qui concerne l'envoi de données par mail, le SAP ORES conserve une trace de l'ensemble des activités dans des environnements sécurisés et dont l'accessibilité est maîtrisée.

Les services liés à l'infrastructure réseau WIFI / LAN / WAN et la téléphonie sont de la responsabilité d'ORES. Les éléments suivants font partie du catalogue de services réseau ORES :

- Réseau d'accès aux utilisateurs finaux (25+ bâtiments) ;
- Commutateurs et routeurs ;
- Wi-Fi ;
- DNS/ DHCP / IPAM ;
- Contrôle d'accès au réseau ;
- Monitoring et Gestion opérationnelle.

Ceci permet d'illustrer la maîtrise d'ORES en ce qui concerne les contrôle d'accès et d'activités sur le réseau informatique. Le réseau OT (*Operational Technology*) est quant à lui la propriété d'ORES qui en assure également la gestion. De même, ORES a la maîtrise de l'ensemble des services et des outils de gestion de ses « *devices* » utilisateurs (station de travail, outils de mobilité).

L'implémentation d'un DLP (*Data Loss Prevention*) a été analysée en 2021. Une plateforme IT a été mise en œuvre. Un groupe de travail ORES a été créé afin de définir la gouvernance et les règles métiers qui seront implémentés dans la plateforme IT.
En 2022, ORES a travaillé sur la liste des données qui devront être bloquées par le DLP ainsi que sur un mode d'implémentation progressive afin d'avoir une bonne acceptation par son personnel. Des « bandeaux d'information » vont par ailleurs être mis dans un premier temps avant de passer en mode « blocage ».

Chapitre VII – Partage des systèmes et infrastructures IT avec d'autres sociétés

Aux fins de remplir sa mission, ORES partage certains systèmes et certaines infrastructures IT avec des partenaires. Il est prêté une attention très particulière à la mise en place de mesures de sécurité robustes garantissant la ségrégation, la confidentialité et l'intégrité de nos données dans ces systèmes et infrastructures partagés.

La gouvernance de Sécurité de l'information d'ORES s'aligne sur la norme ISO 27001.
La séparation des données ainsi partagées est basée sur les principes suivants :

- le « moindre privilège » (« *least privilege* ») : par défaut ne doivent être attribués à un utilisateur que les droits d'accès strictement nécessaires à la réalisation de sa tâche ;
- la « séparation des tâches » (« *segregation of duties* ») : une seule et même personne ne peut pas avoir le contrôle/l'accès complet sur l'ensemble d'un processus critique/sensible ;
- le « besoin de connaître » (« *need to know* ») : un utilisateur ne peut consulter une information que lorsqu'un réel besoin métier le nécessite. En d'autres termes, disposer des accès potentiels pour manipuler une information n'est pas suffisant pour justifier l'accès à cette information.

Pour tous ces cas, la gestion des droits d'accès aux applications « métiers » ORES reste de la responsabilité exclusive d'ORES.

Ci-après, les principaux partages de systèmes et infrastructures IT :

- <u>Fluvius (IMDMS)</u>

  Le système de « *clearing* » IMDMS est partagé avec Fluvius. Ce système permet de centraliser et d'organiser les opérations sur le marché de l'énergie.
  Dans le système actuel, Fluvius a la possibilité de voir toutes les données afin de pouvoir remplir son rôle de gestionnaire de la *Clearing House* (allocation, réconciliation, *infeed*).
  Une révision des droits d'accès des utilisateurs d'ORES a été effectuée afin de limiter les actions sur les données d'ORES. Lorsqu'une personne quitte ORES, son compte est automatiquement bloqué lors de la révision des mots de passe qui intervient tous les trois mois.
  De son côté, Fluvius procède régulièrement à l'effacement des comptes bloqués.
  Il est à noter que le rôle de *Clearing House* est assuré par Atrias depuis le 29 novembre 2021.

- <u>ENGIE IT (principal fournisseur de services IT)</u>

  Comme pour l'ensemble des fournisseurs IT d'ORES, les relations avec ENGIE IT sont contractualisées et reprennent des clauses de confidentialité, des clauses de sécurité et des clauses RGPD. L'accès d'ENGIE IT aux données d'ORES est monitoré.

- N-ALLO

  ORES a recours aux infrastructures techniques de N-Allo (via l'utilisation de sa plateforme de téléphonie ININ qui est utilisée par les *back offices* d'ORES), notamment lorsque ces *back offices* agissent en deuxième ligne de notre *contact center* (Comnexio).
  Comme pour tous les fournisseurs de services, N-Allo s'est contractuellement engagée à respecter des clauses de confidentialité, des clauses de sécurité et des clauses RGPD.
  Le remplacement de la plateforme de téléphonie ININ est actuellement en cours. A partir du 30 juin 2023, ORES ne recourra plus aux services de N-Allo.

- Cas particulier : *Connect My Home*
  L'initiative « *Connect My Home* » est la réalisation de synergies dans les travaux de raccordement des particuliers et regroupe à ce stade les opérateurs suivants : ORES, la SWDE, Proximus, VOO et Telenet.
  Afin de pouvoir bénéficier du service « *Connect My Home* », les clients peuvent s'inscrire par le biais d'un portail unique dont la gestion a été confiée à ORES. Tout a été mis en œuvre contractuellement et opérationnellement pour que la sécurité et la confidentialité des données des particuliers ainsi que les possibilités pour ces derniers d'exercer leurs droits « RGPD » soient strictement garanties.

Chapitre VIII – Déploiement des compteurs communicants

Pour souscrire à l'obligation de déploiement de la nouvelle technologie, ORES s'est alliée à un consortium avec d'autres GRD (Fluvius et RESA) dans le but de mutualiser des coûts et de fournir au citoyen une solution plus rapide et plus cohérente.

Une gouvernance a été mise en place en vue de respecter le principe de protection et de confidentialité des données dès la conception.

Les compteurs communicants transmettent les index de relève à ORES une seule fois par jour (même pour les données intrajournalières). Ces index sont transmis via un prestataire qui n'a pas connaissance de l'identité des clients d'ORES.
Pour garantir la protection des données de comptage ainsi transmises, celles-ci sont chiffrées depuis le compteur jusque chez ORES. Des tests de pénétration spécifiques ont été réalisés.

L'implémentation des compteurs communicants chez ORES fait l'objet d'une approche phasée. Depuis 2020, des compteurs communicants sont installés chez des particuliers. Dans aucun cas, ORES n'impose le nouveau compteur au citoyen.

Au regard des principes en matière de protection des données, voici les réponses apportées par ORES :

- Dans la phase actuelle, seuls des traitements dont les finalités sont directement liées à la mission classique du GRD et aux obligations légales sont d'actualité. D'autres traitements sont envisagés pour l'avenir. Ceux-ci seront fondés sur un consentement explicite, spécifique, préalable et informé des citoyens ;

- <u>Principe de transparence et droit à l'information</u>
  Dès la prise de rendez-vous pour l'installation des nouveaux compteurs, les personnes concernées sont averties du caractère communiquant de ceux-ci.
  Une brochure explicative est remise à l'installation des compteurs. Une page sur notre site[5] répond aux questions en matière de protection des données. Les collaborateurs en contact avec les clients sont formés. Notre délégué à la protection des données (DPO) est également disponible pour toutes questions en lien avec le respect de la vie privée et la protection des données. Une mise à jour de notre notice de vie privée a été réalisée en janvier 2023 ;

- <u>Minimisation, qualité et durée de conservation</u>
  Seules les données nécessaires à la réalisation des missions décrites sont collectées.
  En matière de conservation, les données sont traitées comme les données classiques de relève. Sans accord du client, seuls les index journaliers sont captés ;

- <u>Sous-traitance</u>
  Un contrat de sous-traitance est conclu conformément à l'article 28 du RGPD avec chacun de nos partenaires ;

[5] www.ores.be/particuliers-et-professionnels/comptage-intelligent.

- Sécurité
  Des mesures techniques et organisationnelles adaptées ont été mises en œuvre pour garantir la protection (confidentialité et intégrité) des données des clients d'ORES : les compteurs communicants font l'objet d'une veille en matière de cybersécurité qui prend en compte les aspects liés à la protection des données et à l'application des lois en vigueur.

Les risques de sécurité intentionnels ont été évalués dans la cadre d'ateliers de travail suivant la méthode EBIOS afin d'apprécier les risques Sécurité des systèmes d'information (entités et vulnérabilités, méthodes d'attaques et éléments menaçants, éléments essentiels et besoins de sécurité...) et de contribuer à leur traitement en spécifiant les exigences de sécurité à mettre en place.

Il est à noter que trois compagnies des eaux présentes sur le territoire flamand sont aujourd'hui entrées dans le consortium, ce qui a pour conséquence que le système d'acquisition des données (HES) est aujourd'hui partagé par sept sociétés (Fluvius, Resa, Sibelga, Pidpa, De Watergroep et Farys).

Les données récoltées par les compteurs communicants n'ont pas vocation à être conservées par le HES. Des mesures de sécurité adaptées au risque ont été implémentées. En effet, des règles de séparation « logiques » sont en place afin d'éviter un accès inapproprié aux données des autres opérateurs ainsi qu'un mauvais routage des données.
Si à l'avenir un rôle était assigné à ORES dans le cadre de la gestion des données des compteurs d'eau (transfert des données via les compteurs électriques par exemple), il est évident que des mesures appropriées seront mises en place afin de répondre aux objectifs de ségrégation des rôles.