



RAPPORT CONFIDENTIALITE DE CONNEXIO

TABLE DES MATIERES

Chapitre I – Préambule.....	3
Chapitre II – Obligations du personnel et des membres des organes de gestion en matière de confidentialité des données	5
1. Obligations du personnel en matière de confidentialité des données	5
2. Obligations des membres des organes de gestion en matière de confidentialité des données	5
Chapitre III – Mesures de sécurité quant à l'accès du personnel aux données à caractère personnel et aux données commerciales.....	7
Chapitre IV – Mesures de sécurité quant à l'accès des fournisseurs et des clients aux données confidentielles.....	9
Chapitre V – Mesures de sécurité quant à l'accès des sous-traitants aux données confidentielles	11
Chapitre VI – Traçabilité comme vecteur de confidentialité	12
Chapitre VII – Partage des systèmes et infrastructures IT avec d'autres sociétés	13

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 Assets¹, 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 Connexio. 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 décretaal dont il est question ci-dessous.

Il convient de garder à l'esprit que la gestion opérationnelle et journalière des activités d'ORES Assets² 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 Connexio à compter du 1^{er} 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.

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. ...* ».

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.

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 2024 de Connexio en tant que filiale d'ORES Assets chargée d'exercer les tâches de *contact center* d'ORES Assets depuis le 1^{er} juin 2019.

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 conformément à l'article 13 des statuts »).

Vu la suppression du Comité d’Ethique de Connexio suite à la modification des décrets organisant les marchés régionaux de l’électricité et du gaz par le décret du 5 mai 2022³, ce rapport a été approuvé par le Conseil d’administration de Connexio réuni en date du 19 mars 2025.

Il est à noter par ailleurs que, à l’instar d’ORES Assets et dans le cadre de la gouvernance commune, le Conseil d’administration de Connexio du 23 novembre 2022 a également désigné Audrey Réveillon en cette même qualité de coordinateur confidentialité.

Il convient de rappeler que, afin d’être opérationnelle au 1^{er} juin 2019, Connexio avait conclu un contrat de services de transition avec N-Allo. Cette convention avait pour objectif de définir les services de transition à fournir par N-Allo à Connexio. Le trajet dotant Connexio de ses propres outils de *contact center* pour exécuter ses missions indépendamment de N-Allo a pris fin le 30 juin 2023, N-Allo ne fournit plus de service de transition à Connexio.

Depuis le 25 mai 2023, un contrat de prestation de services est en cours avec NTT pour l’acquisition d’une solution de centre de contacts intégrée dans l’écosystème Connexio/ORES. Cette convention permet à Connexio d’utiliser la plateforme de centre de contacts Genesys Cloud.

En ce qui concerne les services IT de base, le contrat de service de support avec ORES SC continue d’être appliqué.

Enfin, notons également que Connexio exerce ses activités de *contact center* pour ORES Assets uniquement.

³ Décret du 5 mai 2022 modifiant diverses dispositions en matière d’énergie dans le cadre de la transposition partielle des directives 2019/944/UE du 5 juin 2019 concernant des règles communes pour le marché intérieur de l’électricité et 2018/2001/UE du 11 décembre 2018 relative à la promotion de l’utilisation de l’énergie produite à partir de sources renouvelables et en vue d’adapter les principes relatifs à la méthodologie tarifaire.

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

Les contrats de travail types des membres du personnel prévoient des clauses leur imposant une obligation de confidentialité.

Ainsi, les membres du personnel s'engagent 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 de Connexio, à restituer à Connexio 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.

Connexio poursuit un effort constant dans l'application des principes du règlement général sur la protection des données (ci-après « RGPD ») ainsi que dans la sensibilisation du personnel.

En termes de protection de la confidentialité des données, les mesures prises incluent :

- l'imposition via le règlement de travail d'un nombre d'obligations en matière de confidentialité ;
- 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 ;
- depuis fin 2020 et de manière continue, des campagnes de conscientisation sont menées sur divers sujets de sécurité en fonction des mesures de l'état de connaissance des collaborateurs ainsi que des menaces principales pesant sur nos données ;
- depuis 2022, un point de contact unique (« SPOC ») RGPD a été désigné au sein de Connexio afin d'être un relais privilégié avec le délégué à la protection des données (« DPO »).

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.

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 de Connexio sont sensibilisés à leur obligation de confidentialité via les règles de gouvernance adoptées et appliquées en son sein (en l'occurrence, la « Charte de gouvernance d'entreprise » par ailleurs accessible sur le site 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, § 1^{er}, du Code de la Démocratie Locale et de la Décentralisation en signant une déclaration sur l'honneur à cet effet.

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

Lorsque Connexio traite des données à caractère personnel en relation avec la clientèle d'ORES, tout est mis en place, que ce soit au niveau du personnel, des sous-traitants ultérieurs 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...

Tant ORES que Connexio ont 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, des exercices relatifs à la mise à jour de son registre de traitement et de « *Data Protection Impact Assessment* » (ci-après « *DPIA* ») sont conduits afin d'analyser et d'évaluer les risques liés aux traitements de données existants préalablement à l'entrée en vigueur du RGPD et de prévoir un plan de remédiation pour ceux-ci. L'aspect « accès » aux données à caractère personnel est évalué dans ces exercices.

En outre, une procédure impose la tenue de tels DPIA pour tout nouveau traitement susceptible « *d'engendrer un risque élevé pour les droits et libertés des personnes physiques* » clientes d'ORES.

Les mesures techniques et organisationnelles suivantes sont en place :

- la gestion des autorisations aux applications informatiques hébergées par ORES est centralisée et automatisée au travers de l'outil « *SAP Identity Management* » (par exemple : Sap : lopex, procli ; *Active directory* : Mercure ; Oracle : netgis) ;
- la méthodologie appliquée pour la distribution des accès est le « contrôle d'accès basé sur les rôles » auquel ORES (en qualité de prestataire de service IT de Connexio) 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 des identités informatiques est quant à lui automatiquement aligné sur la gestion du personnel ;
- les droits d'accès aux applications informatiques sont gérés par ORES et validés dans le chef de Connexio par le *service delivery manager* ;
- les cahiers des charges concernant les nouvelles applications mentionnent spécifiquement le besoin d'intégration au système de gestion des identités et accès informatiques mis en place par ORES SC (en qualité de prestataire de service IT de Connexio).

A noter en ce qui concerne la Coupole⁴ :

- Le passage par la Coupole permet à Connexio, d'une part, de filtrer l'accès aux informations clients et, d'autre part, de filtrer ce à quoi les conseillers clientèle peuvent avoir accès une fois connectés ;
- En cas de départ d'un membre du personnel de Connexio ou d'un remplacement, une procédure d'urgence a été mise en place. Les accès sont alors retirés ou autorisés selon les cas ;
- Le personnel de Connexio dispose d'un *login* via une station de travail ORES sur un réseau géré par ORES.

⁴ Depuis le 31 décembre 2020, Connexio n'utilise plus la coupole N-Allo. Cette dernière a été remplacée par une application développée par ORES. La coupole ORES est une interface facilitant le traitement des interactions (identification du client et automatisation des processus de relève d'index) pour les conseillers clientèle de Connexio et permettant le traçage des raisons d'appel.

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

Connexio dispose d'accès aux informations du CMS (*Central Market System*) ou encore de Mercure pour répondre aux appels de première ligne des clients.

La gestion des accès aux applications par Connexio et la manière dont des informations sont communiquées aux clients sont expliquées au point suivant.

Mesures spécifiques adoptées

- *Le registre d'accès (CMS)*

L'infrastructure informatique est sécurisée et l'accès à l'application est réservé. Toute nouvelle demande d'accès est transmise à ORES qui l'approuve selon sa procédure interne. Pour le surplus, nous renvoyons aux rapports établis pour ORES Assets et ORES SC.

La procédure appliquée au sein de Connexio est maîtrisée.

Les conseillers clientèle ne communiquent des renseignements par téléphone, par courrier, par mail, par chat ou par Messenger 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. 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.

Ainsi, 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 qu'après vérification 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 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, sa demande est encodée et traitée via courriel/courrier.

Ces appels et communications sont tracés dans la Coupole.

Connexio 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.

- *Système Mercure*

L'infrastructure informatique est sécurisée et l'accès à l'application est individualisé et réservé en mode 'modification' au personnel de Connexio mais uniquement via une interface web (*Coupole*) sécurisée par un mot de passe.

Pour le surplus, nous renvoyons aux rapports établis pour ORES Assets et ORES SC.

La procédure appliquée au sein de Connexio est maîtrisée.

Les conseillers clientèle ne communiquent des renseignements par téléphone, par courrier ou par mail qu'au client (ou à une personne mandatée par ce dernier) reconnu par son EAN et seulement durant la période d'occupation de ce client. Il lui sera demandé de communiquer son numéro de compteur pour vérification.

Si le client appelle 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 le site web d'ORES. 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.

- *Enregistrements*

En règle avec les prescrits de la loi relative aux communications électroniques, les communications entre les conseillers clientèle de Connexio et les interlocuteurs sont enregistrées.

Depuis le 25 mai 2023, Connexio recueille et enregistre les communications électroniques et les données qui y sont échangées (calls, e-mails, chats...) émanant des conseillers clientèle de Connexio sur sa nouvelle plateforme de centre de contacts.

Par défaut, ces enregistrements sont conservés pendant un mois à compter de la date de la communication. Cependant, pour les enregistrements recueillis en vertu d'obligation légales spécifiques (ex. appels odeurs gaz), la durée de conservation des appels est adaptée pour répondre aux obligations légales.

Un outil d'intelligence artificiel de type *speech to text* (transcription des appels en texte et analyse textuelle) est en cours de test chez Connexio. Une analyse d'impact sur les données est également en cours afin de s'assurer de la conformité de ce processus au RGPD et aux futures obligations découlant de l'*Artificial Intelligence Act*.

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

Mesures contractuelles

Lors de la conclusion de marchés ou de contrats avec ses partenaires, des clauses « RGPD » y sont insérées systématiquement. Elles précisent 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...

Dès lors que des données sont partagées en dehors de l'Union européenne, des mesures équivalentes de protection des données sont mises en place et les clauses contractuelles types sont appliquées par préférence.

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

Mesures spécifiques

Une plateforme de centre de contacts (Genesys Cloud) est utilisée par Connexio. Cette plateforme est mise à disposition par un partenaire NTT.

Les mesures contractuelles ad hoc ont été mises en place avec le nouveau sous-traitant dans le but d'assurer la protection des données à caractère personnel des personnes concernées (ce sous forme d'un *data processing* agreement ou accord de traitement des données additionnel aux documents de marché). Un DPIA a été réalisé en novembre 2023. Une analyse de risque de sécurité a été menée selon la méthodologie EBIOS, un test de pénétration a par ailleurs été réalisé en septembre 2023 et les points (faibles) ont été traités.

Services IT

Connexio a confié à la Direction IT d'ORES SC tous les services IT de base tels que la fourniture, l'installation et le support des stations de travail, le *printing*, l'accès internet, la gestion de l'*Active Directory*, l'accès réseau...

Chapitre VI – Traçabilité comme vecteur de confidentialité

Connexio délègue à ORES SC la gestion de son service IT.

Plus de détails sur la gestion par ORES SC de la traçabilité des accès sont donnés dans le rapport confidentialité d'ORES SC.

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

Les systèmes et infrastructures IT de Connexio sont gérés par ORES SC en vertu du contrat de services de support susvisé entre ORES SC et Connexio. A cet égard, la gouvernance de Sécurité de l'information de Connexio est celle d'ORES qui s'aligne sur la norme ISO 27001.

De manière générale, il convient de souligner qu'ORES Assets est une entité essentielle au sens de la réglementation NIS 2⁵. 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 est en phase finale pour l'obtention de la certification ISO 27001. Le bureau de certification ayant remis un avis favorable en janvier 2025, ORES devrait obtenir sa certification pour fin mars 2025.

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.

Les mesures spécifiques concernant NTT ont été reprises ci-avant.

⁵ Réglementation NIS 2 : directive (UE) 2022/2555 du Parlement européen et du Conseil du 14 décembre 2022 concernant des mesures destinées à assurer un niveau élevé commun de cybersécurité dans l'ensemble de l'Union, modifiant le règlement (UE) n° 910/2014 et la directive (UE) 2018/1972, et abrogeant la directive (UE) 2016/1148 (directive SRI 2) et loi belge du 26 avril 2024 établissant un cadre pour la cybersécurité des réseaux et des systèmes d'information d'intérêt général pour la sécurité publique.