RAPPORT CONFIDENTIALITE DE COMNEXIO

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 6

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 14

Chapitre VII – Partage des systèmes et infrastructures IT avec d'autres sociétés 15

Chapitre I - Préambule

Chaque année depuis 2014, ORES Assets publie un rapport de confidentialité à l'attention de la CWaPE.
Pour le rapport relatif à l'année 2019, la CWaPE a demandé à ORES Assets[1] que trois rapports distincts et spécifiques soient établis : l'un pour ORES Assets et deux autres pour chacune de ses filiales, à savoir ORES SC et Comnexio. Ces trois rapports ont été établis sur 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. … »*.

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'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 sont désormais invités à démontrer dans leur rapport confidentialité que l'ensemble de ces bonnes pratiques est effectivement mis en œuvre.

Le présent rapport couvre les activités de Comnexio en tant que filiale d'ORES Assets chargée d'exercer les tâches de *contact center* d'ORES Assets à compter du 1er juin 2019.

[1] Conclusions provisoires du contrôle sur le niveau d'implémentation des règles de gouvernance, courrier de la CWaPE du 15/10/2019.
[2] Article 12 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.

Ce rapport a été approuvé par le Comité d'Ethique de Comnexio lequel s'est tenu – dans le contexte exceptionnel de force majeure causé par la crise sanitaire – selon une procédure à distance et par voie électronique – le 25 mars 2020.

A titre liminaire, il convient de rappeler qu'afin d'être opérationnelle au 1er juin 2019, Comnexio a conclu les contrats de services principaux suivants :

- un contrat de services de transition avec N-Allo. Cette convention a pour objectif de définir les services de transition à fournir par N-Allo à Comnexio; et
- un contrat de service de support avec ORES SC, notamment en ce qui concerne les services IT de base.

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

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 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 Comnexio, à restituer à Comnexio 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.

Faisant suite à l'entrée en vigueur du règlement général sur la protection des données (ci-après « RGPD »), Comnexio poursuit un effort constant dans l'application des principes du règlement ainsi que dans la sensibilisation du personnel.
Dans le courant du deuxième semestre 2020, il est prévu que des collaborateurs soient formés afin de seconder le délégué à la protection des données (en abrégé « DPO » pour « *Data Protection Officer* ») sur le terrain.

Concrètement, cela inclut :

- 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 ;
- l'achat en 2019 par ORES d'une plateforme de conscientisation afin de former le personnel. Les sujets de confidentialité des données, d'obligations RGPD ainsi que de bonnes pratiques concernant la sécurité de l'information y sont entre autres abordés en mettant l'accent sur les comportements et obligations des utilisateurs. La stratégie adoptée est de déployer un cours de base reprenant ces éléments dès le mois de mars 2020. Ces formations seront mises à disposition des collaborateurs de Comnexio. Ces messages seront ensuite appuyés, dès 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 ainsi que des menaces principales pesant sur nos données ;

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 Comnexio sont conscientisés 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, §1er, 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 Comnexio 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 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 Comnexio ont mis en place des procédures de protection des données dès la conception (« *Privacy by design* ») de manière à ce que les aspects relatifs aux 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, Comnexio a lancé début 2020 des exercices relatifs à la mise à jour de son registre de traitement et de « Data Protection Impact Assessment » (ci-après « DPIA ») 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 en cours de rédaction 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 tant par ORES que par N-Allo 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 Comnexio) 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 Comnexio 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 Comnexio).

A noter en ce qui concerne la Coupole :

- Le passage par la Coupole permet à Comnexio, 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 Comnexio 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 Comnexio dispose d'un *login* via une station de travail ORES sur un réseau géré par ORES.

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

Comnexio dispose d'accès aux informations du registre d'accès ou encore de Mercure pour répondre aux appels de première ligne des clients.

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

Mesures spécifiques adoptées

- *Le registre d'accès*

  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 Comnexio 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 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 registre d'accès (*supplier web*), 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 communiqué. Si le client ne peut communiquer son numéro de compteur, l'EAN ne pourra lui être communiqué par téléphone mais lui sera envoyé par courrier à l'adresse de consommation. 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 seront tracés dans la Coupole.

  Il est à noter qu'un trajet d'amélioration est en cours au sein d'ORES en collaboration avec Comnexio concernant les demandes « connaître son EAN » afin de ne communiquer ces informations qu'au seul client actif sur le point d'accès.

  Comnexio 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 Comnexio mais uniquement via une interface web (*Measure Web*) 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 Comnexio 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.

- *Enregistrements*

  En règle avec les prescrits de la loi relative aux communications électroniques, les communications entre les conseillers clientèle de Comnexio et les interlocuteurs sont enregistrées. Ainsi, dans le cadre du contrat de transition susvisé entre N-Allo et Comnexio et à la demande de cette dernière, N-Allo recueille et enregistre des communications électroniques et les données qui y sont échangées (calls, e-mails, chats...) émanant des conseillers clientèle de Comnexio. Enfin, si la plateforme N-Allo permet l'enregistrement des interactions entre les clients et les conseillers clientèle de Comnexio, ces enregistrements contenus dans les répertoires réservés à Comnexio sont exclusivement à la disposition du personnel de Comnexio.

  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, une extraction régulière est prévue à des fins de conservation par Comnexio.

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, les clauses contractuelles types sont appliquées.

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

Mesures spécifiques

La convention de transition conclue entre N-Allo et Comnexio impose aux parties une obligation de confidentialité dans leur chef. Ainsi, elles s'engagent notamment à préserver la confidentialité des données, à les utiliser uniquement dans le cadre de l'exécution de la convention, à préserver la confidentialité de telles données et à prendre des mesures de précaution afin de les protéger, à ne pas les divulguer à un tiers, sauf accord écrit préalable de l'autre partie et à retourner ou détruire les informations confidentielles dans la mesure où elles ne sont plus utiles à l'autre partie.

En outre, dans le cadre du RGPD, lorsque N-Allo ou Comnexio traite des données à caractère personnel relatives aux clients d'ORES, ORES agit en qualité de responsable du traitement, Comnexio en qualité de sous-traitant et N-Allo en qualité de sous-traitant de second rang en vertu du contrat de transition. Comnexio n'intervient sur les données d'ORES que sur instruction de celle-ci.

En pratique, N-Allo met à la disposition de Comnexio un ensemble d'applications que l'on peut classer en deux catégories.

La première catégorie concerne les applications qui contiennent des données considérées comme plus sensibles quelle que soit la nature de ces données. Cette catégorie reprend principalement la Coupole. La Coupole est l'interface facilitant le traitement des interactions pour les conseillers clientèle de Comnexio et permettant le traçage des raisons d'interaction.

Le personnel de Comnexio a accès via ces applications aux données clients (voir ci-dessous pour plus de détails). L'accès à l'application Coupole est réservé au seul personnel de Comnexio. N-Allo n'y a par principe pas d'accès, à l'exception d'un nombre restreint d'employés du Service Informatique qui dispose d'un *login* technique permettant de faire les tests techniques, et le cas échéant, d'assurer la gestion des systèmes d'information (dans le cadre strict de cette mission).

La seconde catégorie reprend les applications qui ne contiennent pas de données sensibles comme la plateforme de communication et les applications associées (*call flows*, IVR,…). Ces applications ne contiennent donc qu'un nombre très limité de donnés clients.
Il convient de noter toutefois que la plateforme de communication permet l'enregistrement des interactions entre les clients et les conseillers clientèle de Comnexio. Nous nous référons à cet égard aux développements repris au Chapitre IV du présent rapport au sujet des enregistrements.

L'équipe technique qui assure la gestion des systèmes d'information dispose également dans le cadre strict de cette mission des accès aux bases de données.

L'environnement de *reporting* ne contient que des données opérationnelles limitées, celles-ci pouvant être liées aux agents de Comnexio. Par contre, il n'y a aucune donnée 'client' au sein de cet environnement de *reporting*.

Enfin, il en est de même pour l'application Nice WFM permettant la planification des ressources. Elle contient des données sur les agents de Comnexio mais aucune donnée sur les utilisateurs du réseau.

Services IT

Comnexio a confié au Département 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… L'implication de N-Allo se limite strictement à la gestion de tickets (incidents ou *service requests*) relatifs aux applications que N-Allo met à disposition de Comnexio. Ce périmètre d'implication de N-Allo est contractuellement défini de façon stricte dans la convention de services de transition susmentionnée. De façon pratique, cette implication est cadrée par des procédures précises et gérée entièrement au travers du Département IT d'ORES SC sans contact direct entre N-Allo et les agents de Comnexio.

Lors de la constitution de Comnexio, un dispositif en matière de sécurité informatique a été mis en place et soumis à l'approbation de la CWaPE [4]. Il prévoit entre autres :

- un cloisonnement informatique des systèmes et applications mises à disposition de Comnexio par N-Allo (« *Chinese Wall* ») tel que prévu dans la convention de services de transition entre Comnexio et N-Allo :
    - N-Allo garantit une limitation des accès aux données des applications mises à disposition exclusive de Comnexio aux seuls agents de Comnexio et au personnel de N-Allo pour lequel un accès est strictement nécessaire pour la fourniture des services informatiques. Ces données sont par ailleurs stockées dans des environnements informatiques propres à Comnexio, et totalement distincts des environnements informatiques des clients de N-Allo ;
    - Comnexio se réserve le droit de procéder aux vérifications qu'elle jugerait nécessaires pour contrôler notamment le bon cloisonnement informatique des applications mises à sa disposition par N-Allo ainsi que des données liées. Si suite à ces vérifications, il s'avérait que N-Allo ne respectait pas

[4] Demande d'obtention de l'accord de la CWaPE du 29/03/2019 en vue de confier à une nouvelle filiale d'ORES Assets les activités de *contact center*.

(plus) ses obligations en termes de cloisonnement, N-Allo s'engage à une mise en conformité dans les meilleurs délais ;

- une véritable séparation entre les activités de Comnexio et de N-Allo même si les bâtiments restent partagés (séparation physique des équipes).

Chapitre VI – Traçabilité comme vecteur de confidentialité

Comnexio 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 Comnexio sont gérés par ORES SC en vertu du contrat de services de support susvisé entre ORES SC et Comnexio. A cet égard, la gouvernance de Sécurité de l'information de Comnexio est celle d'ORES qui s'aligne sur la norme ISO27001.
En conséquence, 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 N-Allo ont été reprises ci-avant.