



**VERTROUWELIJKHEIDSVERSLAG VAN
CONNEXIO**

INHOUD

Hoofdstuk I - Inleiding	3
Hoofdstuk II – Verplichtingen van het personeel en van de leden van de bestuursorganen inzake de vertrouwelijkheid van de gegevens	5
1. Verplichtingen van het personeel inzake de vertrouwelijkheid van de gegevens	5
2. Verplichtingen van de leden van de bestuursorganen inzake de vertrouwelijkheid van de gegevens	5
Hoofdstuk III – Beveiligingsmaatregelen betreffende de toegang van het personeel tot persoons- en commerciële gegevens	7
Hoofdstuk IV – Beveiligingsmaatregelen in verband met de toegang van leveranciers en klanten tot de vertrouwelijke gegevens.....	9
Hoofdstuk V – Beveiligingsmaatregelen betreffende de toegang van onderaannemers tot vertrouwelijke gegevens.....	11
Hoofdstuk VI – Traceerbaarheid als vector van vertrouwelijkheid	12
Hoofdstuk VII – Het delen van IT-systemen en -infrastructuren met andere bedrijven.....	13

Hoofdstuk I - Inleiding

Sinds 2014 publiceert ORES Assets elk jaar een vertrouwelijkheidsverslag ter attentie van de CWaPE.

Om te voldoen aan het door de CWaPE aan ORES Assets¹ gerichte verzoek, worden er voor de Groep ORES drie afzonderlijke en specifieke verslagen opgemaakt, namelijk één voor ORES Assets en twee andere voor elke dochteronderneming, namelijk ORES cv en Connexio. Deze drie verslagen worden volgens dezelfde structuur opgemaakt. Ze geven een uitvoerige beschrijving van de goede praktijken op het vlak van de vertrouwelijkheid. Ze streven ernaar te beantwoorden aan de voorschriften van het hieronder vermelde decreet.

Men dient in gedachten te houden dat het operationeel en dagelijks beheer van de activiteiten van ORES Assets² aan ORES cv is toevertrouwd, met inbegrip van de uitoefening van de strategische en vertrouwelijke taken enerzijds en de vertegenwoordiging van ORES Assets in het kader van dat beheer anderzijds.

Wat de *contact center*-activiteiten betreft, deze werden vanaf 1 juni 2019 toevertrouwd aan Connexio.

De wijze waarop deze beheersactiviteiten door voornoemde filialen worden uitgeoefend, wordt bepaald in bijlagen 6 en 7 van de statuten van ORES Assets en door de Raad van Bestuur voor elke bijkomende beslissing.

Artikel 17 van het besluit van 21 maart 2002 betreffende de netbeheerders, gewijzigd door het besluit van 6 december 2018, bepaalt: *“De netbeheerder zorgt ervoor dat hij de persoonlijke en commerciële gegevens waarvan hij kennis krijgt bij de uitvoering van zijn taken, verzamelt en bewaart in een vorm en onder voorwaarden die de vertrouwelijkheid beschermen. Hij garandeert dat die gegevens systematisch gescheiden worden van de gegevens die openbaar kunnen worden gemaakt. ...”*

Artikel 7 van het besluit van 16 oktober 2003 betreffende de gasnetbeheerders, gewijzigd door het besluit van 6 december 2018, bevat identieke bepalingen.

Sinds de invoering van de inventaris van goede praktijken inzake vertrouwelijkheid, die in 2019 door de CWaPE werd opgesteld in het kader van zijn controle van de governance-regels bij de DNB's en hun dochterondernemingen, tonen die DNB's en hun dochterondernemingen in hun vertrouwelijkheidsverslag aan dat al deze goede praktijken daadwerkelijk werden toegepast.

Dit verslag bestrijkt de activiteiten in 2024 van Connexio als dochteronderneming van ORES Assets, belast met de uitoefening van de taken van *contactcenter* van ORES Assets sinds 1 juni 2019.

Door de afschaffing van het Ethisch Comité van Connexio na de wijziging van de decreten betreffende de organisatie van de gewestelijke elektriciteits- en gasmarkt door

¹ Voorlopige conclusies van de controle op het vlak van de implementering van de bestuursvoorschriften, schrijven van de CWaPE van 15 oktober 2019.

² Artikel 13 van de statuten van ORES Assets (zie ook bijlage 6: “Modaliteiten van de operationele en dagelijkse uitbating verwezenlijkt door de exploitatievennootschap ORES overeenkomstig artikel 13 van de statuten”).

het decreet van 5 mei 2022³, werd dit verslag goedgekeurd door de Raad van Bestuur van Connexio, die hierover heeft vergaderd op 19 maart 2025.

Er moet ook worden opgemerkt dat, naar het voorbeeld van ORES Assets en in het kader van het gezamenlijke bestuur, de Raad van Bestuur van Connexio op 23 november 2022 ook Audrey Réveillon heeft aangesteld in dezelfde hoedanigheid van vertrouwelijkheidscoördinator.

Er dient ook aan herinnerd te worden dat Connexio, om operationeel te zijn op 1 juni 2019, met N-Allo een overgangsdienstverleningscontract had afgesloten. Deze overeenkomst had tot doel om te bepalen welke overgangsdiensten door N-Allo aan Connexio moesten worden geleverd. Het traject om Connexio met eigen contactcenter-tools uit te rusten om haar opdrachten onafhankelijk van N-Allo uit te voeren, is afgelopen op 30 juni 2023. N-Allo levert niet langer overgangsdiensten aan Connexio.

Sinds 25 mei 2023 loopt er een dienstverleningsovereenkomst met NTT voor de aanschaf van een contactcenteroplossing die is geïntegreerd in het ecosysteem van Connexio/ORES. Dankzij deze overeenkomst kan Connexio het Genesys Cloud contactcenterplatform gebruiken.

Wat de IT-basisdiensten betreft, wordt het contract voor supportdiensten met ORES cv verder toegepast.

Tot slot moet ook worden opgemerkt dat Connexio haar contactcenteractiviteiten alleen uitvoert voor ORES Assets.

³ Decreet van 5 mei 2022 tot wijziging van diverse bepalingen inzake energie in het kader van de gedeeltelijke omzetting van Richtlijn 2019/944/EU van 5 juni 2019 betreffende gemeenschappelijke regels voor de interne markt voor elektriciteit en Richtlijn 2018/2001/EU van 11 december 2018 ter bevordering van het gebruik van energie uit hernieuwbare bronnen en met het oog op de aanpassing van de beginselen inzake tariefmethodologie.

Hoofdstuk II – Verplichtingen van het personeel en van de leden van de bestuursorganen inzake de vertrouwelijkheid van de gegevens

1. Verplichtingen van het personeel inzake de vertrouwelijkheid van de gegevens

De type-arbeidscontracten van de personeelsleden bevatten clausules die hun een verplichting tot vertrouwelijkheid opleggen.

Zo verbinden de personeelsleden er zich met name toe om vertrouwelijke gegevens niet openbaar te maken, om ze uitsluitend in het kader van de uitvoering van hun arbeidscontract te gebruiken, om deze gegevens niet te kopiëren of te reproduceren zonder voorafgaande uitdrukkelijke schriftelijke toestemming van Connexio, om de gegevens die op het ogenblik van de beëindiging van het arbeidscontract nog in hun bezit zijn aan Connexio terug te geven en dit onmiddellijk na de beëindiging van het arbeidscontract.

Connexio blijft permanent inspanningen leveren om de principes van de Algemene Verordening Gegevensbescherming (hierna “AVG”) toe te passen en het personeel bewust te maken van het belang ervan.

Wat de bescherming van de vertrouwelijkheid van de gegevens betreft, omvatten de genomen maatregelen:

- het opleggen van een aantal verplichtingen inzake vertrouwelijkheid via het arbeidsreglement;
- de terbeschikkingstelling van een *Welcome Pack* met een hoofdstuk over cyberveiligheid aan elke medewerker bij zijn aankomst;
- de terbeschikkingstelling van een korte video met uitleg over het belang van gegevensveiligheid en de rol die elke medewerker daarbij moet spelen;
- sinds eind 2020 en op permanente wijze worden er bewustmakingscampagnes over diverse veiligheidsonderwerpen gehouden, afhankelijk van de kennis die bij de medewerkers wordt vastgesteld en de belangrijkste bedreigingen waaraan onze gegevens zijn blootgesteld;
- sinds 2022 is er binnen Connexio één enkel AVG-contactpunt opgericht (“SPOC”) dat als bevoorrecht doorgeefluik met de Data Protection Officer (“DPO”) fungeert.

Ter herinnering: de bovenstaande informatie maakte reeds het voorwerp uit van een verslag van de CWaPE in het kader van haar controle op de toepassing van de governance-regels.

2. Verplichtingen van de leden van de bestuursorganen inzake de vertrouwelijkheid van de gegevens

Naast de algemene plicht tot terughoudendheid die elke bestuurder van een vennootschap heeft, worden de bestuurders van Connexio bewust gemaakt van

hun vertrouwelijkheidsplicht via de governance-regels die binnen de onderneming zijn aangenomen en worden toegepast (in casu het “Bestuurscharter van het bedrijf”, dat trouwens toegankelijk is via de website).

De bestuurders hebben er zich eveneens individueel toe verbonden om onder andere de deontologische regels na te leven, in het bijzonder op het vlak van belangenconflicten, het gebruik van voorwetenschap, loyaliteit, discretie en goed beheer van overheidsmiddelen, overeenkomstig artikel L1532-1, § 1, van het Wetboek van de Lokale Democratie en de Decentralisatie, en dit door een verklaring op eer in dat verband te ondertekenen.

Hoofdstuk III – Beveiligingsmaatregelen betreffende de toegang van het personeel tot persoons- en commerciële gegevens

Wanneer Connexio persoonsgegevens verwerkt in verband met de klanten van ORES, wordt er alles aan gedaan, op het vlak van personeel, latere onderaannemers of IT-beveiliging, om de vertrouwelijkheid van de ter beschikking gestelde persoons- en commerciële gegevens te bewaren. De persoonsgegevens van de netgebruikers die bij diverse gesprekspartners worden ingezameld, beperken zich tot de informatie die noodzakelijk is voor de uitvoering van de taken in verband met de legitieme missies van ORES: aansluitingen, geplande werken, meting, ODV, enz.

Zowel ORES als Connexio voerden reeds in de ontwerpfase (*“Privacy by design”* en *“Security by design”*) beschermingsprocedures in op zo’n manier dat er van bij het opstarten van nieuwe projecten of ter gelegenheid van wijzigingen van de bestaande verwerkingen rekening wordt gehouden met de aspecten die te maken hebben met de persoonsgegevens van haar klanten.

Tegelijkertijd werden er oefeningen opgestart in verband met het bijwerken van haar verwerkingsregister en de *“Data Protection Impact Assessments”* (hierna *“DPIA”*) met het oog op het analyseren en evalueren van de risico’s verbonden aan gegevensverwerkingen die reeds vóór de inwerkingtreding van de AVG bestonden en het voorzien van een plan om eraan te verhelpen. Het aspect *“toegang”* tot de persoonsgegevens wordt in deze oefeningen geëvalueerd.

Bovendien schrijft een procedure voor dat dergelijke DPIA moeten worden uitgevoerd voor elke nieuwe verwerking die zou kunnen *“resulteren in een hoog risico voor de rechten en vrijheden van natuurlijke personen”* die klanten van ORES zijn.

De volgende technische en organisatorische maatregelen worden toegepast:

- het beheer van de machtigingen voor de IT-applicaties die door ORES worden gehost is gecentraliseerd en geautomatiseerd met behulp van de tool *“SAP Identity Management”* (bijvoorbeeld: Sap: lopex, procli; *Active directory*: Mercure, Oracle: netgis);
- de methodologie die voor de toegangs distributie wordt toegepast is de *“op rollen gebaseerde toegangscontrole”*, waaraan ORES (in de hoedanigheid van IT-dienstverlener van Connexio) de twee volgende principes toevoegt: *“least privilege”* en *“need to know”*;
- bevoorrechte toegangen tot gegevens of applicaties maken het voorwerp van een specifiek goedkeuringsproces uit;
- de levenscyclus van de IT-identiteiten wordt automatisch afgestemd op het personeelsbeheer;
- toegangsrechten tot IT-toepassingen worden beheerd door ORES en binnen Connexio gevalideerd door de *service delivery manager*;
- bestekken betreffende de nieuwe applicaties vermelden specifiek de behoefte aan integratie in het systeem voor het beheer van IT-identiteiten en -toegangen dat door ORES cv werd ingevoerd (in de hoedanigheid van IT-dienstverlener van Connexio).

In verband met de Koepel⁴ dient het volgende te worden opgemerkt:

- Door de Koepel te gebruiken is Connexio in staat om enerzijds de toegang tot de klanteninformatie te filteren en anderzijds om te filteren waartoe de klantenadviseurs toegang krijgen nadat zij ingelogd zijn;
- Wanneer een personeelslid van Connexio het bedrijf verlaat of vervangen wordt, wordt er een spoedprocedure gebruikt. De toegangen worden, afhankelijk van het geval, ingetrokken of toegestaan;
- Het personeel van Connexio beschikt over een login via een ORES-werkstation op een door ORES beheerd netwerk.

⁴ Sinds 31 december 2020 gebruikt Connexio de N-Allo-koepel niet meer. Deze werd vervangen door een door ORES ontwikkelde applicatie. De ORES-koepel is een interface die de verwerking van de interacties (identificatie van de klant en automatisering van de meteropnameprocessen) vergemakkelijkt voor de klantenadviseurs van Connexio en het traceren van de redenen van de oproepen mogelijk maakt.

Hoofdstuk IV – Beveiligingsmaatregelen in verband met de toegang van leveranciers en klanten tot de vertrouwelijke gegevens

Connexio heeft toegang tot de informatie van het CMS (*Central Market System*) of van Mercure om de eerstelijnsoproepen van de klanten te beantwoorden.

Het beheer van de toegang tot de applicaties door Connexio en de manier waarop de informatie aan de klanten wordt meegedeeld, worden in het volgende punt uitgelegd.

Specifieke maatregelen

- *Toegangsregister (CMS)*

De computerinfrastructuur is beveiligd en de toegang tot de applicatie is voorbehouden.

Elke nieuwe aanvraag tot toegang wordt overgemaakt aan ORES, die deze volgens haar interne procedure goedkeurt. Voor het overige verwijzen wij naar de verslagen die voor ORES Assets en ORES cv werden opgesteld.

De procedure die binnen Connexio wordt toegepast, wordt beheerst.

De klantenadviseurs geven via telefoon, per brief, per e-mail, per chat of per Messenger enkel inlichtingen door aan de klant (of aan een door hem gemachtigde persoon) die op het toegangspunt erkend is en enkel gedurende de periode van bewoning van deze klant. Er zal hem gevraagd worden zijn meternummer voor controle mede te delen. Als een klant aan de DNB vraagt welke leverancier aan het toegangspunt gekoppeld is, zal die informatie hem per brief naar het installatieadres worden gestuurd.

Als de aanvraag dus uitgaat van een commerciële leverancier, dan wordt hij automatisch naar het CMS-portaal verwezen, afhankelijk van de toegangen waarover hij beschikt.

Maar als het om een klant gaat, dan kan hij zijn EAN slechts krijgen nadat zijn meternummer is gecontroleerd. De informatie wordt dan niet mondeling maar per sms verstuurd naar het mobiele telefoonnummer dat de klant heeft moeten meedelen. Als de klant zijn verzoek schriftelijk indient of als hij geen mobiel telefoonnummer heeft, wordt de informatie per post op naam verstuurd. Als het verzoek meer dan twee EAN's betreft, wordt het verzoek geregistreerd en verwerkt per e-mail of per post.

Van deze gesprekken en berichten blijft een spoor bewaard in de Koepel.

Connexio verstrekt ook klanteninformatie aan de OCMW's. Het OCMW beschikt over een specifiek contactnummer om informatie op te vragen over zijn inwoners (toestand van een dossier, actieve leverancier voor een leveringspunt, verbruikshistoriek, enz.). Het OCMW beschikt over een permanent mandaat voor het opvragen van informatie over zijn inwoners. Aan de OCMW's wordt gevraagd dit contactnummer nooit openbaar te maken.

- *Mercure-systeem*

De IT-infrastructuur is beveiligd en toegang tot de applicatie is geïndividualiseerd en in de “wijzigings-“modus voorbehouden voor het personeel van Connexio, maar enkel via een met een wachtwoord beveiligde webinterface (*Koepel*).

Voor het overige verwijzen wij naar de verslagen die voor ORES Assets en ORES cv werden opgesteld.

De procedure die binnen Connexio wordt toegepast, wordt beheerst.

De klantenadviseurs geven via telefoon, per brief of per e-mail enkel inlichtingen door aan de klant (of aan een door hem gemachtigde persoon) die aan de hand van zijn EAN-code herkend wordt en enkel gedurende de periode van bewoning van deze klant. Er zal hem gevraagd worden zijn meternummer voor controle mede te delen.

Als de klant opbelt om zijn verbruikshistoriek te kennen, zal hem volgens de geldende procedure het volgende worden meegedeeld:

- als het om een meteropname op afstand gaat (buiten de digitale meter), moet men de klant vragen zijn aanvraag via de website van ORES in te dienen. Hij ontvangt dan een historiek over maximaal de laatste drie jaren;
- als het om een jaarlijkse of maandelijks meteropname gaat, worden de klantenadviseurs er eerst aan herinnerd dat verbruiksgegevens privé-informatie zijn. Als een eigenaar het verbruik van zijn huurders wenst te kennen, moet hij dat rechtstreeks aan zijn huurders vragen;
- als het om een digitale meter gaat, krijgt de klant toegang tot zijn verbruikshistorieken via het portaal dat hem ter beschikking is gesteld. De toegangen worden dus eveneens strikt opgevolgd op veiligheidsgebied.

- *Registratie*

Overeenkomstig de bepalingen van de wet op de elektronische communicatie, wordt de communicatie tussen de klantenadviseurs van Connexio en hun gesprekspartners opgenomen.

Sinds 25 mei 2023 verzamelt en bewaart Connexio op zijn nieuw contactcenterplatform de elektronische communicatie en de zo uitgewisselde gegevens (oproepen, e-mails, chatverkeer, enz.), afkomstig van de klantenadviseurs van Connexio.

Standaard worden deze registraties bewaard gedurende een maand vanaf de datum van de communicatie. Maar bij registraties die krachtens specifieke wettelijke verplichtingen gebeuren (bijv. gasgeurmeldingen), wordt de bewaartermijn aangepast om aan de wettelijke vereisten te voldoen.

Bij Connexio wordt momenteel een speech to text toepassing op basis van artificiële intelligentie getest (transcriptie van oproepen naar tekst en tekstanalyse). Er wordt ook een privacy-impactanalyse uitgevoerd om te verzekeren dat dit proces in overeenstemming is met de GDPR en met de toekomstige verplichtingen voortvloeiend uit de Artificial Intelligence Act.

Hoofdstuk V – Beveiligingsmaatregelen betreffende de toegang van onderaannemers tot vertrouwelijke gegevens

Contractuele maatregelen

Wanneer er transacties of contracten met partners worden gesloten, worden daarin systematisch “AVG”-clausules ingevoegd. Deze bepalen alle in artikel 28 van de AVG voorziene elementen: duur, toepassingsgebied, finaliteit, verwerkingsinstructies, voorafgaande toestemming wanneer er een beroep wordt gedaan op een onderaannemer, terbeschikkingstelling van alle documentatie waaruit de conformiteit blijft, onmiddellijke kennisgeving van elke gegevensschending, enz.

Van zodra er gegevens buiten de Europese Unie worden gedeeld, worden gelijkwaardige maatregelen voor gegevensbescherming genomen en worden bij voorkeur de contractuele typebedingen toegepast.

Er worden eveneens ruimere vertrouwelijkheidsbepalingen in de contracten voorzien.

Specifieke maatregelen

Connexio gebruikt een contactcenterplatform (Genesys Cloud), dat ter beschikking wordt gesteld door partner NTT.

Er werden met de nieuwe onderaannemer ad hoc contractuele maatregelen ingevoerd om de bescherming van de persoonsgegevens van de betrokken personen te verzekeren (in de vorm van een gegevensverwerkingsovereenkomst als aanvulling op de contractdocumenten). In november 2023 werd een DPIA uitgevoerd. Er werd een beveiligingsrisicoanalyse uitgevoerd volgens de EBIOS-methodologie. Bovendien werd er in september 2023 een penetratietest uitgevoerd en de zwakke punten zijn aangepakt.

IT-diensten

Connexio heeft alle basis-IT-diensten, zoals de levering, installatie en support van de werkstations, het printen, de internettoegang, het *Active Directory*-beheer, de netwerktoegang, enz. toevertrouwd aan het IT-departement van ORES cv.

Hoofdstuk VI – Traceerbaarheid als vector van vertrouwelijkheid

Connexio delegeert het beheer van zijn IT-dienst aan ORES cv.

Meer bijzonderheden over het beheer van de traceerbaarheid van de toegangen door ORES cv zijn terug te vinden in het vertrouwelijkheidsverslag van ORES cv.

Hoofstuk VII – Het delen van IT-systemen en -infrastructuren met andere bedrijven

De IT-systemen en -infrastructuren van Connexio worden beheerd door ORES cv krachtens het hierboven vermelde contract inzake ondersteuningsdiensten tussen ORES cv en Connexio. In dat verband is het informatieveiligheidsbeheer het beheer van ORES, dat de ISO27001-norm volgt.

Over het algemeen moet worden opgemerkt dat ORES Assets een essentiële entiteit is in de zin van de NIS2-regelgeving⁶. ORES heeft bijgevolg een document opgesteld dat de systemen beschrijft die de essentiële diensten bestemd voor de FOD Economie en het Centrum voor Cybersecurity België (CCB) ondersteunen. ORES zit ook in de eindfase voor het verkrijgen van het ISO 27001-certificaat. Het certificatiebureau heeft in januari 2025 een positief advies uitgebracht, waardoor ORES naar verwachting haar certificering tegen eind maart 2025 zal behalen.

Bijgevolg is de scheiding van de aldus gedeelde gegevens gebaseerd op de volgende principes:

- het “minste voorrecht” (“*least privilege*”): aan een gebruiker moeten standaard enkel de toegangsrechten worden toegekend die strikt noodzakelijk zijn voor de uitvoering van zijn taak;
- de “scheiding van de taken” (“*segregation of duties*”): de volledige controle op/toegang tot het geheel van een kritisch/gevoelig proces mag niet in handen van één enkele persoon zijn;
- de “noodzaak tot kennisname” (“*need to know*”): een gebruiker mag bepaalde gegevens enkel raadplegen wanneer zijn functie dit werkelijk vereist. Met andere woorden, het feit dat men over een potentiële toegang beschikt om informatie te behandelen volstaat niet om de toegang tot die informatie te rechtvaardigen.

De specifieke maatregelen betreffende NTT werden hierboven reeds behandeld.

⁶ NIS2-regelgeving: Richtlijn (EU) 2022/2555 van het Europees Parlement en de Raad van 14 december 2022 betreffende maatregelen voor een hoog gezamenlijk niveau van cyberbeveiliging in de Unie, tot wijziging van Verordening (EU) nr. 910/2014 en Richtlijn (EU) 2018/1972 en tot intrekking van Richtlijn (EU) 2016/1148 (NIS 2-richtlijn), evenals de Belgische wet van 26 april 2024 tot vaststelling van een kader voor de cyberbeveiliging van netwerk- en informatiesystemen van algemeen belang voor de openbare veiligheid.