# VERSLAG Nr. 22
# VAN DE
# VERTROUWELIJKHEIDSCOÖRDINATOR
# VAN ORES ASSETS

**Artikel 17, 2de lid, van het besluit van 21 maart 2002 betreffende de netbeheerders en artikel 7, 2de lid, van het besluit van 16 oktober 2003 betreffende de gasnetbeheerders**

# INHOUD


Hoofdstuk I – Inleiding ..... 3

Hoofdstuk II – Verplichtingen van het personeel en van de leden van de bestuursorganen inzake vertrouwelijkheid van de gegevens ..... 6

1. Verplichtingen van het personeel inzake de vertrouwelijkheid van de gegevens ..... 6

2. Verplichtingen van de leden van de bestuursorganen inzake vertrouwelijkheid van de gegevens ..... 7

Hoofdstuk III – Beveiligingsmaatregelen betreffende de toegang van het personeel tot commerciële en persoonsgegevens ..... 9

Hoofdstuk IV – Beveiligingsmaatregelen in verband met de toegang van leveranciers en klanten tot vertrouwelijke gegevens ..... 11

1. Betrokken diensten van ORES cv ..... 11

2. Specifieke maatregelen ..... 12

Hoofdstuk V – Beveiligingsmaatregelen betreffende de toegang van onderaannemers tot vertrouwelijke gegevens ..... 17

Hoofdstuk VI – Traceerbaarheid als vector van vertrouwelijkheid ..... 18

Hoofdstuk VII – Het delen van IT-systemen en -infrastructuur met andere bedrijven ..... 20

Hoofdstuk VIII – Invoering van digitale meters ..... 22

# 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 Assets[1] 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 Comnexio. 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 de activiteiten die tot de openbaredienstverplichtingen van ORES Assets behoren, aan ORES cv werden toevertrouwd.
Wat de *contact center*-activiteiten betreft, deze werden vanaf 1 juni 2019 toevertrouwd aan Comnexio.
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.
De specifieke situatie die te maken heeft met de maatschappelijke structuur en de operationele realiteit van ORES Assets en ORES cv, waarbij ORES Assets de DNB is en ORES cv[2] het exploiterend bedrijf, heeft tot gevolg dat de inhoud van hun verslag praktisch identiek is.

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.*
*De netbeheerder wijst onder zijn personeelsleden een persoon aan die specifiek verantwoordelijk is voor de coördinatie van de ter uitvoering van dit artikel getroffen maatregelen. De CWAPE kan de aldus aangewezen persoon te allen tijde om een verslag over de toepassing van deze maatregelen verzoeken".*

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

Aangezien artikel 16, § 1, van het decreet van 12 april 2001 betreffende de organisatie van de gewestelijke elektriciteitsmarkt (hierna het "elektriciteitsdecreet) en artikel 17, § 1, van het decreet van 19 december 2002 betreffende de organisatie van de gewestelijke gasmarkt (hierna het "gasdecreet") de DNB toelaten de activiteiten die tot zijn openbaredienstverplichtingen behoren, toe te vertrouwen aan een filiaal dat over eigen personeel beschikt, werd een personeelslid van ORES cv, dochteronderneming van ORES Assets, door het Directiecomité van ORES cv op 1 februari 2019 aangesteld tot vertrouwelijkheidscoördinator, namelijk Audrey Réveillon.

[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 3 van de statuten van ORES cv.

Sedert de invoering van de inventaris van goede praktijken inzake vertrouwelijkheid, die in 2019 door de CWaPE in het kader van haar controle van de governanceregels binnen de DNB's en hun dochterondernemingen werd opgesteld, tonen die DNB's en hun dochterondernemingen in hun vertrouwelijkheidsverslag aan dat al deze goede praktijken daadwerkelijk werden toegepast.

Dit verslag bestrijkt de activiteiten van ORES Assets op het hele grondgebied dat bediend wordt door ORES Assets, zowel voor elektriciteit als aardgas.
Het heeft tot doel de maatregelen uiteen te zetten die in de loop van het jaar 2023 genomen of voortgezet werden om nog beter de doelstelling te verwezenlijken die erin bestaat de vertrouwelijkheid te bewaren van de informatie waarvan ORES Assets op de hoogte is in het kader van de uitvoering van de taken die aan haar werden toevertrouwd.

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

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

Omdat ORES Assets de activiteiten die overeenkomstig artikel 16, § 1 van het elektriciteitsdecreet en artikel 17, § 1 van het gasdecreet tot haar openbaredienstverplichtingen behoren, heeft toevertrouwd aan ORES cv, is het geheel van het personeel dat voor rekening van ORES Assets taken uitvoert, gebonden door een arbeidscontract met ORES cv. De bepalingen die volgen zijn dan ook de bepalingen die bij ORES cv van toepassing zijn.
De arbeidscontracten van de personeelsleden bevatten clausules die hun een verplichting tot vertrouwelijkheid opleggen.
Zo verbinden de personeelsleden er zich in hun arbeidscontract 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 ORES cv, om de gegevens die op het ogenblik van de beëindiging van het arbeidscontract nog in hun bezit zijn aan ORES cv terug te geven en dit onmiddellijk na de beëindiging van het arbeidscontract.
Bovendien werd de Ethische Gedragscode herzien die voor alle personeelsleden geldt. Deze ethische en deontologische gedragscode omvat de verplichtingen van het personeel inzake gegevensbescherming en de verplichting om deze na te leven. Hij geldt ook voor externe partners (consultants, onderaannemers, uitzendkrachten enz.). Hij maakt deel uit van de contractuele documentatie die medewerkers ontvangen bij hun indiensttreding.
Ook met de externe medewerkers en uitzendkrachten worden aangepaste vertrouwelijkheidscontracten ondertekend.
Al deze clausules werden herzien en de inhoud ervan voldoet aan de ISO 27001-normen.

Overeenkomstig de Algemene Verordening Gegevensbescherming (hierna “AVG” genoemd) heeft ORES cv een reeks processen ingevoerd en beschrijft het de rol en verantwoordelijkheid van alle betrokkenen. Bovendien blijft ORES cv permanent inspanningen leveren om de principes van de Verordening beter toe te passen en het personeel bewust te maken van het belang ervan.
In 2019 werd er een algemene beleidsverklaring uitgeschreven en intern gepubliceerd. Ze geeft het personeel van ORES cv de richtsnoeren die het bedrijf zichzelf inzake de AVG oplegt. Deze verklaring wordt regelmatig door het Directiecomité van ORES cv herzien en ze werd voor het laatst bijgewerkt in 2024.
Binnen elke Directie werden medewerkers opgeleid om de afgevaardigde voor de gegevensbescherming (afgekort “DPO”, wat staat voor “Data Protection Officer”) bij te staan op het terrein.

Concreet houdt de bewustmaking van het personeel het volgende in:

- een ethische en deontologische gedragscode met de verplichtingen inzake bescherming van de gegevens die aan alle personeelsleden van ORES cv en

aan de externe partners (consultants, onderaannemers, uitzendkrachten, enz.) ter beschikking worden gesteld;
- de verspreiding van basisinformatie over de verplichtingen inzake vertrouwelijkheid, via het lezen en ondertekenen van een vertrouwelijkheidsclausule;
- het ondertekenen van een Verbintenis tot vertrouwelijkheid en niet-openbaarmaking op het ogenblik van de overhandiging van het draagbaar IT-materiaal door de Directie Informatica;
- het opleggen van een aantal verplichtingen inzake vertrouwelijkheid via het arbeidsreglement;
- de verbintenis die de nieuwe werknemers van ORES aangaan om het Charter van het informatiesysteem na te leven, waarin wordt bepaald binnen welk kader de werknemers de telecommunicatiemiddelen mogen gebruiken;
- de terbeschikkingstelling van een *Welcome Pack* met een hoofdstuk over cyberveiligheid aan elke medewerker bij zijn aankomst;
- de terbeschikkingstelling van een reeks video's waarin acteurs in het bedrijf worden geconfronteerd met veiligheidssituaties. Aan het einde legt de video uit wat het juiste gedrag is in de getoonde situatie. Om de twee maanden worden twee afleveringen uitgezonden;
- het aanmaken van een SharePoint-website over informatieveiligheid, waarop documenten over veiligheid beschikbaar zijn die voldoen aan de ISO 27001-norm (policy's, normen, procedures, *best practices)*;
- een verplichte *e-learning* over « AVG » en diverse *e-learning*-modules over informatieveiligheid staan ter beschikking van alle medewerkers. Deze cursussen zijn verplicht voor alle ORES-medewerkers en voor alle nieuwkomers. Deze boodschappen worden permanent herhaald via bewustmakingscampagnes over diverse veiligheidsonderwerpen, afgestemd op het kennisniveau dat bij de ORES-medewerkers werd gemeten en aangepast aan de voornaamste bedreigingen voor onze gegevens. Er worden campagnes opgezet om het ORES-personeel bewust te maken voor de gevaren van phishing;
- het openen van een aan de AVG gewijde samenwerkingsruimte die ter beschikking staat van alle medewerkers, voor het vergemakkelijken van de toegang tot relevante informatie en tot de procedures die gelden wanneer er persoonsgegevens bij betrokken zijn.

Ter herinnering, de bovenstaande informatie maakte reeds het voorwerp uit van een verslag van de CWaPE in het kader van haar controle op de implementering van de governanceregels.
Op 6 december 2019 bevestigde de CWaPE aan ORES dat er voor ORES cv geen enkele aanbeveling werd geformuleerd betreffende de verplichtingen van het personeel inzake de vertrouwelijkheid van de gegevens.

## 2. <u>Verplichtingen van de leden van de bestuursorganen inzake vertrouwelijkheid van de gegevens</u>

Naast de algemene plicht tot terughoudendheid die elke bestuurder van een vennootschap heeft, worden de bestuurders van ORES Assets (DNB) en van de filialen ORES cv en Comnexio bewust gemaakt van hun vertrouwelijkheidsplicht via

de governanceregels die binnen de onderneming zijn aangenomen en worden toegepast (in casu het Huishoudelijk Reglement voor ORES Assets en de Bestuurscharters van ORES cv en Comnexio, die trouwens toegankelijk zijn via de website).

Bovendien werd de ethische en deontologische gedragscode meegedeeld aan de leden van de Raad van Bestuur van ORES Assets en ORES cv.

De bestuurders van ORES Assets, ORES cv en Comnexio 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, loyauteit, 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.

Bovendien hebben de bestuurders van ORES Assets en ORES cv een MAR-gedragscode[3] aangenomen en hebben zij individueel een verklaring ondertekend in hun hoedanigheid van geïnitieerde persoon.

[3] Europese verordening “Marktmisbruik” die er naar streeft de integriteit van de markten en de bescherming van de investeerders te verbeteren.

# Hoofdstuk III – Beveiligingsmaatregelen betreffende de toegang van het personeel tot commerciële en persoonsgegevens

Wanneer ORES cv voor rekening van ORES Assets persoonsgegevens verwerkt in verband met de klanten van ORES, wordt er alles aan gedaan, op het vlak van personeel, verwerkers, subverwerkers of IT-beveiliging, om de vertrouwelijkheid van de ter beschikking gestelde commerciële en persoonsgegevens 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.

ORES voerde reeds in de ontwerpfase beschermingsprocedures ("*Privacy by design"* en *"Security by design*") 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 voert ORES cv voor elke geplande nieuwe verwerking en elke wijziging in de processen AVG-analyses uit, die "voorafgaande vragenlijst" worden genoemd. Bovendien worden er DPIA (*Data Protection Impact Assessments*) uitgevoerd voor elke nieuwe verwerking die zou kunnen "*resulteren in een hoog risico voor de rechten en vrijheden van natuurlijke personen*". Het aspect "toegang" tot de persoonsgegevens wordt in elke oefening geëvalueerd. Verder worden er veiligheidsrisicoanalyses uitgevoerd voor de nieuwe bedrijfsprocessen. De bestaande bedrijfsprocessen worden inzake analyse van de informatiebeveiligingsrisico's om de drie jaar herzien.

De volgende technische en organisatorische maatregelen worden toegepast:

- het beheer van de machtigingen voor onze IT-applicaties is gecentraliseerd en geautomatiseerd met behulp van de tool "*SAP Identity Management"* (bijvoorbeeld: Sap: lopex, procli; *Active directory*: Mercure, rijksregister, Oracle: netgis);
- de methodologie die voor de toegangsdistributie wordt toegepast is de "*role-based* toegangscontrole", waaraan ORES cv de twee volgende principes toevoegt: "*least privilege"* en "*need to know"*;
- bevoorrechte toegangen maken het voorwerp van een specifiek goedkeuringsproces uit;
- de levenscyclus van de IT-identiteiten wordt automatisch afgestemd op het personeelsbeheer;
- toegangsrechten per beroepscategorie worden gevalideerd door HR en door de managers van elke dienst;
- bestekken betreffende nieuwe applicaties vermelden specifiek de behoefte aan integratie in ons systeem voor het beheer van IT-identiteiten en -toegangen;
- toegang tot het rijksregister wordt enkel aan het intern personeel verleend, na het ondertekenen van een document waarin wordt uitgelegd waarom de toegang tot het register nodig was. Dat document wordt gevalideerd door de hiërarchische meerdere en naar de HR Directie gestuurd, om in het persoonlijk dossier van de

werknemer te worden gevoegd. De lijst van de toegangen wordt om de zes maanden door de managers nagezien. Er wordt een register van de raadplegingen van het rijksregister bijgehouden.

- er worden beveiligde wachtwoordkluizen gebruikt.

In april 2024 werd de Dienst Informatie Veiligheid Office bovendien gereorganiseerd om alle veiligheidscompetenties onder de CISCO van ORES te hergroeperen.
Er werden drie teams samengesteld:

- het Team *Governance, Risk and Compliance,* dat verantwoordelijk is voor het aanpassen van het beleid en de normen inzake informatiebeveiliging volgens de ISO 27001-norm;
- het Team Cyberdefensie, dat toezicht houdt op de IT-activiteiten door de logbestanden van de verschillende onderdelen (*firewalls*, WAF, antivirus, enz.) te analyseren.
  Bovendien heeft ORES een contract voor beveiligingstoezicht gesloten, 24 u per dag en 7 dagen per week;
- het Team *Identity and Access Management,* dat de volledige levenscyclus van een gebruiker van het informatiesysteem van ORES beheert (creëren van de gebruiker, toekennen van toegangsrechten en verwijderen van de gebruiker).

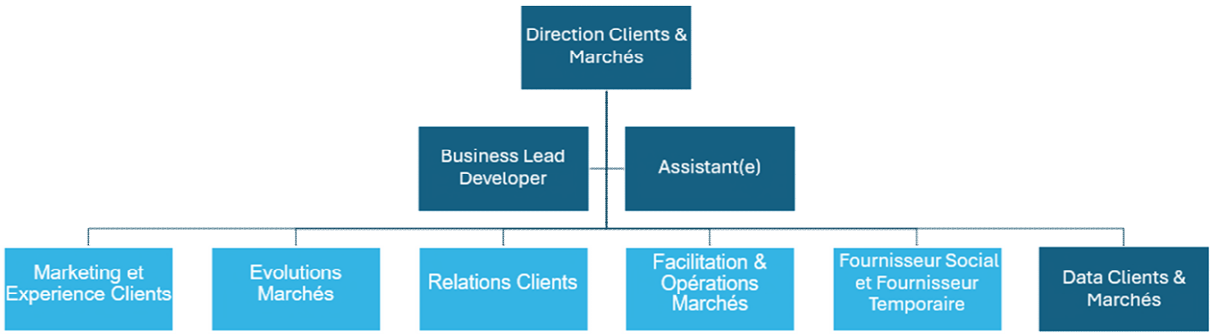
Over het algemeen moet worden benadrukt dat ORES Assets, in het kader van de wet van 7 april 2019 tot vaststelling van een kader voor de beveiliging van netwerk- en informatiesystemen van algemeen belang voor de openbare veiligheid (hieronder “NIS” genoemd), op 1 november 2022 werd aangesteld als aanbieder van essentiële diensten. ORES Assets is een essentiële entiteit in de zin van NIS 2-reglementering[4].
ORES heeft daarom een document opgesteld dat de systemen beschrijft die de essentiële diensten voor de FOD Economie en het Centrum voor Cybersecurity België (CCB) ondersteunen.
In maart 2025 verkreeg ORES het ISO 27001-certificaat.

[4] NIS 2-reglementering: 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) en 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.

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

De Directie Klanten & Markten omvat "*Define*"-teams en "*Run*"-teams.

Het volgende schema bevat de verschillende Diensten:




## 1. Betrokken diensten van ORES cv

De Dienst *Facilitering en Marktoperaties* maakt deel uit van de Directie Klanten & Markten. Deze Directie beheert alle processen die verband houden met de geliberaliseerde markt (*Assets, structure, measure, settle* en *rectification*), alle gegevensprocessen en flexibiliteitsprocessen. Ook de openbaredienstverplichtingen van sociale aard worden binnen deze Directie beheerd.
Het team *Correctie Marktanomalieën* binnen de Dienst *Facilitering en Marktoperaties* beheert het federaal toegangsregister (CMS Atrias, *Central Market System*) voor de ORES-portefeuille, alsook de operationele contacten met de energieleveranciers.

Het CMS is het federaal IT-platform dat het uitwisselen en verwerken van gegevens tussen alle spelers op de Belgische energiemarkt vergemakkelijkt op basis van MIG's (*Message Implementation Guide*).

Elk toegangspunt tot het net (*headpoint*) staat erin vermeld met zijn EAN-code. Achter deze code staan de klantgegevens, de gegevens van zijn leverancier en andere nuttige informatie. Achter het *headpoint* bevinden zich ook de mogelijke diensten en configuraties, afhankelijk van het type installatie (bijvoorbeeld voor een prosument met een digitale meter zijn de compensatiedienst en de configuraties dag/nacht, het enkelvoudig tarief of het aanmoedigingstarief zichtbaar).
Het CMS, dat op het niveau van ORES via een grote *orchestrator* (BPMS, *Business Process Management System*) is gekoppeld aan MDM/Mercure (de database met het verbruik van elk leveringspunt), maar ook met de SAP ISU back-end (met alle

technische informatie over elk leveringspunt), geeft een compleet beeld van de markt.

Voortaan worden de meterstanden van de elektromechanische meters opgenomen in de Dienst *Essentieel Klanten*.

Voor de digitale meters is het team *Toezicht op Communicatieketens* binnen de Dienst *Facilitering en Marktoperaties* verantwoordelijk voor controle van de goede werking van de communicatieketens en het doorsturen van de meterstanden. Er werd een platform voor automatische opname van de meterstanden ingevoerd: COMET, een applicatie voor het verzamelen van gegevens van digitale meters. Een ander platform, Prism, beheert de teleoperaties naar het HES (*Head-End System*). Het is enerzijds verbonden met MDM/Mercure en anderzijds met de communicatieketen van de meters. Het MARCO-platform beheert de communicatie met het voorafbetalingsplatform (federaal platform dat door Atrias wordt beheerd).

De teams *Validatie B2C en B2B* binnen de Dienst *Facilitering en Marktoperaties* controleren of de opgenomen meterstanden coherent zijn met de verbruiksstatistieken (ook in het verleden) en met de klimatologische criteria.

Het team *Toezicht op Transversale Processen* behandelt de blokkeringen die op transversaal niveau ontstaan. Andere gevallen worden door andere teams behandeld, eveneens binnen de Dienst *Facilitering en Marktoperaties*: team *Rectificaties* voor de Atrias-klachten ingediend bij de Waalse dienst SRME, het team *Marktinteractie en Relatiebeheer* voor de vragen van leveranciers en klanten.
Het team *Beheer Voorafbetalingen* verwerkt de interactie met de klanten en het voorafbetalingsplatform.

Het team *Procesregularisatie*, dat deel uitmaakt van de Dienst *Facilitering en Marktoperaties*, heeft ook toegang tot de gegevens in het CMS voor het uitvoeren van de processen *Drop*, *End-Of-Contract*, *Initiate Leaving Customer* (ILC) en Installatie voorafbetalingsmeter die door de energieleveranciers worden geïnitieerd. De medewerkers versturen brieven, nemen contact op met klanten (bijv. een onderzoek in verband met een ILC-dossier) en/of de commerciële leveranciers (bijv. een beveiligde annulering).

Tot slot heeft ons *contactcenter* Comnexio, een dochteronderneming van ORES Assets, eveneens toegang tot de informatie van het CMS of van Mercure om de eerstelijnsoproepen van klanten te beantwoorden.

Het beheer van de toegang tot deze applicaties door deze verschillende medewerkers en de manier waarop de informatie aan de klanten en/of aan de commerciële leveranciers wordt meegedeeld, worden in het volgend punt uitgelegd.

## 2. Specifieke maatregelen

- **Toegangsregister (CMS)**

  De computerinfrastructuur is beveiligd en de toegang tot de applicatie is geïndividualiseerd en voorbehouden – onder andere via een tool voor *Business*

*Object* (BO) rapportering – aan de leden van de teams binnen de Dienst *Facilitering en Marktoperaties* (lezen en schrijven).
Elke nieuwe aanvraag tot toegang wordt voor goedkeuring overgemaakt aan de *owner Structuring*-applicatie. De toegangsbeheerder wordt - via de HR-functiefiches, die naast de beschrijving van de taken ook de lijst van de toepassingen en transacties bevat waartoe de betrokkene uit hoofde van zijn functie gemachtigd is – ingelicht over de specifieke toegangsbevoegdheden voor iedereen.

De leveranciers hebben eveneens toegang tot de applicatie (voor raadpleging maar eveneens om marktprocessen op te starten/te annuleren), maar enkel via het CMS-portaal. Een leverancier kan enkel toegang krijgen tot de gegevens van de klanten waarvoor hij een in het toegangsregister geregistreerd contract heeft. De klantengegevens die de leverancier kan raadplegen zijn gegevens die door de leveranciers zelf werden verstrekt, via marktboodschappen naar de DNB.
Hij kan eveneens beschikken over de technische gegevens in verband met de toegangspunten waarvoor hij als leverancier erkend is. Deze gegevens zullen door de DNB enkel voor de duur van zijn contract worden meegedeeld.
Hij heeft dus geen toegang tot klantengegevens die bij een andere leverancier actief zijn. De beveiligings- en toegangsregels van de IT-applicatie beheren deze beperkte terbeschikkingstelling van de aan het toegangspunt verbonden informatie. Naast deze beveiliging via de IT-applicatie, worden de teams *Correctie Marktanomalieën, Procesregularisatie* en *Marktinteractie en Relatiebeheer* opgeleid om enkel aan de op dat toegangspunt erkende leverancier inlichtingen per mail of telefonisch mede te delen.

De teams *Correctie Marktanomalieën, Procesregularisatie, Marktinteractie en Relatiebeheer* en *Validatie en Rectificaties* geven via telefoon, per brief of per e-mail enkel inlichtingen door aan de klant (of aan een door hem gemachtigde persoon) die bekend is op het toegangspunt en enkel gedurende de periode van bewoning van deze klant. Er zal hem gevraagd worden zijn meternummer voor controle mede te delen. De eindklant heeft geen toegang tot de IT-applicatie zelf. 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.

De procedure die door ons *contactcenter* Comnexio wordt toegepast, wordt eveneens gemanaged. Als de aanvraag uitgaat van een commerciële leverancier, zal hij automatisch naar het portaal van het CMS verwezen worden, gezien de toegangen waarover hij beschikt.
Als het om een klant gaat, zal zijn EAN enkel aan hem worden meegedeeld nadat zijn meternummer is gecontroleerd. De informatie zal hem vervolgens niet mondeling worden meegedeeld, maar via een sms naar het gsm-nummer dat de klant ons vooraf moet hebben meegedeeld. Als de klant zijn aanvraag schriftelijk stuurt of als hij niet over een gsm-nummer beschikt, dan zal de informatie hem in een brief op naam worden gestuurd. Als het gaat om een aanvraag van meer dan twee EAN-codes, dan zal zijn aanvraag in het systeem worden ingegeven en via e-mail/brief worden behandeld.
Deze oproepen en gegevensuitwisselingen blijven bewaard in het systeem.

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

Er wordt een spoor bewaard van alle transacties van de markt en van de verzending van gegevens.

Tot slot moet worden opgemerkt dat als een leverancier een *drop* marktscenario of de *installatie van een meter met voorafbetalingsfunctie* lanceert – wat betekent dat de klant betalingsmoeilijkheden heeft -, een andere leverancier die een *switch* zou lanceren (verandering van leverancier) voor dit toegangspunt, niet automatisch als feedback het bericht ontvangt dat er een *drop* of een *installatie van een meter met voorafbetalingsfunctie* bezig is. De nieuwe leverancier is hierdoor niet op de hoogte van de betalingsmoeilijkheden van de klant. Er dient te worden opgemerkt dat een leverancier ingevolge de nieuwe wanbetalingsprocedure in het kader van het zogeheten "Vrederechterdecreet", steeds een Switch-aanvraag kan opstarten voor een EAN waarvoor een aanvraag tot installatie van een meter met voorafbetalingsfunctie werd gedaan, zonder dat hem een afwijzing wordt toegestuurd.

- **Mercure-systeem**

De IT-infrastructuur is beveiligd en toegang tot de applicatie is geïndividualiseerd en in de "wijzigings-"modus voorbehouden voor leden van de Dienst *Facilitering en Marktoperaties*.
Elke nieuwe aanvraag tot toegang (in modus "lezen" of "wijziging") is onderworpen aan de goedkeuring van de *application Owner Measure* die – per beroep en HR-functie – beschikt over de toegangsrechten tot de applicatie waarvoor deze *application owner* verantwoordelijk is.

Het *contactcenter* Comnexio heeft eveneens toegang tot de applicatie, maar uitsluitend via een met een wachtwoord beveiligde webinterface. De toegangen tot de webinterface worden eveneens door de *application owner* goedgekeurd.

De beveiligings- en toegangsregels van de IT-applicatie beheren deze beperkte terbeschikkingstelling van informatie in verband met het verbruik van het toegangspunt.

Een klant die zijn verbruikshistoriek wenst te kennen, kan deze op verschillende manieren raadplegen:

- via de website van ORES, met zijn EAN-code en meternummer;
- via het MyORES-portaal: de toegangen worden op veiligheidsgebied strikt opgevolgd;
- via een aanvraag bij een van de operationele diensten.

De verbruikshistoriek kan ook naar een andere persoon of een leverancier gestuurd worden, maar deze laatsten moeten over een schriftelijke en

ondertekende volmacht van de klant van het betrokken toegangspunt beschikken.
Er wordt een spoor bewaard van alle transacties van de markt en van de verzending van gegevens.

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

- als het om een meteropname op afstand gaat (behalve wat de digitale meter betreft), moet men de klant vragen zijn aanvraag via onze website in te dienen. Hij ontvangt dan een historiek over maximaal de laatste drie jaren;
- als het om een jaarlijkse of maandelijkse meteropname gaat, worden de klantenadviseurs er eerst aan herinnerd dat de 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.

De klant wordt vervolgens verzocht zijn aanvraag te formuleren via onze website, maar als hij dat niet wenst te doen, wordt de aanvraag behandeld door de adviseur en wordt er naar het verbruiksadres een brief gestuurd waarin de historiek van maximaal de laatste drie jaren vermeld wordt.
Aangezien aan de klanten al vanaf het begin van de oproep wordt meegedeeld dat het gesprek wordt opgenomen, kunnen de teams die voor de processen instaan (*Process Owner*) de opgenomen telefoongespreken beluisteren om te controleren of de geldende regels correct worden toegepast.

De meteropnemers kunnen de meterstanden die ze ter plaatse noteren in het systeem invoeren via een mobiele app die ook beveiligd is met persoonlijke inloggegevens, op basis van een gebruikersnaam en een wachtwoord.

Tot slot wordt in het kader van de meteropnames aan de klanten die dat wensen toegang verleend tot een gedigitaliseerde ruimte om er hun meteropnames mede te delen. Na beveiligde inschrijving kan de klant zijn briefwisseling over de meteropnames in digitaal formaat ontvangen. Dit proces is onderworpen aan alle AVG-regels en in geval van verandering van klant wordt deze functie automatisch stopgezet.

- **BPMS**

  Alleen gemachtigde IT-teams hebben toegang tot de BPMS-tool in “wijzigings”-modus. Maar ook de teams van de Dienst *Facilitering & Marktoperaties* kunnen in “alleen lezen”-modus toegang krijgen tot de tool om analyses uit te voeren. Toegang tot deze applicatie wordt verleend door de *Owner-applicatie* op basis van de IT-beroepenfiches. Geen enkel ander team heeft toegang tot deze applicatie nodig.

- **Prism, HES, COMET en MARCO**

De HES is alleen toegankelijk voor de externe dienstverlener die hem ter beschikking stelt. Wat Prism betreft: dit is in “alleen lezen”-modus toegankelijk voor het team *Toezicht op Communicatieketens*, maar ook – eveneens op basis van een beroepenfiche – voor het team *Beheer Voorafbetalingen* (GDP), dat het opnieuw opladen van de digitale meters in voorafbetalingsmodus beheert (via de PPP-tool die gehost wordt binnen Atrias).
Ingrepen op afstand worden uitgevoerd via Prism, met behulp van het systeem SAP CS (bij ORES wordt deze tool LoPex genoemd). Alle toegangen tot de LoPex-applicatie worden gecontroleerd op basis van de HR-beroepenfiches.
COMET is toegankelijk voor de teams *B2C-validaties*.
MARCO is toegankelijk voor de teams *B2C-validaties* en voor de teams *Beheer Voorafbetalingen*.

- **ORES en artificiële intelligentie**

  ORES bestudeert momenteel hoe het artificiële intelligentie (AI) in zijn activiteiten kan integreren, onder andere om de energietransitie te begeleiden en bepaalde recurrente taken te optimaliseren.

  ORES is zich bewust van de uitdagingen die het gebruik van deze technologieën met zich meebrengt en waakt erover dat de implementatie omkaderd wordt door een strikte interne governance die voldoet aan de geldende regelgeving, met name de AVG en *de Artificial Intelligence Act*. Dit wettelijke kader garandeert een ethisch en veilig gebruik van AI, dat innovatie en de bescherming van de rechten van individuen met elkaar verzoent.

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

Technische en organisatorische maatregelen

Diverse aan de risico's aangepaste beveiligingsmaatregelen werden ingevoerd, met onder meer:

- gebruik van een unieke login voor de aannemers en beperking van de toegangsrechten tot de werven;
- gebruik van pseudoniemen in de gegevens die toegankelijk worden gemaakt voor IT-ontwikkelingsbedrijven die voor ORES werkzaam zijn;
- scheiding van de toegangen tot de productiegegevens en de testgegevens;
- beperking van de toegangen tot de productiegegevens;
- beperking van de toegangen tot de gegevens door externe leveranciers voor onderhoudsredenen;
- beheer van de administratie- en ondersteuningsaccounts van externe dienstverleners via een "kluis"-systeem (het product CyberArk wordt momenteel uitgerold);
- uitvoeren van audits en penetratietests;
- minimalisering van de verstrekte gegevens;
- invoeren van een ethische gedragscode die ook geldt voor externe medewerkers.

Contractuele maatregelen

Bij het sluiten van transacties of contracten met zijn partners, voegt ORES systematisch "AVG"-bedingen in, waarin alle in artikel 28 van de AVG voorziene elementen vermeld worden: duur, toepassingsgebied, finaliteit, verwerkingsinstructies, voorafgaande toestemming wanneer er een beroep wordt gedaan op een onderaannemer, terbeschikkingstelling van alle documentatie waaruit de conformiteit blijkt, onmiddellijke kennisgeving van elke gegevensinbreuk.
Wanneer de contractuele afspraken niet onder de regelgeving voor overheidsopdrachten vallen, wordt er een *data processing agreement* tussen de partijen gesloten.

Van zodra er gegevens buiten de Europese Unie worden gedeeld, worden evenwaardigde gegevensbeschermingsmaatregelen genomen en worden bij voorkeur contractuele typebedingen toegepast.

Er worden eveneens ruimere vertrouwelijkheidsbepalingen in de contracten voorzien.

# Hoofdstuk VI – Traceerbaarheid als vector van vertrouwelijkheid

ORES gebruikt de “SAP”-oplossingen en opteerde voor een meer diepgaande parametrering van de traceerbaarheid dan de door SAP aanbevolen standaard parametrering. Wat de traceerbaarheid betreft van de activiteiten van de gebruikers en van de technische accounts die gelinkt zijn aan de oplossingen van derden, bewaart ORES in de SAP-databank:

- een geaggregeerd overzicht van het dagelijks gebruik tijdens 31 dagen,
- een geaggregeerd overzicht van het wekelijks gebruik tijdens 20 weken,
- een geaggregeerd overzicht van het maandelijks gebruik tijdens 20 maanden.

We voegen hier nog aan toe dat SAP een spoor van de transacties die door een persoon werden opgestart bewaart, maar geen gegevens die dankzij deze transactie geraadpleegd konden worden. De context wordt niet bewaard. De aggregatie heeft betrekking op het ogenblik van de uitvoering van de transactie.

Wat de verzending van gegevens per e-mail betreft, bewaart het SAP-systeem van ORES een spoor van alle activiteiten in beveiligde omgevingen en waarvan de toegankelijkheid gemanaged wordt.

Diensten in verband met de WIFI/ LAN/ WAN-netinfrastructuur en de telefonie vallen onder de verantwoordelijkheid van ORES. De volgende elementen maken deel uit van de catalogus van ORES-netwerkdiensten:

- Toegangsnetwerk tot de eindgebruikers (25+ gebouwen),
- Schakelaars en routers,
- Wifi,
- DNS/ DHCP/ IPAM,
- Toegangscontrole tot het netwerk (801.1X),
- Monitoring en operationeel beheer.

Dit illustreert in welke mate ORES de toegangs- en activiteitencontroles op het IT-netwerk managet. Het OT-netwerk (*Operational Technology*) is eigendom van ORES, dat eveneens het beheer ervan verzekert. ORES managet ook het geheel van diensten en beheertools van zijn gebruikers-“devices” (werkstation, mobiliteitstools).

In 2024 heeft ORES een tool geïmplementeerd waarmee gebruikers van Microsoft-kantoorsoftware documenten kunnen markeren. Er gelden vier markeringsniveaus:

- C1 – OPENBARE informatie: de informatie is openbaar en mag aan iedereen worden doorgegeven, zowel binnen als buiten ORES.
- C2 – INTERNE informatie: al wie bij ORES werkt, zowel interne medewerkers als externe werkkrachten (met een contract) en eventueel zelfs bepaalde partners mogen over deze informatie beschikken.
- C3 – BEPERKTE informatie: slechts een beperkt aantal personen, bijvoorbeeld een team, een dienst of zelfs een Directie mag deze informatie kennen/ raadplegen;
- C4 – VERTROUWELIJKE informatie: alleen enkele met naam aangeduide personen mogen deze informatie kennen/ raadplegen.

En 2025 heeft ORES een tool (SIEM) in gebruik genomen om beveiligingslogs van de ORES-systemen te recupereren. ORES heeft een contract gesloten met een extern bedrijf (SOC) dat 24 u/24 en 7 dagen per week de beveiligingsactiviteiten van ORES bewaakt. Bij een inbraak in de systemen, wordt de 24 u/24 en 7 dagen/7 bewakingsdienst gewaarschuwd, die dan het incident verder afhandelt.

# Hoofdstuk VII – Het delen van IT-systemen en -infrastructuur met andere bedrijven

Om haar taak te kunnen vervullen, deelt ORES bepaalde IT-systemen en -infrastructuren met partners. Er wordt heel in het bijzonder aandacht besteed aan het toepassen van krachtige beveiligingsmaatregelen, die de scheiding, de vertrouwelijkheid en de integriteit van onze gegevens in deze gedeelde systemen en infrastructuren waarborgen.

Het informatiebeveiligingsbeheer van ORES is afgestemd op de ISO 27001-norm. De scheiding van de op deze manier gedeelde gegevens steunt 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 tot informatie beschikt, volstaat niet om de toegang tot die informatie te rechtvaardigen.

Voor al deze gevallen blijft het beheer van de toegangsrechten tot de “beroepen”-applicaties van ORES de uitsluitende verantwoordelijkheid van ORES.

Dit zijn de belangrijkste gevallen waarin IT-systemen en -infrastructuren worden gedeeld:

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

  Het IMDMS “*clearing”*-systeem wordt gedeeld met Fluvius. Met dit systeem kunnen de verrichtingen op de energiemarkt worden gecentraliseerd en georganiseerd.
  In het huidige systeem heeft Fluvius de mogelijkheid alle gegevens te zien om zijn rol van beheerder van het *Clearing House* (toewijzing, reconciliatie, *infeed*) te kunnen vervullen.
  Er vond een aanpassing van de toegangsrechten van de gebruikers van ORES plaats om het aantal acties op de gegevens van ORES te beperken. Wanneer iemand ORES verlaat, wordt zijn account automatisch geblokkeerd bij de aanpassing van wachtwoorden, die om de drie maanden plaatsvindt.
  Fluvius van zijn kant gaat regelmatig over tot het wissen van geblokkeerde accounts. Er dient te worden opgemerkt dat de rol van *Clearing House* sedert 29 november 2021 door Atrias verzekerd wordt.

- <u>ENGIE IT (IT-dienstenleverancier)</u>

  Zoals voor alle IT-leveranciers van ORES zijn de relaties met ENGIE IT in contracten opgenomen en bevatten zij vertrouwelijkheids-, veiligheids- en AVG-clausules. De toegang van ENGIE IT tot de gegevens van ORES wordt gemonitord.

In aansluiting op de brief van 28 maart 2024, waarin de CWaPE de voorwaarden bepaalt om de uitstap van ENGIE IT op 31 december 2030 goed te keuren, wordt de uitvoering van het uitstapplan regelmatig gemonitord ten opzichte van de CWaPE.
In dit verband bezorgt ORES halfjaarlijks (in juni 2025 en juli 2025) een bijgewerkt uitstapplan per brief aan de CWaPE.
De overname van de IT-diensten door ORES werd aan de CWaPE uitgelegd, evenals de voorwaarden daarvoor.
Tot slot is de streefdatum voor de beëindiging van de IT-diensten die ENGIE IT in dit kader levert, uiteindelijk vastgesteld op 31 december 2027, met dien verstande dat er met ENGIE IT een afspraak is gemaakt over de mogelijkheid om enkele resterende diensten na die datum van 31 december 2027 over te nemen, mocht dat nodig blijken.

- Bijzonder geval: *Connect My Home*

  Het initiatief "*Connect My Home* "is een manier om in het kader van de aansluitingswerken voor particulieren de werkzaamheden van de volgende operatoren te bundelen: ORES, RESA, SWDE, Proximus, Orange en Telenet.
  Om van de dienst "*Connect My Home*" te genieten, kunnen klanten zich inschrijven via één enkel portaal waarvan het beheer aan ORES werd toevertrouwd. Contractueel en operationeel werd alles in het werk gesteld om de veiligheid en vertrouwelijkheid van de gegevens van particulieren en hun mogelijkheden om hun "AVG"-rechten uit te oefenen, strikt te garanderen.

# Hoofdstuk VIII – Invoering van digitale meters

Om de verplichting tot invoering van de nieuwe meettechnologie na te komen, is ORES samen met andere DNB's (Fluvius, Sibelga en RESA) toegetreden tot een consortium om de kosten onder elkaar te verdelen en aan de burger een snellere en meer coherente oplossing te bieden.

Er werd een governance opgezet om het principe van de bescherming en de vertrouwelijkheid van de gegevens vanaf de ontwerpfase na te leven.

De digitale meters sturen eenmaal per dag de opgenomen meterstanden door naar ORES (ook gegevens die meerdere keren per dag worden gemeten). Deze meterstanden worden doorgegeven via een dienstverlener die de identiteit van de klanten van ORES niet kent.
Om de bescherming van de aldus doorgegeven meetgegevens te waarborgen, worden deze van aan de meter tot bij ORES versleuteld. Er werden specifieke penetratietests uitgevoerd.

Voor de invoering van digitale meters bij ORES werd gekozen voor een gefaseerde aanpak. Sinds 2020 worden er bij particulieren digitale meters geïnstalleerd. Met uitzondering van het gebruik van de voorafbetalingsfunctie en de vervanging van de meters om metrologische redenen, verplicht ORES in geen geval de burgers om de communicatiefunctie van de nieuwe meter te gebruiken. Als burgers dit uitdrukkelijk vragen, worden de meters in "vliegtuigstand" gezet. De wijziging van het decreet inzake de invoering van digitale meters in Wallonië van 27 maart 2024, goedgekeurd door het Waalse Parlement op 24 april 2024, legt de verplichting op om op tegen december 2029 100% digitale meters te hebben geïnstalleerd op alle leveringspunten voor elektriciteit.

Om deze ambitieuze doelstelling te bereiken, heeft ORES het project ACDC opgezet, waarbij de vervanging van de meters volledig is uitbesteed (inclusief het klantentraject en dus ook een afspraak maken). Voor dit project werden zowel een analyse van de gevolgen voor de gegevens als een veiligheidsrisicoanalyse uitgevoerd.

In het licht van de principes inzake gegevensbescherming neemt ORES de volgende maatregelen:

- In de huidige fase worden enkel de verwerkingen toegepast waarvan de finaliteiten rechtstreeks verband houden met de klassieke opdracht van de DNB en met de wettelijke verplichtingen. Voor de toekomst zijn er nog andere verwerkingen gepland. Deze zullen gebaseerd zijn op een uitdrukkelijke, specifieke, voorafgaande en geïnformeerde toestemming van de burgers.

- <u>Principe van transparantie en recht op informatie</u>
  Onmiddellijk bij het maken van de afspraak voor de installatie van de nieuwe meters, worden de betrokken personen ervan op de hoogte gebracht dat de digitale meters gegevens doorsturen.

Bij de installatie van meters is een brochure met uitleg beschikbaar. Een pagina op onze website[5] geeft antwoorden op vragen over gegevensbescherming. Medewerkers van ORES die in contact staan met klanten krijgen een opleiding. Ook onze afgevaardigde voor gegevensbescherming (DPO) beantwoordt alle vragen in verband met privacy- en gegevensbescherming. Onze privacyverklaring werd bijgewerkt in augustus 2025.

- Minimalisering, kwaliteit en bewaarduur
  Enkel de gegevens noodzakelijk voor de uitvoering van de beschreven opdrachten worden verzameld.
  Wat het bewaren betreft, worden de gegevens verwerkt zoals de klassieke gegevens van meteropnames.

- Verwerking
  Overeenkomstig artikel 28 van de AVG wordt met elk van onze partners een verwerkingscontract gesloten.

- Beveiliging
  Er werden aangepaste technische en organisatorische maatregelen genomen om de bescherming (vertrouwelijkheid en integriteit) van de gegevens van de klanten van ORES te waarborgen: de digitale meters worden gemonitord inzake cybersecurity, waarbij rekening wordt gehouden met de aspecten in verband met de gegevensbescherming en de toepassing van de geldende wetten.

De intentionele veiligheidsrisico's worden ingeschat in het kader van workshops, waarbij de EBIOS RM 2018-methode wordt toegepast om de veiligheidsrisico's van informatiesystemen (entiteiten en kwetsbaarheden, aanvalsmethodes en bedreigingen, essentiële elementen en veiligheidsbehoeften…) te beoordelen en bij te dragen tot hun behandeling door het specificeren van de toe te passen veiligheidsvereisten.
Om de gegevens continu te beheren werden er in 2025 risicoanalyses uitgevoerd (AVG en beveiliging) en werden de processen in verband met de communicatieketen bijgewerkt.

Drie watermaatschappijen die actief zijn op het Vlaamse grondgebied zijn toegetreden tot het consortium, wat tot gevolg heeft dat het gegevensverzamelingssysteem (HES) vandaag met zes andere vennootschappen gedeeld wordt (Fluvius, Resa, Sibelga, Pidpa, De Watergroep en Farys).

Het is niet de bedoeling dat de gegevens die door de digitale meters worden ingezameld door het HES bewaard worden. Er werden aan het risico aangepaste beveiligingsmaatregelen geïmplementeerd. Er gelden namelijk "logische" scheidingsregels om ongewenste toegang tot de gegevens van de andere operatoren en een slechte routering van de gegevens te vermijden.

Mocht er in de toekomst aan ORES een rol worden toebedeeld in het kader van het beheer van de gegevens van de watermeters (overdracht van de gegevens via de elektriciteitsmeters bijvoorbeeld), dan is het vanzelfsprekend dat er gepaste

[5] https://www.ores.be/particulieren/digitale-meter-werking - rubriek *Vragen in verband met dit onderwerp* "Wat doet ORES met mijn gegevens?".

maatregelen zullen worden ingevoerd om aan de doelstellingen inzake scheiding van de rollen te voldoen.