VERSLAG Nr. 21
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

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 het operationeel en dagelijks beheer van de activiteiten van ORES Assets[2] 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 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[3] 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 dagelijkse uitbating van zijn activiteiten volledig of gedeeltelijk toe te vertrouwen aan een

[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").
[3] Artikel 3 van de statuten van ORES cv.

dochteronderneming die over eigen personeel beschikt, werd een personeelslid van ORES cv, dochteronderneming van ORES Assets, door het Directiecomité van ORES cv op 1 februari 2018 aangesteld tot vertrouwelijkheidscoördinator, namelijk Audrey Réveillon.

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 2024 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 de vertrouwelijkheid van de gegevens

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

Door het feit dat ORES Assets, overeenkomstig artikel 16, § 1 van het elektriciteitsdecreet en artikel 17, § 1 van het gasdecreet, de dagelijkse uitbating aan ORES cv heeft toevertrouwd, 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 is de ethische gedragscode die van toepassing is op al het personeel herzien. Deze nieuwe ethische en deontologische code bevat de verplichtingen van het personeel op het gebied van gegevensbescherming, evenals de verplichting om zich eraan te houden. De code is ook van toepassing op externe partners (consultants, onderaannemers, uitzendkrachten…). Hij maakt deel uit van de contractuele documentatie die wordt verstrekt in het kader van nieuwe samenwerkingen.
Ook met de externe medewerkers en uitzendkrachten worden aangepaste vertrouwelijkheidscontracten ondertekend.
Al deze clausules zijn herzien en de inhoud ervan is conform de normen van ISO 27001.

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 elk jaar door het Directiecomité van ORES cv herzien en ze werd voor het laatst bijgewerkt in maart 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:

- Het opstellen van een nieuwe ethische en deontologische code waarin de verplichtingen inzake gegevensbescherming zijn opgenomen, evenals de communicatie ervan aan alle personeelsleden van ORES CV en externe partners (consultants, onderaannemers, uitzendkrachten…);
- de verspreiding van basisinformatie over de verplichtingen inzake vertrouwelijkheid, via het lezen en ondertekenen van een vertrouwelijkheidsclausule waarin het personeel zich ertoe verbindt om de verplichtingen na te leven;
- 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;
- het bezorgen van de CAO ICT (informatie- en communicatietechnologieën) aan alle nieuwe personeelsleden van ORES. Dit document bepaalt 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;
- het ter beschikking stellen van een reeks video's waarin bedrijfssituaties worden gesimuleerd waarin medewerkers worden geconfronteerd met beveiligingsproblemen. Elke video legt uit over het juiste gedrag in de geschetste situatie. Twee afleveringen worden om de twee maanden verspreid;
- de oprichting van een SharePoint-site over informatiebeveiliging met toegang tot documenten betreffende beveiliging, conform ISO 27001 (beleidslijnen, standaarden, procedures, best practices);
- een verplichte *e-learning "*AVG" en diverse *e-learning*-modules inzake informatiebeveiliging worden georganiseerd. Deze cursussen zijn verplicht voor alle ORES-medewerkers en voor alle nieuwkomers. De daarin gebrachte boodschap wordt permanent ondersteund door bewustmakingscampagnes over diverse veiligheidsonderwerpen, afhankelijk van het kennisniveau dat bij de ORES-medewerkers wordt vastgesteld alsook van de belangrijkste gevaren waaraan onze gegevens zijn blootgesteld. De campagnes richten zich op het bewustmaken van het ORES-personeel voor de gevaren van phishing;
- het openen van een aan de AVG gewijde samenwerkingsinterface die ter beschikking staat van alle medewerkers, voor het vergemakkelijken van de toegang tot de relevante informatie en de toe te passen procedures wanneer er persoonsgegevens in het spel 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. 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 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).

Tevens werd de nieuwe ethische en deontologische code gecommuniceerd naar de leden van de Raden van Bestuur van ORES Assets en ORES cv.

De bestuurders van ORES Assets, ORES cv en Comnexio hebben zich eveneens individueel ertoe 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.

De bestuurders van ORES Assets en ORES cv hebben bovendien een MAR-gedragscode[4] aangenomen en hebben zij individueel een verklaring ondertekend in hun hoedanigheid van geïnitieerde persoon.

[4] Europese verordening “Marktmisbruik” die ernaar streeft de integriteit van de markten en de bescherming van de investeerders te verbeteren.

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

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, onderaannemers, volgende 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.

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 deze oefeningen geëvalueerd. Verder worden er veiligheidsrisicoanalyses uitgevoerd voor de nieuwe bedrijfsprocessen. De bestaande bedrijfsprocessen worden elke drie jaar inzake risicoanalyse voor informatiebeveiliging.

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 de 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;

- het opzetten van beveiligde kluizen voor wachtwoorden.

Een reorganisatie van de dienst Informatie Veiligheid Office vond in April 2024 plaats om alle veiligheidscompetenties onder de CISCO van ORES te hergroeperen.
Er werden drie teams opgericht, namelijk:

- Het team Governance, Risk and Compliance: dit team is verantwoordelijk voor de ontwikkeling van het informatiebeveiligingsbeleid en de beveiligingsstandaarden, in overeenstemming met de ISI 27001-norm;
- Het team Cyberdefense: dit team houdt toezicht op IT-activiteiten via loganalyse van verschillende componenten (firewalls, WAF, antivirus, enz.)
  Bovendien heeft ORES een contract afgesloten voor 24/7 beveiligingstoezicht;
- Het team Idendity and Access Management: dit team beheert de volledige levenscyclus van een gebruiker binnen het informatiesystem van ORES (aanmaak van de gebruiker, toekenning van toegangsrechten en verwijdering).

Over het algemeen moet worden opgemerkt dat 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), ORES Assets op 1 november 2022 werd aangesteld als aanbieder van essentiële diensten. ORES Assets is een essentiële entiteit in de zin van de NIS 2-regelgeving. 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. Hiertoe is voor de herfst van 2024 een externe audit gepland. Het certificatiebureau heeft in januari 2025 een positief advies uitgebracht, waardoor ORES naar verwachting haar certificering tegen eind maart 2025 zal behalen.

[5]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.

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

De Directie Klanten & Markten is sinds januari 2024 gereorganiseerd. Voor het leesgemak staan de namen van de voormalige afdelingen tussen haakjes.

1. De betrokken diensten van ORES cv

De dienst Facilitering en Marktoperaties (voorheen Structurering, Measure & Settlement) maakt deel uit van de Directie Klanten & Markten. Deze Directie beheert alle processen die verband houden met geliberaliseerde markten (Assets, structuur, measure, settle en rectification), van de gegevens alsook van de flexibiliteit. Sociale verplichtingen worden ook door deze Directie beheerd.
Het team Correctie Marktanomalieën *(voorheen Beheer van het Toegangsregister binnen de dienst Facilitering en Marktoperaties) beheert* het federaal toegangsregister (CMS Atrias, *Central Market System)* waarvan de *go live* plaatsvond in december 2021 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 of enkelvoudig tarief zichtbaar en in de toekomst bijvoorbeeld het aanmoedigingstarief).
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.

Het opnemen van de elektromechanische meters gebeurt voortaan binnen de nieuwe dienst Klantbeleving. Voor de digitale meters is het team Toezicht op Communicatieketens (voorheen Smart Control Room), binnen de dienst Facilitering en Marktoperaties, verantwoordelijk voor het controleren van de goede werking van de ketens, het doorsturen van de indexen (onder andere via het Prism tool), alsook voor de saldi op de budgetmeters. Sinds er digitale meters worden geïnstalleerd, is er een nieuw platform voor automatische meteropname geïnstalleerd. Deze Prism tool (een applicatie om gegevens van de digitale meters te verzamelen en de telecommunicatie met HES, het *Head-End System* te beheren) is enerzijds verbonden met MDM/Mercure en anderzijds met de communicatieketen van de meters.

De teams Validatie (B2Cen B2B), binnen de dienst Facilitering en Marktoperaties, controleren de coherentie van deze opnames op basis van verbruiksstatistieken, -historieken of klimatologische criteria.

Sinds de go-live van MIG6 kampt ORES met marktblokkeringen. De meest complexe gevallen worden behandeld door het team Toezicht op Transversale Processen (voorheen Market Service Center). Andere gevallen, worden opgevolgd door andere teams – ook binnen de dienst Facilitering en Marktoperaties – zoals Correcties (voorheen GPAM) voor Atrias-klachten die bij de SRME zijn ingediend, en Marktinteractie en Relatiebeheer voor verzoeken van leveranciers en klanten.

Het team Regularisatie van Processen (voorheen Beheer van Marktprocessen, nu geïntegreerd binnen de dienst Facilitering en Marktoperaties) heeft eveneens toegang tot de gegevens in het CMS om de processen *Drop*, *End-Of-Contract*, Initiate Leaving Customer (ILC) en Plaatsing van meters met voorafbetalingsfunctie, die door de energieleveranciers worden opgestart, tot een goed einde te brengen. Naast het sturen van brieven behoort het ook tot de taken van de medewerkers om contact op te nemen met klanten (bv. bij een onderzoek over een ILC-dossier) en/of de commerciële leveranciers (bv. bij 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 3 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 portaal van het CMS. 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, Regularisatie van Processen 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, Regularisatie van Processen, Marktinteractie en Relatiebeheer en Validatie en Correcties geven via telefoon, per brief of per e-mail 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. 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, dan kan hij zijn EAN slechts krijgen 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 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 om een aanvraag van meer dan twee EAN-codes gaat, wordt het verzoek geregistreerd en verwerkt per e-mail of per post.
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 over een permanent mandaat om informatie op te vragen over zijn inwoners. 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 smart verbruiksportaal: 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 (buiten de digitale meter), 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 PDA's (*Personal Digital Assistant*) van de meteropnemers die het invoeren van de meterstand ter plaatse mogelijk maken, zijn eveneens beveiligd met een persoonlijke identificatie op basis van de 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. De teams van de dienst Facilitering en Marktoperaties kunnen er toch voor analyses in leesmodus toegang toe krijgen. Toegang tot deze applicatie wordt verleend door de *application Owner* op basis van de IT-beroepenfiches. Geen enkel ander team heeft toegang tot deze applicatie nodig.

- **Prism en HES**

  De HES is alleen toegankelijk voor de externe dienstverlener die hem ter beschikking stelt. Wat Prism betreft: deze is toegankelijk voor het team Toezicht op de Communicatieketens in leesmodus, maar ook – steeds op basis van een beroepenfiche – voor het team Beheer van Voorafbetalingen (BVV), dat steeds het opladen van de budgetmeters heeft beheerd (Talexus) en nu ook de digitale meters in voorafbetalingsmodus (via de bij Atrias gehoste PPP-tool).

  Operaties op afstand (bv. het activeren van poort P1 of het aanvragen van addIndex) worden uitgevoerd door Prism via het SAP CS-systeem (een tool die bij ORES LoPex wordt genoemd); Alle toegangen tot de LoPex-applicatie worden gecontroleerd op basis van de HR-beroepenfiches.

- ORES en de kunstmatige intelligentie

ORES denkt er tegenwoordig na om de kunstmatige intelligentie (KI) in haar activiteiten te integreren, met als doel onder andere de energietransitie te ondersteunen en bepaalde repetitieve taken te optimaliseren.

ORES is zich bewust van de uitdagingen die gepaard gaan met het gebruik van deze technologieën en ziet erop toe dat de implementatie ervan plaatsvindt binnen een strikt intern governancekader dat in overeenstemming is met de geldende regelgeving, waaronder de AVG ende Artificial Intelligence Act. Dit wettelijke kader waarborgt een ethisch en veilig gebruik van KI, waarbij innovatie wordt verzoend met de bescherming van de rechten van individuen.

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

Technische en organisatorische maatregelen

Diverse aan het risico aangepaste beveiligingsmaatregelen werden ingevoerd en onder meer:

- gebruik van een unieke login voor de aannemers en beperking van de toegangsrechten tot de werven;
- het gebruik van pseudoniemen in de gegevens die toegankelijk worden gemaakt voor IT-ontwikkelingsbedrijven die voor ORES werkzaam zijn;
- de 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 (product CyberArk);
- uitvoeren van audits;
- minimalisering van de verstrekte gegevens;
- de invoering van een ethische en deontologische code die ook van toepassing is op externe medewerkers.

Contractuele maatregelen

Bij het sluiten van transacties of contracten met zijn partners, voegt ORES systematisch “AVG”-bedingen in, waarin alle in het 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.

Zodra gegevens buiten de Europese Unie worden gedeeld, worden er gelijkwaardige maatregelen voor gegevensbescherming getroffen en worden bij voorkeur de contractuele standaardclausules 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 van de activiteiten van de gebruikers en van de aan de oplossingen van derden verbonden technische accounts betreft, 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 SAP ORES een spoor van het geheel van de 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,
- Monitoring en operationeel beheer.

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

De implementering van een DLP (*Data Loss Prevention*) werd in 2021 onderzocht. Er werd een IT-platform ontwikkeld. Binnen ORES werd er een werkgroep opgericht voor het definiëren van de governance- en beroepenregels die op het IT-platform geïmplementeerd zullen worden.
In 2024 heeft ORES een tool uitgerold waarmee gebruikers van Microsoft-kantoortools documenten kunnen markeren. Er zijn vier markeringsniveaus gedefinieerd:

- C1 - OPENBARE informatie: de informatie is openbaar en mag met iedereen worden gedeeld, zowel binnen als buiten ORES;
- C2 - INTERNE informatie: de informatie mag gekend zijn door iedereen die bij ORES werkt, zowel interne als externe medewerkers (met contract) en eventueel bepaalde partners;

- C3 - BEPERKTE informatie: de informatie mag alleen gekend/ geraadpleegd worden door een beperkte groep mensen, bijvoorbeeld een team, een dienst of een directie;
- C4 - VERTROUWELIJKE informatie: de informatie mag alleen gekend /geraadpleegd worden door een paar met name vermelde personen.

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

Om haar taak te kunnen vervullen, deelt ORES bepaalde IT-systemen en -infrastructuren met haar 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.

2023 stelde ORES in staat om samen te werken met ENGIE IT om gedeelde diensten (back-up, serverinfrastructuur, opslagruimte, netwerkcomponenten, enz.) over te brengen naar een model dat speciaal voor ORES is gemaakt. De systemen die de ORES-applicaties hosten, waren al aanwezig in de ORES-silo. Sinds Juli 2023 bevinden alle gebruikte diensten, inclusief de historisch gedeelde diensten, zich in de ORES-silo en dus op ORES-specifieke hardware. De netwerkcomponenten van het datacenter zijn ook herzien en worden uitsluitend gebruikt om diensten aan ORES te leveren. Dankzij deze overstap naar speciale hardware voor gedeelde diensten heeft ORES zijn zichtbaarheid op de operationele activiteiten van ENGIE IT verder kunnen verbeteren.

In haar brief van 28 maart 2024 heeft de CWaPE de voorwaarden verduidelijkt voor de aanvaarding van de uitstapdatum van ENGIE IT (op 31 december 2030). Ze vraagt onder andere dat ORES een regelmatige opvolging ten aanzien van de CWaPE organiseert betreffende de uitvoering van het uitstapplan.
In dit kader bezorgt ORES tweemaal per jaar (in juni en december) een geactualiseerd uitstapplan per post. Elke bijgewerkte versie wordt bovendien ook toegelicht tijdens een presentatievergadering met de CWaPE.
De eerste status werd in juni 2024 naar de CWaPE gestuurd.

- 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, de SWDE, Proximus, ORANGE en Telenet.
  Om van de dienst “Connect My Home” te kunnen 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 verbintenis inzake de invoering van de nieuwe technologie 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 de burger in geen geval om de communicatiefunctie van de nieuwe meter te gebruiken (voor burgers die hier uitdrukkelijk om vragen, worden de meters in "vliegtuigmodus" geplaatst). De wijziging van het decreet dat het uitrollen van digitale meters in Wallonië regelt, goedgekeurd door het Waals Parlement op 24 april 2024 en gedateerd op 27 maart 2024, bepaalt dat op 31 december 2029 100% van de elektriciteitspunten uitgerust moeten zijn met een digitale meter.

Om dit ambitieuze doel te bereiken, heeft ORES het project ACDC ("Accélération des compteurs communiquants") gelanceerd via volledige uitbesteding (inclusief het kanttraject en dus het maken van afspraken). Er wordt een gegevensimpactanalyse en een beveiligingsrisicoanalyse uitgevoerd voor dit project.

ORES neemt de volgende maatregelen in het kader van de gegevensbeschermingsprincipes:

- 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 de meters wordt er een brochure met uitleg overhandigd. Een pagina op onze website[5] bevat antwoorden op vragen in verband met de gegevensbescherming. Medewerkers die in contact komen met klanten krijgen een opleiding. Ook onze afgevaardigde voor gegevensbescherming (DPO) staat ter beschikking. Onze privacyverklaring werd bijgewerkt in februari 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;

- Onderaanneming
  Er wordt een onderaannemingscontract gesloten overeenkomstig artikel 28 van de AVG met elk van onze partners;

- 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.
In het kader van voortdurende gegevensbeheersing zijn risicoanalyses (AVG en beveiliging) en updates van de processen betreffende de communicatieve keten gepland in 2025.

Het is vermeldenswaard dat drie watermaatschappijen die actief zijn op het Vlaamse grondgebied tot het consortium zijn toegetreden, 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 maatregelen zullen worden ingevoerd om aan de doelstellingen inzake scheiding van de rollen te voldoen.

[5] https://www.ores.be/particulier/compteur-communicant-fonctionnement.