VERTROUWELIJKHEIDSVERSLAG VAN ORES CV

INHOUDSOPGAVE

Hoofdstuk I - Inleiding

Ieder jaar sedert 2014 publiceert ORES Assets een vertrouwelijkheidsverslag ter attentie van de CWaPE.
Teneinde 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 de twee andere voor elke van haar dochterondernemingen, namelijk ORES CV en Comnexio. Deze drie verslagen worden volgens dezelfde structuur opgemaakt en geven een uitvoerige beschrijving van de goede praktijken die op het vlak van de vertrouwelijkheid worden toegepast. Zij streven ernaar te beantwoorden aan de voorschriften van het decreet waarvan hierna sprake.
Men dient in gedachten te houden dat het operationeel en dagelijks beheer van de activiteiten van ORES Assets[2], 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, aan ORES CV is toevertrouwd.
Wat de contact center-activiteiten betreft, deze werden vanaf 1 juni 2019 toevertrouwd aan Comnexio.
De wijze waarop deze beheersactiviteiten door voornoemde dochterondernemingen worden uitgeoefend, wordt bepaald in de bijlagen 6 en 7 van de statuten van ORES Assets en door de Raad van Bestuur voor elke bijkomende beslissing.
Het specifiek karakter verbonden aan de maatschappelijke structuur en aan 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.

Het artikel 17 van het besluit van 21 maart 2002 betreffende de netbeheerders, zoals gewijzigd door het besluit van 6 december 2018, bepaalt: "*De netbeheerder zorgt ervoor dat de persoonlijke en commerciële gegevens waarover hij beschikt om zijn taken uit te oefenen, zodanig ingezameld worden dat ze vertrouwelijk blijven. Hij zorgt ervoor dat die gegevens systematisch gescheiden worden van de gegevens die vatbaar zijn voor publiciteit. …*"

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

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 bestuursvoorschriften 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.

Onderhavig verslag dekt de activiteiten van ORES CV op het volledige door ORES Assets bediende grondgebied, zowel wat elektriciteit als aardgas betreft.

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

Het heeft tot doel de maatregelen uiteen te zetten die in de loop van het jaar 2021 genomen of voortgezet werden om nog beter de doelstelling te verwezenlijken die erin bestaat de vertrouwelijkheid van de informatie waarvan ORES CV in het kader van de uitvoering van de haar toevertrouwde taken op de hoogte is, te bewaren.

Dit verslag werd goedgekeurd door het Ethisch Comité van ORES CV dat werd gehouden op 23 maart 2022.

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

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

De arbeidscontracten van de personeelsleden bevatten bepalingen die hun een vertrouwelijkheidsplicht opleggen.
In hun arbeidsovereenkomst verbinden de personeelsleden er zich aldus met name toe de vertrouwelijke gegevens niet openbaar te maken, deze uitsluitend in het kader van de uitvoering van hun arbeidscontract te gebruiken, deze niet te kopiëren of te reproduceren zonder voorafgaande uitdrukkelijke schriftelijke toestemming van ORES CV, 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 vermeldt een ethische Gedragscode die op het geheel van de personeelsleden van toepassing is eveneens de verbintenis van de medewerkers van ORES CV om een geheel van ethische regels na te leven, met name de verplichting om blijk te geven van gezond verstand en behoedzaamheid inzake informatie betreffende hun beroepsactiviteit.

Ingevolge de inwerkingtreding van de Algemene Verordening Gegevensbescherming (hierna “AVG”) levert ORES CV een permanente inspanning om de principes van de verordening toe te passen en het personeel te sensibiliseren.
In 2019 werd er een verklaring inzake privacybeleid uitgeschreven en intern gepubliceerd, die het personeel van ORES CV een kijk geeft op de richtsnoeren die het bedrijf zichzelf inzake de AVG oplegt. Deze verklaring wordt elk jaar door het Directiecomité van ORES CV herzien en werd voor het laatst bijgewerkt op 11 februari 2022.
In elk Departement 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 sensibilisering van het personeel in:

- de verspreiding van basisinformatie over de verplichtingen inzake vertrouwelijkheid, via het lezen en ondertekenen van een vertrouwelijkheidsclausule waartoe het zich verbindt;
- het ondertekenen van een Verbintenis tot vertrouwelijkheid en niet-openbaarmaking op het ogenblik van de overhandiging van het draagbaar computermateriaal door het Departement Informatica;
- het opleggen van een aantal verplichtingen inzake vertrouwelijkheid via het arbeidsreglement;
- het overmaken van de CAO ICT (informatie- en communicatietechnologieën) aan alle nieuwe werknemers van ORES. Dat document legt het gebruikskader van telecommunicatiemiddelen door de werknemers vast;
- de terbeschikkingstelling van een *Welcome Pack* dat een luik cyberveiligheid bevat aan elke medewerker bij zijn aankomst;

- de terbeschikkingstelling van een korte video die het belang van de veiligheid en de rol die elke medewerker daarbij moet spelen toelicht;
- het houden van een informatiesessie, waarin de cyberveiligheid aan bod komt. Deze sessie komt na een “IT”-tevredenheidsonderzoek, waaruit een aantal vragen of problemen met het begrijpen naar boven kwamen (bijvoorbeeld: Waarom zijn sommige websites geblokkeerd? Waarom kan die software niet geïnstalleerd worden?,…). Deze sessie was zowel fysiek als via videoconferentie toegankelijk;
- de organisatie van een verplichte *e-learning “*RGPD” en diverse *e-learning*-modules inzake informatiebeveiliging in de zomer van 2020. Deze cursussen zijn verplicht voor alle ORES-medewerkers en voor alle nieuwelingen. De daarin gebrachte boodschap wordt sedert eind 2020 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. In 2021 richtten de campagnes zich op het sensibiliseren van het personeel van ORES 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 bestuursvoorschriften.
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 op elke bestuurder van een vennootschap rust, worden de bestuurders van ORES Assets (DNB), maar ook van ORES CV en van Comnexio (dochterondernemingen) bewust gemaakt van hun vertrouwelijkheidsplicht via de bestuursvoorschriften die in hun schoot zijn aangenomen en toegepast (in casu het Huishoudelijk Reglement voor ORES Assets en de Bestuurscharters van ORES CV en Comnexio, die trouwens toegankelijk zijn op de websites).

Zij hebben er zich eveneens individueel toe verbonden, met name, 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 het artikel L1532-1, § 1, van het Wetboek van de Lokale Democratie en de Decentralisatie, en dit door het ondertekenen van een verklaring op eer in dat verband.

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

[4] 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 persoons- en commerciële gegevens

Wanneer ORES CV persoonsgegevens verwerkt in verband met haar cliënteel, wordt er alles aan gedaan, of het nu is op het vlak van personeel, onderaannemers of computerbeveiliging, 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 taken van ORES: aansluitingen, geplande werken tellingen, ODV,…

ORES voerde reeds in de ontwerpfase ("*Privacy by design"* en *"Security by design"*) beschermingsprocedures in op zodanige wijze dat er van bij het opstarten van nieuwe projecten of ter gelegenheid van wijzigingen van de bestaande verwerkingen rekening wordt gehouden met de aspecten betreffende 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*", die klanten van ORES zijn. Het aspect "toegang" tot de persoonsgegevens wordt in elke oefening geëvalueerd. Verder worden er veiligheidsrisicoanalyses uitgevoerd voor de nieuwe bedrijfsprocessen.

De volgende technische en organisatorische maatregelen worden toegepast:

- het beheer van de machtigingen voor onze computerapplicaties 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 regeling van de toegangen wordt toegepast is de "op rollen gebaseerde toegangscontrole", waaraan ORES CV de twee volgende principes toevoegt: "*least privilege"* en "*need to know"*;
- in het geval van geprivilegieerde toegangen, maken deze laatste het voorwerp van een specifiek goedkeuringsproces uit;
- wat de levenscyclus van onze computeridentiteiten betreft, deze wordt automatisch aan het personeelsbeheer aangepast;
- de toegangsrechten per functie worden gevalideerd door HR en de managers van elke dienst;
- de bestekken betreffende de nieuwe applicaties vermelden specifiek de behoefte tot integratie in ons systeem voor het beheer van de computeridentiteiten en -toegangen;
- de 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 het HR-departement 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.

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

1. De betrokken diensten van ORES CV

De dienst *Structuring, Measure & Settlement (SMS)* maakt deel uit van het Departement Marktbeheer & Cliënteel. Dat Departement beheert met name alle processen van de geliberaliseerde markt alsook alle verplichtingen van een openbare dienst met sociaal karakter.
Binnen de Dienst SMS is het het team *Beheer van het Toegangsregister (BTR)* dat het toegangsregister en de contacten met de energieleveranciers beheert.

Het toegangsregister is de hoeksteen van de geliberaliseerde markt. Het is de databank van waaruit de relaties en uitwisselingen tussen de verschillende actoren van de markt en DNB's georganiseerd worden. In feite is het de tool die het bijwerken en de doorstroming van de informatie garandeert. Elk toegangspunt (ook leveringspunt genoemd) wordt daarin geïnventariseerd via zijn EAN-code. Achter die code vindt men hoofdzakelijk de gegevens van de klant, deze van zijn leverancier en enkele andere nuttige inlichtingen. Gekoppeld aan de MDM MDM/Mercure (de databank die het verbruik van elk leveringspunt inventariseert), maar ook aan de backend SAP ISU (waarin alle technische informatie in verband met een leveringspunt is opgenomen) geeft het toegangsregister een volledig beeld van de markt.

Het is het *Measure*-team van de Dienst SMS – waarvan onder meer de opnemers en de valideerders deel uitmaken – dat de verbruiksgegevens bij de klanten voor het hele grondgebied dat door ORES gedekt wordt opneemt en valideert, d.w.z. verifieert of de opnames coherent zijn in vergelijking met de verbruiksstatistieken en -historieken of klimaatcriteria. Het team beheert tegelijkertijd de jaarlijkse meteropname bij de residentiële klanten en kleine professionals (een bezoek om de twee jaar en het sturen van een kaart het andere jaar), de maandelijkse opname (een maandelijks bezoek) en de opname vanop afstand met regelmatige tussenpozen voor de grote verbruikers (per kwartier voor de elektriciteit en per uur voor gas).
Het dagelijks beheer van de door de voornoemde Dienst gebruikte computerapplicaties – het toegangsregister en MDM/Mercure – werd tot de Go Live van Atrias in samenwerking met Fluvius verzekerd. Sinds de Go Live van Atrias wordt het toegangsregister van alle Belgische DNB's door het CMS (*Central Market System)* beheerd.

Het team *Beheer van de Marktprocessen* (BMP) – Dienst Werken Klanten Markten (WKM) bij het Departement Markt & Cliënteel – moet eveneens toegang krijgen tot de in het CMS opgenomen gegevens om de processen *Drop*, *End-Of-Contract*, Initiate Leaving Customer (ILC) en Plaatsing van een budgetmeter, 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 de klanten (bv. bij een onderzoek over een ILC-dossier) en/of de commerciële leveranciers (bv. bij een beveiligde annulering).

Ten slotte heeft ons *contact center* Comnexio, een dochteronderneming van ORES Assets, eveneens toegang tot de informatie van het CMS of nog van Mercure om de eerstelijnsoproepen van de 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

- **Het toegangsregister (CMS)**

  De computerinfrastructuur is beveiligd en de toegang tot de applicatie is geïndividualiseerd en voorbehouden – met name via een *reporting Business Object* (BO) tool – aan de leden van de BTR- (lezen en schrijven) en BMP-teams (lezen en schrijven).
  Elke nieuwe aanvraag tot toegang is onderworpen aan de goedkeuring van 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 elkeen.

  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 geraadpleegde klantengegevens zullen de gegevens zijn 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 zal dus geen toegang hebben tot de gegevens van een klant die bij een andere leverancier actief is. De beveiligings- en toegangsregels van de computerapplicatie beheren deze beperkte terbeschikkingstelling van de aan het toegangspunt verbonden informatie. Naast deze beveiliging via de computerapplicatie, worden de BTR- en BMP-teams opgeleid om enkel aan de op dat toegangspunt erkende leverancier inlichtingen per mail of telefonisch mede te delen.

  De BTR- en BMP-teams geven via de telefoon, per brief of per 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 computerapplicatie zelf.
  Als een klant aan de DNB vraagt welke leverancier aan het toegangspunt

verbonden is, zal die informatie hem per brief naar het installatieadres worden gestuurd.

De procedure die door ons *contact center* Comnexio wordt toegepast, wordt eveneens beheerst. 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 hem zijn EAN enkel kunnen worden meegedeeld op voorwaarde dat hij zijn meternummer opgeeft. De informatie zal hem vervolgens niet mondeling worden meegedeeld, maar via een SMS naar het GSM-nummer dat de klant ons zal moeten hebben meegedeeld. Als de klant zijn aanvraag schriftelijk stuurt of als hij niet over een GSM-nummer beschikt, zal de informatie hem in een brief op naam worden gestuurd. Als het gaat om een aanvraag betreffende meer dan twee EAN-codes, dan zal aan de klant gevraagd worden zijn aanvraag per brief of per e-mail, samen met de lijst van de betrokken adressen en meternummers, te sturen.
Deze oproepen en berichten zullen in het systeem nagetrokken worden.

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 bestuurden (staat van een dossier, leverancier actief op een punt, verbruikshistoriek, …) voor wie het over een permanent mandaat beschikt. Aan de OCMW's wordt gevraagd dit oproepnummer nooit openbaar te maken.

Alle markttransacties alsook de verzendingen van gegevens laten een spoor na.

Ten slotte dient er te worden opgemerkt dat wanneer een leverancier een marktscenario *drop* of *plaatsing van een budgetmeter* opstart – wat veronderstelt dat de klant betalingsmoeilijkheden heeft – een andere leverancier, die een *switch* (verandering van leverancier) op het toegangspunt zou opstarten, per kerende geen bericht zal ontvangen dat er een *drop* of een *plaatsing van een budgetmeter* in uitvoering is, maar enkel een afwijzing met de vermelding dat er een einde-contract-scenario lopende is. Daardoor zal de nieuwe leverancier geen kennis kunnen nemen van de betalingsmoeilijkheden van de klant. Er dient te worden opgemerkt dat een leverancier ingevolge de publicatie in het Belgisch Staatsblad van de aanpassingen van het elektriciteitsdecreet betreffende de nieuwe wanbetalingsprocedure (vaak "Vrederechterdecreet" genoemd) steeds een Switch-aanvraag kan opstarten over een EAN waarvoor een aanvraag tot plaatsing van een budgetmeter werd gedaan, zonder dat hem een afwijzing wordt toegestuurd.

- **Mercure-systeem**

De computerinfrastructuur is beveiligd en de toegang tot de applicatie is geïndividualiseerd en voorbehouden in de "wijzigings-"modus aan de leden van de dienst SMS.
Elke nieuwe aanvraag tot toegang (in modus "lezen" of "wijziging") is onderworpen aan de goedkeuring van de *application Owner Measure* die – per

beroep en functie HR – over de toegangsrechten tot de applicatie waarvoor deze *application owner* verantwoordelijk is, beschikt.

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

De leveranciers hebben toegang tot de applicatie via een webinterface, maar elke leverancier kan enkel de gegevens raadplegen van klanten/toegangspunten waarvoor hij een aanvaarding van de registratie op het toegangspunt ontvangen heeft vanwege het toegangsregister. Bovendien wordt de terbeschikkingstelling van de gegevens beperkt op basis van de contractuele gegevens tussen de klant en de leverancier.

De beveiligings- en toegangsregels van de computerapplicatie beheren deze beperkte terbeschikkingstelling van de informatie in verband met de verbruiken van het toegangspunt.

Een klant die zijn verbruikshistoriek wenst te kennen, kan deze raadplegen via de website van ORES door middel van een beveiligde identificatie. Hij kan naar een andere persoon of naar een leverancier gestuurd worden, maar deze laatsten moeten over een schriftelijke en ondertekende volmacht van de klant van het betrokken toegangspunt beschikken.
Alle markttransacties evenals de verzendingen van gegevens laten een spoor na.

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

- als het om een opname vanop afstand gaat (buiten de digitale meter), moet men de klant verzoeken zijn aanvraag via onze website in te dienen. Hij ontvangt dan een historiek over de drie laatste jaren maximum;
- als het om een jaarlijkse of maandelijkse opname gaat, worden de klantenadviseurs er eerst aan herinnerd dat de verbruiksgegevens privé-inlichtingen 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 via het te zijner beschikking gesteld portaal toegang tot zijn verbruikshistorieken en dus worden de toegangen eveneens op een strikte manier opgevolgd op het vlak van de veiligheid.

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 schrijven gestuurd waarin de historiek van de drie laatste jaren maximum vermeld wordt.
Aangezien de klanten bij het begin van de oproep worden ingelicht dat het gesprek wordt opgenomen, kunnen de teams die voor de processen instaan (*Process Owner*) de opgenomen telefoongespreken beluisteren teneinde de correcte toepassing van de geldende regels te controleren.

De PDA's (*Personal Digital Assistant*) van het opnamepersoneel die het invoeren van de meterstand ter plaatse mogelijk maken, zijn eveneens beveiligd met een persoonlijke identificatie op basis van de gebruikersnaam en een paswoord.

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 in verband met de verzoeken tot opname in digitaal formaat ontvangen. Dat proces is onderworpen aan het geheel van regels van de AVG en in geval van verandering van klant wordt deze functie automatisch stopgezet.

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

Technische en organisatorische maatregelen

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

- het gebruik van een unieke identificatiecode voor de aannemers en de beperking van de toegangsrechten tot de werven;
- het gebruik van pseudoniemen in de gegevens die toegankelijk worden gemaakt voor computerontwikkelingsbedrijven die voor ORES werkzaam zijn;
- de scheiding van de toegangen tot de productiegegevens en tot de testgegevens;
- de beperking van de toegangen tot de productiegegevens;
- de beperking van de toegangen tot de gegevens door externe leveranciers voor onderhoudsredenen;
- het beheer van de administratie- en ondersteuningsaccounts van externe dienstverleners via een “kluis”-systeem (Product CyberArk);
- de uitvoering van audits;
- de minimalisering van de verstrekte gegevens.

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 gepreciseerd worden: duur, toepassingsgebied, finaliteit, verwerkingsinstructies, voorafgaande toestemming in het geval dat er beroep wordt gedaan op een onderaannemer, terbeschikkingstelling van alle documentatie waaruit de conformiteit blijft, onmiddellijke kennisgeving van elke schending van gegevens …

Van zodra er gegevens buiten de Europese Unie worden gedeeld, worden de contractuele typebedingen toegepast.

Er worden eveneens ruimere vertrouwelijkheidsbepalingen in de contracten voorzien.

Hoofdstuk VI – Traceerbaarheid als vector van vertrouwelijkheid

ORES gebruik 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 en van de aan de oplossingen van derden verbonden technische accounts betreft, bewaart ORES in de SAP-databank:

- een samengevoegd overzicht van het dagelijks gebruik gedurende 31 dagen;
- een samengevoegd overzicht van het wekelijks gebruik gedurende 20 weken;
- een samengevoegd overzicht van het maandelijks gebruik gedurende 20 maanden.

Wij verduidelijken nog 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 samenvoeging heeft betrekking op het ogenblik van de uitvoering van de transactie.

Wat de verzending van gegevens per mail betreft, bewaart de SAP ORES een spoor van het geheel van de activiteiten in beveiligde omgevingen en waarvan de toegankelijkheid beheerst wordt.

De diensten in verband met de netinfrastructuur WIFI / LAN / WAN en de telefonie vallen onder de verantwoordelijkheid van ORES:

- Toegangsnetwerk tot de eindgebruikers (25+ gebouwen);
- Schakelaars en routers;
- Wi-Fi;
- DNS/ DHCP / IPAM ;
- Toegangscontrole tot het netwerk;
- Monitoring en operationeel Beheer.

Dit laat toe te illustreren in welke mate ORES de toegangscontrole en de controle van de activiteiten op het computernetwerk beheerst. Wat het OT-netwerk (*Operational Technology*) betreft, dat is eigendom van ORES dat eveneens het beheer ervan verzekert. ORES beheerst 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 beheers- en beroepsregels die op het IT-platform geïmplementeerd zullen worden.

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 beheer van de Veiligheid van de informatie bij ORES conformeert zich aan de ISO27001-norm. De scheiding van de aldus gedeelde gegevens is gebaseerd op de volgende principes:

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

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

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

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

  Het IMDMS “*clearing”*-systeem wordt gedeeld met Fluvius. Dat systeem laat toe de verrichtingen op de energiemarkt te centraliseren en te organiseren.
  In het huidig systeem heeft Fluvius de mogelijkheid alle gegevens te zien teneinde zijn rol van beheerder van het *Clearing House* (toewijzing, verzoening, *infeed*) te kunnen vervullen.
  Er vond een aanpassing van de toegangsrechten van de gebruikers van ORES plaats teneinde de acties op de gegevens van ORES te beperken. Wanneer een persoon ORES verlaat, wordt zijn account automatisch geblokkeerd bij de verandering van de paswoorden, die om de drie maanden plaatsvindt.
  Fluvius van zijn kant gaat regelmatig over tot het wissen van de geblokkeerde rekeningen. Er dient te worden opgemerkt dat de rol van *Clearing House* sedert 29 november 2021 door Atrias verzekerd wordt.

- <u>ENGIE IT (hoofdleverancier van IT-diensten)</u>

  Zoals voor alle IT-leveranciers van ORES zijn de relaties met ENGIE IT in contracten opgenomen en bevatten zij vertrouwelijkheidsbedingen,

veiligheidsbedingen en AVP-bedingen. De toegang van ENGIE IT tot de gegevens van ORES wordt gecontroleerd.

- N-ALLO

  ORES doet beroep op de technische infrastructuren van N-Allo (via het gebruik van zijn telefonieplatform ININ dat door de *back offices* van ORES wordt gebruikt), met name wanneer deze *back offices* handelen in tweede lijn van ons *contact center* (Comnexio).
  Zoals voor alle dienstverleners, heeft N-Allo zich contractueel verbonden tot het naleven van vertrouwelijkheidsbedingen, veiligheidsbedingen en AVG-bedingen.
  Momenteel loopt er een traject om het telefonieplatform ININ te vervangen. Na afloop van dat traject, dat tegen 30 juni 2023 verwezenlijkt zal worden, zal ORES niet langer beroep doen op de diensten van N-Allo.

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

Hoofdstuk VIII – Invoering van digitale meters

Voor het aangaan van de verbintenis inzake de invoering van de nieuwe technologie, is ORES samen met andere DNB's (Fluvius en RESA) toegetreden tot een consortium en dit eveneens met het doel de kosten onder elkaar te verdelen en aan de burger een snellere en meer coherente oplossing te bieden.

Wij wijzen erop dat er vanaf het opstarten van het project beheersmaatregelen werden genomen met het oog op de naleving van het principe van de bescherming en de vertrouwelijkheid van de gegevens vanaf de ontwerpfase.

De digitale meters sturen eenmaal per dag de opgenomen meterstanden door naar ORES. Deze meterstanden worden doorgegeven via een verzendingsdienstverlener, die de identiteit van de klanten van ORES niet kent.
Om de bescherming van de aldus doorgegeven meetgegevens te waarborgen, worden zij van aan de meter tot bij ORES versleuteld. Er werden specifieke penetratietests uitgevoerd.

Voor de invoering van de digitale meters bij ORES werd gekozen voor een gefaseerde aanpak. Vanaf 2020 werden er bij particulieren digitale meters geïnstalleerd. ORES legt in geen geval de nieuwe meter op aan de burger, deze laatste kan nog altijd voor een traditionele meter kiezen.

In verband met de principes inzake gegevensbescherming geeft ORES de volgende antwoorden:

- In de huidige fase zijn enkel de verwerkingen actueel waarvan de finaliteiten rechtstreeks verband houden met de klassieke opdracht van de DNB en met de wettelijke verplichtingen. Voor de toekomst worden 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 op de hoogte gebracht van hun communicerend karakter.
  Op het ogenblik van 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. De medewerkers die in contact komen met de klanten ontvangen een opleiding. Onze afgevaardigde voor gegevensbescherming staat eveneens ter beschikking. Onze privacynotitie werd eveneens bijgewerkt;

- <u>Minimalisering, kwaliteit en bewaarduur</u>
  Enkel de gegevens noodzakelijk voor de uitvoering van de beschreven opdrachten worden verzameld.

[5] www.ores.be/particuliers-et-professionnels/comptage-intelligent.

Wat het bewaren betreft, worden de gegevens verwerkt zoals de klassieke gegevens van de opnames. Zonder toestemming van de klant worden enkel de dagelijkse meterstanden opgevangen;

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

- Beveiliging
  Er werden aangepaste technische en organisatorische maatregelen ingevoerd om de bescherming (vertrouwelijkheid en integriteit) van de gegevens van de klanten van ORES te waarborgen: voor het toezicht op de *Smart Metering* wordt beroep gedaan op cybersecurity die rekening houdt met de aspecten in verband met de gegevensbescherming en de toepassing van de geldende wetten.
  Het programma volgt het door het bedrijf toegepast beheer, wat onder meer het evalueren van de invloed op de privacy en een validatie via het beheer van het project inhoudt. ORES voerde en voert voor elke fase van de invoering impactanalyses uit met betrekking tot de bescherming van de gegevens.

De intentionele veiligheidsrisico's worden ingeschat in het kader van workshops, waarbij de EBIOS-methode wordt toegepast, die toelaat 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, maar ook het volledige veiligheidsdossier voor te bereiden dat noodzakelijk is voor de aanvaarding van de risico's en alle nuttige elementen te leveren voor de communicatie in verband met de risico's.

Het is vermeldenswaard dat drie watermaatschappijen die actief zijn op het Vlaams grondgebied vandaag tot het consortium zijn toegetreden, wat tot gevolg heeft dat het gegevensverzamelingssysteem (HES) vandaag door zeven 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 een ongepaste 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), is het vanzelfsprekend dat er gepaste maatregelen zullen worden ingevoerd om aan de doelstellingen inzake scheiding van de rollen te beantwoorden.

Met het oog op het verzekeren van de naleving van de NIS-richtlijn[6] heeft ORES een ISO27001-certificatietraject opgestart.

[6] Richtlijn (EU) 2016/1148 van het Europees Parlement en de Raad van 6 juli 2016 houdende maatregelen voor een hoog gemeenschappelijk niveau van beveiliging van netwerk- en informatiesystemen in de Unie