VERTRAULICHKEITSBERICHT VON ORES GEN.

INHALTSVERZEICHNIS

Abschnitt I - Vorbemerkung

Seit 2014 veröffentlicht ORES Assets jedes Jahr einen Vertraulichkeitsbericht, der für die wallonische Energiekommission CWaPE bestimmt ist.
Um der Anforderung der CWaPE an ORES Assets[1] nachzukommen, werden für den ORES-Konzern drei separate spezifische Berichte verfasst: einer für ORES Assets und zwei weitere für jede ihrer Tochtergesellschaften, also ORES Gen. und Comnexio. Diese drei Berichte werden auf Basis der gleichen Struktur verfasst und detaillieren die bewährten Vertraulichkeitspraktiken, die angewandt werden. Ihr Zweck ist es, die weiter unten vermerkten, per Dekret auferlegten Vorschriften zu erfüllen.
Hierbei ist zu bedenken, dass die mit dem öffentlichen Dienstleistungsauftrag verbundenen Tätigkeiten von ORES Assets dem Unternehmen ORES Gen. anvertraut werden.
Die Tätigkeiten des *Kontaktzentrums* wurden ihrerseits am 1. Juni 2019 Comnexio anvertraut.
Die entsprechenden Verwaltungsmodalitäten für diese Tochtergesellschaften sind in den Anlagen 6 und 7 der Satzung von ORES Assets festgelegt und der Verwaltungsrat trifft diesbezüglich jede zusätzliche Entscheidung.
Aufgrund der Besonderheit der gesellschaftlichen Struktur und der operativen Realität von ORES Assets und ORES Gen., wobei ORES Assets der VNB und ORES Gen.[2] die Betreibergesellschaft ist, ist der Inhalt ihres jeweiligen Berichts fast identisch.

Laut Artikel 17 des Erlasses vom 21. März 2002 über die Netzbetreiber (in seiner durch den Erlass vom 6. Dezember 2018 abgeänderten Fassung) gilt Folgendes: „*Der Netzbetreiber sorgt dafür, dass die persönlichen und gewerblichen Informationen, von denen er im Rahmen der Erfüllung seiner Aufgaben Kenntnis hat, in einer Form und unter Bedingungen gesammelt und verzeichnet werden, die deren Vertraulichkeit bewahren. Er garantiert die systematische Trennung dieser Daten von denjenigen, die öffentlich werden können.“*

Artikel 7 des Erlasses vom 16. Oktober 2033 über die Gasverteilernetzbetreiber (in seiner durch den Erlass vom 6. Dezember 2018 abgeänderten Fassung) enthält gleiche Bestimmungen.

Seit der Bestandsaufnahme der bewährten Vertraulichkeitspraktiken vonseiten der CWaPE im Jahr 2019 im Rahmen ihrer Überprüfung der Regeln der Unternehmensführung innerhalb der VNB und ihrer Tochtergesellschaft beweisen die besagten VNB und ihre Tochtergesellschaft in ihrem Vertraulichkeitsbericht, dass sämtliche dieser bewährten Praktiken effektiv angewandt werden.

Vorliegender Bericht deckt die Tätigkeiten von ORES Gen. auf dem gesamten von ORES Assets belieferten Gebiet sowohl für Elektrizität als auch für Erdgas.
Sein Zweck ist es, die Maßnahmen darzulegen, die im Laufe des Jahres 2025 getroffen bzw. fortgesetzt wurden, um die Vertraulichkeit der Informationen, von denen ORES Gen. bei der Ausführung der ihr anvertrauten Aufgaben Kenntnis erhält, noch besser zu gewährleisten.

[1] Vorläufige Schlussfolgerungen über die Kontrolle der Implementierung der Governance-Regeln – Schreiben der CWaPE vom 15. Oktober 2019.
[2] Artikel 3 der Statuten von ORES SC.

Da der Ethik-Ausschuss von ORES Gen. infolge der Abänderung der Dekrete über die Organisation der regionalen Strom- und Gasmärkte durch das Dekret vom 5. Mai 2022[3] aufgelöst wurde, ist vorliegender Bericht vom Verwaltungsrat von ORES Gen. in seiner Sitzung vom 18. März 2026 genehmigt worden.
Es ist außerdem darauf hinzuweisen, dass der Verwaltungsrat von ORES Gen. am 23. November 2022 Frau Audrey Réveillon - genauso wie ORES Assets und im Rahmen der gemeinsamen Unternehmensführung - als Vertraulichkeitskoordinatorin bezeichnet hat.

[3] Dekret zur Abänderung verschiedener Bestimmungen im Bereich der Energie im Rahmen der teilweisen Umsetzung der Richtlinien 2019/944/UE vom 5. Juni 2019 mit gemeinsamen Vorschriften für den Elektrizitätsbinnenmarkt und der Richtlinie 2018/2001/UE vom 11. Dezember 2018 zur Förderung der Nutzung von Energie aus erneuerbaren Quellen im Hinblick auf eine Anpassung der Tarifmethodik.

Abschnitt II – Verpflichtungen des Personals und der Mitglieder der Verwaltungsorgane in Sachen Datenvertraulichkeit

1. Verpflichtungen des Personals in Sachen Datenvertraulichkeit

Die Arbeitsverträge der Personalmitglieder enthalten Klauseln über Vertraulichkeitsverpflichtungen.
So verpflichten sich die Personalmitglieder in ihrem Arbeitsvertrag insbesondere dazu, die vertraulichen Daten nicht mitzuteilen, sie ausschließlich im Rahmen der Ausführung ihres Arbeitsvertrags zu nutzen, sie ohne vorherige schriftliche und ausdrückliche Genehmigung von ORES Gen. weder zu kopieren noch zu vervielfältigen, und alle Daten, die zum Zeitpunkt der Beendigung des Arbeitsvertrags noch in ihrem Besitz sind, unmittelbar nach Beendigung des Arbeitsvertrags an ORES Gen. zurückzugeben.
Darüber hinaus ist der für sämtliche Personalmitglieder geltende Verhaltenskodex überarbeitet worden. Dieser berufsethische Verhaltenskodex legt die Verpflichtungen des Personals in Sachen Datenschutz sowie ihre zwingende Erfüllung fest. Er gilt außerdem für die externen Partner (Berater, Subunternehmer, Zeitarbeitskräfte, …). Er ist fester Bestandteil der vertraglichen Dokumente, die jedem neu eingestellten Mitarbeiter überreicht werden.
Mit den externen Mitarbeitern und den Zeitarbeitskräften werden ebenfalls entsprechende Vertraulichkeitsabkommen unterzeichnet.
Alle diese Klauseln sind überarbeitet und inhaltlich im Einklang mit den Standards nach ISO 27001 gebracht worden.

Gemäß der Datenschutz-Grundverordnung (im Folgenden kurz „DSGVO“ genannt) hat ORES Gen. eine Reihe von Prozessen eingeführt und die Aufgaben und Verantwortungen jedes Einzelnen beschrieben. ORES Gen. ist darüber hinaus stets bemüht, die Anwendung der DSGVO-Prinzipien zu verbessern und sein Personal dafür zu sensibilisieren.
So wurde eine Erklärung zu den allgemeinen politischen Richtlinien verfasst und im Jahr 2019 betriebsintern veröffentlicht. Sie informiert das Personal von ORES Gen. über die Leitlinien, die bezüglich der DSGVO für das Unternehmen Pflicht sind, und wird vom Direktionsausschuss von ORES Gen. regelmäßig revidiert. Die letzte Aktualisierung erfolgte im Jahr 2024.
Bei jeder Direktion sind Mitarbeiter ausgebildet worden, um den Datenschutzbeauftragten (im Folgenden kurz „DPO" für „*Data Protection Officer*" genannt) auf Basisebene zu unterstützen.

Konkret umfasst die Sensibilisierung des Personals:

- die Bereitstellung eines berufsethischen Verhaltenskodex mit den Verpflichtungen in Sachen Datenschutz für das gesamte Personal von ORES Gen. und die externen Partner (Berater, Subunternehmer, Zeitarbeitskräfte, …);
- die Erteilung von Basisinformationen über die Verpflichtungen in Sachen Vertraulichkeit durch die Kenntnisnahme und Unterzeichnung einer Vertraulichkeitsklausel bei der Einstellung jedes Mitarbeiters;

- die Unterzeichnung einer Vertraulichkeits- und Geheimhaltungsvereinbarung bei der Überreichung des mobilen IT-Materials durch die Direktion IT;
- die Auferlegung einer Reihe von Verpflichtungen in Sachen Vertraulichkeit durch die Arbeitsordnung;
- die Verpflichtung der neuen Arbeitnehmer von ORES zur Einhaltung der Charta des IT-Systems, die den Rahmen für die Nutzung der Telekommunikationsmittel durch die Mitarbeiter festlegt;
- die sofortige Überreichung eines Willkommenspakets bei jedem Neuzugang, das auch das Thema Cybersicherheit umfasst;
- die Bereitstellung einer Video-Serie zur Veranschaulichung konkreter Situationen, in denen die Akteure im Unternehmen mit Sicherheitsproblemen konfrontiert werden. Dabei wird abschließend die korrekte Verhaltensweise erläutert, die in der jeweiligen Situation erforderlich ist. Alle zwei Monate werden zwei Folgen ausgestrahlt;
- die Einrichtung einer SharePoint-Webseite über die Informationssicherheit, auf der die einschlägigen ISO-27001-konformen Dokumente (Politiken, Standards, Prozesse, Best Practices) zur Verfügung stehen;
- ein obligatorisches *E-Learning* über die DSGVO und diverse *E-Learning*-Module zur Informationssicherheit, die für sämtliche Mitarbeiter eingerichtet worden sind. Diese Ausbildungen sind für alle Mitarbeiter von ORES sowie jeden Neuzugang Pflicht. Diese Mitteilungen werden anschließend durch Sensibilisierungskampagnen über verschiedene Sicherheitsaspekte ständig unterstützt, und zwar je nach dem ermittelten Kenntnisstand der Mitarbeiter von ORES sowie den Hauptrisiken für unsere Daten. Bestimmte Kampagnen betreffen die Sensibilisierung des Personals von ORES für das Phishing-Risiko;
- die Schaffung eines spezifischen Zusammenarbeitsbereichs für die DSGVO, der sämtlichen Mitarbeitern zur Verfügung steht, um den Zugang zu den sachdienlichen Informationen und den anzuwendenden Prozeduren zu erleichtern, sobald personenbezogene Daten im Spiel sind.

Zur Erinnerung: Die oben genannten Informationen waren bereits Gegenstand eines Berichts der CWaPE im Rahmen ihrer Überprüfung der Implementierung der Regeln der Unternehmensführung.
Die CWaPE hat ORES gegenüber am 6. Dezember 2019 bestätigt, dass keine Empfehlung bezüglich der Verpflichtungen des Personals in Sachen Datenvertraulichkeit für ORES Gen. formuliert wurde.

2. Verpflichtungen der Mitglieder der Verwaltungsorgane in Sachen Datenvertraulichkeit

Neben der allgemeinen Schweigepflicht, die jedem Verwaltungsratsmitglied eines Unternehmens obliegt, wird den Verwaltungsratsmitgliedern von ORES Assets (dem VNB), jedoch auch von ORES Gen. und Comnexio (den Tochtergesellschaften), ihre Vertraulichkeitsverpflichtung bewusst gemacht, und zwar durch die intern eingeführten und angewandten Regeln der Unternehmensführung (im vorliegenden Fall durch die Geschäftsordnung von ORES Assets und die Chartas zur Unternehmensführung von ORES Gen. und Comnexio, die zudem auf den Webseiten eingesehen werden können).

Darüber hinaus ist der berufsethische Verhaltenskodex den Mitgliedern der Verwaltungsräte von ORES Assets und ORES Gen. mitgeteilt worden.

Die Verwaltungsratsmitglieder von ORES Assets, ORES Gen. und Comnexio haben sich durch Unterzeichnung einer Erklärung auf Ehrenwort ebenfalls einzeln dazu verpflichtet, die berufsethischen Regeln einzuhalten, insbesondere in Sachen Interessenkonflikte, Nutzung von Insider-Informationen, Loyalität, Diskretion und verantwortungsvollem Umgang mit öffentlichen Geldern, gemäß Artikel L1532-1, §1 des Kodex für lokale Demokratie und Dezentralisierung.

Darüber hinaus haben die Verwaltungsratsmitglieder von ORES Assets und ORES Gen. einen Verhaltenskodex MAR[4] verabschiedet und einzeln eine Erklärung in ihrer Eigenschaft als Insider unterzeichnet.

[4] Europäische Verordnung „Marktmissbrauch“ zur Verbesserung der Integrität der Märkte und des Investorenschutzes.

Abschnitt III – Sicherheitsmaßnahmen für den Zugriff des Personals auf die personenbezogenen und kommerziellen Daten

Wenn ORES Gen. personenbezogene Daten in Verbindung mit ihrer Kundschaft verarbeitet, wird beim Personal, bei den Subunternehmern und den nachfolgenden Subunternehmern sowie im Bereich der IT-Sicherheit alles darangesetzt, die Vertraulichkeit der persönlichen und kommerziellen Informationen zu wahren, die ihr zur Verfügung gestellt werden. Die persönlichen Daten, die bei den verschiedenen Ansprechpartnern über die Netznutzer gesammelt werden, beschränken sich auf die Informationen, die für die Ausführung der Arbeiten im Zusammenhang mit den berechtigten Aufgaben von ORES erforderlich sind: Anschlüsse, Planarbeiten an Zähleranlagen, GWV, …

ORES hat von Beginn an Datenschutzverfahren nach dem Prinzip „*Privacy by design*“ und „*Security by design*“ eingerichtet, damit die Aspekte in Verbindung mit dem Schutz der personenbezogenen Daten seiner Kunden bereits beim Start neuer Projekte oder bei Abänderung der bestehenden Verarbeitungsweisen berücksichtigt werden.

Parallel dazu führt ORES Gen. für jede geplante neue Verarbeitung und jede Abänderung in den Verfahren DSGVO-Analysen durch, die Vorabfragebögen genannt werden. Darüber hinaus werden Datenschutz-Folgenabschätzungen (DPIA - *Data Protection Impact Assessments*) für jede neue Verarbeitung durchgeführt, die „*ein hohes Risiko für die Rechte und Freiheiten der natürlichen Personen*“ darstellen kann. Der Aspekt des Zugriffs auf die personenbezogenen Daten wird bei diesen Übungen bewertet. Außerdem werden Sicherheitsrisikoanalysen für die neuen Geschäftsprozesse durchgeführt. Die bestehenden Geschäftsprozesse werden alle drei Jahre in Sachen Risikoanalyse der Informationssicherheit überarbeitet.

Folgende technische und organisatorische Maßnahmen werden angewandt:

- Das Management der Zugangsberechtigungen für unsere Computeranwendungen wird über das Tool „*SAP Identity Management*“ zentralisiert und automatisiert (Beispiele: SAP: Lopex, procli; Active directory: Mercure, Nationalregister; Oracle: netgis).
- Die für das Zugangsmanagement angewandte Methodologie ist die sogenannte rollenbasierte Zugriffskontrolle, die von ORES Gen. durch die Prinzipien der geringsten Privilegien („*least privilege*“) und der Kenntnis nur bei Bedarf („*need to know*“) vervollständigt wird.
- Die privilegierten Zugriffe sind Gegenstand eines spezifischen Genehmigungsverfahrens.
- Der Lebenszyklus unserer IT-Identitäten richtet sich seinerseits automatisch nach dem Personalmanagement.
- Die Zugriffsrechte pro Tätigkeitsbereich werden von den HR und den Managern jedes Dienst validiert.
- Die Lastenhefte für die neuen Softwares verweisen spezifisch auf die obligatorische Integration in unser System zum Management der Identitäten und IT-Zugriffsrechte.

- Der Zugriff auf das Nationalregister wird nur dem betriebsinternen Personal nach Unterzeichnung eines Dokuments gewährt, in dem der Grund für diesen Zugriff erläutert wird. Dieses Dokument wird vom Vorgesetzten für gültig erklärt und der Direktion HR übermittelt, um der Personalakte des Mitarbeiters beigefügt zu werden. Die Liste der Zugriffe wird alle sechs Monate von den Managern geprüft. Es wird ein Register über die Abfragen des Nationalregisters geführt.
- Für die Passwörter gibt es sichere digitale Safes.

Im April 2024 ist der Dienst Information Office-Sicherheit zudem umstrukturiert worden, um sämtliche Sicherheitskompetenzen dem Chief Information Security Officer (CISO) von ORES zuzuteilen.
Dabei sind drei Teams gebildet worden:

- das Team Steuerung, Risikomanagement und Regelkonformität: Es ist für die Weiterentwicklung der Politiken und Standards bezüglich der Informationssicherheit im Einklang mit der Norm ISO 27001 zuständig;
- das Team Cyberabwehr: Es überwacht die IT-Tätigkeiten durch Analyse der Logs von verschiedenen Bestandteilen (*Firewalls*, WAF, Virenschutz usw.). ORES hat außerdem einen Vertrag für das 24/7-Monitoring der Informationssicherheit abgeschlossen.
- das Team *Identitäts- und Zugriffsmanagement*: Es verwaltet den gesamten Lebenszyklus eines Nutzers des Informationssystems von ORES (Anlegung des Nutzers, Vergabe der Zugriffsrechte und Löschung).

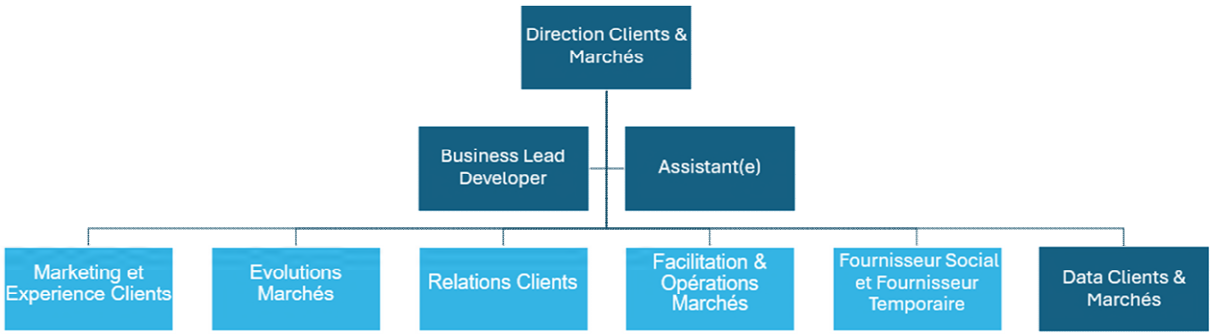
Insgesamt sollte betont werden, dass ORES Assets aufgrund des Gesetzes vom 7. April 2019 über die Schaffung eines Rahmens für die Sicherheit der gemeinnützigen Netze und Informationssysteme zugunsten der öffentlichen Sicherheit (im Folgenden kurz „NIS" genannt) am 1. November 2022 als Betreiber wesentlicher Dienstleistungen benannt worden ist. ORES Assets ist somit ein wesentliches Unternehmen im Sinne der Regelungen zu NIS 2[5]. Dementsprechend hat ORES für den FÖD Wirtschaft und das Zentrum für Cybersicherheit Belgien (ZCB) ein beschreibendes Dokument über die Systeme verfasst, die seine wesentlichen Dienstleistungen unterstützen.
ORES hat im März 2025 die Zertifizierung nach ISO 27001 erhalten.

[5] Regelungen zu NIS 2: Richtlinie (EU) 2022/2555 des Europäischen Parlaments und des Rates vom 14. Dezember 2022 über Maßnahmen für ein hohes gemeinsames Cybersicherheitsniveau in der Union, zur Änderung der Verordnung (EU) Nr. 910/2014 und der Richtlinie (EU) 2018/1972 sowie zur Aufhebung der Richtlinie (EU) 2016/1148 (NIS-2-Richtlinie) und belgisches Gesetz vom 26. April 2024 über die Schaffung eines Rahmens für die Cybersicherheit der gemeinnützigen Netze und Informationssysteme zugunsten der öffentlichen Sicherheit.

Abschnitt IV – Sicherheitsmaßnahmen bezüglich des Zugriffs der Energieversorger und der Kunden auf die vertraulichen Daten

Die Direktion Kunden & Märkte (Clients & Marchés) setzt sich aus mehreren Teams zusammen, die sich mit den Bereichen „*Define*“ bzw. „*Run*“ befassen.

Hier ein Schema der verschiedenen Dienste:



1. Die betroffenen Dienste von ORES Gen.

Der Dienst *Facilitation & Marktprozesse* (Facilitation & Opérations Marchés) ist Teil der Direktion Kunden & Märkte (Clients & Marchés). Diese Direktion managt sämtliche Prozesse in Verbindung mit den liberalisierten Märkten (*assets, structure, measure, settle, rectification*), den Daten und der Flexibilität. Die Gemeinwohlverpflichtungen mit sozialem Charakter werden ebenfalls innerhalb dieser Direktion verwaltet.
Das Team *Berichtigung Marktanomalien* des Dienstes *Facilitation & Marktprozesse* verwaltet das föderale Zugangsregister (CMS Atrias, Central Market System) für das Portfolio von ORES sowie die Kontakte mit den Energieversorgern auf operativer Ebene.

Das CMS ist die föderale IT-Plattform zur Erleichterung des Austauschs und der Bearbeitung der Informationen unter allen Akteuren auf dem belgischen Energiemarkt auf Basis des MIG (*Message Implementation Guide*).

Jede Zugriffsstelle (headpoint) ist darin mit seinem EAN-Code aufgelistet. Anhand dieses Codes findet man hauptsächlich die Daten des Kunden, seines Energieversorgers sowie weitere zweckdienliche Informationen. Diese Zugriffsstelle ist auch mit den sensiblen Dienstleistungen und Konfigurationen je nach Art der Anlage verbunden (für einen Prosumentenkunden mit einem Smart Meter findet man beispielsweise die Ausgleichsleistung und die Tages-/Nachtkonfigurationen, den Einheitstarif oder die anreizschaffende Tarifgestaltung).
Da das CMS-Register bei ORES über einen großen Orchestrator (BPMS, *Business Process Management System*) mit der MDM/Mercure (Datenbank zur Erfassung der

Verbrauchswerte jeder Versorgungsstelle) sowie mit dem Back-End SAP ISU (dieses umfasst sämtliche technische Informationen über eine Versorgungsstelle) vernetzt ist, liefert es ein vollständiges Bild des Marktes.

Die Ablesung der elektromechanischen Zähler erfolgt von nun an innerhalb des Dienstes *Essentiels Clients*.

Für die Smart Meter ist das Team *Überwachung der Kommunikationsketten* des Dienstes *Facilitation & Marktprozesse* für die Kontrolle der guten Funktionsweise der Kommunikation und der Mitteilung der Zählerstände zuständig. ORES hat auch eine Plattform zur automatisierten Zählerablesung eingerichtet worden. Dabei handelt es sich um COMET, einer Software zur Sammlung der Daten der Smart Meter. Prism, eine andere Plattform, verwaltet die Teleoperationen mit dem *Head-End System* (HES). Sie ist einerseits mit dem MDM/Mercure und andererseits mit der Kommunikationskette der Zähler verbunden. Die Plattform MARCO verwaltet ihrerseits den Austausch mit der von Atrias gemanagten föderalen Vorauszahlungsplattform.

Die Teams *Validierungen* (B2C und B2B) innerhalb des Dienstes *Facilitation & Marktprozesse* prüfen die Kohärenz dieser Ablesungen angesichts der statistischen Daten, chronologischen Verbrauchsübersichten sowie klimabezogenen Kriterien.

Das Team *Überwachung der Querschnittsprozesse* ist für die Blockierungen zuständig, die transversal auftreten. Sonstige Fälle werden von anderen Teams gemanagt, die ebenfalls zum Dienst *Facilitation & Marktprozesse* gehören: *Berichtigungen* für die von Atrias beim SRME eingereichten Beschwerden, *Marktkontaktaufnahme* für die Anträge der Energieversorger und Kunden.
Das Team *Verwaltung der Vorauszahlungen* ist für die Interaktionen mit den Kunden und der Vorauszahlungsplattform zuständig.

Das Team *Regularisierung von Prozessen* innerhalb des Dienstes *Facilitation & Marktprozesse* hat außerdem Zugriff auf die im CMS enthaltenen Daten, um die von den Energieversorgern eingeleiteten Prozesse *Drop, End-Of-Contract, Initiate Leaving Customer* (ILC) sowie die Anbringung von Vorauszahlungszählern zu vollenden. Neben der Sendung von Schreiben kontaktieren die Mitarbeiter auch manchmal die Kunden (beispielsweise für die Prüfung eines ILC-Dossiers) und/oder die kommerziellen Energieversorger (beispielsweise für eine abgesicherte Annullierung).

Schließlich hat unser *Kontaktzentrum* Comnexio als Tochtergesellschaft von ORES Assets ebenfalls Zugriff auf die Daten des CMS und die Datenbank Mercure, um die telefonischen Anfragen der Kunden an vorderster Front zu beantworten.

Das Management des Zugriffs auf die Softwares vonseiten dieser verschiedenen Mitarbeiter sowie die Art und Weise, wie die Informationen den Kunden und/oder den kommerziellen Energieversorgern mitgeteilt werden, sind im folgenden Punkt erläutert.

2. Eingeleitete spezifische Maßnahmen

- **Zugangsregister (CMS)**

  Die IT-Infrastruktur ist abgesichert; der Zugriff auf die Software ist individuell festgelegt und den Mitgliedern der Teams innerhalb des Dienstes *Facilitation & Marktprozesse* unter anderem über ein Reporting-Tool *Business Object* (BO) vorbehalten (Lese- und Schreibrechte).
  Jeder neue Zugriffsantrag bedarf der Genehmigung des Anwenderprogramms *Owner Structuring*. Dem Zugangsverwalter sind die spezifischen Zugriffe für jede Person bekannt, und zwar über die Berufsmerkblätter HR, die zusätzlich zur Aufgabenbeschreibung auch die Liste der Zugriffsrechte jeder Funktion für die Anwenderprogramme und Transaktionen enthalten.

  Die Energieversorger haben auch Zugang zur Software (Dateneinsicht sowie Einleitung/Annullierung der Marktprozesse), jedoch ausschließlich über das CMS-Portal. Ein Energieversorger kann also nur auf die Daten der Kunden zugreifen, für die er einen im Zugangsregister registrierten Vertrag hat. Die eingesehenen Kundendaten sind diejenigen, die vom Energieversorger selbst über die Marktmitteilungen an den VNB übermittelt werden.
  Er kann ebenfalls über technische Daten im Zusammenhang mit den Zugriffsstellen verfügen, für die er als Energieversorger anerkannt ist. Diese Daten werden nur für die jeweilige Vertragsdauer vom VNB mitgeteilt.
  Er hat also keinen Zugriff auf Daten eines Kunden, der aktiver Abnehmer bei einem anderen Energieversorger ist. Die Sicherheits- und Zugangsvorschriften der Software-Anwendung regeln diese beschränkte Bereitstellung von Informationen bezüglich der Zugriffsstelle. Neben diesen Datenschutzmaßnahmen innerhalb der Software-Anwendung werden die Teams *Berichtigung Marktanomalien, Regularisierung von Prozessen* und *Märkte – Erfassung der Interaktionen* so geschult, dass sie Auskünfte über die Zugriffsstelle nur dem für diese Zugriffsstelle anerkannten Versorger per E-Mail oder Telefon erteilen.

  Die Teams *Berichtigung Marktanomalien, Regularisierung von Prozessen, Marktkontaktaufnahme* sowie *Validierungen und Berichtigungen* erteilen Auskünfte per Telefon, Postschreiben oder E-Mail ausschließlich an den Kunden (oder an einen seiner Beauftragten), der für die Zugriffsstelle anerkannt ist, und zwar nur während des entsprechenden Nutzungszeitraums dieses Kunden, der seine Zählernummer zur Überprüfung mitzuteilen hat. Der Endabnehmer hat keinen Zugang zur eigentlichen Software. Falls ein Kunde den VNB fragt, welcher Energieversorger mit der Zugriffsstelle verbunden ist, wird ihm die Antwort per Postschreiben an die Installationsadresse geschickt.

  Das vom unserem *Kontaktzentrum* Comnexio angewandte Verfahren ist ebenfalls genau festgelegt. Falls ein kommerzieller Energieversorger die Frage stellt, wird er automatisch an das Portal des CMS weitergeleitet, da es über die entsprechenden Zugriffsrechte verfügt.
  Handelt es sich um einen Kunden, so kann dieser seinen EAN-Code nur nach Überprüfung seiner Zählernummer erfahren. Die Information wird ihm anschließend nicht mündlich mitgeteilt, sondern per SMS an die Handynummer geschickt, die der Kunde uns angeben muss. Falls der Kunde seine Anfrage schriftlich stellt oder über keine Handynummer verfügt, wird ihm die Information

per Postschreiben an seine namentliche Anschrift übermittelt. Handelt es sich um eine Anfrage für mehr als zwei EAN-Codes, so wird diese erfasst und per Mail oder Postschreiben bearbeitet.
Diese Telefonate und Mitteilungen werden im System aufgezeichnet und verfolgt.

Der VNB teilt auch den ÖSHZ Kundeninformationen mit. Das ÖSHZ verfügt über eine spezifische Kontaktnummer für die Anfrage von Informationen über seine Anspruchsberechtigten, für die es eine ständige Vollmacht hat (Fortschrittsstand eines Dossiers, aktiver Energieversorger an der Zugriffsstelle, chronologische Verbrauchsübersicht, …). Die ÖSHZ werden gebeten, diese Rufnummer nie weiterzugeben.

Für alle Transaktionen des Energiemarktes und Datenübermittlungen ist eine Rückverfolgbarkeit möglich.

Abschließend ist noch Folgendes zu erwähnen: Falls ein Energieversorger ein Abgangsszenario (auch *Drop* genannt) einführt oder einen Vorauszahlungszähler anbringt, - was voraussetzt, dass der Kunde Zahlungsschwierigkeiten hat -, erhält ein anderer Energieversorger, der einen Versorgerwechsel (auch *Switch* genannt) an der Zugriffsstelle einleitet, nicht als Rückmeldung, dass das Szenario eines Drops oder der Anbringung eines Vorauszahlungszählers läuft. So kann der neue Versorger nicht Kenntnis der Zahlungsschwierigkeiten des Kunden nehmen. Es sei darauf hingewiesen, dass ein Stromversorger infolge des im Rahmen des Dekrets (oft „Friedensrichter-Dekret“ genannt) neu eingeführten Verfahrens bei einer Nichtzahlung jederzeit einen Switch-Antrag (Versorgerwechsel) für einen EAN-Code stellen kann, der Gegenstand der Beantragung eines Vorauszahlungszählers ist, ohne dass ihm eine Ablehnung zugeschickt wird.

- **Mercure-System**

Die IT-Infrastruktur ist geschützt und der Zugang zur Software ist individuell festgelegt und den Mitgliedern des Dienstes *Facilitation & Marktprozesse* im Abänderungsmodus vorbehalten.
Jeder neue Zugriffsantrag (mit Lese- oder Abänderungsberechtigung) ist dem Programm *Owner Measure* zur Genehmigung zu unterbreiten, das je nach Tätigkeitsbereich und Funktion laut HR über die Zugriffsrechte für die Software verfügt, für die dieses Programm *Owner* zuständig ist.

Das *Kontaktzentrum* Comnexio hat zwar auch Zugang zur Software, jedoch nur über eine passwortgeschützte Web-Schnittstelle. Die Zugänge zur Web-Schnittstelle werden ebenfalls vom Programm *Owner* genehmigt.

Die Sicherheits- und Zugangsvorschriften der Software-Anwendung regeln diese beschränkte Bereitstellung von Informationen bezüglich der Verbrauchswerte an der Zugriffsstelle.

Ein Kunde, der seine chronologische Verbrauchsübersicht erhalten möchte, kann diese über verschiedene Wege einsehen:

- über die Webseite von ORES (anhand seines EAN-Codes und seiner Zählernummer),
- über das Portal MyORES: Der Zugriff wird sicherheitstechnisch streng überwacht,
- über einen Antrag an einen der operativen Dienste.

Diese chronologische Verbrauchsübersicht kann an eine andere Person oder einen Energieversorger geschickt werden, sofern diese über eine vom Kunden der betreffenden Zugriffsstelle schriftlich erteilte und unterzeichnete Bevollmächtigung verfügen.
Für alle Transaktionen des Energiemarktes und Datenübermittlungen ist eine Rückverfolgbarkeit möglich.

Wenn der Kunde unser *Kontaktzentrum* Comnexio anruft, um seine chronologische Verbrauchsübersicht zu erhalten, wird je nach Fall folgende Prozedur angewandt:

- Handelt es sich um eine Fernablesung (außer Smart Meter), so muss der Kunde aufgefordert werden, seinen Antrag über die Webseite von ORES zu stellen. Er erhält dann einen chronologischen Überblick, der höchstens die letzten drei Jahre umfasst.
- Handelt es sich um eine jährliche oder monatliche Ablesung, so werden die Kundenberater zuerst daran erinnert, dass die Verbrauchsdaten persönliche Informationen sind. Falls ein Hauseigentümer die Verbrauchswerte seiner Mieter erfahren möchte, muss er Letztere direkt darum bitten.
- Handelt es sich um einen Smart Meter, so kann der Kunde seine chronologischen Verbrauchsübersichten auf dem ihm zur Verfügung stehenden Portal einsehen; sicherheitstechnisch werden also auch die Zugänge strikt überwacht.

Der Kunde wird anschließend aufgefordert, seinen Antrag auf unserer Webseite zu stellen; falls er dies jedoch nicht wünscht, wird der Antrag vom Berater bearbeitet und ein Schreiben mit dem chronologischen Überblick, der höchstens die letzten drei Jahre umfasst, an die Verbrauchsadresse geschickt.
Da die Kunden zu Beginn ihres Anrufs unmittelbar auf die Aufzeichnung des Telefongesprächs hingewiesen werden, können die für die Prozesse zuständigen Teams (*Process Owner*) die aufgezeichneten Telefonate im Nachhinein abhören, um die korrekte Anwendung der geltenden Regeln zu prüfen.

Die Zählerableser können die vor Ort aufgezeichneten Zählerstände über eine mobile Software eingeben, die durch eine persönliche Identifizierung anhand eines Benutzernamens und eines Passwortes ebenfalls abgesichert ist.

Schließlich können die Kunden im Rahmen der Zählerablesungen auf Wunsch Zugang zu einem Online-Bereich haben, um ihre Zählerstände mitzuteilen. Nach gesicherter Anmeldung kann der Kunde seine Schreiben für den Ablesungsantrag im Digitalformat erhalten. Diese Verfahren unterliegt sämtlichen Regeln der DSGVO und die Funktionalität wird bei jedem Kundenwechsel automatisch blockiert.

- **Das BPMS**

  Die befugten IT-Teams sind die Einzigen, die Zugang zum BPMS-Tool im Abänderungsmodus haben. Die Teams des Dienstes *Facilitation & Marktprozesse* können allerdings im Lesemodus darauf zurückgreifen, um Analysen durchzuführen. Die Zugriffe auf diese Software werden durch die Anwendung *Owner* auf Basis der IT-Berufsmerkblätter erteilt. Keine weiteren Teams brauchen den Zugriff auf diese Software.

- **Prism, HES, COMET und MARCO**

  Das HES ist nur für den externen Dienstleister zugänglich, der es zur Verfügung stellt.

  Prism ist im Lesemodus dem Team *Überwachung der Kommunikationsketten* sowie – wiederum auf Basis eines Berufsmerkblatts – dem Team *Verwaltung der Vorauszahlungen* (GDP) zugänglich, das die Aufladung der Smart Meter im Vorauszahlungsmodus (über das innerhalb von Atrias gehostete PPP-Tool) verwaltet.
  Die Teleoperationen von Prism laufen über das System SAP CS (bei ORES wird es Lopex genannt). Sämtliche Zugriffe auf die Software Lopex werden auf Basis der Berufsmerkblätter der HR kontrolliert.
  COMET ist für die Teams *Validierungen B2C* zugänglich.
  Zugriff auf MARCO haben die Teams *Validierung B2C* und *Verwaltung der Vorauszahlungen*.

- **ORES und die künstliche Intelligenz**

  Bei ORES laufen zurzeit Überlegungen, wie die künstliche Intelligenz (K.I.) in die Tätigkeiten des Unternehmens integriert werden kann, um insbesondere die Energiewende zu unterstützen und bestimmte immer wiederkehrende Aufgaben zu optimieren.

  ORES ist sich der Herausforderungen im Zusammenhang mit der Verwendung dieser Technologien durchaus bewusst und daher bemüht, ihre Implementierung durch eine gewissenhafte interne Unternehmensführung zu regeln, die die geltenden Vorschriften (insbesondere die DSGVO und den *Artificial Intelligence Act*) einhält. Dieser gesetzliche Rahmen garantiert eine ethische und abgesicherte Nutzung der K.I., bei der Innovation und Schutz der Rechte des Einzelnen in Einklang gebracht werden.

Abschnitt V – Sicherheitsmaßnahmen bezüglich des Zugriffs der Subunternehmer auf die vertraulichen Daten

Technische und organisatorische Maßnahmen

Es wurden verschiedene Sicherheitsmaßnahmen eingeleitet, die den bestehenden Risiken angepasst sind, und zwar unter anderem:

- die Nutzung eines einmaligen Log-ins für die Unternehmer und die Einschränkung der Zugangsrechte zu den Baustellen,
- die Pseudonymisierung der Daten, die den für ORES arbeitenden IT-Entwicklungsfirmen zugänglich gemacht werden,
- die Trennung der Zugriffe auf die Produktions- und Testdaten,
- die Einschränkung der Zugriffe auf die Produktionsdaten,
- die Einschränkung der Zugriffe auf die Daten der externen Lieferanten aus Wartungsgründen,
- das Management der Verwaltungs- und Supportkonten der externen Dienstleister über ein digitales Safe-System (CyberArk - zurzeit im Rollout),
- die Durchführung von Audits und Penetrationstests,
- die Minimierung der mitgeteilten Daten,
- die Einführung eines berufsethischen Verhaltenskodex, der auch für die externen Mitarbeiter gilt.

Vertragliche Maßnahmen

Bei Vergabe von Aufträgen oder Abschluss von Verträgen mit seinen Partnern fügt ORES systematisch Klauseln der Datenschutz-Grundverordnung ein, die sämtliche Aspekte des Artikels 28 der DSGVO präzisieren: Dauer, Umfang, Ziel, Bearbeitungsanweisungen, Vorabgenehmigung beim Einsatz eines Subunternehmers, Bereitstellung der gesamten Dokumentation zur Konformitätsbestätigung, sofortige Mitteilung jeder Verletzung des Datenschutzes.
Falls der Vertragsabschluss nicht in den Anwendungsbereich der Vorschriften über die öffentlichen Aufträge fällt, wird ein Auftragsverarbeitungsvertrag (*data processing agreement)* unter den Partnern vereinbart.

Beim Austausch von Daten außerhalb der Europäischen Union werden gleichwertige Datenschutzmaßnahmen getroffen und vorzugsweise Muster-Vertragsklauseln angewandt.

Umfangreichere Vertraulichkeitsklauseln sind in den Verträgen ebenfalls vorgesehen.

Abschnitt VI – Rückverfolgbarkeit als Vertraulichkeitsgarantie

ORES nutzt die SAP-Lösungen und hat sich für eine weitergehende Parametrierung der Rückverfolgbarkeit als die von SAP empfohlene Standard-Parametrierung entschieden. Zur Rückverfolgbarkeit der Benutzertätigkeiten und der technischen Konten im Zusammenhang mit Drittlösungen wird Folgendes in der SAP-Datenbank von OES gespeichert:

- eine aggregierte Übersicht über die tägliche Nutzung während 31 Tagen,
- eine aggregierte Übersicht über die wöchentliche Nutzung während 20 Wochen,
- eine aggregierte Übersicht über die monatliche Nutzung während 20 Monaten.

Es sei darauf hingewiesen, dass SAP zwar die Transaktionen verfolgt, die eine Person in die Wege geleitet hat, jedoch keine Daten, deren Einsicht bei der jeweiligen Transaktion möglich war. Der Kontext wird nicht gespeichert. Die Aggregierung betrifft den Ausführungszeitpunkt der Transaktion.

Bei der Datenübermittlung per E-Mail verfolgt das SAP-System von ORES sämtliche Aktivitäten innerhalb von gesicherten Bereichen, deren Zugang kontrolliert wird.

ORES ist verantwortlich für die Dienstleistungen im Zusammenhang mit der Infrastruktur der WIFI-, LAN- und WAN-Netze sowie für die Telefonie. Folgende Aspekte gehören zum Katalog der Netzdienstleistungen von ORES:

- Zugriffsnetz für die Endnutzer (25+ Gebäude),
- Schalter und Router,
- WLAN,
- DNS / DHCP / IPAM,
- Kontrolle des Netzzugriffs (801.1X),
- Monitoring und operatives Management.

Dies verdeutlicht die Fähigkeiten und Mittel von ORES in Sachen Zugangs- und Tätigkeitskontrollen auf dem IT-Netz. Das OT-Netz (*Operational Technology*) ist seinerseits Eigentum von ORES und wird auch vom Unternehmen verwaltet. Ebenso hat ORES die Kontrolle über alle Dienstleistungen und Managementinstrumente seiner Benutzergeräte (Arbeitsplatz, Mobilitätstools).

ORES hat 2024 ein Tool eingeführt, womit die Nutzer der Office-Programme von Microsoft die Dokumente kennzeichnen können. Dabei sind vier Kennzeichnungsniveaus festgelegt worden:

- C1 – ÖFFENTLICHE Information: Die Information ist öffentlich und kann jeder beliebigen Person innerhalb und außerhalb von ORES übermittelt werden;
- C2 – INTERNE Information: Die Information kann von allen Personen, die bei ORES arbeiten, also von den internen Mitarbeitern sowie den (unter Vertrag stehenden) externen Mitarbeitern und eventuell von bestimmten Partnern zur Kenntnis genommen werden;
- C3 – EINGESCHRÄNKTE Information: Die Information ist ausschließlich einem begrenzten Personenkreis (z. B. einem Team, einem Dienst oder einer Direktion) bekannt bzw. zugänglich;

- C4 – VERTRAULICHE Information: Die Information ist ausschließlich einigen namentlich bezeichneten Personen bekannt bzw. zugänglich.

ORES hat 2025 ein Tool (SIEM) für das Einlesen der Sicherheitslogs der Assets eingeführt und einen Vertrag mit einer externen Firma (SOC) für das 24/7-Monitoring seiner Sicherheitstätigkeiten geschlossen. Bei Erkennung eines Angriffs wird der 24/7-Bereitschaftsdienst von ORES alarmiert, der sich dann um den Vorfall kümmert.

Abschnitt VII – Gemeinsame Nutzung der IT-Systeme und -Infrastrukturen mit anderen Unternehmen

Auf seine Aufgabe zu erfüllen, teilt ORES bestimmte IT-Systeme und –Infrastrukturen mit seinen Partnern. Dabei wird ganz besonders dafür gesorgt, dass ständig solide Sicherheitsmaßnahmen zur Gewährleistung der Trennung, Vertraulichkeit und Integrität der Daten von ORES in diesen gemeinsam genutzten Systemen und Infrastrukturen angewandt werden.

Die Lenkung der IT-Sicherheit bei ORES richtet sich nach der Norm ISO 27001. Die Abtrennung der gemeinsam genutzten Daten beruht auf folgende Prinzipien:

- die Erteilung des „geringsten Privilegs“ („*least privilege*“): Standardgemäß dürffen einem Nutzer nur die Zugriffsrechte erteilt werden, die für die Ausführung seiner Arbeit unbedingt erforderlich sind,
- die „Funktionstrennung“ („*segregation of duties*“): Eine einzige Person darf keine vollständige Kontrolle über einen kritischen/sensiblen Prozess bzw. keinen vollständigen Zugang dazu haben,
- das „*Need-to-know*“-Prinzip: Ein Nutzer darf eine Information nur einsehen, wenn dies aufgrund eines reellen Bedarfs des Tätigkeitsbereichs erforderlich ist. Mit anderen Worten: Die Verfügung über potenzielle Zugänge für den Umgang mit einer Information reicht als Grund für den Zugang zu dieser Information nicht aus.

In all diesen Fällen ist und bleibt ORES ausschließlich zuständig für die Verwaltung der Rechte für den Zugriff auf die Softwares seiner Tätigkeitsbereiche;

Im Folgenden werden die wichtigsten gemeinsamen Nutzungen der IT-Systeme und -Infrastrukturen erläutert:

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

  Das *Clearing*-System IMDMS wird mit Fluvius geteilt. Dieses System ermöglicht die Zentralisierung und Organisation der Geschäftsvorgänge auf dem Energiemarkt.
  Im aktuellen System hat Fluvius die Möglichkeit, sämtliche Daten einzusehen, um seine Aufgabe als Verwalter der Clearinggesellschaft (Zuordnung, Abgleich, *Infeed*).
  Eine Revision der Zugangsrechte der Nutzer von ORES wurde durchgeführt, um die mögliche Bearbeitung der Daten von ORES einzuschränken. Beim Abgang eines Personalmitglieds von ORES wird sein Konto bei der Revision der Passwörter, die alle drei Monate stattfindet, automatisch blockiert.
  Fluvius löscht seinerseits regelmäßig die blockierten Konten.
  Es ist festzuhalten, dass Atrias am 29. November 2021 die Aufgabe der Clearinggesellschaft übernommen hat.

- ENGIE IT (Anbieter von IT-Dienstleistungen)

  Wie für sämtliche IT-Dienstleister von ORES sind die Beziehungen mit ENGIE IT vertraglich festgelegt worden; sie enthalten Vertraulichkeits-, Sicherheits- und DSGVO-Klauseln. Der Zugang von ENGIE IT auf die Daten von ORES wird überwacht.

  Infolge ihres Schreibens von 28. März 2024, in dem die CWaPE die Annahmebedingungen für das Datum des Austritts aus ENGIE IT am 31. Dezember 2030 festlegt, hat ORES der Regulierungsinstanz regelmäßig über den Fortschrittsstand des Austrittsplans berichtet.
  So hat ORES ihr halbjährlich (im Juni und Dezember 2025) einen aktualisierten Austrittsplan per Postschreiben übermittelt.
  Die Übernahme der IT-Dienstleistungen durch ORES sowie die entsprechenden Bedingungen sind der CWaPE dargelegt worden.
  Schließlich ist der angestrebte Endtermin für die von ENGIE IT erbrachten IT-Dienstleistungen in diesem Kontext auf den 31. Dezember 2027 festgelegt worden, da ein Abkommen mit ENGIE IT über die eventuelle Übernahme einiger restlichen Leistungen nach diesem Datum geschlossen wurde.

- Sonderfall: *Connect My Home*

  Die Initiative „*Connect My Home*“ bezeichnet die Realisierung von Synergien im Rahmen von Anschlussarbeiten bei Privatpersonen und vereint zurzeit folgende Betreibergesellschaften: ORES, RESA, die wallonische Wassergesellschaft SWDE, Proximus, Orange und Telenet.
  Um die Dienstleistung „*Connect My Home*“ in Anspruch nehmen zu können, melden sich die Kunden über ein einmaliges Portal an, dessen Management ORES anvertraut wurde. Auf vertraglicher und operativer Ebene wurde alles darangesetzt, um die Sicherheit und Vertraulichkeit der Daten der Privatpersonen sowie ihre Möglichkeiten der Ausübung ihrer Rechte laut der DSGVO strikt zu gewährleisten.

Abschnitt VIII – Rollout der Smart Meter

Um seiner Verpflichtung des Rollouts der neuen Zählertechnologie nachzukommen, hat ORES eine Arbeitsgemeinschaft mit anderen VNB (Fluvius, Sibelga und RESA) gebildet, um die Kosten umlegen und dem Bürger eine schnellere und kohärentere Lösung bieten zu können.

Es ist eine Lenkungsform eingerichtet worden, um die Einhaltung des Prinzips des Datenschutzes und der Datenvertraulichkeit bereits in die Planung mit einzubeziehen.

Die Smart Meter übermitteln die abgelesenen Zählerstände ein einziges Mal pro Tag an ORES (auch für die Innertagesdaten). Diese Zählerstände werden über einen Dienstleister übermittelt, dem die Identität der Kunden von ORES nicht bekannt ist.
Um den Schutz der so übermittelten Zählerdaten zu garantieren, sind diese vom Zähler bis zum IT-System von ORES durchgehend verschlüsselt. Außerdem werden spezifische Penetrationstests durchgeführt.

Die Implementierung der Smart Meter bei ORES erfolgt phasenweise. Seit 2020 werden Smart Meter bei Privatpersonen installiert. Außer für die Verwendung der Vorauszahlungsfunktion und die Auswechselung der Zähler aus messtechnischen Gründen zwingt ORES den Bürger auf keinen Fall zur Nutzung der Kommunikationsfunktion des neuen Zählers; für die Bürger, die dies ausdrücklich beantragen, werden die Zähler im Flugzeugmodus montiert. Laut der am 27. März 2024 abgeänderten Fassung des Dekrets zur Regelung des Rollouts der Smart Meter in der Wallonie, die am 24. April 2024 vom wallonischen Parlament genehmigt worden ist, sind bis zum 31. Dezember 2029 sämtliche Zugriffsstellen für Strom zu 100 % mit Smart Metern auszustatten.

Um dieses ehrgeizige Ziel zu erreichen, hat ORES das Projekt ACDC (Frz. „Accélération des Compteurs Communicants“) durch Weitervergabe sämtlicher Auswechselungsarbeiten (einschließlich der Kundenroute und somit auch der Terminvereinbarung) an Subunternehmer realisiert. Für dieses Projekt hat ORES eine Abschätzung der Auswirkungen auf die Daten sowie eine Sicherheitsrisikoanalyse veranlasst.

Hinsichtlich der Datenschutzprinzipien ergreift ORES folgende Maßnahmen:

- In der aktuellen Phase finden ausschließlich Datenverarbeitungen statt, deren Ziele mit der klassischen Aufgabe des VNB verbunden und den gesetzlichen Vorschriften vereinbar sind. Weitere Datenverarbeitungen sind in Zukunft vorgesehen. Diese werden auf einer ausdrücklichen, spezifischen und wissentlichen Vorabgenehmigung der Kunden beruhen.

- Prinzip der Transparenz und Recht auf Information
  Bei der ersten Terminvereinbarung für die Anbringung der neuen Zähler werden die Betreffenden bereits auf ihre Kommunikationsfunktion hingewiesen.
  Eine Infobroschüre ist bei der Anbringung der Zähler verfügbar. Auf einer Seite unserer Webseite[6] werden die Fragen in Sachen Datenschutz beantwortet. Die Mitarbeiter von ORES, die im Kontakt mit den Kunden sind, werden entsprechend ausgebildet. Unser Datenschutzbeauftragter (DPO) ist außerdem für alle Fragen in Verbindung mit dem Schutz der Privatsphäre und dem Datenschutz zuständig. Unsere Datenschutzrichtlinie ist im August 2025 aktualisiert worden.

- Minimierung, Qualität und Dauer der Datenspeicherung
  Nur die Daten werden gesammelt, die für die Ausführung der beschriebenen Aufgaben erforderlich sind.
  Bei der Speicherung werden die Daten wie die herkömmlichen Ablesungsdaten verarbeitet.

- Subunternehmer
  Gemäß Artikel 28 der DSGVO wird mit jedem unserer Partner ein Subunternehmervertrag geschlossen.

- Sicherheit
  Es wurden angemessene technische und organisatorische Maßnahmen eingeleitet, um den Kunden von ORES Datenschutz (Vertraulichkeit und Integrität) zu garantieren: Die Smart Meter sind Gegenstand einer Cybersicherheit-Überwachung, die den Aspekten im Zusammenhang mit dem Datenschutz und der Anwendung der geltenden Gesetze Rechnung trägt.

Die Sicherheitsrisiken absichtlicher An- und Eingriffe werden im Rahmen von Workshops nach der Methode EBIOS RM 2018 ermittelt, die eine Abschätzung der Sicherheitsrisiken der IT-Systeme ermöglicht (Betriebseinheiten und Schwachstellen, Angriffsmethoden und bedrohende Aspekte, wesentliche Elemente und Sicherheitsbedürfnisse, …) und deren Bearbeitung durch Spezifizierung der zu erfüllenden Sicherheitsanforderungen fördert.
Im Sinne einer kontinuierlichen Datenkontrolle sind 2025 Risikoanalysen (DSGVO und Sicherheit) bei der Aktualisierung der Prozesse in Verbindung mit der Kommunikationskette durchgeführt worden.

Es ist festzuhalten, dass drei Wasserversorgungsunternehmen, die auf dem flämischen Gebiet aktiv sind, inzwischen eine Arbeitsgemeinschaft gegründet haben; dies hat zur Folge, dass das Datenerfassungssystem (HES) nun von sieben Gesellschaft geteilt wird (Fluvius, Resa, Sibelga, Pidpa, De Watergroep und Farys).

Die von den Smart Metern gesammelten Daten sind nicht zur Speicherung im HES bestimmt. Es wurden risikoadäquate Sicherheitsmaßnahmen eingeleitet. So gelten beispielsweise „logische“ Trennungsregeln, um einen unsachgemäßen Datenzugang

[6] https://www.ores.be/particulier/compteur-communicant-fonctionnement - Rubrik Fragen zum Thema „Was macht ORES mit meinen Daten?“..

vonseiten der anderen Betreibergesellschaften sowie ein schlechtes Routing der Daten zu verhindern.
Sollte ORES in Zukunft eine Aufgabe im Rahmen der Datenverwaltung der Wasserverbrauchszähler (beispielsweise die Datenübermittlung über die Stromzähler) zugeteilt werden, so würden selbstverständlich entsprechende Maßnahmen eingeleitet, um die Anforderungen der Aufgabentrennung zu erfüllen.