BERICHT Nr.21
DES VERTRAULICHKEITSKOORDINATORS VON ORES ASSETS

Artikel 17, Absatz 2 des Erlasses vom 21. März 2002 bezüglich der Stromversorgungslizenz und Artikel 7, Absatz 2 des Erlasses vom 16. Oktober 2003 bezüglich der Betreiber von Gasnetzen

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 Konzern ORES 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 der 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 das operative und tägliche Management der Tätigkeiten von ORES Assets[2], einschließlich einerseits der Erfüllung der strategischen und vertraulichen Aufgaben und andererseits der Vertretung von ORES Assets im Rahmen dieses Managements dem Unternehmen ORES Gen. anvertraut wird.
Die Tätigkeiten des Kontaktcenters wurden ihrerseits ab dem 1. Juni 2019 Comnexio anvertraut.
Die Modalitäten dieses Managements vonseiten der besagten Tochtergesellschaften sind in Anhang 6 und 7 der Statuten von ORES Assets definiert und werden für jede zusätzliche Entscheidung vom Verwaltungsrat bestimmt.
Aufgrund der Besonderheit der gesellschaftlichen Struktur und der operativen Realität von ORES Assets und ORES Gen., wobei ORES Assets der VNB und ORES Gen.[3] die Betreibergesellschaft ist, ist der Inhalt ihres jeweiligen Berichts fast identisch.

Artikel 17 des Erlasses vom 21. März 2002 bezüglich der Netzbetreiber, abgeändert durch den Erlass vom 6. Dezember 2018, schreibt Folgendes vor: *„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.*
Der Netzbetreiber bezeichnet unter seinen Personalmitgliedern eine Person, die insbesondere mit der Koordinierung der in Anwendung des vorliegenden Artikels ergriffenen Maßnahmen beauftragt wird. Die CWaPE kann jederzeit von dieser Person einen Bericht über die Anwendung dieser Maßnahmen verlangen.“

Artikel 7 des Erlasses vom 16. Oktober 2003 über die Erdgasnetzbetreiber, abgeändert durch den Erlass vom 6. Dezember 2018, enthält dieselben Bestimmungen.

Aufgrund von Artikel 16, §1 des Dekrets vom 12. April 2001 über die Organisation des regionalen Elektrizitätsmarktes (im Folgenden „Dekret über den Strommarkt“ genannt) und Artikel 17, §1 des Dekrets vom 19. Dezember 2002 über die Organisation des regionalen Gasmarktes (im Folgenden „Dekret über den Gasmarkt“), wonach der VNB eine Tochtergesellschaft, die über ihr eigenes Personal verfügt, ganz oder teilweise mit dem täglichen Betrieb beauftragen kann, wurde am 1. Februar 2019 ein

[1] Vorläufige Schlussfolgerungen über die Kontrolle der Implementierung der Governance-Regeln – Schreiben der CWaPE vom 15. Oktober 2019.
[2] Artikel 13 der Statuten von ORES Assets (siehe auch Beilage 6: Modalitäten für den operativen und täglichen Betrieb vonseiten der Betriebsgesellschaft ORES gemäß Artikel 13 der Statuten).
[3] Artikel 3 der Statuten von ORES SC.

Personalmitglied von ORES Gen., Tochtergesellschaft von ORES Assets, zum Vertraulichkeitskoordinator vom Direktionsausschuss von ORES Gen. bezeichnet. Diese Person ist Frau Audrey Réveillon.

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 Assets auf dem ganzen belieferten Gebiet sowohl für Elektrizität als auch für Erdgas.
Zweck des vorliegenden Berichts ist es, die Maßnahmen darzulegen, die im Laufe des Jahres 2024 getroffen bzw. fortgesetzt wurden, um die Vertraulichkeit der Informationen, von denen ORES Assets bei der Ausführung der ihr anvertrauten Aufgaben Kenntnis erhält, noch besser zu gewährleisten.

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

1. Verpflichtungen des Personals in Sachen Datenvertraulichkeit

Da ORES Assets laut Artikel 16, §1 des Dekrets über den Strommarkt und Artikel 17, §1 des Dekrets über den Gasmarkt ORES Gen. mit dem täglichen Betrieb ihrer Tätigkeiten beauftragt hat, steht das gesamte Personal, das im Auftrag von ORES Assets arbeitet, unter Arbeitsvertrag bei ORES Gen. Die folgenden Bestimmungen sind daher jene, die bei ORES Gen. gelten.
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 wurde der berufsethische Verhaltenskodex, der für alle Personalmitglieder gilt, überarbeitet. Dieser neue Ethik- und Deontologiekodex umfasst die Verpflichtungen des Personals in Bezug auf den Datenschutz sowie die Pflicht, diesen einzuhalten. Es gilt ebenfalls für externe Partner (Berater, Subunternehmer, Zeitarbeitskräfte usw.). Er ist Bestandteil der vertraglichen Dokumentation, die im Rahmen neuer Kooperationen übergeben wird.
Angepasste Vertraulichkeitsvereinbarungen werden darüber hinaus mit den externen Mitarbeitern und den Zeitarbeitskräften unterzeichnet.
Alle diese Klauseln wurden überprüft und der Inhalt entspricht den Standards der Norm ISO-27001.

Gemäß der Datenschutz-Grundverordnung (im Folgenden kurz „DSGVO“ genannt) hat ORES Gen. eine Reihe von Prozessen eingerichtet und beschreibt die Aufgaben und Verantwortlichkeiten eines jeden. Darüber hinaus ist ORES Gen. durchgehend darum bemüht, die Anwendung der Prinzipien dieser Verordnung zu verbessern und das 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 jedes Jahr vom Direktionsausschuss von ORES Gen. revidiert. Die letzte Aktualisierung erfolgte im März 2024.
In jeder Direktion wurden Mitarbeiter ausgebildet, um den Datenschutzbeauftragten (im Folgenden kurz "DPO" für "*Data Protection Officer*" genannt) auf Basisebene zu unterstützen.

Konkret umfasst die Sensibilisierung des Personals:

- Die Erstellung eines neuen Ethik- und Deontologiekodexes, der die Verpflichtungen in Bezug auf den Datenschutz beinhaltet, sowie dessen

Bekanntmachung gegenüber allen Mitarbeitenden von ORES Gen. Und an externe Partner (Berater, Subunternehmer, Zeitarbeitskräfte usw.);

- 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 IT-Direktion,
- die Auferlegung einer Reihe von Verpflichtungen in Sachen Vertraulichkeit durch die Arbeitsordnung;
- die Übermittlung des kollektiven Arbeitsabkommens CCT IKT (Informations- und Kommunikations-Technologien) an alle neue Mitarbeiter von ORES. Dieses Dokument steckt den Rahmen für die Nutzung der Telekommunikationsmittel vonseiten der Arbeitnehmer;
- die sofortige Überreichung eines Willkommenspakets bei jedem Neuzugang, das auch das Thema Cybersecurity umfasst;
- die Bereitstellung einer Reihe von Videos, in denen Schauspieler innerhalb des Unternehmens mit Sicherheitsproblemen konfrontiert werden. Schließlich erklärt das Video das richtige Verhalten in der dargestellten Situation. Alle zwei Monate werden zwei Folgen ausgestrahlt;
- Die Erstellung einer SharePoint-Website zum Thema Informationssicherheit, die den ISO-27001-Normen entsprechen (Richtlinien, Standards, Verfahren, Best Practices), zur Verfügung gestellt werden;
- ein verpflichtendes E-Learning über die DSGVO und diverse E-Learning-Module zur Informationssicherheit, die für alle Mitarbeiter eingerichtet wurden. Diese Ausbildungen sind für alle Mitarbeiter von ORES sowie jeden Neuzugang Pflicht. Diese Mitteilungen werden durch ständige Sensibilisierungskampagnen über verschiedene Sicherheitsaspekte unterstützt, und zwar je nach dem ermittelten Kenntnisstand der Mitarbeiter von ORES sowie den Hauptrisiken für unsere Daten. Kampagnen konzentrieren sich auf die Sensibilisierung des Personals von ORES für das Phishing-Risiko;
- die Schaffung eines spezifischen Zusammenarbeitsbereichs für die DSGVO, die sämtlichen Mitarbeitern zur Verfügung steht, um den Zugang zu den sachdienlichen Informationen und den anzuwendenden Prozeduren zu erleichtern, sobald persönliche 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 Websites eingesehen werden können).

Außerdem wurde der neue Ethik- und Deontologiekodex auch den Mitgliedern der Verwaltungsräte von ORES Assets und ORES Gen. mitgeteilt.

Die Verwaltungsratmitglieder 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.

Die Verwaltungsratsmitglieder von ORES Assets und ORES Gen. haben darüber hinaus einen Verhaltenskodex MAR[5] verabschiedet und einzeln eine Erklärung in ihrer Eigenschaft als Insider unterzeichnet.

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

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

Wenn ORES Gen. im Auftrag von ORES Assets persönliche Daten in Verbindung mit ihrer Kundschaft verarbeitet, wird beim Personal und bei den Subunternehmern, bei 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 …

Sowohl ORES als auch Comnexio haben Datenschutzverfahren nach dem Prinzip „*Privacy by design*“ und "*Security by design*“ eingerichtet, damit der Schutz und die Verarbeitung der persönlichen Daten der Kunden von ORES 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 persönlichen Daten wird in diesen Geschäftsjahren bewertet. Außerdem werden Sicherheitsrisikoanalysen für die neuen Geschäftsprozesse durchgeführt. Die bereits bestehenden Geschäftsprozesse werden alle drei Jahre hinsichtlich der 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 bei 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 Dienstes validiert.
- Die Lastenhefte für die neuen Anwenderprogramme 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 der Abfragen des Nationalregisters geführt;
- Die Einführung sicherer Passwortspeicher.

Eine Umstrukturierung des Informationssicherheitsdienstes hat darüber hinaus im April 2024 stattgefunden, um sämtliche Sicherheitskompetenzen unter dem CISO von ORES zu bündeln.
Drei Teams wurden gebildet, nämlich:
- Das Team Governance, Risk und Compliance: ein Team, das für die Weiterentwicklung der Informationssicherheitsrichtlinien und -standards in Übereinstimmung mit der ISO-27001-Norm verantwortlich ist.
- Das Team Cyber Defense: ein Team, das die IT-Aktivitäten durch die Analyse von Logs verschiedener Komponenten (Firewalls, WAF, Antivirenprogramme usw.) überwacht.
Zusätzlich hat ORES einen Vertrag für eine 24/7-Sicherheitsüberwachung abgeschlossen.
- Das Team Identity and Access Management: ein Team, das den gesamten Lebenszyklus eines Nutzers des ORES-Informationssystems verwaltet (Benutzererstellung, Zuweisung von Zugriffsrechten und Löschung).

Es ist allgemein hervorzuheben, dass ORES Assets am 1. November 2022 im Rahmen des Gesetzes vom 7. April 2019 zur Schaffung eines Rahmens für die Sicherheit von Netz- und Informationssystemen von allgemeinem Interesse für die öffentliche Sicherheit (im Folgenden „NIS“) als Betreiber eines wesentlichen Dienstes bezeichnet wurde. ORES Assets ist im Sinne der NIS-2-Regulierung[5] eine wesentliche Einheit. Folglich hat ORES ein Dokument mit der Beschreibung der diesen wesentlichen Diensten zugrunde liegenden Systemen zu Händen des FÖD Wirtschaft und des Zentrums für Cybersicherheit Belgien (CCB) verfasst und befindet sich in der letzten Phase zur Erlangung des ISO-27001-Zertifikats. Nachdem die Zertifizierungsstelle im Januar 2025 eine positive Stellungnahme abgegeben hat, sollte ORES die Zertifizierung bis Ende März 2025 erhalten.

[5] NIS-2-Richtlinie: 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 Gesetz vom 26. April 2024 zur Festlegung eines Rahmens für die Cybersicherheit von Netz- und Informationssystemen von allgemeinem Interesse für die öffentliche Sicherheit.

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

Die Direktion Kunden & Märkte wurde ab Januar 2024 umstrukturiert. Zur besseren Lesbarkeit werden die vorherigen Namen der Teams/Dienste in Klammern angegeben.

1. Die betroffenen Dienste von ORES Gen.

Der Dienst Facilitation und Marktprozesse (ehemals Structuring, Measure & Settlement) gehört zur Direktion Kunden & Märkte. Diese Direktion verwaltet alle Prozesse der liberalisierten Märkte (Assets, Structure, Measure und Berichtigung), Datenmanagement sowie Flexibilität. Die sozialen Gemeinwohlverpflichtungen werden innerhalb dieser Direktion betreut.
Das Team Berichtigung Marktanomalien (ehemals Führung des Zugangsregisters) innerhalb des Dienstes Berichtigung Marktanomalien führt das föderale Zugangsregister (CMS Atrias, Central Market System), dessen Go-live im Dezember 2021 stattgefunden hat für den Geschäftsbereich von ORES und verwaltet die Kontakte auf operativer Ebene mit den Energieversorgern.

Das CMS ist die föderale IT-Plattform, die den Austausch und die Bearbeitung der Information zwischen allen Akteuren des belgischen Energiemarktes auf der Grundlage der MIGs (*Message Implementation Guide)* erleichtert.

Jede Zugriffsstelle (Headpoint) ist darin mit ihrem EAN-Code erfasst. Hinter diesem Code findet man hauptsächlich die Daten des Kunden, seines Energieversorgers sowie einige weitere zweckdienliche Informationen. Hinter diesem Headpoint findet man außerdem die Dienste und möglichen Konfigurationen je nach der Art der Anlage (für einen Prosumerkunden mit einem Smart Meter wird es beispielsweise den Dienst betreffend den Ausgleich und die Konfigurationen Tag/Nacht oder einheitlicher Tarif geben, und in Zukunft zum Beispiel die anreizschaffende Tarifgestaltung).

Durch die Vernetzung – auf Ebene von ORES – mit der MDM/Mercure (der Datenbank zur Erfassung der Verbrauchswerte jeder Lieferstelle) über ein umfassendes Organisationssystem (BPMS, *Business Process Management* System) sowie mit dem Back-End SAP ISU (dieses umfasst sämtliche technischen Informationen über eine Lieferstelle) liefert das CMS ein vollständiges Bild des Marktes.

Im neuen Dienst Kundenerlebnis wird nun die Ablesung der elektromechanischen Zähler sichergestellt. Für die Smart Meter ist das Team Überwachung der Kommunikationsketten (ehemals „Smart Control Room“) innerhalb des Dienstes Facilitation und Marktprozesse verantwortlich für die Überwachung des ordnungsgemäßen Funktionierens der Kommunikationsketten, die Übermittlung der Zählerstände (insbesondere über das Prism-Tool) sowie die Übermittlung der Guthabenstände an die Vorauszahlungszähler. Seit dem Einbau der Smart Meter wurde eine neue Plattform für die automatisierte Ablesung der Zählerstände

eingerichtet. Es handelt sich um das Tool mit dem Namen Prism (einer Anwendung, die die Erfassung der Daten der Smart Meter ermöglicht und Teleoperationen zum HES, Head-End System verwaltet), das einerseits mit dem MDM/Mercure und andererseits mit der Kommunikationskette der Zähler verbunden ist.

Die Teams Validierung (B2C und B2B) innerhalb des Dienstes Facilitation und Marktprozesse überprüfen die Plausibilität dieser Ablesungen anhand von Verbrauchsstatistiken, dem Verbrauchsverlauf sowie klimatischen Kriterien.

Seit dem Go-Live von MIG6 hat ORES mit Problemen im Zusammenhang mit Marktblockierungen zu kämpfen. Das Team Überwachung der Querschnittsprozesse (ehemals Market Service Center) übernimmt die komplexesten Fälle. Weitere Fälle werden von anderen Teams innerhalb des Dienstes Facilitation und Marktprozesse bearbeitet: Berichtigungen (ehemals GPAM) für Atrias-Beschwerden, die beim SRME eingereicht wurden, sowie Marktkontaktaufnahme für Anfragen von Lieferanten und Kunden.

Das Team Regularisierung von Prozessen (ehemals „Management der Marktprozesse“), das nun in den Dienst Markterleichterungen und -Aktivitäten integriert ist, greift ebenfalls auf die im CMS enthaltenen Daten zugreifen, um die von den Energieversorgern eingeleiteten Prozesse Drop, Initiate Leaving Customer (ILC) und 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 Kontaktcenter Comnexio (Tochtergesellschaft von ORES Assets) ebenfalls Zugriff auf die Daten des CMS und die Datenbank Mercure, um die Telefonate der Kunden an vorderster Front entgegenzunehmen.

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, werden 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 und Marktprozesse (Lese- und Schreibrechte) unter anderem über ein Reporting Business Object (BO) vorbehalten.
  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 Marktkontaktaufnahme so ausgebildet, dass sie Auskünfte über die Zugriffsstelle nur an den für diese Zugriffsstelle anerkannten Versorger per E Mail oder Telefon erteilen.

Die Teams Berichtigung Marktanomalien, Regularisierung von Prozessen; Marktkontaktaufnahme und Validierung 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 Nutzungszeitraums dieses Kunden; dabei hat Letzterer seine Zählernummer zur Überprüfung mitzuteilen. Der Endabnehmer hat keinen Zugang zur eigentlichen Software-Anwendung. Falls ein Kunde den VNB fragt, welcher Energieversorger mit der Zugriffsstelle verbunden ist, wird ihm die Antwort per Postschreiben an die Installationsadresse geschickt.

Das von unserem Kontaktcenter Comnexio angewandte Verfahren ist ebenfalls genau festgelegt. Falls ein kommerzieller Energieversorger die Frage stellt, wird sie automatisch an das CMS-Portal weitergeleitet, da dieses über die entsprechenden Zugriffsrechte verfügt.
Handelt es sich um einen Kunden, wird sein EAN Code erst nach Überprüfung seiner Zählernummer mitgeteilt. 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 bezüglich mehr als zwei EAN Codes, so wird diese erfasst und per E-Mail/ 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 sei auf Folgendes hingewiesen: 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 ist festzuhalten, dass ein Stromversorger infolge des neuen Verfahrens bei einer Nichtzahlung des Kunden im Rahmen des Dekrets, das üblicherweise „Friedensrichter-Dekret“ genannt wird, 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 und 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 dieser Programm Owner zuständig ist.

Das Kontaktcenter 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.

Dem Kunden, der seine chronologische Verbrauchsübersicht einsehen möchte, werden verschiedene Möglichkeiten geboten:

- über die Website von ORES anhand seines EAN-Codes und seiner Zählernummer;
- über das smarte Verbrauchsportal: Die Zugriffe sind in Bezug auf die Sicherheit streng kontrolliert;
- über einen Antrag an einen der operativen Dienste.

Diese Verbrauchsübersicht kann an eine andere Person oder einen Versorger geschickt werden, sofern diese(r) eine schriftliche Bevollmächtigung hat.
Für alle Transaktionen des Energiemarktes und Datenübermittlungen ist eine Rückverfolgbarkeit möglich.

Wenn der Kunde unser Kontaktcenter 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 Website 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 Website 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 PDAs (*Personal Digital Assistant*) der Zählerableser, anhand derer der Zählerstand vor Ort erfasst werden kann, sind ebenfalls durch eine persönliche Identifizierung (Benutzername und Passwort) geschützt.

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. Dieses Verfahren unterliegt sämtlichen Regeln der DSGVO und die Funktionalität wird bei jedem Kundenwechsel automatisch blockiert.

- **Die BPMS**

  Bei den Teams, die Zugriff auf das BPMS-Tool im Änderungsmodus haben, handelt sich ausschließlich um die berechtigten IT-Teams. Die Teams des Dienstes Facilitation und Marktprozesse haben jedoch einen Lesezugriff im Rahmen ihres Analysebedarfs. Die Zugriffe auf dieses Anwenderprogramm werden vom Anwenderprogramm Owner auf Basis der IT-Berufsmerkblätter erteilt. Es gibt keine weiteren Teams, die einen Zugriff auf dieses Anwenderprogramm benötigen.

- **Prism und HES**

DAS HES ist nur für den externen Dienstleister, der dieses zur Verfügung stellt, zugänglich.

Das Prism seinerseits ist nur im Lesezugriff für das Team Überwachung der Kommunikationsketten zugänglich, jedoch darüber hinaus – wiederum auf der Grundlage eines Berufsmerkblatts – für das Team der Verwaltung der Vorauszahlungen (GDP – Gestion des Prépaiements), das seit jeher die Aufladungen der Budgetzähler (Talexus) verwaltet und nun der Smart Meter im Vorauszahlungsmodus (über das PPP-Tool, das bei Atrias gehostet ist).

Die Teleoperationen (z. B. Aktivierung des Ports P1 oder Anfrage von addIndex) werden über den Prism anhand des Systems SAP CS (dieses Tool wird bei ORES Lopex genannt) ausgeführt. Alle Zugriffe auf das Anwenderprogramm Lopex werden auf der Grundlage der Berufsmerkblätter HR kontrolliert.

• ORES und die künstliche Intelligenz

ORES beschäftigt sich derzeit mit der Einführung der künstlichen Intelligenz (KI) in ihren Tätigkeiten, insbesondere mit dem Ziel, die Energiewende zu unterstützen und bestimmte wiederkehrende Aufgaben zu optimieren.
ORES ist sich der Herausforderungen im Zusammenhang mit der Nutzung dieser Technologien bewusst und stellt sicher, dass deren Implementierung durch einen strengen internen Regelungsrahmen geregelt wird, der die geltenden Vorschriften, insbesondere die DSGVO und den Artificial Intelligence Act, einhält. Dieser rechtliche Rahmen garantiert eine ethische und sichere Nutzung der KI, die Innovation mit dem Schutz der Rechte des Einzelnen in Einklang bringt.

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),
- die Durchführung von Audits,
- die Minimierung der mitgeteilten Daten;
- die Einführung eines Ethik- und Verhaltenskodexes, der auch für externe Mitarbeitende 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 Daten außerhalb der Europäischen Union geteilt werden, werden gleichwertige Maßnahmen zum Datenschutz eingeführt und vorzugsweise Standardvertragsklauseln angewendet.

Umfangreichere Vertraulichkeitsklauseln sind in den Verträgen ebenfalls vorgesehen.

Abschnitt VI – Rückverfolgbarkeit als Vertraulichkeitsgarantie

ORES nutzt die SAP-Lösungen und hat sich für eine verstärkte Parametrierung der Rückverfolgbarkeit als die von SAP angeratene Standard-Parametrierung entschieden. Zur Rückverfolgbarkeit der Nutzertätigkeiten und der technischen Konten im Zusammenhang mit Drittlösungen wird Folgendes in der SAP-Datenbank von ORES 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 geleitetet 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 WLAN-, 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,
- 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 Nutzergeräte (Arbeitsplatz, Mobilitätstools).

Im Jahr 2021 wurde die Implementierung einer DLP (Data Loss Prevention) geprüft. Es wurde eine IT-Plattform eingerichtet. ORES hat eine Arbeitsgruppe gebildet, um die Lenkungsform und die Regeln der Tätigkeitsbereiche festzulegen, die innerhalb der IT-Plattform implementiert werden sollen.

Im Jahr 2024 hat ORES ein Tool eingeführt, das den Nutzern der Microsoft-Office-Anwendungen ermöglicht, Dokumente zu kennzeichnen. Vier kennzeichnungsstufen wurden definiert:
• C1 – ÖFFENTLICHE Information: Die Information ist öffentlich und kann an jedermann weitergegeben werden, sowohl innerhalb von ORES als auch außerhalb;

• C2 – INTERNE Information: Die Information darf allen Personen zugänglich sein, die bei ORES arbeiten, sowohl internen Mitarbeitenden als auch externen Mitarbeitenden (mit Vertrag) und gegebenfalls bestimmten Partnern;
• C3 – BESCHRÄNKTE Information: Die Information ist nur für einen begrenzten Personenkreis bestimmt, beispielsweise ein Team, ein Dienst oder eine Direktion;
• C4 – VERTRAULICHE Information: Der Zugriff auf die Information ist ausschließlich namentlich benannten Personen vorbehalten.

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 dürfen 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) erfüllen zu können.
  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.

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

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

2023 konnte ORES mit ENGIE IT arbeiten, um die vergemeinschaftlichten Dienste (Backup, Serviceinfrastruktur, Speicherplatz, Netzbestandteil …) auf ein ORES dediziertes Modell zu übertragen. Die Systeme, die die Anwenderprogramme von ORES beherbergen, waren bereits im Silo von ORES vorhanden. Seit Juli 2023 befinden sich alle genutzten Dienste, einschließlich der historisch vergemeinschaftlichten Dienste, im Silo von ORES und somit auf einem Material, das ORES dediziert ist. Die Data-Center-Netzbestandteile wurden ebenfalls überarbeitet und werden ausschließlich für die Bereitstellung der Dienste an ORES genutzt. Dank diesem Wechsel zu einem dedizierten Material für die vergemeinschaftlichten Dienste konnte ORES seine Sichtbarkeit bei den von ENGIE IT ausgeführten operativen Tätigkeiten weiter verbessern.

In ihrem Schreiben vom 28. März 2024 hat die CWaPE die Bedingungen für die Annahme des Austrittsdatums von ENGIE IT zum 31. Dezember 2030 präzisiert.
Sie fordert unter anderem, dass ORES der CWaPE eine regelmäßige Überwachung der Umsetzung des Austrittsplans gewährleistet.
Im Rahmen dessen übermittelt ORES halbjährlich (im Juni und im Dezember) per Schreiben einen aktualisierten Austrittplan. Jede aktualisierte Version wird zudem in einer Präsentationssitzung bei der CWaPE vorgestellt.
Der erste Statusbericht wurde im Juni 2024 an die CWaPE übermittelt.

- <u>Sonderfall: Connect My Home</u>

  Die Initiative „Connect My Home“ bezeichnet die Realisierung von Synergien im Rahmen von Anschlussarbeiten bei Privatpersonen und vereint im jetzigen Stadium folgende Betreibergesellschaften: ORES, RESA, die wallonische Wassergesellschaft SWDE, Proximus, ORANGE und Telenet.

  Um den Service „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 Technologie nachzukommen, hat ORES eine Arbeitsgemeinschaft mit zwei anderen VNB (Fluvius, Sibelga und RESA) gebildet; zu deren Zielen gehört auch die Vergemeinschaftung der Kosten und die Lieferung einer schnelleren und kohärenteren Lösung für den Bürger.

Es sei darauf hingewiesen, dass zu Beginn des Projekts schon eine Lenkungsform eingerichtet wurde, um die Anwendung des Prinzips des Schutzes und der Vertraulichkeit der Daten bereits in die Planung mit einzubeziehen.

Die Smart Meter übermitteln die aktuellen Zählerstände einmal pro Tag (sogar für die Innertagesdaten) an ORES. 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 Eindringungstests durchgeführt.

Die Implementierung der Smart Meter bei ORES erfolgt phasenweise. Seit 2020 werden Smart Meter bei Privatpersonen installiert. Ausgenommen für die Nutzung der Vorauszahlungsfunktion und des Zähleraustausches aus messtechnischen Gründen zwingt ORES die Bürger in keiner Weise dazu, die Kommunikationsfunktion der neuen Zähler zu aktivieren (für Bürger, die dies ausdrücklich verlangen, werden die Zähler im „Flugmodus“ betrieben). Die Änderung des Dekrets zur Regelung der Einführung der Smart Meter in der Wallonie vom 27. März 2024, die vom wallonischen Parlament am 24. April 2024 verabschiedet wurde, legt die Verpflichtung fest, bis zum 31. Dezember 2029 100% der Stromzähler al kommunizierende Zähler auszustatten.

Um dieses ehrgeizige Ziel zu erreichen, hat ORES das Projekt ACDC („accélération des compteurs communicants“) gestartet, das eine vollständige Auslagerung (einschließlich des gesamten Kundenprozesses und der Terminvereinbarung) vorsieht. Für dieses Projekt werden eine Datenschutz- Folgenabschätzung (DPIA) sowie eine Sicherheitsrisikoanalyse durchgeführt.

Aufgrund 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 Bürger beruhen.

- <u>Prinzip der Transparenz und Recht auf Information</u>
  Bei der ersten Terminvereinbarung für die Anbringung der neuen Zähler werden die Betreffenden bereits auf ihre Kommunikationsfunktion hingewiesen.
  Eine Infobroschüre wird dem Kunden bei der Anbringung der Zähler ausgehändigt.
  Auf einer Seite unserer Website[4] werden die Fragen in Sachen Datenschutz beantwortet. Die Mitarbeiter, die im Kontakt mit den Kunden sind, werden

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

entsprechend ausgebildet. Unser Datenschutzbeauftragter (DPO) steht ebenfalls zur Beantwortung aller Fragen in Verbindung mit dem Schutz des Privatlebens und dem Datenschutz zur Verfügung. Unsere Datenschutzerklärung wurde im Februar 2024 aktualisiert.

- 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 Cybersecurity-Überwachung, die den Aspekten im Zusammenhang mit dem Datenschutz und der Anwendung der geltenden Gesetze Rechnung trägt.

Die Sicherheitsrisiken absichtlicher An- und Eingriffe wurden im Rahmen von Workshops nach der EBIOS-Methode RM 2018 geprüft, um die Sicherheitsrisiken für die IT-Systeme (Betriebseinheiten und Schwachstellen, Angriffsmethoden und bedrohende Aspekte, wesentliche Bestandteile und Sicherheitsbedürfnisse …) einzuschätzen und deren Bearbeitung durch Spezifizierung der zu erfüllenden Sicherheitsanforderungen zu fördern.

Im Sinne einer kontinuierlichen Datenkontrolle sind für 2025 Risikoanalysen (DSGVO und Sicherheit) sowie Aktualisierungen der Prozesse im Zusammenhang mit der Kommunikationskette geplant.

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 sechs Gesellschaften 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 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 Funktionstrennung zu erfüllen.