BERICHT NR.17
DES VERTRAULICHKEITSKOORDINATORS VON ORES ASSETS

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

INHALTSVERZEICHNIS

Abschnitt I - Vorbemerkung 3

Abschnitt II – Verpflichtungen des Personals und der Mitglieder der Verwaltungsorgane in Sachen Datenvertraulichkeit 6

1. Verpflichtungen des Personals in Sachen Datenvertraulichkeit 6
2. Verpflichtungen der Mitglieder der Verwaltungsorgane in Sachen Datenvertraulichkeit 7

Abschnitt III – Sicherheitsmaßnahmen für den Zugriff des Personals auf die persönlichen und kommerziellen Daten 9

Abschnitt IV – Sicherheitsmaßnahmen bezüglich des Zugriffs der Energieversorger und der Kunden auf die vertraulichen Daten 11

1. Die betroffenen Abteilungen von ORES Gen. 11
2. Eingeleitete spezifische Maßnahmen 12

Abschnitt V – Sicherheitsmaßnahmen bezüglich des Zugriffs der Subunternehmer auf die vertraulichen Daten 16

Abschnitt VI – Rückverfolgbarkeit als Vertraulichkeitsgarantie 17

Abschnitt VII – Gemeinsame Nutzung der IT-Systeme und -Infrastrukturen mit anderen Unternehmen 18

Abschnitt VIII – Projekt des Rollouts der intelligenten Zähler 20

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 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 Contact Centers wurden ihrerseits ab dem 1.6.2019 dem Unternehmen 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).
[3] Artikel 3 der Statuten von ORES Gen..

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 2020 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 enthält ein berufsethischer Verhaltenskodex, der für alle Personalmitglieder gilt, die Verpflichtung für die Mitarbeiter von ORES Gen., sämtliche Regeln in Sachen Berufsethik einzuhalten, insbesondere die Verpflichtung, mit gesundem Menschenverstand und der gebotenen Vorsicht beim Umgang mit Informationen über ihre Berufstätigkeit vorzugehen.

Infolge des Inkrafttretens der Datenschutz-Grundverordnung (im Folgenden kurz „DSGVO“ genannt) ist ORES Gen. bemüht, die Prinzipien dieser Verordnung konsequent anzuwenden und das Personal dafür zu sensibilisieren.
Eine Politik zum Schutz der Privatsphäre wurde im Jahr 2019 betriebsintern schriftlich festgelegt und veröffentlicht, um dem Personal von ORES Gen. die Leitlinien zu geben, die bezüglich der DSGVO für das Unternehmen Pflicht sind.
In jedem Geschäftsbereich 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 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 den Geschäftsbereich IT;
- 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 eines Videoclips zur Erläuterung der Wichtigkeit der Sicherheit und der Aufgabe, die jedem Mitarbeiter diesbezüglich obliegt;
- die Abhaltung einer Informationssitzung, die auch den Themenbereich Cybersecurity betrifft. Diese Sitzung wurde nach einer Zufriedenheitsumfrage zum Thema IT eingeführt, bei der sich herausstellte, dass es eine Reihe von Fragen bzw. Verständnisproblemen gibt (beispielsweise: Weshalb sind manche Websites blockiert? Weshalb kann man eine bestimmte Software nicht installieren? …). An dieser Sitzung konnte man vor Ort oder per Videokonferenz teilnehmen;
- ein obligatorisches E-Learning über die DSGVO und diverse E-Learning-Module zur Informationssicherheit, die im Sommer 2020 für sämtliche Mitarbeiter eingerichtet wurden. Diese Ausbildungen sind für alle Mitarbeiter von ORES sowie jeden Neuzugang Pflicht. Seit Ende 2020 werden diese Mitteilungen durch ständige Sensibilisierungskampagnen über verschiedene Sicherheitsaspekte unterstützt, und zwar je nach dem ermittelten Kenntnisstand der Mitarbeiter von ORES sowie den Hauptrisiken für unsere Daten;
- 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).

Sie 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. Es wurde ein Mitteilungssystem eingerichtet, um sie in jeder entscheidenden Phase des Finanzlebens des Unternehmens an ihre entsprechenden Verpflichtungen zu erinnern.

[4] 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 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, geplanten Arbeiten an Zähleranlagen, GWV, …

ORES hat Datenschutzverfahren nach dem Prinzip „*Privacy by design*“ eingerichtet, damit der Schutz und die Verarbeitung der persönlichen Daten ihrer 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“, die Kunden bei ORES sind, darstellen kann. Der Aspekt des Zugriffs auf die persönlichen Daten wird in jedem Geschäftsjahr bewertet. Außerdem werden Sicherheitsrisikoanalysen für die neuen Geschäftsprozesse durchgeführt.

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 jeder Abteilung 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 den 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.

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

1. Die betroffenen Abteilungen von ORES Gen.

Die Abteilung *Structuring, Measure & Settlement (*kurz *SMS)* gehört zum Geschäftsbereich Marktverwaltung & Kundschaft. Dieser Geschäftsbereich verwaltet insbesondere alle Prozesse des liberalisierten Marktes sowie die sozialen Gemeinwohlverpflichtungen.
Das Team „Führung des Zugangsregisters“ (kurz *GRA – Gestion du Registre d'accès*) innerhalb der SMS-Abteilung führt das Zugangsregister und verwaltet die Kontakte mit den Energieversorgern.

Das Zugangsregister ist das Kernstück des liberalisierten Marktes. Es handelt sich um die Datenbank, auf deren Grundlage die Beziehungen und Austausche zwischen den verschiedenen Marktteilnehmern und den VNBs organisiert werden. Es ist eigentlich das Mittel, das die Aktualisierung und die Informationsflüsse garantiert. Jede Zugriffsstelle (auch Versorgungs-/Lieferstelle genannt) ist darin mit seinem EAN-Code erfasst. Hinter diesem Code findet man hauptsächlich die Daten des Kunden, seines Energieversorgers sowie einige weitere zweckdienliche Informationen. Durch die Vernetzung mit der MDM/Mercure (der Datenbank zur Erfassung der Verbrauchswerte jeder Lieferstelle) sowie mit dem Back-End SAP ISU (dieses umfasst sämtliche technischen Informationen über eine Lieferstelle) liefert das Zugangsregister ein vollständiges Bild des Marktes.

Aufgabe des Teams *Measure* der SMS-Abteilung (dazu gehören unter anderem die Zählerableser und die Validierer) ist es, die Verbrauchsdaten der Kunden im ganzen Versorgungsgebiet von ORES abzulesen und zu validieren, d. h., die erfassten Zählerstände auf ihre Kohärenz mit der statistischen und chronologischen Entwicklung des Verbrauchs oder den klimatischen Kriterien zu prüfen. Das Team verwaltet sowohl die jährliche Ablesung der Zähler der Haushaltsabnehmer und kleinen Gewerbekunden (ein Besuch alle zwei Jahre und die Zusendung einer Karte im anderen Jahr), die monatliche Ablesung (ein Besuch jeden Monat) als auch die regelmäßige Fernablesung der Zähler der Großabnehmer (viertelstündlich für Strom und stündlich für Gas).
Das tägliche Management der Computeranwendungen (Zugangsregister und MDM/Mercure, die von der o. g. Abteilung benutzt werden, erfolgt in Zusammenarbeit mit Fluvius.

Das Team „Management der Marktprozesse“ (kurz *GPM – Gestion des Processus de Marché*) - Abteilung „Arbeiten Kunden Märkte“ (kurz *TCM – Travaux Clients Marchés*) innerhalb des Geschäftsbereichs „Markt & Kundschaft“ - muss ebenfalls auf die im Zugangsregister enthaltenen Daten zugreifen, um die von den Energieversorgern eingeleiteten Prozesse *Drop, End-Of-Contract*, MOZ und Anbringung von Budgetzählern zu vollenden. Neben der Sendung von Schreiben kontaktieren die Mitarbeiter auch manchmal die Kunden (beispielsweise für die

Prüfung eines MOZA –Dossiers) und/oder die kommerziellen Energieversorger (beispielsweise für eine abgesicherte Annullierung).

Schließlich hat unser Contact Center Comnexio (Tochtergesellschaft von ORES Assets) ebenfalls Zugriff auf die Daten des Zugangsregisters 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**

  Die IT-Infrastruktur ist abgesichert; der Zugriff auf die Software ist individuell festgelegt und den Mitgliedern der Teams GRA (Lese- und Schreibrechte) und GPM (Lese-und Schreibrechte) über eine Web-Schnittstelle (MySupplierWeb) sowie ein *Reporting Business Object* (BO) vorbehalten.
  Jeder neue Zugriffsantrag bedarf der Genehmigung des Anwenderprogramms *Owner Structuring*. Letzterem 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 Supplier-Web. 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 GRA und GPM so ausgebildet, dass sie Auskünfte über die Zugriffsstelle nur an den für diese Zugriffsstelle anerkannten Versorger per E-Mail oder Telefon erteilen.

  Die Teams GRA und GPM 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 vom unserem Contact Center Comnexio angewandte Verfahren ist ebenfalls genau festgelegt. Falls ein kommerzieller Energieversorger die Frage stellt, wird sie automatisch an das Zugangsregister (*Supplier-Web*) weitergeleitet, da dieses über die entsprechenden Zugriffsrechte verfügt.
Handelt es sich um einen Kunden, so kann dieser seinen EAN-Code nur nach Mitteilung seiner Zählernummer erfahren. Kennt der Kunde seine Zählernummer nicht, so kann ihm der EAN-Code zwar nicht telefonisch mitgeteilt, jedoch per Postschreiben an die Verbrauchsadresse zugeschickt werden. Handelt es sich um eine Anfrage bezüglich mehr als zwei EAN-Codes, so wird der Kunde gebeten, diese unter Beifügung der Liste der betroffenen Zähleradressen und -nummern per Postschreiben oder E-Mail zu beantragen.
Diese Telefonate und Mitteilungen werden im System aufgezeichnet und verfolgt.

Es sei darauf hingewiesen, dass die Bearbeitungsweise der Anfragen bezüglich der EAN-Codes zurzeit verbessert wird, damit diese Informationen nur noch dem an der Zugriffsstelle aktiven Kunden mitgeteilt werden.

Der VNB teilt auch den ÖSHZ Kundeninformationen mit. Das ÖSHZ verfügt über eine spezifische Kontaktnummer für die Anfrage von Informationen über seine Anspruchsberechtigten (Fortschrittsstand eines Dossiers, aktiver Energieversorger an der Zugriffsstelle, chronologische Verbrauchsübersicht, …), für die es eine ständige Vollmacht hat. 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 Budgetzähler* 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 Budgetzählers*, sondern einer Vertragsbeendigung läuft. So kann der neue Versorger nicht Kenntnis der Zahlungsschwierigkeiten des Kunden nehmen.

- **Mercure-System**

Die IT-Infrastruktur ist geschützt und der Zugang zur Software ist individuell festgelegt und den Mitgliedern der Abteilung SMS 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 es zuständig ist.

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

Die Energieversorger haben auch Zugang zur Software, aber jeder Versorger kann nur über die Daten der Kunden verfügen, für die das Zugangsregister ihm eine Registrierungserlaubnis an der Zugriffsstelle gewährt hat. Außerdem ist die Bereitstellung der Daten aufgrund der zwischen dem Kunden und dem Versorger festgelegten Vertragsdaten beschränkt.

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 einsehen möchte, kann dies dank einer sicheren Identifizierung auf der Website von ORES tun. Die Verbrauchsübersicht kann an eine andere Person oder einen Versorger geschickt werden, sofern diese eine schriftliche Bevollmächtigung haben.
Für alle Transaktionen des Energiemarktes und Datenübermittlungen ist eine Rückverfolgbarkeit möglich.

Wenn der Kunde unser Contact Center Comnexio anruft, um seine chronologische Verbrauchsübersicht zu erhalten, wird je nach Fall folgende Prozedur angewandt:
Handelt es sich um eine Fernablesung (außer Zähler mit Kommunikationsfunktion), so muss der Kunde aufgefordert werden, seinen Antrag über unsere Website zu stellen. Er erhält dann einen chronologischen Überblick über maximal die letzten drei Jahre.
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.
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 über maximal die letzten drei Jahre 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. Diese Verfahren unterliegt sämtlichen Regeln der DSGVO und die Funktionalität wird bei jedem Kundenwechsel automatisch blockiert.

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.

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 ausgetauscht werden, gelten Muster-Vertragsklauseln.

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 Benutzertätigkeiten 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 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,
- 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).

Die Implementierung eines DLP-Systems (*Data Loss Prevention*) wird zurzeit geprüft. Es hat zum Zweck, den Übergang auf Windows 10 (laut Zeitplan im 2. Halbjahr 2021) zu ermöglichen.

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).
  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.

- <u>ENGIE IT (wichtigster 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.

- N-ALLO

  ORES nutzt die technischen Infrastrukturen von N-Allo (über seine Telefonie-Plattform ININ, die von den Back-Offices von ORES genutzt wird), insbesondere wenn diese Back-Offices als zweite Anlaufstelle nach unserem Contact Center Comnexio agieren.
  Wie alle Dienstleister hat sich N-Allo vertraglich dazu verpflichtet, Vertraulichkeits-, Sicherheits- und DSGVO-Klauseln einzuhalten.

Abschnitt VIII – Projekt des Rollouts der intelligenten Zähler

Um seiner Verpflichtung des Rollouts der neuen Technologie nachzukommen, hat ORES eine Arbeitsgemeinschaft mit zwei anderen VNB (Fluvius 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 intelligenten Zähler übermitteln die aktuellen Zählerstände einmal pro Tag 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 intelligenten Zähler bei ORES erfolgt phasenweise. Seit 2020 wurden Zähler mit Kommunikationsfunktion bei Privatpersonen installiert. ORES zwingt dem Bürger die Anbringung des neuen Zählers keinesfalls auf; er kann sich jederzeit für den herkömmlichen Zähler entscheiden.

Aufgrund der Datenschutzprinzipien hält sich ORES an folgende Regeln:

- 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[5] werden die Fragen in Sachen Datenschutz beantwortet. Die Mitarbeiter, die im Kontakt mit den Kunden sind, werden entsprechend ausgebildet. Unser Datenschutzbeauftragter steht ihnen ebenfalls zur Verfügung. Unsere Datenschutzrichtlinie wurde auch aktualisiert.

- <u>Minimierung, Qualität und Dauer der Datenspeicherung</u>
  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. Ohne Einwilligung des Kunden werden lediglich die täglichen Zählerstände erfasst.

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

- 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: Das Smart Metering ist Gegenstand einer Cybersecurity-Überwachung, die den Aspekten im Zusammenhang mit dem Datenschutz und der Anwendung der geltenden Gesetze Rechnung trägt.
  Das Programm verfolgt das Sicherheitsmanagement innerhalb des Unternehmens, das unter anderem die Bewertung der Auswirkungen auf die Privatsphäre und eine Validierung auf der Grundlage der Projektlenkung voraussetzt. Für jede Phase des Rollouts wurden und werden weiterhin Auswirkungsstudien in Sachen Datenschutz von ORES durchgeführt.

Die Sicherheitsrisiken absichtlicher An- und Eingriffe werden im Rahmen von Workshops nach der EBIOS-Methode geprüft. Diese ermöglicht eine Abschätzung der Sicherheitsrisiken für die IT-Systeme (Betriebseinheiten und Schwachstellen, Angriffsmethoden und bedrohende Aspekte, wesentliche Bestandteile und Sicherheitsbedürfnisse, …) und fördert deren Bearbeitung durch Spezifizierung der zu erfüllenden Sicherheitsanforderungen; sie ermöglicht jedoch auch die Vorbereitung des umfassenden Sicherheitsdossiers, der für die Risikoakzeptanz erforderlich ist, sowie die Ausarbeitung der nützlichen Elemente zur Kommunikation über die Risiken.