VERTRAULICHKEITSBERICHT VON COMNEXIO

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.

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. …*“.

Artikel 7 des Erlasses vom 16. Oktober 2003 über die Erdgasnetzbetreiber, abgeändert durch den Erlass vom 6. Dezember 2018, enthält dieselben 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 des Jahres 2023 von Comnexio als Tochtergesellschaft von ORES Assets, die seit dem 1. Juni 2019 als Kontaktcenter von ORES Assets fungiert.

Angesichts der Auflösung des Ethikausschusses von Comnexio infolge der Abänderung der Dekrete bezüglich der Organisation der regionalen Elektrizitäts- und Gasmärkte

[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).

durch das Dekret vom 5. Mai 2022[3] wurde dieser Bericht vom Verwaltungsrat von Comnexio auf seiner Sitzung vom 20. März 2024 genehmigt.

Es sei außerdem darauf hingewiesen, dass der Verwaltungsrat von Comnexio vom 23. November 2022, dem Beispiel von ORES Assets folgend sowie im Rahmen der gemeinsamen Unternehmensführung, ebenfalls Audrey Réveillon in dieser gleichen Eigenschaft als Vertrauenskoordinatorin ernannt hat.

Es sei daran erinnert, dass Comnexio einen Übergangs-Dienstleistungsvertrag mit N-Allo abgeschlossen hatte, um am 1. Juni 2019 einsatzbereit zu sein. Zweck dieses Vertrags war die Festlegung der Übergangsleistungen, die N-Allo für Comnexio erbringen sollte. Das Projekt zur Ausstattung von Comnexio mit eigenen spezifischen Kontaktcenter-Tools, damit es seine Aufgaben unabhängig von N-Allo ausführen kann, endete am 30. Juni 2023; N-Allo erbringt keine Übergangsleistungen mehr für Comnexio.

Seit dem 25. Mai 2023 besteht ein Dienstleistungsvertrag mit NTT für die Implementierung einer Kontaktcenter-Lösung, die in das Comnexio/ORES-Ökosystem integriert ist. Dank dieser Vereinbarung kann Comnexio die Genesys-Cloud-basierte Kontaktcenter-Plattform nutzen.

Für die grundlegenden IT-Dienstleistungen findet der Supportvertrag mit ORES Gen. weiterhin Anwendung.
Abschließend ist noch darauf hinzuweisen, dass Comnexio seinen Tätigkeiten als Kontaktcenter ausschließlich für ORES Assets nachgeht.

[3] Dekret vom 5. Mai 2022 zur Abänderung bestimmter Bestimmungen in Sachen Energie im Rahmen der teilweisen Umsetzung der Richtlinien 2019/944/EU vom 5. Juni 2019 über die gemeinsamen Vorschriften für den Elektrizitätsbinnenmarkt und 2018/2001/EU vom 11. Dezember 2018 über die Förderung der Nutzung von Energie aus erneuerbaren Quellen und zur Anpassung der Kriterien für die Tarifberechnungsmethode.

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

1. Verpflichtungen des Personals in Sachen Datenvertraulichkeit

Die Muster-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 Comnexio 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 Comnexio zurückzugeben.

Infolge des Inkrafttretens der Datenschutz-Grundverordnung (im Folgenden kurz „DSGVO“ genannt) ist Comnexio bemüht, die Prinzipien dieser Verordnung konsequent anzuwenden und das Personal dafür zu sensibilisieren.

Zum Schutz der Vertraulichkeit der Daten umfassen die getroffenen Maßnahmen Folgendes:

- die Auferlegung einer Reihe von Verpflichtungen in Sachen Vertraulichkeit durch die Arbeitsordnung;
- 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.
- Seit Ende 2020 werden kontinuierlich Sensibilisierungskampagnen über verschiedene Sicherheitsaspekte organisiert, und zwar je nach dem ermittelten Kenntnisstand der Mitarbeiter sowie den Hauptrisiken für unsere Daten.
- Seit 2022 wurde ein alleiniger Ansprechpartner in Sachen DSGVO („SPOC“) innerhalb von Comnexio ernannt, um als privilegierter Mittler zum Datenschutzbeauftragten („DSB“, frz. „DPO“) zu fungieren.

Zur Erinnerung: Die oben genannten Informationen waren bereits Gegenstand eines Berichts der CWaPE im Rahmen ihrer Überprüfung der Implementierung der Regeln der Unternehmensführung.

2. Verpflichtungen der Mitglieder der Verwaltungsorgane in Sachen Datenvertraulichkeit

Neben der allgemeinen Schweigepflicht, die jedem Verwaltungsratsmitglied eines Unternehmens obliegt, wird den Verwaltungsratsmitgliedern von Comnexio ihre Vertraulichkeitsverpflichtung bewusst gemacht, und zwar durch die intern eingeführten und angewandten Regeln der Unternehmensführung (im vorliegenden Fall durch die „Charta zur Unternehmensführung“, die zudem auf der Website eingesehen werden kann).

In diesem Sinn haben sie 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

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

Wenn Comnexio persönliche Daten in Verbindung mit der Kundschaft von ORES 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, 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 laufen Aktualisierungsübungen mit seinem Register, das der Datenverarbeitung und dem „Data Protection Impact Assessment“ (im Folgenden kurz "DPIA" genannt) dient, um die Risiken im Zusammenhang mit der Verarbeitung bestehender Daten vor Inkrafttreten der DSGVO zu analysieren bzw. einzuschätzen und einen Plan mit entsprechenden Abhilfemaßnahmen vorzusehen. Der Aspekt des Zugriffs auf die persönlichen Daten wird bei diesen Übungen bewertet.
Darüber hinaus wird durch eine Prozedur die Abhaltung solcher DPIA für jede neue Datenverarbeitung auferlegt, „*die ein hohes Risiko für die Rechte und Freiheiten der natürlichen Personen darstellt*“, zumal diese Kunden von ORES sind.

Folgende technische und organisatorische Maßnahmen werden angewandt:

- Das Management der Zugangsberechtigungen für die Computeranwendungen bei ORES (und bei N-Allo bis Juni 2023) wird über das Tool „*SAP Identity Management*“ zentralisiert und automatisiert (Beispiele: SAP: Lopex, procli; *Active directory*: Mercure; Oracle: netgis).
- Die für das Zugangsmanagement angewandte Methodologie ist die sogenannte rollenbasierte Zugriffskontrolle, die von ORES (als IT-Dienstleister von Comnexio) durch die zwei 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 Zugangsrechte für die Computeranwendungen werden von ORES verwaltet und bei Comnexio vom „*Service Delivery Manager*“ validiert.
- Die Lastenhefte für die neuen Softwares verweisen spezifisch auf die obligatorische Integration in das System zum Management der Identitäten und IT-Zugriffsrechte, das von ORES Gen. (als IT-Dienstleister von Comnexio) eingerichtet wurde.

Bezüglich der digitalen Kuppel[4] ist Folgendes zu bemerken:

- Dank des Durchgangs durch die digitale Kuppel kann Comnexio einerseits den Zugriff auf die Kundeninformationen genau überprüfen und andererseits bestimmen, welche Daten die Kundenberater nach ihrem Einloggen einsehen können.
- Eine Dringlichkeitsprozedur wurde für den Fall eingerichtet, dass ein Personalmitglied Comnexio verlässt oder ersetzt wird. Die Zugänge werden dann je nach Fall gesperrt oder zugelassen.
- Das Personal von Comnexio verfügt über ein Log-in an einer Arbeitsstation von ORES auf einem von ORES betriebenen Netz.

[4] Seit dem 31. Dezember 2020 benutzt Comnexio nicht mehr die digitale Kuppel von N-Allo. Letztere wurde durch eine von ORES entwickelte Applikation ersetzt. Die digitale Kuppel von ORES ist eine Schnittstelle, die den Kundenberatern von Comnexio die Bearbeitung der Interaktionen (Identifizierung des Kunden und Automatisierung des Prozesses der Zählerablesung) erleichtert und die Rückverfolgung der Anrufgründe ermöglicht.

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

Comnexio hat Zugriff auf die Daten des CMS (*Central Market System*) und die Datenbank Mercure, um die Telefonate der Kunden an vorderster Front entgegenzunehmen.

Das Management des Zugriffs auf die Softwares vonseiten von Comnexio sowie die Art und Weise, wie die Informationen den Kunden mitgeteilt werden, werden im folgenden Punkt erläutert.

Eingeleitete spezifische Maßnahmen

- *Zugangsregister (CMS)*

  Die IT-Infrastruktur ist abgesichert und der Zugriff auf die Software ist den Berechtigten vorbehalten.
  Jeder neue Zugriffsantrag wird ORES übermittelt, das diesen gemäß seiner internen Prozedur genehmigt. Im Übrigen verweisen wir auf die für ORES Assets und ORES Gen. verfassten Berichte.

  Die innerhalb von Comnexio angewandte Prozedur wird kontrolliert.
  Die Kundenberater 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. Falls ein Kunde den VNB fragt, welcher Energieversorger mit der Zugriffsstelle verbunden ist, wird ihm die Antwort per Postschreiben an die Installationsadresse geschickt.
  Falls ein kommerzieller Energieversorger die Frage stellt, wird sie automatisch an das Portal des CMS 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. Die Information wird ihm anschließend nicht mündlich mitgeteilt, sondern per SMS an die Handynummer geschickt, die der Kunde 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 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 in der digitalen Kuppel aufgezeichnet und verfolgt.

  Comnexio 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..

- *Mercure-System*

  Die IT-Infrastruktur ist geschützt und der Zugang zur Software ist individuell festgelegt und dem Personal von Comnexio im Abänderungsmodus vorbehalten, jedoch nur über eine passwortgeschützte Web-Schnittstelle (*Kuppel*).

  Im Übrigen verweisen wir auf die für ORES Assets und ORES Gen. verfassten Berichte.

  Die innerhalb von Comnexio angewandte Prozedur wird kontrolliert.
  Die Kundenberater erteilen Auskünfte per Telefon, Postschreiben oder E-Mail ausschließlich an den Kunden (oder an einen seiner Beauftragten), der durch seinen EAN-Code anerkannt ist, und zwar nur während des Nutzungszeitraums dieses Kunden. Dabei wird Letzterer aufgefordert, seine Zählernummer zur Überprüfung mitzuteilen.
  Wenn der Kunde 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.

- *Aufzeichnungen*

  Im Einklang mit den Vorschriften des Gesetzes über die elektronischen Kommunikationen werden die Gespräche zwischen den Kundenberatern von Comnexio und den Ansprechpartnern aufgezeichnet.
  So wurden im Rahmen des oben genannten Übergangsvertrags zwischen N-Allo und Comnexio auf Anfrage Letzterer die elektronischen Kommunikationen und die dabei ausgetauschten Daten (Telefonate, Mails, Chats …) der Comnexio-Kundenberater von N-Allo bis zum 25. Mai 2023 gesammelt und aufgezeichnet. Falls die Plattform N-Allo die Aufzeichnung der Interaktionen zwischen den Kunden und den Kundenberatern von Comnexio ermöglichte, standen diese Aufzeichnungen, die in den Comnexio vorbehaltenen Verzeichnissen enthalten sind, schließlich nur noch dem Personal von Comnexio zur Verfügung.

Seit dem 25. Mai 2023 werden die elektronischen Kommunikationen und die dabei ausgetauschten Daten (Telefonate, Mails, Chats …) der Kundenberater von Comnexio auf ihrer neuen Kontaktcenter-Plattform gesammelt und aufgezeichnet.

Standardgemäß werden diese Aufzeichnungen während eines Monats ab dem Datum der Kommunikation aufbewahrt. Für die aufgrund gesetzlicher Verpflichtungen gesammelten Aufzeichnungen ist allerdings eine regelmäßige Extraktion zu Aufbewahrungszwecken vonseiten Comnexio vorgesehen.

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

Vertragliche Maßnahmen

Bei Vergabe von Aufträgen oder Abschluss von Verträgen mit seinen Partnern werden systematisch DSGVO-Klauseln eingefügt. Diese präzisieren sämtliche Aspekte des Artikels 28 der DSGVO: 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.

Spezifische Maßnahmen

Bis zum 25. Mai 2023 im Rahmen des Übergangsvertrags zwischen N-Allo und Comnexio:
In dem zwischen N-Allo und Comnexio geschlossenen Übergangsvertrag ist den Vertragspartnern eine eigene Vertraulichkeitsverpflichtung auferlegt. So hatten sie insbesondere folgende Verpflichtungen zu erfüllen: die Wahrung der Datenvertraulichkeit, die ausschließliche Nutzung im Rahmen der Ausführung der Vereinbarung, die Wahrung der Vertraulichkeit solcher Daten und die Ergreifung von Vorsichtsmaßnahmen zum Datenschutz, keine Weitergabe an Dritte ohne vorherige schriftliche Genehmigung des anderen Vertragspartners und die Rückgabe oder Löschung der vertraulichen Informationen, sofern sie für den anderen Vertragspartner nicht mehr nützlich waren.

Darüber hinaus waren die Rollen im Rahmen der DSGVO wie folgt verteilt, wenn N-Allo oder Comnexio persönliche Daten über die Kunden von ORES verarbeitete: ORES war für die Datenverarbeitung verantwortlich, Comnexio agierte als Subunternehmer und N-Allo als zweitrangiger Subunternehmer aufgrund des Übergangsvertrags. Comnexio bearbeitete die Daten von ORES ausschließlich auf deren Anweisung.

In der Praxis stellte N-Allo dem Unternehmen Comnexio eine Reihe von Applikationen zur Verfügung, die keine sensiblen Daten enthielten, beispielsweise die Kommunikationsplattform und die zugehörigen Applikationen (call flows, IVR ...). Diese Applikationen enthielten also eine sehr begrenzte Anzahl an Kundendaten.
Es sei allerdings darauf hingewiesen, dass die Kommunikationsplattform die Aufzeichnung der Interaktionen zwischen den Kunden und den Kundenberatern von Comnexio ermöglichte. Wir beziehen uns diesbezüglich auf die Erläuterungen des Punktes „Aufzeichnungen“ im Kapitel IV des vorliegenden Berichts.

Das technische Team, welches das Management der Informationssysteme gewährleistete, verfügte ebenfalls über die Zugriffe auf die Datenbanken im strikten Rahmen seines Aufgabenbereichs.

Die Reporting-Umgebung enthielt lediglich beschränkte operative Daten, die mit den Mitarbeitern von Comnexio zusammenhängen konnten. Es befanden sich hingegen keine Kundendaten innerhalb dieser Reporting-Umgebung.

Dasselbe galt schließlich auch für die Applikation Nice WFM zur Ressourcenplanung. Sie enthielt zwar Daten über die Mitarbeiter von Comnexio, jedoch keine über die Netznutzer.

Seit dem 25. Mai 2023 im Rahmen der Vereinbarung zwischen ORES/Comnexio und NTT:
Eine neue (Genesys-Cloud-basierte) Kontaktcenter-Plattform wird von Comnexio genutzt. Diese Plattform wird von einem NTT-Partner bereitgestellt. Das bedeutet, dass Comnexio die N-Allo-Lösung nicht mehr nutzt.
Die entsprechenden vertraglichen Maßnahmen wurden mit dem neuen Subunternehmer umgesetzt, um den Schutz der personenbezogenen Daten der betroffenen Personen (in Form eines *Data Processing Agreement* oder Vereinbarung über die Datenverarbeitung zusätzlich zu den Marktunterlagen) zu gewährleisten. Ein DPIA wurde im November 2023 durchgeführt. Eine Analyse der Sicherheitsrisiken wurde gemäß der EBIOS-Methode durchgeführt, darüber hinaus wurde ein Penetrationstest im September 2023 durchgeführt und die (Schwach)punkte bearbeitet.

IT-Dienstleistungen

Comnexio hat die IT-Direktion von ORES Gen. mit sämtlichen IT-Grundleistungen beauftragt: Lieferung, Installation und Support von Arbeitsstationen, Drucken, Internetzzugang, Verwaltung des *Active Directory*, Netzzugang …

Bis zum 25. Mai 2023 beschränkte sich die Einbindung von N-Allo strikt auf die Verwaltung der Tickets (Vorfälle oder *Service Requests*) bezüglich der Applikationen, die N-Allo dem Unternehmen Comnexio zur Verfügung stellte. Dieser Einbindungsumfang für N-Allo war im oben genannten Übergangsvertrag strikt festgelegt. Der Rahmen dieser Einbindung war in der Praxis durch präzise Prozeduren abgesteckt und wurde vollständig über die IT-Direktion von ORES Gen. ohne direkten Kontakt zwischen N-Allo und den Mitarbeitern von Comnexio verwaltet.

Bei der Gründung von Comnexio war ein IT-Sicherheitssystem eingerichtet und der CWaPE[5] zur Genehmigung unterbreitet worden. Darin ist unter anderem Folgendes vorgesehen:

- eine Unterteilung der IT-Systeme und -Applikationen, die N-Allo dem Unternehmen Comnexio zur Verfügung stellt („*Chinese Wall*"), wie sie im Übergangsvertrag, der zwischen Comnexio und N-Allo für die Dienstleistungen geschlossen wurde, vorgesehen ist:
    - N-Allo garantierte eine Einschränkung der Zugriffe auf die Daten der Applikationen, die ausschließlich den Mitarbeitern von Comnexio und jenem Personal von N-Allo zur Verfügung gestellt wurden, das für die Erbringung von IT-Dienstleistungen unbedingt einen strikten Zugriff benötigte. Diese

[5] Antrag vom 29. März 2019 zur Genehmigung vonseiten der CWaPE bezüglich der Beauftragung einer neuen Tochtergesellschaft von ORES Assets mit den Tätigkeiten eines Kontaktcenters.

Daten wurden darüber hinaus in IT-Umgebungen gespeichert, die Comnexio gehörten und von den IT-Umgebungen der Kunden von N-Allo völlig getrennt waren.

- Comnexio behielt sich das Recht vor, die von ihr für notwendig erachteten Überprüfungen durchzuführen, um insbesondere die effiziente Unterteilung der IT-Applikationen, die von N-Allo zur Verfügung gestellt wurden, sowie die zugehörigen Daten zu kontrollieren. Stellte sich infolge dieser Überprüfungen heraus, dass N-Allo seinen Verpflichtungen in Sachen Unterteilung nicht (mehr) nachkam, so verpflichtete sich N-Allo zur entsprechenden Nacherfüllung innerhalb kürzester Frist.

- eine konkrete Trennung der Tätigkeiten von Comnexio und N-Allo, obwohl beide Unternehmen sich weiterhin die gleichen Gebäude teilten (physikalische Trennung der Teams).

Abschnitt VI – Rückverfolgbarkeit als Vertraulichkeitsgarantie

Comnexio überträgt ORES Gen. die Verwaltung seiner IT-Abteilung.

Detaillierte Informationen über die Verwaltung der Rückverfolgbarkeit der Zugriffe seitens ORES Gen. werden im Vertraulichkeitsbericht von ORES Gen. erteilt.

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

Die IT-Systeme und -Infrastrukturen von Comnexio werden von ORES Gen. aufgrund des oben genannten Support-Dienstleistungsvertrags zwischen ORES Gen. und Comnexio verwaltet. In diesem Zusammenhang entspricht die Lenkung der IT-Sicherheit bei Comnexio derjenigen von ORES, die sich nach der Norm ISO 27001 richtet.

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. 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. Ein externes Audit ist zum Herbstende 2024 geplant.

Folglich beruht die Abtrennung der gemeinsam genutzten Daten auf folgenden 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.

Die spezifischen Maßnahmen bezüglich N-Allo und NTT werden weiter oben erläutert.