



**VERTRAULICHKEITSBERICHT VON
COMNEXIO**

INHALTSVERZEICHNIS

| | |
|--|-----------|
| Abschnitt I - Vorbemerkung..... | 3 |
| Abschnitt II – Verpflichtungen des Personals und der Mitglieder der Verwaltungsorgane in Sachen Datenvertraulichkeit | 5 |
| 1. Verpflichtungen des Personals in Sachen Datenvertraulichkeit..... | 5 |
| 2. Verpflichtungen der Mitglieder der Verwaltungsorgane in Sachen Datenvertraulichkeit..... | 6 |
| Abschnitt III – Sicherheitsmaßnahmen für den Zugriff des Personals auf die persönlichen und kommerziellen Daten | 7 |
| Abschnitt IV – Sicherheitsmaßnahmen bezüglich des Zugriffs der Energieversorger und der Kunden auf die vertraulichen Daten..... | 9 |
| Abschnitt V – Sicherheitsmaßnahmen bezüglich des Zugriffs der Subunternehmer auf die vertraulichen Daten | 12 |
| Abschnitt VI – Rückverfolgbarkeit als Vertraulichkeitsgarantie..... | 14 |
| Abschnitt VII – Gemeinsame Nutzung der IT-Systeme und -Infrastrukturen mit anderen Unternehmen..... | 15 |

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 Assets¹ 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 Connexio. 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 Assets², 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 Connexio 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 2020 von Connexio als Tochtergesellschaft von ORES Assets, die seit dem 1. Juni 2019 als Contact Center von ORES Assets fungiert.

Dieser Bericht wurde vom Ethik-Ausschuss von Connexio genehmigt, dessen Sitzung am 24. März 2021 per Videokonferenz mit TEAMS abgehalten wurde, und zwar aufgrund der Gesundheitssituation und gemäß den Vorschriften des Dekrets vom 14. Januar 2021 über die Organisation - bis einschließlich 31. März - der abgehaltenen Sitzungen der

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).

Interkommunalen und Gesellschaften mit bedeutender öffentlicher Beteiligung in Form einer Anwesenheitssitzung und per Videokonferenz.

Vorab sei daran erinnert, dass folgende wichtige Dienstleistungsverträge von Connexio abgeschlossen wurden, um am 1. Juni 2019 einsatzbereit zu sein:

- ein Übergangsvertrag mit N-Allo. Zweck dieses Vertrags ist die Festlegung der Übergangsleistungen, die N-Allo für Connexio erbringen muss, sowie
- ein Supportvertrag mit ORES Gen., insbesondere für die grundlegenden IT-Dienstleistungen.

Abschließend ist noch darauf hinzuweisen, dass Connexio seinen Tätigkeiten als Contact Center ausschließlich für ORES Assets nachgeht.

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 Connexio 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 Connexio zurückzugeben.

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

Im Laufe des zweiten Halbjahres 2020 wurde das gesamte Linienmanagement und Supportpersonal vom Datenschutzbeauftragten (im Folgenden kurz „DPO“ für „*Data Protection Officer*“ genannt) für die DSGVO sensibilisiert. Diese Mitarbeiter können somit den DPO vor Ort unterstützen.

Darüber hinaus wurde eine Seite des Intranets, die sämtlichen Mitarbeitern von Connexio zugänglich ist, gezielt der IT-Sicherheit und der Datenschutz-Grundverordnung (DSGVO) gewidmet.

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; ein E-Learning über die DSGVO und diverse E-Learning-Module zur Informationssicherheit, die im Jahr 2020 für sämtliche Mitarbeiter eingerichtet wurden. Seit Ende 2020 werden diese Mitteilungen durch ständige Sensibilisierungskampagnen über verschiedene Sicherheitsaspekte unterstützt, und zwar je nach dem ermittelten Kenntnisstand der Mitarbeiter sowie den Hauptrisiken für unsere Daten.

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 Connexio 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 Connexio 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, geplante Arbeiten an Zähleranlagen, GWV, ...

Sowohl ORES als auch Connexio haben Datenschutzverfahren nach dem Prinzip „*Privacy 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 hat Connexio Anfang 2020 Aktualisierungsübungen mit seinem Register gestartet, 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 derzeit abgefasste 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 N-Allo wird über das Tool „SAP Identity Management“ zentralisiert und automatisiert (Beispiele: SAP: Lopex, procli; Active Directory: Mercure, Nationalregister; Oracle: netgis).
- Die für das Zugangsmanagement angewandte Methodologie ist die sogenannte rollenbasierte Zugriffskontrolle, die von ORES (als IT-Dienstleister von Connexio) 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 Connexio 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 Connexio) eingerichtet wurde.

Bezüglich der digitalen Kuppel³ ist Folgendes zu bemerken:

- Dank des Durchgangs durch die digitale Kuppel kann Connexio 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 Connexio verlässt oder ersetzt wird. Die Zugänge werden dann je nach Fall gesperrt oder zugelassen.
- Das Personal von Connexio verfügt über ein Log-in an einer Arbeitsstation von ORES auf einem von ORES betriebenen Netz.

³ Seit dem 31. Dezember 2020 benutzt Connexio nicht mehr die digitale Kuppel von N-Allo. Letztere wurde durch eine von ORES entwickelte Anwendung ersetzt. Die digitale Kuppel von ORES ist eine Schnittstelle, die den Kundenberatern von Connexio 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

Connexio hat 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 von Connexio sowie die Art und Weise, wie die Informationen den Kunden mitgeteilt werden, werden im folgenden Punkt erläutert.

Eingeleitete spezifische Maßnahmen

- *Zugangsregister*

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 Connexio 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 er automatisch an das Zugangsregister (*Supplier-Web*) weitergeleitet, da dieser 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 in der digitalen Kuppel aufgezeichnet und verfolgt.

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

Connexio 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 Connexio im Abänderungsmodus vorbehalten, jedoch nur über eine passwortgeschützte Web-Schnittstelle (*Measure Web*).

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

Die innerhalb von Connexio 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 Zähler mit Kommunikationsfunktion), 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.

- *Aufzeichnungen*

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

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 Connexio 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

In dem zwischen N-Allo und Connexio geschlossenen Übergangsvertrag ist den Vertragspartnern eine eigene Vertraulichkeitsverpflichtung auferlegt. So haben 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 sind.

Darüber hinaus sind die Rollen im Rahmen der DSGVO wie folgt verteilt, wenn N-Allo oder Connexio persönliche Daten über die Kunden von ORES verarbeiten: ORES ist für die Datenverarbeitung verantwortlich, Connexio agiert als Subunternehmer und N-Allo als zweitrangiger Subunternehmer aufgrund des Übergangsvertrags. Connexio bearbeitet die Daten von ORES ausschließlich auf deren Anweisung.

In der Praxis stellt N-Allo dem Unternehmen Connexio eine Reihe von Anwendungen zur Verfügung, die keine sensiblen Daten enthalten, beispielsweise die Kommunikationsplattform und die zugehörigen Anwendungen (*call flows*, IVR, ...). Diese Anwendungen enthalten 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 Connexio ermöglicht. Wir beziehen uns diesbezüglich auf die Erläuterungen des Punktes „Aufzeichnungen“ im Kapitel IV des vorliegenden Berichts.

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

Die Reporting-Umgebung enthält lediglich beschränkte operative Daten, die mit den Mitarbeitern von Connexio zusammenhängen können. Es befinden sich hingegen keine Kundendaten innerhalb dieser Reporting-Umgebung.

Dasselbe gilt schließlich auch für die Anwendung Nice WFM zur Ressourcenplanung. Sie enthält zwar Daten über die Mitarbeiter von Connexio, jedoch keine über die Netzbenutzer.

IT-Dienstleistungen

Connexio hat den IT-Geschäftsbereich von ORES Gen. mit sämtlichen IT-Grundleistungen beauftragt: Lieferung, Installation und Support von Arbeitsstationen, Drucken, Internetzugang, Verwaltung des Active Directory, Netzzugang, ... Die Einbindung von N-Allo beschränkt sich strikt auf die Verwaltung der Tickets (Vorfälle oder *Service Requests*) bezüglich der Anwendungen, die N-Allo dem Unternehmen Connexio zur Verfügung stellt. Dieser Einbindungsumfang für N-Allo ist im oben genannten Übergangsvertrag strikt festgelegt. Der Rahmen dieser Einbindung ist in der Praxis durch präzise Prozeduren abgesteckt und wird vollständig über den IT-Geschäftsbereich von ORES Gen. ohne direkten Kontakt zwischen N-Allo und den Mitarbeitern von Connexio verwaltet.

Bei der Gründung von Connexio wurde ein IT-Sicherheitssystem eingerichtet und der CWaPE⁴ zur Genehmigung unterbreitet. Darin ist unter anderem Folgendes vorgesehen:

- eine Unterteilung der IT-Systeme und -Anwendungen, die N-Allo dem Unternehmen Connexio zur Verfügung stellt („Chinese Wall“), wie sie im Übergangsvertrag, der zwischen Connexio und N-Allo für die Dienstleistungen geschlossen wurde, vorgesehen ist:
 - o N-Allo garantiert eine Einschränkung der Zugriffe auf die Daten der Anwendungen, die ausschließlich den Mitarbeitern von Connexio und jenem Personal von N-Allo zur Verfügung gestellt werden, das für die Erbringung von IT-Dienstleistungen unbedingt einen strikten Zugriff benötigt. Diese Daten werden darüber hinaus in IT-Umgebungen gespeichert, die Connexio gehören und von den IT-Umgebungen der Kunden von N-Allo völlig getrennt sind.
 - o Connexio behält sich das Recht vor, die von ihr für notwendig erachteten Überprüfungen durchzuführen, um insbesondere die effiziente Unterteilung der IT-Anwendungen, die von N-Allo zur Verfügung gestellt werden, sowie die zugehörigen Daten zu kontrollieren. Stellt sich infolge dieser Überprüfungen heraus, dass N-Allo seinen Verpflichtungen in Sachen Unterteilung nicht (mehr) nachkommt, so verpflichtet sich N-Allo zur entsprechenden Nacherfüllung innerhalb kürzester Frist.
- Eine konkrete Trennung der Tätigkeiten von Connexio und N-Allo, obwohl beide Unternehmen sich weiterhin die gleichen Gebäude teilen (physikalische Trennung der Teams).

⁴ Antrag vom 29.3.2019 zur Genehmigung vonseiten der CWaPE bezüglich der Beauftragung einer neuen Tochtergesellschaft von ORES Assets mit den Tätigkeiten eines Contact Centers.

Abschnitt VI – Rückverfolgbarkeit als Vertraulichkeitsgarantie

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

Folglich beruht die Abtrennung der gemeinsam genutzten Daten auf folgende Prinzipien:

- die Erteilung des „geringsten Privilegs“ („*least privilege*“): Standardgemäß dürfen einem Benutzer 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 Benutzer darf eine Information nur einsehen, wenn dies aufgrund eines realen 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 werden weiter oben erläutert.