Vertrag zur Auftragsverarbeitung gemäß Art. 28 DS-GVO

zur Unified Communications Plattform Rainbow

Vereinbarung

zwischen dem/der

Auftraggeber

Straße

Hausnummer

- Verantwortlicher - nachstehend Auftraggeber genannt -

und dem/der

ALE International

32 avenue Kléber

92707 Colombes cedex / FRANKREICH

- Auftragsverarbeiter - nachstehend Auftragnehmer genannt

1. Gegenstand und Dauer des Auftrags

(1) Gegenstand

Art und Zweck der Verarbeitung personenbezogener Daten durch den Auftragnehmer für den Auftraggeber:

a) Bereitstellung einer Online-Plattform für die digitale Zusammenarbeit („Rainbow“) unter der Domain https://www.openrainbow.com.

Die Cloud-Plattform „Rainbow“ bietet folgende Funktionalitäten (Features):

- das Anlegen von Nutzerkonten
- das Löschen von Nutzerkonten
- das Anlegen und Management von Terminen in der Kalenderfunktion
- das Anlegen von virtuellen Konferenzräumen („Bubbles“)
- das Anzeigen von Präsenzstatus von Nutzern
- das Versenden von Einladungen aus „Rainbow“
- die virtuelle Zusammenarbeit per Chat

- die virtuelle Zusammenarbeit per Audio und Videokonferenz
- das Speichern und Teilen von Dateien

Die Funktionalitäten können jederzeit durch den Auftragnehmer erweitert werden. Die Nutzung der angebotenen Erweiterungen steht dem Auftraggeber frei.

b) Technischer Support

Insofern angefordert, bietet der Auftragnehmer technischen Support an. Dieser erfolgt durch Fernzugriff über eine verschlüsselte Verbindung.

Die Erbringung der vertraglich vereinbarten Datenverarbeitung findet auf Servern am Standort Deutschland statt. Wartungs- und Servicearbeiten können von anderen Standorten des Auftragsnehmers in Mitgliedsstaaten der Europäischen Union oder in einem anderen Vertragsstaat des Abkommens über den Europäischen Wirtschaftsraum erfolgen. Jede Verlagerung in ein Drittland bedarf der vorherigen Zustimmung des Auftraggebers und darf nur erfolgen, wenn die besonderen Voraussetzungen der Art. 44 ff. DS-GVO erfüllt sind.

(2) Dauer

Die Dauer dieses Auftragsverarbeitungsvertrags gilt unbefristet, beziehungsweise solange eine Geschäftsbeziehung zwischen den beiden Parteien besteht.

2. Datenkategorien und betroffenen Personengruppen

(2) Art der Daten

Gegenstand der Verarbeitung personenbezogener Daten sind folgende Datenarten/-kategorien:

- Namen
- Vornamen
- Titel
- Nutzernamen
- Telefonnummern
- E-Mail-Adressen
- Firmenzugehörigkeit
- ggf. Funktion oder Abteilung
- Bilder (Profilbilder)
- Audiodaten im Rahmen von Audiokonferenzen und Videokonferenzen
- Videodaten im Rahmen von Videokonferenzen
- Logfiles (An- und Abmeldungen)
- Im Kontext der virtuellen Zusammenarbeit durch den Auftraggeber hochgeladene Daten

(3) Kategorien betroffener Personen

Die Kategorien der durch die Verarbeitung betroffenen Personen umfassen:

- Beschäftigte des Auftraggebers
- ggf. Partner, Kunden oder Interessenten des Auftraggebers
- ggf. Dienstleister oder Lieferanten des Auftraggebers
- ggf. sonstige nicht näher bestimmbare Dritte Personen, die der Auftraggeber zur Kommunikation in Rainbow einlädt

3. Technisch-organisatorische Maßnahmen

(1) Der Auftragnehmer hat die Umsetzung der im Vorfeld der Auftragsvergabe dargelegten und erforderlichen technischen und organisatorischen Maßnahmen vor Beginn der Verarbeitung, insbesondere hinsichtlich der konkreten Auftragsdurchführung zu dokumentieren und dem Auftraggeber zur Prüfung zu übergeben. Bei Akzeptanz durch den Auftraggeber werden die dokumentierten Maßnahmen Grundlage des Auftrags. Soweit die Prüfung/ein Audit des Auftraggebers einen Anpassungsbedarf ergibt, ist dieser einvernehmlich umzusetzen.

(2) Der Auftragnehmer hat die Sicherheit gem. Art. 28 Abs. 3 lit. c, 32 DS-GVO insbesondere in Verbindung mit Art. 5 Abs. 1, Abs. 2 DS-GVO herzustellen. Insgesamt handelt es sich bei den zu treffenden Maßnahmen um Maßnahmen der Datensicherheit und zur Gewährleistung eines dem Risiko angemessenen Schutzniveaus hinsichtlich der Vertraulichkeit, der Integrität, der Verfügbarkeit sowie der Belastbarkeit der Systeme. Dabei sind der Stand der Technik, die Implementierungskosten und die Art, der Umfang und die Zwecke der Verarbeitung sowie die unterschiedliche Eintrittswahrscheinlichkeit und Schwere des Risikos für die Rechte und Freiheiten natürlicher Personen im Sinne von Art. 32 Abs. 1 DS-GVO zu berücksichtigen.

(3) Die technischen und organisatorischen Maßnahmen unterliegen dem technischen Fortschritt und der Weiterentwicklung. Insoweit ist es dem Auftragnehmer gestattet, alternative adäquate Maßnahmen umzusetzen. Dabei darf das Sicherheitsniveau der festgelegten Maßnahmen nicht unterschritten werden. Wesentliche Änderungen sind zu dokumentieren.

4. Berichtigung, Einschränkung und Löschung von Daten

(1) Der Auftragnehmer darf die Daten, die im Auftrag verarbeitet werden, nicht eigenmächtig, sondern nur nach dokumentierter Weisung des Auftraggebers berichtigen, löschen oder deren Verarbeitung einschränken. Soweit eine betroffene Person sich diesbezüglich unmittelbar an den Auftragnehmer wendet, wird der Auftragnehmer dieses Ersuchen unverzüglich an den Auftraggeber weiterleiten.

(2) Soweit vom Leistungsumfang umfasst, sind Löschkonzept, Recht auf Vergessenwerden, Berichtigung, Datenportabilität und Auskunft nach dokumentierter Weisung des Auftraggebers unmittelbar durch den Auftragnehmer sicherzustellen.

5. Qualitätssicherung und sonstige Pflichten des Auftragnehmers

Der Auftragnehmer hat zusätzlich zu der Einhaltung der Regelungen dieses Auftrags gesetzliche Pflichten gemäß Art. 28 bis 33 DS-GVO; insofern gewährleistet er insbesondere die Einhaltung folgender Vorgaben:

a) Schriftliche Bestellung eines Datenschutzbeauftragten, der seine Tätigkeit gemäß Art. 38 und 39 DS-GVO ausübt.

   Name und Kontaktdaten des Konzern-Datenschutzbeauftragten der ALE International:
   Louis-Philippe Ollier
   dataprivacy@al-enterprise.com

   Name des lokalen Datenschutzbeauftragten für ALE Deutschland GmbH:
   Fabian Henkel
   info@externer-datenschutzbeauftragter-stuttgart.de
   Tel. +497152 564773
   Fax. +497152 564771

   Die jeweils aktuellen Kontaktdaten des Datenschutzbeauftragten finden Sie in der Datenschutzerkläung des ALE international Internetauftritts.

b) Die Wahrung der Vertraulichkeit gemäß Art. 28 Abs. 3 S. 2 lit. b, 29, 32 Abs. 4 DS-GVO. Der Auftragnehmer setzt bei der Durchführung der Arbeiten nur Beschäftigte ein, die auf die Vertraulichkeit verpflichtet und zuvor mit den für sie relevanten Bestimmungen zum Datenschutz vertraut gemacht wurden. Der Auftragnehmer und jede dem Auftragnehmer unterstellte Person, die Zugang zu personenbezogenen Daten hat, dürfen diese Daten ausschließlich entsprechend der Weisung des Auftraggebers verarbeiten einschließlich der in diesem Vertrag eingeräumten Befugnisse, es sei denn, dass sie gesetzlich zur Verarbeitung verpflichtet sind.

c) Die Umsetzung und Einhaltung aller für diesen Auftrag erforderlichen technischen und organisatorischen Maßnahmen gemäß Art. 28 Abs. 3 S. 2 lit. c, 32 DS-GVO.

d) Der Auftraggeber und der Auftragnehmer arbeiten auf Anfrage mit der Aufsichtsbehörde bei der Erfüllung ihrer Aufgaben zusammen.

e) Die unverzügliche Information des Auftraggebers über Kontrollhandlungen und Maßnahmen der Aufsichtsbehörde, soweit sie sich auf diesen Auftrag beziehen. Dies gilt auch, soweit eine zuständige Behörde im Rahmen eines Ordnungswidrigkeits- oder Strafverfahrens in Bezug auf die Verarbeitung personenbezogener Daten bei der

Auftragsverarbeitung beim Auftragnehmer ermittelt.

f) Soweit der Auftraggeber seinerseits einer Kontrolle der Aufsichtsbehörde, einem Ordnungswidrigkeits- oder Strafverfahren, dem Haftungsanspruch einer betroffenen Person oder eines Dritten oder einem anderen Anspruch im Zusammenhang mit der Auftragsverarbeitung beim Auftragnehmer ausgesetzt ist, hat ihn der Auftragnehmer nach besten Kräften zu unterstützen.

g) Der Auftragnehmer kontrolliert regelmäßig die internen Prozesse sowie die technischen und organisatorischen Maßnahmen, um zu gewährleisten, dass die Verarbeitung in seinem Verantwortungsbereich im Einklang mit den Anforderungen des geltenden Datenschutzrechts erfolgt und der Schutz der Rechte der betroffenen Person gewährleistet wird.

h) Nachweisbarkeit der getroffenen technischen und organisatorischen Maßnahmen gegenüber dem Auftraggeber im Rahmen seiner Kontrollbefugnisse nach Ziffer 7 dieses Vertrages.

i) Der Auftragnehmer führt ein Verzeichnis der Verarbeitungstätigkeiten nach Art. 30 Abs. 2 DS-GVO.

j) Sollte das Eigentum oder die Vertraulichkeit der Daten des Auftraggebers bei dem Auftragnehmer durch Maßnahmen Dritter (etwa durch Pfändung), durch Insolvenz- oder Vergleichsverfahren oder durch sonstige Ereignisse gefährdet werden, so hat der Auftragnehmer den Auftraggeber unverzüglich zu informieren.

k) Der Auftragnehmer informiert den Auftraggeber unverzüglich bei schwerwiegenden Störungen des Betriebsablaufs, Verdacht auf Verletzungen des Schutzes personenbezogener Daten, anderen Unregelmäßigkeiten bei der Datenverarbeitung, bei Kontrollhandlungen und Maßnahmen einer Aufsichts- oder Ermittlungsbehörde. Der Auftragnehmer benachrichtigt unverzüglich den Auftraggeber, wenn die bei ihm getroffenen Sicherheitsmaßnahmen den Anforderungen des Auftraggebers nicht (mehr) genügen.

6. Unterauftragsverhältnisse

(1) Als Unterauftragsverhältnisse im Sinne dieser Regelung sind solche Dienstleistungen zu verstehen, die sich unmittelbar auf die Erbringung der Hauptleistung beziehen.

Nicht hierzu gehören Nebenleistungen, die der Auftragnehmer z.B. als Telekommunikationsleistungen, Post-/Transportdienstleistungen, Wartung und Benutzerservice oder die Entsorgung von Datenträgern sowie sonstige Maßnahmen zur Sicherstellung der Vertraulichkeit, Verfügbarkeit, Integrität und Belastbarkeit der Hard- und Software von Datenverarbeitungsanlagen in Anspruch nimmt, in deren Kontext kein direkter Zugriff auf Daten des Auftraggebers stattfindet.

Der Auftragnehmer ist jedoch verpflichtet, zur Gewährleistung des Datenschutzes und der Datensicherheit der Daten des Auftraggebers auch bei ausgelagerten Nebenleistungen angemessene und gesetzeskonforme vertragliche Vereinbarungen sowie Kontrollmaßnahmen zu ergreifen.

(2) Der Auftragnehmer darf Unterauftragnehmer (weitere Auftragsverarbeiter) nur nach vorheriger Information des Auftraggebers beauftragen. Der Auftraggeber hat das Recht, den Unterauftragnehmer abzulehnen.

Die Auslagerung auf Unterauftragnehmer oder der Wechsel des bestehenden Unterauftragnehmers sind zulässig, soweit:
- der Auftragnehmer eine solche Auslagerung auf Unterauftragnehmer dem Auftraggeber eine angemessene Zeit vorab schriftlich oder in Textform anzeigt und
- der Auftraggeber nicht bis zum Zeitpunkt der Übergabe der Daten gegenüber dem Auftragnehmer schriftlich oder in Textform Einspruch gegen die geplante Auslagerung erhebt und
- eine vertragliche Vereinbarung nach Maßgabe des Art. 28 Abs. 2-4 DS-GVO zugrunde gelegt wird.

(3) Die Weitergabe von personenbezogenen Daten des Auftraggebers an den Unterauftragnehmer und dessen erstmaliges Tätigwerden sind erst mit Vorliegen aller Voraussetzungen für eine Unterbeauftragung gestattet.

(4) Erbringt der Unterauftragnehmer die vereinbarte Leistung außerhalb der EU/des EWR stellt der Auftragnehmer die datenschutzrechtliche Zulässigkeit durch entsprechende Maßnahmen sicher. Gleiches gilt, wenn Dienstleister eingesetzt werden sollen.

7. Kontrollrechte des Auftraggebers

(1) Der Auftraggeber ist berechtigt, die Einhaltung der Vorschriften über den Datenschutz und die vertraglichen Vereinbarungen im Rahmen des Auftragsverhältnisses im erforderlichen Umfang zu kontrollieren oder durch eine von ihm beauftragte Person kontrollieren zu lassen, insbesondere durch die Einholung von Auskünften und die Einsichtnahme in die gespeicherten Daten und die Datenverarbeitungsprogramme im Rahmen von Inspektionen. .

(2) Der Auftragnehmer stellt sicher, dass sich der Auftraggeber von der Einhaltung der Pflichten des Auftragnehmers nach Art. 28 DS-GVO überzeugen kann. Der Auftragnehmer verpflichtet sich, dem Auftraggeber auf Anforderung die erforderlichen Auskünfte zu erteilen und insbesondere die Umsetzung der technischen und organisatorischen Maßnahmen nachzuweisen.

(3) Der Nachweis solcher Maßnahmen, die nicht nur den konkreten Auftrag betreffen, kann erfolgen durch

- die Einhaltung genehmigter Verhaltensregeln gemäß Art. 40 DS-GVO;
- die Zertifizierung nach einem genehmigten Zertifizierungsverfahren gemäß Art. 42 DS-GVO;
- aktuelle Testate, Berichte oder Berichtsauszüge unabhängiger Instanzen (z.B. Wirtschaftsprüfer, Revision, Datenschutzbeauftragter, IT-Sicherheitsabteilung, Datenschutzauditoren, Qualitätsauditoren);
- eine geeignete Zertifizierung durch IT-Sicherheits- oder Datenschutzaudit (z.B. nach BSI-Grundschutz, DIN-ISO27001 Zertifizierung).

8. Mitteilung bei Verstößen des Auftragnehmers

(1) Der Auftragnehmer unterstützt den Auftraggeber bei der Einhaltung der in den Artikeln 32 bis 36 der DS-GVO genannten Pflichten zur Sicherheit personenbezogener Daten, Meldepflichten bei Datenpannen, Datenschutz-Folgeabschätzungen und vorherige Konsultationen. Hierzu gehören u.a.

a) die Sicherstellung eines angemessenen Schutzniveaus durch technische und organisatorische Maßnahmen, die die Umstände und Zwecke der Verarbeitung sowie die prognostizierte Wahrscheinlichkeit und Schwere einer möglichen Rechtsverletzung durch Sicherheitslücken berücksichtigen und eine sofortige Feststellung von relevanten Verletzungsereignissen ermöglichen.

b) die Verpflichtung, Verletzungen personenbezogener Daten unverzüglich an den Auftraggeber zu melden.

c) die Verpflichtung, dem Auftraggeber im Rahmen seiner Informationspflicht gegenüber dem Betroffenen zu unterstützen und ihm in diesem Zusammenhang sämtliche relevante Informationen unverzüglich zur Verfügung zu stellen.

d) die Unterstützung des Auftraggebers für dessen Datenschutz-Folgenabschätzung.

e) die Unterstützung des Auftraggebers im Rahmen vorheriger Konsultationen mit der Aufsichtsbehörde.

(2) Für Unterstützungsleistungen, die nicht in der Leistungsbeschreibung enthalten oder nicht auf ein Fehlverhalten des Auftragnehmers zurückzuführen sind, kann der Auftragnehmer eine Vergütung beanspruchen.

9. Weisungsbefugnis des Auftraggebers

(1) Der Auftraggeber hat das Recht, dem Auftragnehmer Weisungen zu erteilen hinsichtlich der Verarbeitung der personenbezogenen Daten. Diese sind zu dokumentieren.

(2) Mündliche Weisungen bestätigt der Auftraggeber unverzüglich (mind. Textform).

(3) Der Auftragnehmer hat den Auftraggeber unverzüglich zu informieren, wenn er der Meinung ist, eine Weisung verstoße gegen Datenschutzvorschriften. Der Auftragnehmer ist berechtigt, die Durchführung der entsprechenden Weisung solange auszusetzen, bis sie durch den Auftraggeber bestätigt oder geändert wird.

10. Löschung und Rückgabe von personenbezogenen Daten

(1) Kopien oder Duplikate der Daten werden ohne Wissen des Auftraggebers nicht erstellt. Hiervon ausgenommen sind Sicherheitskopien BACK UPs, soweit sie zur Gewährleistung einer ordnungsgemäßen Datenverarbeitung erforderlich sind, sowie Daten, die im Hinblick auf die Einhaltung gesetzlicher Aufbewahrungspflichten erforderlich sind.

(2) Nach Abschluss der vertraglich vereinbarten Arbeiten oder früher nach Aufforderung durch den Auftraggeber – spätestens mit Beendigung der Leistungsvereinbarung – hat der Auftragnehmer sämtliche in seinen Besitz gelangten Unterlagen, erstellte Verarbeitungs- und Nutzungsergebnisse sowie Datenbestände, die im Zusammenhang mit dem Auftragsverhältnis stehen, dem Auftraggeber auszuhändigen oder nach vorheriger Zustimmung datenschutzgerecht zu vernichten. Gleiches gilt für Test- und Ausschussmaterial. Das Protokoll der Löschung ist auf Anforderung vorzulegen.

(3) Dokumentationen, die dem Nachweis der auftrags- und ordnungsgemäßen Datenverarbeitung dienen, sind durch den Auftragnehmer entsprechend der jeweiligen Aufbewahrungsfristen über das Vertragsende hinaus aufzubewahren. Er kann sie zu seiner Entlastung bei Vertragsende dem Auftraggeber übergeben.

11. Haftung

Der Auftragnehmer haftet für Schäden, die durch die Verletzung seiner Pflichten entstanden sind. Dies betrifft insbesondere Schäden, die durch eine nicht der Datenschutz-Grundverordnung entsprechende Datenverarbeitung verursacht wurden oder die aufgrund einer Nichtbeachtung der Weisungen des Auftraggebers resultieren. Der Auftragnehmer wird von der Haftung befreit, wenn er nachweist, dass er in keiner Weise für einen entstandenen Schaden verantwortlich ist.

12. Sonstiges

(1) Änderungen, Ergänzungen und Nebenabreden dieses Vertrages bedürfen der Schriftform.

(2) Sollten in dieser Vereinbarung eine oder mehrere Bestimmungen unwirksam oder undurchführbar sein oder werden, so wird die Wirksamkeit der übrigen Vertragsbestimmungen hierdurch nicht berührt. Die Vertragspartner werden die unwirksame oder undurchführbare Bestimmung durch eine Bestimmung ersetzen, die deren Sinn und Zweck am nächsten kommt. Gleiches gilt für den Fall einer ungewollten Regelungslücke.

_____	_____
Ort, Datum	Ort, Datum
_____	_____
Unterschrift Auftraggeber	Unterschrift Auftragnehmer

Anlage 1 - Unterauftragnehmer

Firma Unterauftragnehmer	ADRESSE	Leistung	MIT DEM SUBPROZESSOR GETEILTE DATEN	DATENVERARBEITUNGS STANDORT
OVH	2 rue Kellermann, 59100 Roubaix, France	Hosting	Hosting bedeutet hier Rechenzentrumsdienste: Hardware, Konnektivität: kein Zugriff auf Daten	France
IBM France	17 avenue de l'Europe 92275 Bois Colombes Cedex France	Failover für das Hosting	Hosting bedeutet hier Rechenzentrumsdienste: Hardware, Konnektivität: kein Zugriff auf Daten	France
X-act	Luis Morote 6, 6e Planta, 35007 Las Palmas de Gran Canaria, Spain	L1 and L2 support	Beschreibung des Support-Tickets, wie vom Einsender bereitgestellt, und angehängte Protokolle (Protokolle sind anonymisiert und enthalten niemals Inhalte, die vom Endbenutzer im Zusammenhang mit der Nutzung von Rainbow gespeichert oder weitergegeben wurden)	Spain
Slash support / CSS, now "MOVATE" corp.	1900 Mc Carthy Blv. Suite 210, Milpitas California, USA	L1 and L2 support	Beschreibung des Support-Tickets, wie vom Einsender bereitgestellt, und angehängte Protokolle (Protokolle sind anonymisiert und enthalten niemals Inhalte, die vom Endbenutzer im Zusammenhang mit der Nutzung von Rainbow gespeichert oder weitergegeben wurden)	USA, India
SalesForce.com EMEA limited	Floor 26 Salesforce Tower, 110 Bishopsgate London EC2N 4AY, United Kingdom	Support-Ticketing-Tool im SaaS-Betrieb	Speicherung von Support-Tickets (Beschreibung wie vom Endkunden angegeben und anonymisierte Protokolle) und Speicherung von Geschäftspartnerinformationen	UK
LoopUp ltd.	The Tea Building, 56 Shoreditch High Street, London, E1 6JJ, United Kingdom	Telefonkonferenz	CDR für die Abrechnung des Verkehrs im Zusammenhang mit PSTN-Konferenzen. Die CDR enthalten die vom PSTN-Netz bereitgestellte Anrufernummer und die DDI des angerufenen Konferenzdienstes. Weitere personenbezogene Daten sind in diesen CDRs nicht enthalten.	UK
Amigo Software	33 Hatley Avenue, Barkingside, Ilford, Essex IG6 1EG United Kingdom	L3-Unterstützung für spezifische Client-Anwendungen	Beschreibung des Support-Tickets, wie vom Einsender bereitgestellt, und angehängte Protokolle (Protokolle sind anonymisiert und enthalten niemals Inhalte, die vom Endbenutzer im Zusammenhang mit der Nutzung von Rainbow gespeichert oder weitergegeben wurden)	UK, Canada, Pakistan
ASAL technologies	3rd floor, Q Center- companies building Rawabi, Palestine	L3-Unterstützung für spezifische Client-Anwendungen	Beschreibung des Support-Tickets, wie vom Einsender bereitgestellt, und angehängte Protokolle (Protokolle sind anonymisiert und enthalten niemals Inhalte, die vom Endbenutzer im Zusammenhang mit der Nutzung von Rainbow gespeichert oder weitergegeben wurden)	Palestine territories
Zuora	1051 E. Hillsdale Blvd, Suite 600, Foster City, CA 94404, USA	SaaS-Abrechnungstool	CDR für die Abrechnung des Verkehrs im Zusammenhang mit PSTN-Konferenzen. Die CDR enthalten die vom PSTN-Netz bereitgestellte Anrufernummer und die DDI des angerufenen Konferenzdienstes. Weitere personenbezogene Daten sind in diesen CDRs nicht enthalten.	USA

Anlage 2 - Technische und Organisatorische Maßnahmen

Technische und organisatorische Maßnahmen
ALE Corporation und ALE Rainbow

Inhalt

Vorwort

Ziel dieses Dokuments ist es, die bei ALE durchgeführten technischen und organisatorischen Maßnahmen aufzuzeigen, die dem Schutz von Daten, insbesondere personenbezogenen Daten, dienen.

Ziel dieser Maßnahmen ist die Sicherstellung der Kontrollziele Vertraulichkeit, Integrität und Verfügbarkeit, die eine Standardmethodik darstellen, um ein angemessenes Datenschutzniveau aufzuzeigen.

Zusatz für ALE Rainbow

Im Rahmen des Rainbow Service ist ALE Datenverarbeiter und verantwortlich für die Datensicherheit, dies gilt auch beim Einsatz von Unterauftragnehmern. Dies trifft nicht zu, wenn der Dienst Rainbow auf dem Server eines Dritten (on premises) ausgeführt wird.

Zertifizierte Sicherheit

Rainbow ist nach DIN ISO 27001:2013 ISO 27017 und ISO 27018 zertifiziert, die jederzeit zu https://support.openrainbow.com/hc/fr/articles/360003802400-ISO-Certification-EN-

Hosting mit OVH

Da Rainbow bei OVH gehostet wird, gehen wir in diesem Dokument insbesondere auch auf die technischen und organisatorischen Maßnahmen bei OVH ein. OVH setzt sich für die optimale Sicherheit seiner Infrastrukturen ein, einschließlich der Umsetzung einer Sicherheitsrichtlinie für Informationssysteme. Darüber hinaus erfüllen OVH-Infrastrukturen zahlreiche internationale Standards und sind nach PCI DSS, ISO/IEC 27001, SOC 1 TYPE II und SOC 2 TYPE II usw. zertifiziert.

- Weitere Informationen zum Datenschutz und zur Datensicherheit bei OVH finden Sie unter https://www.ovh.de/schutz-personenbezogener-daten/sicherheit.xml.

- Außerdem finden Sie eine Zusammenfassung hier https://www.ovh.de/files/2018-06/plaquette-gdpr-DE-FINAL.pdf.

Relevante Ergänzungen zu den technischen und organisatorischen Maßnahmen bei OVH finden Sie in der Anlage.

1. Vertraulichkeit

1.1 Physische Zutrittskontrolle und -sicherheit

Schließsysteme
ALE verwendet in der Regel elektronische Zutrittskontrollsysteme. Manuelle Verriegelungssysteme werden manchmal noch für kleinere ALE-Standorte eingesetzt.

Die jeweiligen Zutrittsberechtigungen werden organisatorisch und technisch von autorisiertem Personal vergeben.

Jeder ALE Beschäftigte ist zur Einhaltung von Verhaltensregeln im Umgang mit elektronischen Schließsystemen verpflichtet. Insofern ein Transponder (oder Schlüssel) verloren geht, ist dies umgehend zu melden, um entsprechende Maßnahmen einzuleiten.

Verpflichtung zum Tragen von Ausweisen / ALE Badges
Das Tragen von ALE Badges ist verpflichtend und zeigt den Status des Trägers an (Mitarbeiter, Besucher, Gast oder Nicht-Mitarbeiter). Sie bleiben Eigentum des Unternehmens.

Besucherreglung
Besucher werden registriert und müssen zu jedem Zeitpunkt sichtbar ein Badge tragen und von einem ALE-Mitarbeiter begleitet werden.

Sensible Bereiche
Der Zutritt zu sensiblen Bereichen (z.B. Rechenzentrum) wird nach dem Minimalprinzip nach Erforderlichkeit genehmigt und registriert. Sensible Bereiche werden auch außerhalb der regulären Geschäftszeiten überwacht.

Liefer- und Ladezonen
Liefer- und Ladezonen, die für den Empfang oder die Verteilung von Lieferungen genutzt werden, sind mit einer Außen- und Innentür gesichert, die nicht gleichzeitig geöffnet werden können.

Videoüberwachung
Videoüberwachung (CCTV) deckt die wichtigsten Einstiegspunkte, Hauptlobby, Laderampe und Parkplätze für große Standorte ab.

Clean Desk Policy
Jeder Schreibtisch muss am Ende des Arbeitstages aufgeräumt werden, Computer müssen ausgeschaltet werden.

Sicherheitsfenster
Fensteröffnungsbegrenzer sind an den Fenstern im Erdgeschoss installiert.

1.2 Zugangskontrolle auf IT-Ressourcen ALE

Zugangskontrollmaßnahmen zu Infrastrukturressourcen in ALE-Standorten

Identitäts- und Zugriffsverwaltung

Die Identitäts- und Zugriffsverwaltung basiert auf der zu erreichenden Aufgabenfunktion oder Aufgabe; und spiegelt die Grundsätze der Trennung von Pflichten und der geringsten Privilegien wider.

Folgende Kategorien werden verwendet:

Mitarbeiter - Ein Festangestellter oder Teilzeitbeschäftigter, der Zugriffsrechte auf die meisten Unternehmensnetzwerke, Anwendungen und internen Informationen benötigt (die ansonsten keiner Zugriffsbeschränkung unterliegen). Dieser Mitarbeiter führt Aktivitäten aus, die Teil des ALE-Geschäfts sind, im Gegensatz zu peripheren Diensten wie Büroreinigung, Bewachung oder Kantine.

Zeitarbeitnehmer - Eine Person, die Aktivitäten im Rahmen einer (Unterauftrags-)Vereinbarung mit ALE in Bezug auf ein bestimmtes Projekt oder einen bestimmten Auftrag ausführt. Dies kann auch ein Student / Praktikant sein.

Dritte - Eine Person, die eingeschränkte Zugriffsrechte hat, um die unbefugte Weitergabe interner Informationen zu verhindern und das Risiko für das Netzwerk zu begrenzen. Dies umfasst unter anderem: Agenten, Kunden, Lieferanten, Lieferanten, Remote-System-Support und -Wartung, einen externen Prüfer, einen Berater usw.

Eindeutige Benutzer-ID und Zugriff

Jede Person erhält eine eindeutige **Benutzer-ID** für den Zugriff auf ALE-Informationsressourcen. Konto-IDs ermöglichen die Unterscheidung zwischen Benutzer-, Administrator- (privilegierten) und Dienstkonten.

Zu den Benutzerprofilen gehören mindestens:

- Name;
- Kategorisierung des Benutzerzugriffs (z. B. Mitarbeiter, Zeitarbeitnehmer, Dritte);
- Unternehmen (wie juristische Personen, Kunden, Lieferanten);
- eindeutige Kennung (eindeutige Personalkennung);
- Unternehmensverzeichnis-ID (Corporate Short Login);
- Standort (einschließlich Land);
- Supervisor / Hierarchie (Name des ALE-Managers);
- Überprüfungsinformationen zur Authentifizierung der Person (z. B. vertrauliche Informationen, die beim Anfordern eines Zurücksetzens des Kennworts an den Service Desk verwendet werden). Diese können in einem separaten System aufbewahrt werden, wenn dies erforderlich ist.

Benutzer-ID / Dienstkonto Authentifizierung & Kennwortverwaltung

Authentifizierungsmechanismen können
- Passwort / PIN oder
- Zwei-Faktor-Authentifizierung
  (z. B. Passwort mit Software-Token oder digitalen Zertifikat verbunden).

Kennwortrichtlinien

Kennwörter haben

- mindestens acht (8) Zeichen für Benutzerkonten und
- zwanzig (20) Zeichen für Dienstkonten.

Kennwörter müssen drei von für Klassen enthalten:
- Großbuchstaben
- Kleinbuchstaben
- Ziffern
- Sonderzeichen.

Überwachung des Einsatzes von ALE-Informationssystemen

- Sicherstellung und Überwachung der Einhaltung der geltenden Gesetze und Vorschriften;
- Gewährleistung der effektiven Nutzung der Informationssysteme und ihres normalen Betriebs;
- Gewährleistung der effektiven Vertraulichkeit und Integrität der ALE-Daten und Einhaltung deren Sicherheitsverpflichtungen durch die Mitarbeiter;
- Sicherstellung der ALE-Informationssystem durch Funktionen zur Erkennung von Sicherheitsbedrohungen, einschließlich Viren, Trojaner, Würmer, Malware und Spam (unerwünschte Nachrichten).

Ziele der Systemüberwachung

- Sicherstellen, dass die geltenden Gesetze und Vorschriften eingehalten werden;
- Aufdecken von Verstößen gegen geltende Gesetze und Vorschriften.
- Gewährleistung der effektiven Nutzung von Informationssystemen und ihres normalen Betriebs;
- Gewährleistung der wirksamen Vertraulichkeit und Integrität der ALE-Daten sowie der Einhaltung ihrer Sicherheitsverpflichtungen durch die Mitarbeiter;
- Gewährleistung der effektiven Sicherheit von ALE-Informationssystemen durch Implementierung von Funktionen zur Erkennung von Sicherheitsbedrohungen, einschließlich Viren, Trojanern, Würmern, Malware und Spam (unerwünschte Nachrichten);

Organisatorische Maßnahmen und Richtlinien

- Richtlinien für die Authentifizierung
- Leitlinie für Informationssicherheit
- Leitlinie für die Nutzung von Intranet / Internet
- Leitlinie für die E-Mail-Kommunikation

Weitere technische Maßnahmen

- Verwendung von Firewalls
- Verwendung von Antivirensoftware
- Verwendung von Anti-Malware-Software
- Intrusion Prevention-Systeme
- Internet-Proxy-Verwaltung
- SSO / SAML
- Einschränkung des Zugriffs auf Server

Benutzerzugangssteuerung in Rainbow

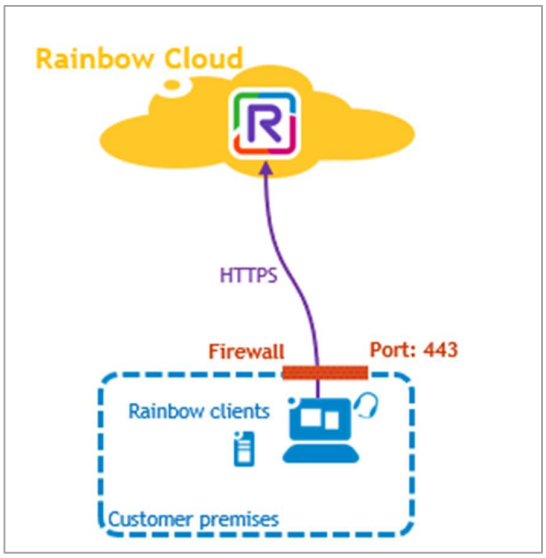
Rainbow bietet verschiedene Möglichkeiten, Benutzer zu authentifizieren

a) Interne Authentifizierung (Standardlösung)

Standardmäßig werden Rainbow-Benutzer für den Rainbow-Dienst authentifiziert. In diesem Fall überprüft Rainbow die Benutzeranmeldeinformationen. Wenn ein Benutzer die Rainbow UCAAS-Anwendung öffnet, wird das Rainbow-Anmeldeformular angezeigt und für die Authentifizierung verwendet.

In der Standardlösung verwaltet Rainbow die Sicherheitsregeln für Login und Password unter der Kontrolle des Rainbow-Administrators.

Interne Authentifizierung



Die interne Authentifizierung implementiert mehrere Sicherheitsregeln:

- Während der Selbstregistrierung wird eine E-Mail gesendet, um die Kontoerstellung zu überprüfen.
- Benutzerkennwörter müssen eine Mindestkomplexitätsstufe einhalten
  Mindestens 8 Zeichen (maximal 64)
  - 1 Kleinbuchstaben
  - 1 Großbuchstaben
  - 1 Zahl und
  - 1 Sonderzeichen.
- Das Zurücksetzen des Kennworts wird durch einen temporären 6-stelligen PIN-Code gesichert, der an die E-Mail-Adresse des Benutzers gesendet wird. Dieser muss beim Aktualisieren des Kennworts eingegeben werden.

Die Zugriffssteuerung für Rainbow-Dienste basiert auf der Rolle, die der Administrator den Benutzern zugewiesen hat:
- Gast
- User
- Company Admin

b) Externe Authentifizierung

Übersicht

Die externe Authentifizierung delegiert die Anmelde-/Kennwortsicherheitsregeln an einen externen zentralen Authentifizierungsserver (z.B. MS Azure AD). Der Admin kann erlauben, dasselbe Kennwort für mehrere Anwendungen freizugeben.

- Unterstützt werden nur Cloud-Authentifizierungsserver.
- Nutzbar mit PCs und Smartphones (iOS, Android).
- Unterstützt HTTPS/SAML v2 und OIDC (OpenID Connect)-Protokolle.
- OIDC (OpenID Connect) basierend auf OAuth2.
- SAML v2 (Security Assertion Markup Language)

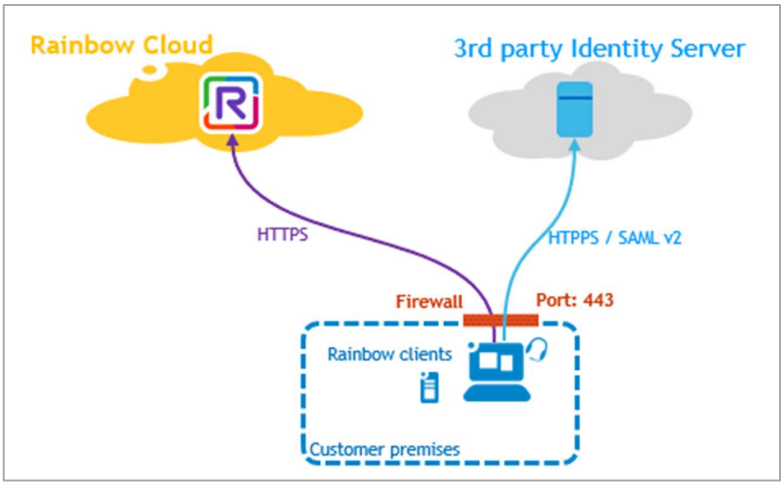
Details

Rainbow ist in der Lage, einen externen Identitätsanbieter basierend auf SAML und OIDC zu verwenden. In diesem Anwendungsfall muss der Administrator des Authentifizierungsdienstes einen neuen externen Dienst im externen Identitätsdienst (wie in der Microsoft Azure-Verwaltungsschnittstelle) deklarieren. Rainbow interagiert mit diesem, wenn sich ein Benutzer anmeldet.

Externe Authentifizierung mit SAML V2

Security Assertion Markup Language (SAMLv2) ist ein Protokoll, das für die Authentifizierung verwendet wird. Dieses Protokoll ist eine Möglichkeit, Zugriff auf eine geschützte Ressource zu gewähren, indem ein zentralisierter Authentifizierungsdienst eingesetzt wird.

Eine Verbindung zu Rainbow-Konten kann mit dem entsprechenden Firmen-Login und -Kennwort hergestellt werden. Da eine Dekorrelation zwischen der geschützten Ressource und dem Element besteht, das die Identität steuert, erlaubt SAMLv2 dem Benutzer, dieselben Anmeldeinformationen für den Zugriff auf eine Vielzahl geschützter Ressourcen oder Dienste zu verwenden. Dieser Anwendungsfall ist auch unter dem Single Sign On (SSO)-Prinzip bekannt.

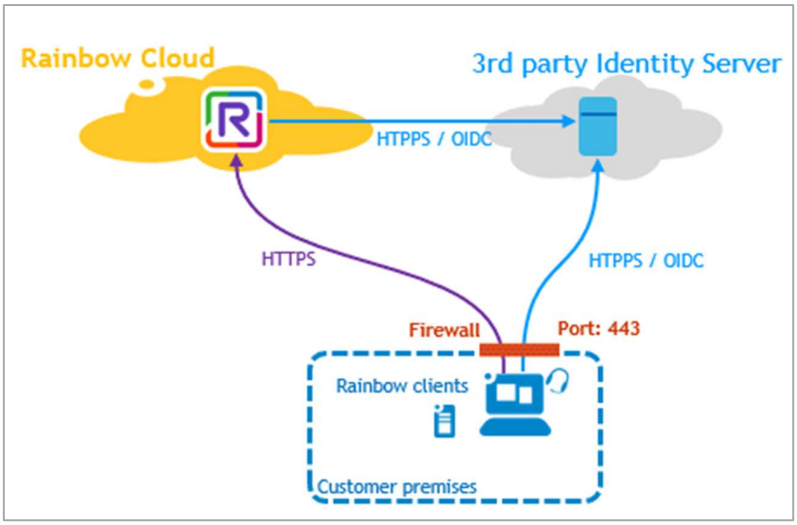


Die externe Authentifizierung mit OAuth2

OAuth2 ist ein Framework, das die externe Autorisierung ermöglicht. Es ist neuer als SAMLv2 und ist primär API-orientiert.

Die externe Authentifizierung mit OIDC

Open ID Connect (OIDC) ist ein auf OAuth2 basierendes Protokoll.



Verschlüsselung und Sicherheit in Rainbow

- Endbenutzerkennwörter werden in der internen Datenbank von Rainbow gehasht.
- Alle Daten (IMs, Dateien), die zwischen Benutzern oder durch Bubbles ausgetauscht werden, werden während der Übertragung und im at rest verschlüsselt.
- Übertragung per HTTPS + WSS über TLS 1.2/1.3
- At rest kommt AES 256-GCM zum Einsatz.
- Die Sprach-/Videokommunikation wird mit DTLS & SRTP nativ verschlüsselt.
- Alle von Benutzern hochgeladenen Dateien werden vor der Speicherung und Übertragung von einem Antivirus (ClamAV) systemisch gescannt.

1.3 Zugriffskontrolle auf Datenverarbeitung und Daten

Maßnahmen zur Verwaltung des Zugriffs auf IS/IT-Ressourcen bei ALE

Zugriffsrichtlinien

Zugriffe werden mithilfe von Rollen und Berechtigungen gesteuert, protokolliert und Aktivitäten überwacht. Dies ist umfassend in der ALE-Sicherheitsdirektive (ALE_000835) dokumentiert.

Grundsätze der Zugriffskontrolle

Berechtigungen werden nach dem Bedarfsprinzip erteilt. User dürfen nur auf Daten zugreifen, die
a) nicht vertraulich (offen) sind
b) für die Erfüllung individueller beruflicher Aufgaben erforderlich sind
c) von einem Supervisor freigegeben wurden.

Verwaltung von Zugriffsrechten

- N+1-Manager sind beteiligt.
- Benutzer-IDs, die 60 Tage lang nicht verwendet wurden, werden automatisch blockiert. Nicht verwendete Dienstkonten (z. B. von Maschine zu Maschine, Stapel) werden nach 1 Jahr deaktiviert.
- Benutzer-IDs / Passwörter / Zertifikate / Token / PINs / Zugriff auf mobile Geräte / physische Karten werden zugewiesen, gelöscht oder deaktiviert, wenn ALE-Mitarbeiter keine Anstellung / Vertragsbeziehung mehr mit dem Unternehmen haben, in Arbeitsgruppen ein- oder auswandern oder auf andere Weise nicht länger müssen Unternehmen auf das System zugreifen.

Netzwerkzugriffskontrolle

- Nur von ALE verwaltete Workstations und andere Geräte haben vollen Zugriff auf das interne Unternehmensnetzwerk. Das ALE-IT-Management genehmigt die Verwendung von nicht von Unternehmen verwalteten Geräten, bevor der vollständige lokale oder Remotezugriff gewährt wird.
- Netzwerk-Switches werden konfiguriert und überwacht, um Abhören, Sitzungsdiebstahl und andere Exploit-Versuche zu verhindern.
- Authentifizierung und Netzwerk- / Transportschichtverschlüsselung werden für drahtlose Verbindungen verwendet, um den drahtlosen Zugriff auf das Unternehmensnetzwerk zu schützen.

System- und Anwendungszugriffssteuerung:

- Sitzungssteuerung:
  IT-Ressourcen, auf die zugegriffen werden kann (Netzwerkabtretung, Desktop, Mobil, Router…) haben spezifische Regeln für das Sperren nach ungültigen erfolglosen Zugriffsersuchen.

- Netzwerkzugriffssteuerung:
  Whitelisting für kabelgebundenen Zugriff; Verschlüsselung für den drahtlosen Zugriff.

- Zugriff auf externe Netzwerkdienste:
  Alle externen Netzwerkdienste werden von Security Devices des Unternehmens gefiltert. Nur bestimmte Protokolle, Ports, Quell- und Ziel-IP-Adressen, Anwendungen und Sitzungstimeouts sind zugelassen (Service Whitelisting).

- Ausgehender Benutzerzugriff:
  Verwendung von Proxy- und Datenverkehrsüberwachung. Der Remotezugriff erfordert eine starke Authentifizierung.

- Remoteverwaltungs- & Diagnoseports

- Netzwerksegregation:
  Nicht IT-verwaltete Netzwerke sind segmentiert (auch wenn keine externe Konnektivität vorhanden ist). Router oder Firewalls werden verwendet, um nur den erforderlichen Datenverkehr, falls vorhanden, in das Unternehmensnetzwerk passieren zu lassen.

- Dual-Homed-Computer:
  Das Herstellen einer Verbindung zu einem Netzwerk außerhalb des Unternehmens mit Unternehmensressourcen ist verboten.

- Netzwerkrouting:
  Die ALE-Netzwerkrouting- und Switching-Infrastruktur wird auf Denial-of-Service-Angriffe überwacht. Der externe Zugriff auf Netzwerkinformationen zum internen Unternehmensnetzwerk ist eingeschränkt.

- DNS (Domain Name Service) ist vor nicht vertrauenswürdigen Netzwerken geschützt.

Maßnahmen zur Verwaltung der Zugriffskontrolle in Rainbow

Rollendefinition

Rainbow-Benutzer in einem Unternehmen haben grundsätzlich eine der folgenden Rollen:

- Company Admin
  - Zusätzlich zu den Rechten des einfachen Benutzers kann er sein Unternehmen verwalten.

- Als einfacher User
  - Zugriff auf die Rainbow-Funktionen hängt sein Rainbow-Abonnement ab.

Einschränken des Zugriffs auf Dateifreigabefunktion

Zur Steuerung des Dateiaustauschs zwischen Benutzern, kann der Zugriff auf die Funktion "Dateifreigabe" (Upload und Übertragung) eingeschränkt werden. Die Konfiguration kann durch den Administrator für das gesamte Unternehmen oder den einzelnen User eingestellt werden.

Sperrung von Änderungen der Benutzernamen

Als Schutz vor Usurpation kann die Änderung von Titeln, Vornamen und Nachnamen durch den Benutzer verboten werden.

Verschlüsselung und Sicherheit

Verschlüsselte Kennwortdatenbankspeicher

Endbenutzerkennwörter werden in der internen Datenbank von Rainbow gehasht.

Verschlüsselung bei Transit und at rest

- Alle Daten (IMs, Dateien), die zwischen Benutzern oder durch Blasen ausgetauscht werden, werden während der Übertragung und im Ruhezustand verschlüsselt.
- Für die Übertragung nur HTTPS + WSS über TLS 1.2/1.3.
- Im Ruhezustand wird AES 256-GCM verwendet.
- Die Sprach-/Videokommunikation wird mit DTLS & SRTP nativ verschlüsselt.

Antivirus-Scan nach Dateien

Alle von Benutzern hochgeladenen Dateien werden vor der Speicherung und Übertragung von einem Antivirus (ClamAV) systemisch gescannt.

1.4 Steuerung der Clientsegregation

- Alle von ALE verwendeten Systeme sind mandantenfähig
- ALE-Mitarbeiterdaten, Kundendaten und Kundendaten werden separat verarbeitet
- Testumgebungen sind von produktiven Umgebungen getrennt
- Netzwerksegregationen

Spezifizierung Rainbow

Multi-Client-Fähigkeit
- Rainbow ist komplett multi-clientfähig
- Logische Trennung von Kundenkonten

Client-dedizierte Funktionen:
Rainbow Edge Offer - Technical Overview - siehe
https://support.openrainbow.com/hc/fr/articles/360012465520

Trennung von Prüf- und Produktionssystemen
- Testumgebung für neue Softwareanwendungen oder wichtige Updates.
- Rollout findet erst nach einem erfolgreichen Test statt.

1.5 Pseudonymisierung

Je nach Dienst, eingesetztem Produkt und Art der Datenverarbeitung setzt ALE nach dem Erforderlichkeitsprinzip Maßnahmen zur Pseudonymisierung ein.

Spezifizierung Rainbow

Pseudonymisierung von Anforderungsprotokollen.

Alle Anfragen an die Rainbow-Anwendung werden protokolliert.

Protokolle

- werden vollständig anonymisiert.
- werden an einen Servercluster gesendet, wo sie redundant gespeichert werden.
- werden während der gesetzlich vorgeschriebenen Mindestdauer aufbewahrt.

2. Integrität

2.1 Weitergabekontrolle

Weitergabekontrolle bei ALE

Richtlinien für die Klassifizierung von Informationen und deren Umgang

Offen:
ist eine Information, die ALE gemäß den Marketing- und Kommunikationsstandards bereit ist, öffentlich mit anderen zu teilen.

Intern:
ist eine Information, die mit allen Mitarbeitern und Zeitarbeitern im Unternehmen geteilt wird. Diese Informationen sind für die allgemeine Verwendung innerhalb von ALE bestimmt und werden nur im Rahmen einer Geheimhaltungsvereinbarung oder einer anderen vertraglichen Vertraulichkeitsbestimmung an Dritte weitergegeben.

Vertraulich:
ist eine Information, die ALE ausschließlich nach dem Need-to-Know Prinzip freigibt. Der Zugriff auf diese Informationen unterliegt einer eingeschränkten Verbreitung und wird nur außerhalb von ALE im Rahmen einer Geheimhaltungsvereinbarung oder einer anderen vertraglichen Vertraulichkeitsbestimmung freigegeben. Vertrauliche Informationen umfassen auch Informationen Dritter, für die eine Pflicht zur Geheimhaltung besteht.

Streng vertraulich:
sind sehr wertvolle oder geheim zu haltende Informationen im Zusammenhang mit disruptiven Technologien oder strategischen Geschäftsaktivitäten. Eine nicht autorisierte Offenlegung würde die Interessen des Unternehmens schädigen und sich langfristig auf das Image, die aktuellen oder zukünftigen Einnahmen auswirken. Der Zugriff auf diese Informationen unterliegt einem kleinen Kreis autorisierter Personen und wird nur außerhalb von ALE im Rahmen einer strengen Geheimhaltungsvereinbarung gemäß der Genehmigung durch den leitenden Angestellten freigegeben.

Für jede Klassifizierung bestehen Richtlinien zum korrekten Umgang und Vorgaben zur sicheren Übertragung.

Einschränkung bei der Verwendung von mobilen Endgeräten und Telearbeitsplätzen

- Ausschließliche Verwendung von ALE Hardware

Sichere Verbindungen zu ALE Informationssystemen

- Schutz durch die Eingabe von Passwort oder PIN
- Betriebssysteme werden auf dem aktuellen Stand gehalten
- Verschlüsselte Verbindungen
- Richtlinien zur Handhabung verlorengegangener Geräte

Netzwerk Sicherheitsmanagement

Unternehmensrichtlinien und Sicherheitsmaßnahmen für die elektronische Kommunikation über

- E-Mail

- VoIP
- Voice Mail
- Online Konferenzen
- Verwendung des Internet Browsers

Übertragung personenbezogener oder anderweitig sensibler Daten

Personenbezogene und andere sensible Daten dürfen nur unter Verwendung einer Verschlüsselungsmethode übertragen werden, die die Integrität der gesendeten Daten gewährleistet.

Verschlüsselte Kommunikation in Rainbow

Klartextverbindungen aus dem Internet werden systematisch verweigert

Es werden ausschließlich HTTPS-Verbindungen verwendet (Port 443)

- Web Sockets sind gesichert
- kein anderer Dienst wird im öffentlichen Internet geöffnet
- Der Zugang von Port 80 wird systematisch zu Port 443 umgeleitet

Aktualität

- OpenSSL wird immer auf dem neuesten Stand gehalten.

SSLv2, SSLv3, TLS 1.0 und TLS 1.1 sind zugunsten von TLS 1.2 und TLS1.3 deaktiviert

- Kein Einsatz veralteter SSL-Protokolle.
- Jede HTTPS-Aushandlung erfolgt nur über TLS

Standard Wildcard SSL/TLS Zertifikate von Gandi / Comodo CA

- mit einem 256-Bit-ECDSA-Schlüssel (elliptische Kurve) und mit RSA-SHA256 signiert.
- Es wird kein selbstsigniertes Zertifikat verwendet.

2.2 Eingabekontrolle

Eingabesteuerungen bei ALE

Ob und von wem Daten in IT-Systemen eingegeben, geändert oder entfernt wurden, kann nachträglich geprüft und bestimmt werden durch:

- Benutzerprofile
- Benutzeridentifikation
- Berechtigungskonzepte

Logging-Funktionen aller Produktivsysteme arbeiten ständig und werden ausreichend festgehalten.

Logging und Monitoring

Sofern dies nicht durch lokale Gesetze verboten ist, kann und wird ALE die individuelle Nutzung von ALE-Netzwerk- und Computerressourcen überwachen - einschließlich der Nutzung von Geräten, Besuchen bestimmter Websites, Instant Messaging und E-Mail.

Sicherheitsereignisprotokolle sind auf ALE-Informationssystemen, die interne, vertrauliche oder höchst vertrauliche Informationen enthalten, und auf physischen ALE-Zugriffssystemen jederzeit aktiv. Diese Protokolle sind vor unbefugtem Zugriff, versehentlicher oder absichtlicher Änderung und Zerstörung geschützt und werden regelmäßig überprüft.

Zu den protokollierten Aktivitäten gehören unter anderem:

- Alle erfolgreichen und erfolglosen Anmeldeversuche, einschließlich der Verwendung von Dienstkonten; Alle Abmeldungen;
- Benutzer, die während einer Online-Sitzung die IDs (oder autorisierten Berechtigungsstufen) wechseln;
- Versuche, nicht autorisierte Funktionen auszuführen oder Systeme anzugreifen;
- Alle Lese- oder Schreibzugriffe auf streng vertrauliche Informationen;
- Hinzufügungen, Löschungen und Änderungen an Benutzerkonten / Berechtigungen;
- Aktivitäten, die von privilegierten Konten ausgeführt werden, Verwendung erweiterter Betriebssystemdienstprogramme und Befehle, die die Systemzugriffskontrollen umgehen;
- Änderungen an den Systemeinstellungen (Parameter einschließlich der Sicherheits- / Überwachungsprotokolle).

Eingabesteuerung in Rainbow (Protokollanalyse)

Rainbow security abstract: https://support.openrainbow.com/hc/en-us/articles/115001019330

Das ALE Rainbow Operation Team hat die Möglichkeit, die gespeicherten Aktivitätsprotokolle genau zu analysieren, bei:

- Angriffen
- verdächtigen Aktivitäten,
- gerichtlicher Aufforderung.

Endkunden und Geschäftspartner haben keinen Zugriff auf Protokolle. Im Notfall kann das ALE Rainbow Operation Team punktuelle Informationen für sie extrahieren.

Die Protokollanalyse ermöglicht die Suche nach:

- Die Quell-IP-Adresse,
- Die Identität des Benutzers,
- Die Daten und die Uhrzeit der Anfragen,
- Der Typ der Anforderungen.

Die Protokollanalyse erlaubt keinen Zugriff auf:

- Gespräche / Konversationen
- Passwörter.

3. Verfügbarkeit & Resilienz

3.1 Verfügbarkeitskontrolle

ALE allgemein

Back Up

Systemadministratoren sind dafür verantwortlich, regelmäßige Sicherungen der ihnen zugewiesenen Informationssysteme durchzuführen.

Backups sollten Folgendes umfassen, sind aber nicht darauf beschränkt:

- Master Files;
- Datenbanken;
- Transaktionsdaten;
- System programs/utilities;
- Application software;
- Parameter settings;
- System documentation.

Für jede kritische Datei wird mindestens eine aktuelle Sicherung verwaltet. Die Sicherungen werden regelmäßig anhand des Originals überprüft, indem sie wiederhergestellt werden. Die Backups werden außerhalb des Standorts unter Einhaltung des desselben Schutzniveau gespeichert. Die Sicherungsmedien werden in einem aktuellen Verzeichnis registriert.

Regelmäßige Überprüfungen werden durchgeführt, um externe Lagereinrichtungen zu inspizieren und die Einhaltung von Aufbewahrungsplänen, Barrierefreiheitsanforderungen, Umweltschutz und physischer Sicherheit zu überprüfen.

Die Wiederherstellung der Sicherung erfordert eine ausdrückliche Genehmigung durch den CISO oder den jeweiligen Informationseigentümer.

Unterbrechungsfreie Stromversorgung

Kritische Informationssysteme verwenden USV-Geräte (unterbrechungsfreie Stromversorgung), um bei einem Stromausfall eine ordnungsgemäße Abschaltung zu ermöglichen. Backup-Generatoren, die mit ausreichend Kraftstoff versorgt werden, und Notbeleuchtung sind für den Fall eines Stromausfalls der Hauptversorgung in Rechenzentren verfügbar.

Notfallausrüstung wie unterbrechungsfreie Stromversorgung (USV) und Notstromaggregate werden gemäß den Empfehlungen des Herstellers gewartet und regelmäßig getestet.

Zertifizierte Rechenzentren

Alle verwendeten Rechenzentren sind nach ISO27001 oder vergleichbar zertifiziert und gewährleisten hohe Verfügbarkeit und Konnektivität.

Die betriebliche Kontinuität der Infrastrukturen (Verfügbarkeit von Geräten, Anwendungen und Betriebsprozessen) wird durch verschiedene Maßnahmen sichergestellt:

- Kontinuierliche Flüssigkeits- und Luftkühlung
- Redundante USVs
- Kapazitätsmanagement für die Geräte unter der Verantwortung von Cloud-Anbietern
- Technischer Support der Dienste
- Redundanz von Geräten und Servern, die für die Systemadministration verwendet werden
- Darüber hinaus stellen andere Mechanismen, z. B. die Sicherung von Netzwerkgerätekonfigurationen, sicher, dass das System im Fehlerfall wieder aufgenommen werden kann

Business Continuity Plan (ALE)

ALE hat einen Business Continuity Plan auf Basis von ISO27001 erstellt und durch die Anforderungen der ISO27018 (Erweiterung auf ISO27001) festgelegt.

Rainbow Hosting (OVH)

Betriebskontinuität (Server)

Die Betriebskontinuität der Infrastrukturen (Verfügbarkeit von Geräten, Anwendungen und Betriebsabläufen) wird durch verschiedene Maßnahmen sichergestellt:

- Kontinuierliche Flüssigkeits- und Luftkühlung
- Kontinuierliche und redundante Stromversorgung
- Kapazitätsmanagement für die Geräte unter der Verantwortung von Cloud-Anbietern
- Technischer Support des Dienstes
- Redundanz von Geräten und Servern für die Systemadministration
- Darüber hinaus stellen andere Mechanismen, wie die Sicherung von Netzwerkgerätekonfigurationen, sicher, dass das System im Falle eines Fehlers wieder aufgenommen werden kann.

Vermeidung von Natur- und Umweltgefahren

- Installation von Blitzleitern zur Reduzierung der begleitenden elektromagnetischen Welle
- Gründung von Cloud-Anbietern in Gebieten, die nicht von Überschwemmungen oder Erdbeben bedroht sind
- Eine unterbrechungsfreie Stromversorgung (USV) mit ausreichender Kapazität und Hilfstransformatoren mit automatischer Lastumschaltung
- Automatische Umstellung auf Stromerzeuger mit einer Mindestleistung von 24 Stunden
- Installation eines Flüssigkeitskühlsystems für die Server (98% der Serverräume verfügen über keine Klimaanlage)
- Einsatz von Heizungslüftungs- und Klimaanlagen,-Einheiten ,,Temperatur und Luftfeuchtigkeit konstant halten
- Verwaltung einer Brandmeldeanlage (Brandübungen werden alle 6 Monate in den Rechenzentren durchgeführt)

Technische Maßnahmen zur Verfügbarkeit

Um eine hohe Verfügbarkeit von Daten zu gewährleisten, gibt es verschiedene Mechanismen:

- Hardwareebene mit HA-Festplatte
- Datenbanken werden gruppiert und repliziert

- Benutzerdateien und statische Daten werden 3 Mal auf replizierten Swift Object Storage-Servern im offenen Stapel gespeichert

Sicherung aller Datenbanken

- Häufigkeit: Stündliches Snapshot des Datenbankdateisystems
- Tägliche Datenbanksicherung an 2 Remote-Standorten

Hohe Verfügbarkeit

- Hohe Verfügbarkeit auf Servern, Storage Bays und Festplatten unter der Verantwortung von ALE
- Electric und Network Verfügbarkeit unter der Verantwortung des Hosts (OVH).

Überwachung

Für alle OVH-Dienste ist eine Überwachungsinfrastruktur vorhanden. Dies hat mehrere Ziele:

- Erkennung von Produktions- und Sicherheitsvorfällen
- Überwachung kritischer Funktionen und Auslösen von Alarmen im Überwachungssystem
- Mitteilung der verantwortlichen Personen und Einleitung der entsprechenden Verfahren
- Garantie der Servicekontinuität bei der Ausführung automatisierter Aufgaben
- Überprüfung der Integrität der überwachten Ressourcen

3.2 Belastbarkeit/Belastbarkeit

ALE allgemein

Intrusion Prevention Systems

Intrusion Prevention Systems (IPS) überwachen folgendes:

- Netzwerksegmente, in denen sich Systeme befinden, auf die über das Internet zugegriffen werden kann;
- eingehender und ausgehender Zugriff über Internet-Gateways, VPN-Gateways, Verbindungen von Drittanbietern und alle anderen externen Routen zum / vom Unternehmensnetzwerk;
- Hauptrechenzentrum.

Die IPS-Signaturen und -Muster werden regelmäßig aktualisiert und optimiert.

IPS-Warnungen und -Protokolle werden kontinuierlich von automatisierten Tools überwacht, um sicherzustellen, dass der CISO über Ereignisse informiert wird, die für die Erkennung von Vorfällen und die Trendanalyse von Interesse sind.

ALE behält sich das Recht vor, alle Kommunikations- und Systemaktivitäten jederzeit im gesetzlich zulässigen Umfang zu überwachen, darauf zuzugreifen, abzurufen, zu lesen und / oder offenzulegen.

Die Ergebnisse aller Überwachungs- und Scanaktivitäten werden als VERTRAULICH eingestuft.

System Monitoring

Alle Systeme werden ständig überwacht. Die Lastkapazitäten werden nachverfolgt und bei Bedarf angepasst.

Rainbow Hosting (OVH)

DDOS-Schutz und Firewall

Detaillierte Informationen finden Sie hier https://www.ovh.de/anti-ddos/.

Rainbow ist dank der von OVH erstellten Lösung VAC (Vacuum) vor DDoS-Angriffen (Distributed Denial of Service) geschützt. Diese wird vollständig von OVH verwaltet.

VAC ist eine Kombination von Technologien, die von OVH entwickelt wurden, um:
- Datenpakete schnell in Echtzeit analysieren
- den eingehenden Datenverkehr Ihres Servers umzuleiten
- nicht-legitime Anfragen von anderen zu trennen und legitimen Datenverkehr passieren zu lassen

Es wird als Blackbox betrachtet, in der Filter aus Sicherheitsgründen nicht offengelegt werden.
- Es handelt sich um Hardware-ASIC-basierte Paketfiltergeräte.

Die VAC-Prozesse erfolgen in vier Schritten

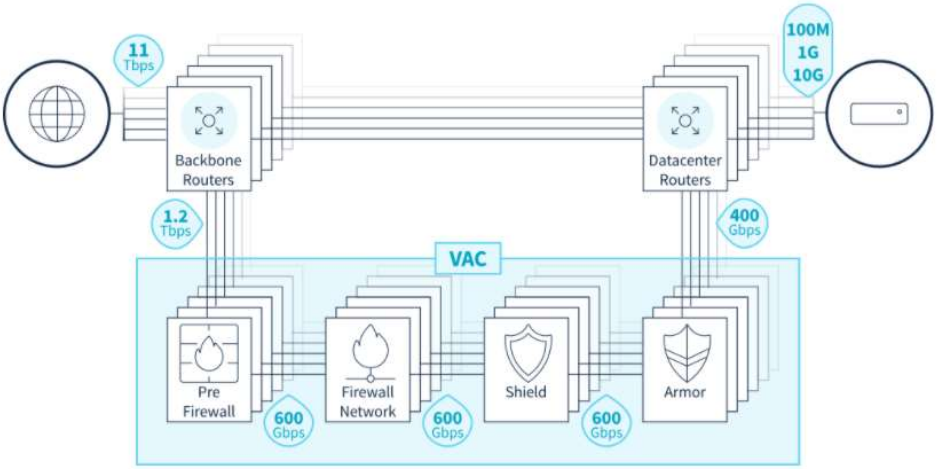
1. Pre-Firewall
   Die vorgelagerte Firewall ist das erste Element unseres VAC Systems. Sie wird vollständig von OVH verwaltet und wendet Regeln an, nach denen Filter Datenpakete zum Firewall Network weiterleiten.

2. Firewall Network
   Firewall Network ist das zweite Element des VAC. Es ist eine Lösung, mit der das Risiko von Angriffen aus dem öffentlichen Netzwerk reduziert wird. Firewall Network wird automatisch bei jedem DDoS-Angriff aktiviert.

3. Shield
   Shield greift im Fall von Amplification-Angriffen (DNS Amp, NTP Amp, ...) ein.

4. Armor
   Armor ist der fortschrittlichste Filter unseres VAC und ist für die Abwehr der ausgefeiltesten DDoS-Angriffe zuständig.

   Shield und Armor werden bei gezielteren Angriffen aktiv und ermöglichen es, den Prozessor des Servers zu entlasten, indem sie einen Teil der Filterung übernehmen.



4. Verfahren zur regelmäßigen Überprüfung, Bewertung und Bewertung (Art. 32 Abs. 1 lit. d DSGVO; Art. 25 Abs. 1 DSGVO)

A. Datenschutz - Management

Die folgenden Richtlinien, Verfahren oder Richtlinien zur Datensicherheit sind im ISMS-System von ALE dokumentiert:

- Geheimhaltungspflicht aller Mitarbeiter (Datengeheimnis)
- Maßnahmen zur Sensibilisierung der Mitarbeiter.
- ALE Security Charter
- ALE Security Directives
- ALE Security Policy
- ALE Data Protection and Privacy Policy
- ALE GDPR policy
- Crisis Management Guidelines Policy & procedure
- Confidential Information Guideline Policy
- Information Management System
- Audits durch den Datenschutzbeauftragten
- Audits durch externe Prüfer
- Dokumentierte Verarbeitungsaktivitäten.
- Regelmäßige Überprüfung der technischen und organisatorischen Maßnahmen.
- Sorgfältige Auswahl der Dienstleister (siehe auch unter Vertragsmanagement).
- Zertifizierung ISO27001 einschließlich ISO27017 und ISO27018

B. Datenschutzbeauftragter

Louis-Philippe Ollier

Mail: dataprivacy@al-enterprise.com

Telefon: +331 5566 3147

Die Kontaktdaten des DSB finden Sie auch: unter https://www.al-enterprise.com/en/legal/privacy

C. Incident-Response-Management

ALE

Richtlinien für das Krisenmanagement

Etablierte und dokumentierte Prozesse für den Umgang mit Vorfällen

- Definierte Verantwortlichkeiten
- Definierte Berichtskanäle
- Verfahren zur Verletzung von Daten

D. Datenschutzfreundliche Voreinstellungen

Grundsätzlich werden im Rainbow Service nur daten gesammelt und verarbeitet, die für geschäftliche Zwecke geeignet und notwendig sind. Verfahren zur automatisierten Datenerfassung und -verarbeitung sind so konzipiert, dass nur die notwendigen Daten erfasst werden.

Es gibt keine Verhaltensdatenverwaltung in Rainbow. Es werden keine Daten, die für Die für Die rainbow Aktivitäten oder Aktivitätenanalyse gesammelt wurden oder die sich aus der Analyse von Rainbow ergeben, an Dritte weitergegeben oder verkauft.

Rainbow kann mit minimalen Informationen, einer E-Mail-Adresse und einem Passwort verwendet werden.

E. Vertragsmanagement

Wenn bei der Datenverarbeitung Unterauftragnehmer eingesetzt werden, gelten bestimmte Vorgaben. Hierzu zählt die Sicherstellung der technischen und organisatorischen Maßnahmen der Unterauftragnehmer im Sinne des Art. 28 DSGVO i.V.m. Art 32 Abs. 1 DSGVO.

Folgende Voraussetzungen für ein Unterauftragsverhältnis gelten:

- Es bestehen detaillierte Angaben über Zweck, Art und Umfang der beauftragten Verarbeitung und Nutzung personenbezogener Daten des Auftraggebers nach Vorgabe des Art. 28 Abs. 3 DSGVO. Die entsprechenden Angaben sind vertraglich fixiert.
- Deutsche / EU Dienstleister haben einen betrieblichen Datenschutzbeauftragten bestellt, sofern eine Bestellung gesetzlich vorgeschrieben ist und sorgen durch die Datenschutzorganisation für dessen angemessene und effektive Einbindung in die relevanten betrieblichen Prozesse.
- Mündliche Aufträge müssen schriftlich bestätigt und dokumentiert werden.
- Eine Vergabe von Einzelaufträgen erfolgt nur über namentlich benannte Ansprechpartner.
- Auf die betreffenden technischen Umgebungen werden nur restriktive Zugriffsberechtigungen vergeben. Bei externem Zugriff auf das System wird der Zugang nach Beendigung der Zusammenarbeit deaktiviert oder gesperrt.
- Für die Übermittlung von personenbezogenen Daten an externe Dienstleister steht eine Vertragsvorlage zur Auftragsdatenverarbeitung zur Verfügung, die entsprechende Regelungen zur Kontrolle enthält.

Anlage 1 – ALE Security Certification

ISO27001 : 2013

afaq
AFNOR CERTIFICATION

Certificat
Certificate

N° 2019/82126.2

AFNOR Certification certifie que le système de management mis en place par :
AFNOR Certification certifies that the management system implemented by:

ALE INTERNATIONAL

exerçant sous la marque */ operating under the brand*

ALCATEL-LUCENT ENTERPRISE

pour les activités suivantes :
for the following activities:

DESIGN, IMPLEMENTATION AND SUPPORT OF CLOUD-BASED SOLUTIONS TO INTEGRATE CUSTOMERS BUSINESS PROCESSES

Statement of Applicability "ISMS-ALE-StatementOfApplicability-PublicVersion" version 4

ont été évaluées et jugées conformes aux exigences requises par :
have been assessed and found to meet the requirements of:

ISO/IEC 27001 : 2013

et est déployé sur les sites suivants :
and is developed on the following locations:

32 AVENUE KLEBER FR-92700 COLOMBES

Liste des sites certifiés en annexe(s) */ List of certified locations on appendix(ces)*

Ce certificat est valable à compter du (année/mois/jour) *This certificate is valid from (year/month/day)* **2019-03-26** Jusqu'au *Until* **2022-03-06**

cofrac
CERTIFICATION DE SYSTÈMES DE MANAGEMENT

Ce document est signé électroniquement. Il constitue un original électronique à valeur probatoire.
This document is electronically signed. It stands for an electronic original with probatory value.

Franck LEBEUGLE
Directeur Général d'AFNOR Certification
Managing Director of AFNOR Certification

Flashez ce QR Code pour vérifier la validité du certificat

Certificat

Certificate

N° 2019/82126.2

Annexe / *Appendix* **n° 1**

ALE INTERNATIONAL

exerçant sous la marque / *operating under the brand*

ALCATEL-LUCENT ENTERPRISE

Liste complémentaire des sites entrant dans le périmètre de la certification :
Complementary list of locations within the certification scope:

ALE INTERNATIONAL 115-225 RUE SAINT EXUPERY FR-29806 BREST CEDEX 9

ALE INTERNATIONAL 1, ROUTE DU DOCTEUR SCHWEITZER FR-67408 ILLKIRCH CEDEX

ALE USA Inc 26801 WEST AGOURA ROAD PO BOX 636 US CALABASAS CA 91301

ISO27018 : 2014

Certificat

Certificate

N° 2020/86660.1

AFNOR Certification certifie que le système de management mis en place par :
AFNOR Certification certifies that the management system implemented by:

ALE INTERNATIONAL

pour les activités suivantes :
for the following activities:

DESIGN, IMPLEMENTATION AND SUPPORT OF CLOUD-BASED SOLUTIONS TO INTEGRATE CUSTOMERS BUSINESS PROCESSES.

Statement of Applicability "ISMS-ALE-StatementOfApplicability_v6_Public".

a été évalué et jugé conforme aux exigences requises par :
has been assessed and found to meet the requirements of :

ISO 27018 : 2014

et est déployé sur les sites suivants :
and is developed on the following locations:

32 AVENUE KLEBER IMMEUBLE LES BOURGOGNES -92700 COLOMBES

26801 WEST AGOURA ROAD US-US CALABASAS CA 91301

1 ROUTE DU DR ALBERT SCHWEITZER -67408 ILLKIRCH CEDEX

115-225 RUE A DE ST EXUPERY ZAC PRAT PIP - GUIPAVAS FR-29806 BREST CEDEX 9

Ce certificat est valable à compter du (année/mois/jour) *This certificate is valid from (year/month/day)* **2020-04-06** Jusqu'au *Until* **2023-04-05**

Ce document est signé électroniquement. Il constitue un original électronique à valeur probatoire.
This document is electronically signed. It stands for an electronic original with probationary value.

Franck LEBEUGLE
Directeur Général d'AFNOR Certification
Managing Director of AFNOR Certification

Seul le certificat électronique, consultable sur www.afnor.org, fait foi en temps réel de la certification de l'organisme. The electronic certificate only, available at www.afnor.org attests in real time that the company is certified. AFAQ est une marque déposée.AFAQ is a registered trademark.CERTI F 0998.8 11/2019

Flashez ce QR Code pour vérifier la validité du certificat

ISO27017 : 2015

Certificat

Certificate

N° 2020/86659.1

AFNOR Certification certifie que le système de management mis en place par :
AFNOR Certification certifies that the management system implemented by:

ALE INTERNATIONAL

pour les activités suivantes :
for the following activities:

DESIGN, IMPLEMENTATION AND SUPPORT OF CLOUD-BASED SOLUTIONS TO INTEGRATE CUSTOMERS BUSINESS PROCESSES.

Statement of Applicability "ISMS-ALE-StatementOfApplicability_v6_Public".

a été évalué et jugé conforme aux exigences requises par :
has been assessed and found to meet the requirements of :

ISO 27017 : 2015

et est déployé sur les sites suivants :
and is developed on the following locations:

32 AVENUE KLEBER IMMEUBLE LES BOURGOGNES -92700 COLOMBES

26801 WEST AGOURA ROAD US-US CALABASAS CA 91301

1 ROUTE DU DR ALBERT SCHWEITZER -67408 ILLKIRCH CEDEX

115-225 RUE A DE ST EXUPERY ZAC PRAT PIP - GUIPAVAS FR-29806 BREST CEDEX 9

Ce certificat est valable à compter du (année/mois/jour) *This certificate is valid from (year/month/day)* **2020-04-06** Jusqu'au *Until* **2023-04-05**

Ce document est signé électroniquement. Il constitue un original électronique à valeur probatoire.
This document is electronically signed. It stands for an electronic original with probatory value.

Franck LEBEUGLE
Directeur Général d'AFNOR Certification
Managing Director of AFNOR Certification

Flashez ce QR Code pour vérifier la validité du certificat

Anlage 2

Relevante Ergänzungen

Technische und Organisatorische Maßnahmen

bei OVH (Subunternehmer Hosting)

1. Physische Zutrittskontrolle und -sicherheit

Das Rechenzentrum wird vom Anbieter OVH betrieben. Einzelheiten zu den Sicherheitsmaßnahmen finden Sie unter https://www.ovh.de/schutz-personenbezogener-daten/sicherheit.xml.

Allgemeine Sicherheitsmaßnahmen der physischen Standorte

Der physische Zugriff basiert auf einer restriktiven Kontextsicherheit, die vom Eingangsbereich aus wirksam ist. Jeder Ort ist wie folgt unterteilt:

- Private Verkehrsbereiche
- Büros, die für alle Mitarbeiter und registrierten Besucher zugänglich sind
- Private Büros nur für autorisiertes Personal zugänglich
- Bereiche mit Rechenzentrumsausrüstung
- Private Rechenzentrumsbereiche
- Rechenzentrumsbereiche, in denen kritische Dienstleistungen untergebracht sind

Folgende Sicherheitsmaßnahmen werden umgesetzt, um den Zugang zu den physischen Standorten von OVH zu kontrollieren:

- Eine Policy für Zutrittsberechtigungen
- Wände (oder ähnliche Vorrichtungen) zwischen jedem Bereich
- Kameras an den Ein- und Ausgängen der Räumlichkeiten sowie in den Serverräumen
- Gesicherte Zugänge, kontrolliert durch Badge-Lesegeräte
- Laserbarrieren auf den Parkplätzen
- Bewegungsmeldesystem
- Einbruchhemmende Mechanismen an Ein- und Ausgängen der Rechenzentren
- Mechanismen zur Erkennung unerlaubten Eindringens (Wachdienst und Videoüberwachung rund um die Uhr)
- Ständiges Überwachungszentrum, das Ein- und Ausgangstüren auf Öffnen überwacht

Die physischen Zutrittskontrollen erfolgen durch ein Badge-System.

Jedes Badge ist mit einem OVH Account verknüpft, und dieser wiederum mit einer bestimmten Person. Dank dieser Maßnahme können jede Person innerhalb der Anlagen identifiziert und die Kontrollmechanismen authentifiziert werden:

- Jede Person, die Standorte von OVH betritt, muss einen mit ihrer Identität verknüpften persönlichen Badge besitzen.
- Jede Identität muss vor der Ausgabe eines Badge überprüft werden.
- Das Badge muss innerhalb der Räumlichkeiten stets sichtbar getragen werden.
- Badges dürfen weder den Namen ihrer Inhaber noch den Namen des Unternehmens zeigen.
- Es muss möglich sein, die Kategorie der anwesenden Personen anhand des Badges sofort zu identifizieren (Mitarbeiter, Dritter, temporärer Zutritt, Besucher).
- Der Badge wird deaktiviert, sobald der Inhaber nicht länger zum Zutritt zu den Räumlichkeiten berechtigt ist.
- Badges von OVH Mitarbeitern werden für die Dauer des Arbeitsvertrages aktiviert; für die anderen Kategorien wird der Badge nach einem festgelegten Zeitraum automatisch deaktiviert.
- Badges, die drei Wochen lang nicht verwendet werden, werden automatisch deaktiviert.

Zutritt an den Türen per Badges. Dies ist die Standard-Zutrittskontrolle in den Räumlichkeiten von OVH:

- Die Tür ist mit dem zentralen Managementsystem für Zutrittsberechtigungen verbunden.
- Die Person muss ihren Badge an das spezielle Lesegerät halten, um die Tür zu entsperren.
- Jeder Zutritt wird beim Auslesen überprüft, um sicherzustellen, dass die Person über die entsprechenden Berechtigungen verfügt.
- Bei einem Ausfall des zentralen Managementsystems für die Zutrittsberechtigungen gelten die zum Zeitpunkt der Störung konfigurierten Berechtigungen für die gesamte Dauer des Vorfalls.
- Die Türschlösser sind gegen Stromausfälle geschützt und bleiben in diesen Situationen geschlossen.

Zugang zu den Türen per Schlüssel. Bestimmte Bereiche oder Geräte sind mit per Schlüssel verschließbaren Schlössern abgesperrt:

- Die Schlüssel werden für jeden Standort in einem zentralisierten Bereich mit eingeschränktem Zutritt aufbewahrt und in einer Inventarliste dokumentiert.
- Jeder Schlüssel ist mit einem Etikett zur Identifikation versehen.
- Es wird ein Bestandsverzeichnis über die Schlüssel geführt.
- Jede Verwendung der Schlüssel kann mittels eines Bereitstellungsmechanismus oder Journals auf Papier zurückverfolgt werden.
- Die Inventarliste der Schlüssel wird täglich mit dem Bestandsverzeichnis abgeglichen.

Zutritt zu den Rechenzentren durch Einpersonenschleusen. Der Zutritt zu unseren Rechenzentren erfolgt ausschließlich über Einpersonenschleusen:

- Jede Schleuse besteht aus zwei Türen und einem abgeschlossenen Bereich zwischen den Kontrollen, um sicherzustellen, dass nur eine Person auf einmal passiert.
- Eine Tür kann nur offen sein, wenn die andere geschlossen ist (Mantrap).
- Die Schleusen verwenden dasselbe Badge-System wie die anderen Türen, und es gelten dieselben Regeln.
- Erkennungsmechanismen prüfen, dass sich nur eine Person in der Schleuse befindet (Anti-Piggybacking).
- Die Konfiguration des Systems verhindert, dass das Badge mehr als einmal in dieselbe Richtung verwendet werden kann (Anti-Passback).
- Mit einer Kamera im Bereich der Schleuse können die Zutritte überwacht werden.

Zutritt zu den Warenschleusen. Der Wareneingang in die Rechenzentren erfolgt ausschließlich über die speziell dafür vorgesehenen Durchgänge:

- Die Lieferzone ist genauso konfiguriert wie eine Einpersonenschleuse, jedoch mit mehr Platz, ohne Volumen- und Gewichtskontrollen sowie mit Badge-Lesegeräten nur außerhalb der Schleuse.
- Nur der gelieferte Artikel passiert die Lieferzone, Personen müssen über die Einpersonenschleusen eintreten.
- In der Lieferzone befindet sich eine Kamera ohne toten Winkel.

Die Bewegungen von Besuchern und gelegentlichen Dienstleistern sind streng geregelt. Diese Personen werden bei ihrer Ankunft am Standort registriert und erhalten einen Besucher- oder Dienstleister-Badge:

- Jeder Besuch muss zuvor angemeldet werden.
- Für Dritte ist immer ein Angestellter verantwortlich und sie werden immer begleitet.
- Jede Identität wird vor dem Zutritt zu den Standorten überprüft.
- Jeder Dritte besitzt ein persönliches Badge für den Tag, den er vor Verlassen des Standorts zurückgeben muss.
- Alle Badges müssen sichtbar getragen werden.
- Die Badges werden am Ende des Besuchs automatisch deaktiviert.

2. Allgemeine Zugangskontrollmaßnahmen bei OVH

Personalisierte Nutzerkonten

- Alle Angestellten verwenden namentliche Benutzerkonten.
- Verbindungssitzungen haben systematisch eine für jede Anwendung angepasste Ablaufzeit.
- Vor jeder Änderung der Authentifizierungsmethoden wird die Identität der Benutzer überprüft.
- Die Nutzung von Standardkonten, generischen und anonymen Konten ist verboten.

Passwortpolitik

- Durch den Einsatz eines automatischen Passwortgenerators wählt der Benutzer sein Passwort nicht selbst.
- Die Mindestlänge eines Passwortes beträgt 10 alphanumerische Zeichen.
- Die Passwörter werden alle 3 Monate geändert.
- Benutzerkonten werden automatisch deaktiviert, wenn das Passwort nicht nach 90 Tagen geändert wird.
- Es ist verboten, Passwörter in unverschlüsselten Dateien, auf Papier oder in Webbrowsern zu speichern.
- Die Verwendung einer lokalen, vom Sicherheitsteam genehmigten Passwortverwaltungssoftware ist vorgeschrieben.
- Vergisst ein Benutzer sein Passwort, sind nur der Vorgesetzte des Mitarbeiters und der Sicherheitsbeauftragte berechtigt, es zurückzusetzen.

3. Zugangs- und Zugriffssteuerung zu Infrastrukturressourcen bei OVH

Folgende Policy wird für die Verwaltung der Administratorzugriffe auf die Plattformen umgesetzt:

- Alle Administratorzugriffe auf ein System in Produktion erfolgen über einen Bastion Host.
- Administratoren verbinden sich via SSH mit den Bastion Hosts, indem sie individuelle und namentliche Paare öffentlicher und privater Schlüssel verwenden.
- Die Verbindung mit dem Zielsystem erfolgt entweder über ein Shared-Service-Konto oder über ein Namenskonto via Bastion Hosts
- Die Verwendung von Standardkonten auf den Systemen und Geräten ist verboten.
- Für Administrator-Fernzugriffe sowie für Zugriffe durch Mitarbeiter in sensiblen Umgebungen ist eine Zwei-Faktor-Authentifizierung mit vollständiger Nachverfolgung erforderlich.
- Administratoren verfügen zusätzlich zu ihrem Benutzerkonto über ein ausschließlich für administrative Aufgaben verwendetes Konto.
- Zugriffsberechtigungen werden von den Vorgesetzten gemäß der Regel der geringsten Berechtigung und dem Prinzip erworbenen Vertrauens erteilt und verfolgt.
- die SSH-Schlüssel sind durch ein Passwort geschützt, das die Anforderungen der Passwort Policy erfüllt.
- Berechtigungen und Zugriffe werden regelmäßig in Zusammenarbeit mit den betreffenden Abteilungen überprüft.

Sicherung der Standardarbeitsplätze

Die folgenden Maßnahmen werden eingesetzt, um die Sicherheit der Standardarbeitsplätze des OVH Personals zu gewährleisten:

- Automatische Updateverwaltung
- Installation und Aktualisierung von Antivirus-Software mit regelmäßigen Scans • Ausschließliche Installation von Anwendungen aus einem genehmigten Anwendungskatalog
- Systematische Verschlüsselung der Festplatten
- Keine Administratorrechte für Mitarbeiter an ihrem Arbeitsplatz
- Festgelegte Vorgehensweise zur Behandlung potenziell kompromittierter Arbeitsplätze
- Standardisierung der Geräte
- Löschen der Sitzungen und Zurücksetzen der Arbeitsplätze beim Verlassen der Mitarbeiter

4. Zugriffskontrolle auf Datenverarbeitung und Daten bei OVH

Maßnahmen zur Verwaltung der Zugriffskontrolle auf Datenverarbeitung und Daten auf Infrastrukturhostingebene (OVH)

- Zugriffsberechtigungen werden von Supervisoren gemäß der Regel der geringsten Berechtigungen und dem Prinzip der progressiven Vertrauenswürdigkeit erteilt und nachverfolgt.
- Soweit möglich, basieren alle Zugriffsberechtigungen auf Rollen und nicht auf Einheitenrechten.
- Die Verwaltung der Zugriffsrechte und Zugriffsberechtigungen, die einem Benutzer oder System gewährt werden, erfolgt durch Registrierung, Änderung und Abmeldung durch Vorgesetzte, interne IT und Personalwesen.
- Jeder Fernzugriff auf das OVH-Informationssystem erfolgt über VPN. Dies erfordert ein Zertifikat, das nur dem Benutzer bekannt ist, und einen gemeinsam genutzten geheimen Schlüssel, der auf der Arbeitsstation konfiguriert ist.
- Die Daten werden at rest und während der Übertragung verschlüsselt.
- Der Cloudinfrastrukturanbieter hat keinen logischen Zugriff auf die Server.

5. Netzwerksicherheit OVH

OVH verwaltet ein privates Hochleistungs-Glasfasernetz, das mit zahlreichen Betreibern und Spediteuren verbunden ist. OVH verwaltet seinen eigenen Backbone intern. Er verteilt die Konnektivität auf die lokalen Netzwerke jedes Rechenzentrums und verbindet diese untereinander.

Alle Geräte sind durch die folgenden Maßnahmen gesichert:

- Bestandsführung in einer Konfigurationsmanagementdatenbank
- Umsetzung eines Härtungsprozesses, mit Anleitungen für die zu verändernden Einstellungen, um eine sichere Konfiguration zu gewährleisten
- Zugriffe auf die Administratorfunktionen der Geräte sind über Kontrolllisten beschränkt
- Alle Geräte werden über einen Bastion Host unter Anwendung des Prinzips der geringsten Berechtigung verwaltet
- Von allen Konfigurationen der Netzwerkgeräte werden Backups erstellt
- Logs werden gesammelt, zentralisiert und ständig vom Netzbetriebsteam überwacht
- Die Implementierung von Konfigurationen erfolgt automatisiert und basiert auf genehmigten Vorlagen

6. Zugriffskontrolle der OVH Cloud-IT-Systeme

OVH wendet eine strenge Richtlinie an, um logische Zugriffsrechte zu verwalten. Diese Richtlinie enthält die folgenden Bestimmungen

- Die Zugriffsrechte werden nach dem "Least Privilege"-Prinzip gewährt.
- Die Zugriffsrechte sollten auf Rollen im Vergleich zu bestimmten Rechten einzelner Einheiten basieren.
- Die Gewährung des Zugriffs auf einen Benutzer oder ein System wird auf der Grundlage von Erstzugriffs-, Änderungs- und Entfernungsbereitstellungsverfahren unter Einbeziehung ihrer Manager, IT-Support /Kerndienste und HR verwaltet.
- Alle Mitarbeiter verwenden eindeutige Benutzer-ID-Konten.
- Systematische Auszeit nach einer Phase der Inaktivität;
- Die Verwendung generischer und/oder anonymer Benutzerkonten ist untersagt.
- Es wird eine strikte Kennwortrichtlinie angewendet.
- Kennwörter sollten nach dem Zufallsprinzip generiert werden.
- Endpunktgeräte haben eine minimale Kennwortlänge von 10 alphanumerischen Zeichen.
- Das Speichern von Passwörtern in unverschlüsselten Dateien, auf Papier oder in Webbrowsern ist verboten.
- Lokale Kennwortverwaltungssoftware, die von IT Security genehmigt wurde, ist erforderlich.

- Der Remote-Zugriff auf OVH-Cloud-IT-Systeme muss über VPN erfolgen. Es muss ein Kennwort verwendet werden, das dem Benutzer bekannt ist, und ein Clientzertifikat, das auf der Arbeitsstation konfiguriert ist.
-

7. Betriebskontinuität (Server)

Die Betriebskontinuität der Infrastrukturen (Verfügbarkeit von Geräten, Anwendungen und Betriebsabläufen) wird durch verschiedene Maßnahmen sichergestellt:

- Kontinuierliche Flüssigkeits- und Luftkühlung
- Kontinuierliche und redundante Stromversorgung
- Kapazitätsmanagement für die Geräte unter der Verantwortung von Cloud-Anbietern
- Technischer Support des Dienstes
- Redundanz von Geräten und Servern für die Systemadministration
- Darüber hinaus stellen andere Mechanismen, wie die Sicherung von Netzwerkgerätekonfigurationen, sicher, dass das System im Falle eines Fehlers wieder aufgenommen werden kann.

8. Vermeidung von Natur- und Umweltgefahren

- Installation von Blitzleitern zur Reduzierung der begleitenden elektromagnetischen Welle
- Gründung von Cloud-Anbietern in Gebieten, die nicht von Überschwemmungen oder Erdbeben bedroht sind
- Eine unterbrechungsfreie Stromversorgung (USV) mit ausreichender Kapazität und Hilfstransformatoren mit automatischer Lastumschaltung
- Automatische Umstellung auf Stromerzeuger mit einer Mindestleistung von 24 Stunden
- Installation eines Flüssigkeitskühlsystems für die Server (98% der Serverräume verfügen über keine Klimaanlage)
- Einsatz von Heizungslüftungs- und Klimaanlagen,-Einheiten ,,Temperatur und Luftfeuchtigkeit konstant halten
- Verwaltung einer Brandmeldeanlage (Brandübungen werden alle 6 Monate in den Rechenzentren durchgeführt)

9. Incident-Response-Management

OVH

Ein Vorfallmanagementprozess ist vorhanden. Es ermöglicht die Prävention, Erkennung und Lösung dieser Ereignisse in den Service-Management-Infrastrukturen und dem Dienst selbst. Dieser Prozess umfasst:

- Leitfaden zur Klassifizierung von Sicherheitsereignissen
- Der Umgang mit Sicherheitsereignissen
- Simulationsübungen für das Krisenteam
- Tests des Reaktionsplans auf Störungen
- Kundenkommunikation im Rahmen eines Krisenmanagement-Teams

Diese Verfahren unterliegen einem kontinuierlichen Verbesserungsprozess zur Überwachung und Bewertung von Fehlern, dem gesamten Fehlermanagement und seinen Korrekturmaßnahmen.