

Auftragsverarbeiter-Vertrag für die No-Q-Software

Zwischen:

bitte ausfüllen

und

Vertical-Life GmbH, Brennerstraße 32, 39042 Brixen (IT), Telefon: +39 0472 611753
E-Mail: office@vertical-life.info, E-Mail Datenschutzbeauftragter:
dpo@vertical-life.info

Dieser Vertrag ist integrierender Bestandteil des Hauptvertrages zwischen Vertical-Life GmbH (im Folgenden "Auftragnehmer" genannt) und dem Kunden (im Folgenden "Auftraggeber"; zusammen die "Parteien") betreffend die Zur-Verfügung-Stellung der No-Q-Software (im Folgenden: Zugrundeliegender Vertrag).

1. Einleitung, Geltungsbereich, Definitionen

1.1 Die vorliegenden Bestimmungen zur Auftragsverarbeitung regeln die Rechte und Pflichten von Auftraggeber und -nehmer in Bezug auf die Verarbeitung von personenbezogenen Daten im Sinne und mit Wirkung laut Artikel 28 Absatz 3 der Verordnung (EU) 679/16 (in der Folge: DSGVO).

1.2 Dieser Vertrag findet auf alle Tätigkeiten Anwendung, bei denen der Auftragnehmer, seine Mitarbeiter oder durch ihn beauftragte Unterauftragnehmer (Subunternehmer) im Auftrag des Auftraggebers im Rahmen des Zugrundeliegenden Vertrages personenbezogene Daten verarbeiten.

1.3 Die in den vorliegenden Bestimmungen zur Auftragsverarbeitung verwendeten Begriffe sind entsprechend ihrer Definition in der DSGVO zu verstehen.

1.4. Soweit nicht ausdrücklich anders geregelt, gilt der Auftraggeber als „Verantwortlicher“ laut Artikel 4 Nr. 7 DSGVO und der Auftragnehmer als „Auftragsverarbeiter“ laut Artikel 4 Nr. 8 DSGVO.

2. Gegenstand und Dauer der Verarbeitung

2.1 Gegenstand: Der Auftragnehmer übernimmt folgende Verarbeitungen: Verarbeitung von Daten zur Ausführung des Dienstes No-Q laut Beschreibung im Zugrundeliegenden Vertrag (im Folgenden auch als „No-Q-System“ bezeichnet).

2.2 Dauer: Dieser Vertrag ist für die gesamte Dauer des Hauptvertrages gültig.

3. Art und Zweck der Datenerhebung, -verarbeitung oder -nutzung

3.1 Art und Zweck der Verarbeitung: Die Verarbeitung ist folgender Art: Sammeln, Speichern, Abänderung auf Anfrage des Kunden, Übermittlung, Anonymisieren laut Vorgaben des Kunden.

Die Verarbeitung dient folgendem Zweck: Ausführung des Dienstes No-Q sowie Generierung eines lesbaren QR-Codes (z.B. für das Portal der Abda) sowie Bestellung, Druck und Versand der Immune-ID.

3.2 Art der Daten: Vorbehaltlich Ziff. 3.3. kann die Verarbeitung durch den Auftragnehmer je nach Konfiguration des No-Q-Systems durch den Auftraggeber folgende Kategorien personenbezogener Daten umfassen:

Daten der Mitarbeiter des Auftraggebers:

Vorname
Nachname
E-Mail-Adresse
Geburtsdatum
Adresse
Stadt
Postleitzahl
Telefon
Mobiltelefon

Daten der Kunden des Auftraggebers:

- Vorname
- Nachname
- E-Mail-Adresse
- Adresse
- Stadt
- Postleitzahl
- Staatsangehörigkeit
- Land (des Wohnsitzes)
- Telefon
- Mobiltelefon
- Geburtsdatum
- Steuernummer / Steueridentifikationsnummer
- IP-Adresse
- Kreditkarteninformationen
- Mitgliedsstatus
- Passport/ID-Nr.
- Angaben zur durchgeführten Buchung: Buchungs-ID, Zeitpunkt der Anmeldung
- Angaben zum durchgeführten Corona-Test: Datum des Tests, Ort des Tests, Analysis, Arzt, Service, Test, Test Kit, Test-Art), Test-Ergebnis (Result)
- Zusätzliche Angaben zum durchgeführten Corona-Test bei Verwendung eines KLS Leseautomaten: Foto des Testkits
- Angaben zur Impfung: Datum des Impfung, Art der Impfung, Impfstoff, Service

(Hersteller), Chargennummer, Chronische Vorerkrankungen, Arzt, Hinweis
Zweitimpfung

Angaben für die Digitalisierung des Impfpasses: Erhaltene(r) Impfstoff(e), Datum der Impfung(en), digitaler Impfnachweis

Daten der Kunden, welche die Immune-ID bestellen: Name, Adresse, digitales COVID-Zertifikat der EU (und darin enthaltene Informationen)

Kategorien der von der Verarbeitung betroffenen Personen:

- Mitarbeiter des Auftraggebers
- Kunden des Auftraggebers

3.3 Verarbeitung besonderer Kategorien personenbezogener Daten (Art. 9): Der Auftragnehmer kann für Supportzwecke Zugang zu Gesundheitsinformationen der betroffenen Personen erhalten. Grundsätzlich beschränkt sich die Verarbeitung von Gesundheitsdaten auf die Bereitstellung des Systems.

3.4 Der Auftraggeber sichert zu und garantiert, dass er alle anwendbaren Gesetze, einschließlich der Datenschutzgesetze, bezüglich der Verarbeitung von Daten und aller Verarbeitungsanweisungen, die er an den Auftragnehmer erteilt, eingehalten hat und weiterhin einhalten wird; und er alle Mitteilungen gemacht hat und weiterhin machen wird und alle Zustimmungen und Rechte, die gemäß den Datenschutzgesetzen für die Verarbeitung von personenbezogenen Daten durch den Auftragnehmer für die in der Vereinbarung beschriebenen Zwecke notwendig sind, erhalten hat und erhalten wird. Der Auftraggeber trägt die alleinige Verantwortung für die Richtigkeit, Qualität und Rechtmäßigkeit der zur Verarbeitung an den Auftragnehmer übergebenen personenbezogenen Daten und die Mittel, mit denen er die Daten erworben hat. Unbeschadet der Allgemeingültigkeit des Vorstehenden erklärt sich der Auftraggeber damit einverstanden, dass er für die Einhaltung aller Gesetze (einschließlich der Datenschutzgesetze) verantwortlich ist.

3.5 Der Auftraggeber versichert, dass die Verarbeitung der Daten durch den Auftragnehmer in Übereinstimmung mit den Anweisungen des Auftraggebers nicht dazu führt, dass der Auftragnehmer gegen geltende Gesetze, Vorschriften oder Regeln verstößt, einschließlich, aber nicht beschränkt auf Datenschutzgesetze.

4. Pflichten des Auftragnehmers

4.1 Der Auftragnehmer verarbeitet personenbezogene Daten ausschließlich wie vertraglich vereinbart oder wie vom Auftraggeber angewiesen, es sei denn, der Auftragnehmer ist gesetzlich zu einer bestimmten Verarbeitung verpflichtet. Sofern solche Verpflichtungen für ihn bestehen, teilt der Auftragnehmer diese dem Auftraggeber vor der Verarbeitung mit, es sei denn, die Mitteilung ist ihm gesetzlich verboten. Der Auftragnehmer verwendet darüber hinaus die zur Verarbeitung überlassenen Daten für keine anderen, insbesondere nicht für eigene Zwecke.

4.2 Der Auftragnehmer bestätigt, dass ihm die einschlägigen, allgemeinen datenschutzrechtlichen Vorschriften bekannt sind. Er beachtet die Grundsätze ordnungsgemäßer Datenverarbeitung.

4.3. Sofern nicht ausdrücklich anders vereinbart, obliegt die Verantwortung für die Einhaltung von Bestimmungen, die über die allgemeinen datenschutzrechtlichen

Vorschriften hinausgehen (beispielsweise die Einhaltung von in Sonderbestimmungen festgelegten Aufbewahrungspflichten), dem Auftraggeber.

4.4 Der Auftragnehmer verpflichtet sich, bei der Verarbeitung die Vertraulichkeit streng zu wahren.

4.5 Personen, die Kenntnis von den im Auftrag verarbeiteten Daten erhalten können, haben sich schriftlich zur Vertraulichkeit zu verpflichten, soweit sie nicht bereits gesetzlich einer einschlägigen Geheimhaltungspflicht unterliegen.

4.6 Der Auftragnehmer sichert zu, dass die bei ihm zur Verarbeitung eingesetzten Personen vor Beginn der Verarbeitung mit den relevanten Bestimmungen des Datenschutzes und dieses Vertrags vertraut gemacht wurden. Entsprechende Schulungs- und Sensibilisierungsmaßnahmen sind angemessen regelmäßig zu wiederholen. Der Auftragnehmer trägt dafür Sorge, dass zur Auftragsverarbeitung eingesetzte Personen hinsichtlich der Erfüllung der Datenschutzanforderungen laufend angemessen angeleitet und überwacht werden.

4.7 Im Zusammenhang mit der beauftragten Verarbeitung hat der Auftragnehmer den Auftraggeber bei Erstellung und Fortschreibung des Verzeichnisses der Verarbeitungstätigkeiten sowie bei Durchführung der Datenschutzfolgeabschätzung zu unterstützen.

4.8 Wird der Auftraggeber durch Aufsichtsbehörden oder andere Stellen einer Kontrolle unterzogen oder machen betroffene Personen ihm gegenüber Rechte geltend, verpflichtet sich der Auftragnehmer den Auftraggeber umgehend zu informieren und im erforderlichen Umfang zu unterstützen, soweit die Verarbeitung im Auftrag betroffen ist.

4.9 Auskünfte an Dritte oder den Betroffenen darf der Auftragnehmer nur nach vorheriger Zustimmung durch den Auftraggeber erteilen. Direkt an ihn gerichtete Anfragen wird er unverzüglich an den Auftraggeber weiterleiten.

4.10 Soweit gesetzlich verpflichtet, bestellt der Auftragnehmer eine fachkundige und zuverlässige Person als Beauftragten für den Datenschutz. Es ist sicherzustellen, dass für den Beauftragten keine Interessenskonflikte bestehen. In Zweifelsfällen kann sich der Auftraggeber direkt an den Datenschutzbeauftragten wenden. Der Auftragnehmer teilt dem Auftraggeber unverzüglich die Kontaktdaten des Datenschutzbeauftragten mit oder begründet, weshalb kein Beauftragter bestellt wurde. Änderungen in der Person oder den innerbetrieblichen Aufgaben des Beauftragten teilt der Auftragnehmer dem Auftraggeber unverzüglich mit.

4.11 Die Auftragsverarbeitung erfolgt grundsätzlich innerhalb der EU oder des EWR.

5. Technische und organisatorische Maßnahmen

5.1 Die in Anhang 3 beschriebenen Datensicherheitsmaßnahmen werden als verbindlich festgelegt.

5.2 Die Datensicherheitsmaßnahmen können der technischen und organisatorischen Weiterentwicklung entsprechend angepasst werden, solange das hier vereinbarte Niveau nicht unterschritten wird. Zur Aufrechterhaltung der Informationssicherheit

erforderliche Änderungen hat der Auftragnehmer unverzüglich umzusetzen. Änderungen sind dem Auftraggeber unverzüglich mitzuteilen. Wesentliche Änderungen sind zwischen den Parteien zu vereinbaren.

5.3 Soweit die getroffenen Sicherheitsmaßnahmen den Anforderungen des Auftraggebers nicht oder nicht mehr genügen, benachrichtigt der Auftragnehmer den Auftraggeber unverzüglich.

5.4 Der Auftragnehmer sichert zu, dass die im Auftrag verarbeiteten Daten von sonstigen Datenbeständen strikt getrennt werden.

5.5 Kopien oder Duplikate werden ohne Wissen des Auftraggebers nicht erstellt. Ausgenommen sind technisch notwendige, temporäre Vervielfältigungen, soweit eine Beeinträchtigung des hier vereinbarten Datenschutzniveaus ausgeschlossen ist.

5.6 Die Verarbeitung von Daten in Privatwohnungen ist gestattet. Soweit eine solche Verarbeitung erfolgt, ist vom Auftragnehmer sicherzustellen, dass dabei ein diesem Vertrag entsprechendes Niveau an Datenschutz und Datensicherheit aufrechterhalten wird.

5.7 Dedizierte Datenträger, die vom Auftraggeber stammen bzw. für den Auftraggeber genutzt werden, werden besonders gekennzeichnet und unterliegen der laufenden Verwaltung. Sie sind jederzeit angemessen aufzubewahren und dürfen unbefugten Personen nicht zugänglich sein. Ein- und Ausgänge werden dokumentiert.

6. Regelungen zur Berichtigung, Löschung und Sperrung von Daten

6.1 Im Rahmen des Auftrags verarbeitete Daten wird der Auftragnehmer nur entsprechend der getroffenen vertraglichen Vereinbarung oder nach Weisung des Auftraggebers berichtigen, löschen oder sperren.

6.2 Den entsprechenden Weisungen des Auftraggebers wird der Auftragnehmer jederzeit Folge leisten. Dienstleistungen, welche nicht Teil des ursprünglichen Auftrags sind, werden jedenfalls in Rechnung gestellt (z.B. Speicherung von Daten).

7. Unterauftragsverhältnisse

7.1 Eine Beauftragung ist gestattet, sofern den Subunternehmern vertraglich mindestens Datenschutzpflichten auferlegt wurden, die mit den in diesem Vertrag vereinbarten, vergleichbar sind.

7.2 Die Verantwortlichkeiten des Auftragnehmers und des Subunternehmers sind eindeutig voneinander abzugrenzen.

7.3 Eine weitere Subbeauftragung durch den Subunternehmer ist zulässig.

7.4 Der Auftragnehmer wählt den Subunternehmer unter besonderer Berücksichtigung der Eignung der vom Subunternehmer getroffenen technischen und organisatorischen Maßnahmen sorgfältig aus.

7.5 Die Beauftragung von Subunternehmern, welche die Verarbeitungen im Auftrag nicht ausschließlich auf dem Gebiet der EU oder des EWR erbringen, ist nur bei Beachtung der in Artikel 5 genannten Bedingungen möglich. Sie ist insbesondere nur

zulässig, soweit und solange der Subunternehmer angemessene Datenschutzgarantien bietet.

7.6 Kommt der Subunternehmer seinen Datenschutzpflichten nicht nach, so haftet hierfür der Auftragnehmer gegenüber dem Auftraggeber.

7.7 Zurzeit sind die in Anlage 1 mit Namen, Anschrift und Auftragsinhalt bezeichneten Subunternehmer mit der Verarbeitung von personenbezogenen Daten in dem dort genannten Umfang beschäftigt.

8. Rechte und Pflichten des Auftraggebers

8.1 Für die Beurteilung der Zulässigkeit der beauftragten Verarbeitung sowie für die Wahrung der Rechte von Betroffenen ist allein der Auftraggeber verantwortlich.

8.2 Der Auftraggeber erteilt alle Aufträge, Teilaufträge oder Weisungen dokumentiert. In Eilfällen können Weisungen mündlich erteilt werden. Solche Weisungen wird der Auftraggeber unverzüglich dokumentiert bestätigen.

8.3 Der Auftraggeber informiert den Auftragnehmer unverzüglich, wenn er Fehler oder Unregelmäßigkeiten bei der Prüfung der Auftragsergebnisse feststellt.

8.4 Der Auftraggeber ist berechtigt, die Einhaltung der Vorschriften über den Datenschutz und der vertraglichen Vereinbarungen beim Auftragnehmer in angemessenem Umfang selbst oder durch Dritte, insbesondere durch die Einholung von Auskünften und die Einsichtnahme in die gespeicherten Daten und die Datenverarbeitungsprogramme zu kontrollieren.

8.5 Kontrollen beim Auftragnehmer haben ohne vermeidbare Störungen seines Geschäftsbetriebs zu erfolgen. Soweit nicht aus vom Auftraggeber zu dokumentierenden, dringlichen Gründen anders angezeigt, finden Kontrollen nach angemessener Vorankündigung und zu Geschäftszeiten des Auftragnehmers, sowie nicht häufiger als alle 12 Monate statt. Für die Ermöglichung von Kontrollen durch den Auftraggeber kann der Auftragnehmer einen Vergütungsanspruch geltend machen.

9. Mitteilungspflichten

9.1 Der Auftragnehmer teilt dem Auftraggeber Verletzungen des Schutzes personenbezogener Daten unverzüglich mit. Die Mitteilung hat spätestens innerhalb von 24 Stunden ab Kenntnis des Auftragnehmers vom relevanten Ereignis an eine vom Auftraggeber benannte Adresse zu erfolgen. Sie muss mindestens folgende Angaben enthalten:

- eine Beschreibung der Art der Verletzung des Schutzes personenbezogener Daten, soweit möglich mit Angabe der Kategorien und der ungefähren Zahl der betroffenen Personen, der betroffenen Kategorien und der ungefähren Zahl der betroffenen personenbezogenen Datensätze;
- den Namen und die Kontaktdaten des Datenschutzbeauftragten oder einer sonstigen Anlaufstelle für weitere Informationen;
- eine Beschreibung der vom Auftragnehmer ergriffenen oder vorgeschlagenen Maßnahmen zur Behebung der Verletzung des Schutzes personenbezogener

Daten und gegebenenfalls Maßnahmen zur Abmilderung ihrer möglichen nachteiligen Auswirkungen

9.2 Ebenfalls unverzüglich mitzuteilen sind erhebliche Störungen bei der Auftragsabwicklung sowie Verstöße des Auftragnehmers oder der bei ihm beschäftigten Personen gegen datenschutzrechtliche Bestimmungen oder die in diesem Vertrag getroffenen Festlegungen.

9.3 Der Auftragnehmer informiert den Auftraggeber unverzüglich von Kontrollen oder Maßnahmen von Aufsichtsbehörden oder anderen Dritten, soweit diese Bezüge zur Auftragsverarbeitung aufweisen.

9.4 Der Auftragnehmer sichert zu, den Auftraggeber bei dessen Pflichten nach Art. 32 und folgende Datenschutz-Grundverordnung im erforderlichen Umfang zu unterstützen.

10. Weisungen

10.1 Der Auftraggeber behält sich hinsichtlich der Verarbeitung im Auftrag ein umfassendes Weisungsrecht vor.

10.2 Auftraggeber und Auftragnehmer benennen die zur Erteilung und Annahme von Weisungen ausschließlich befugten Personen in Anlage 2.

10.3 Bei einem Wechsel oder einer längerfristigen Verhinderung der benannten Personen sind der anderen Partei Nachfolger bzw. Vertreter unverzüglich mitzuteilen.

10.4 Der Auftragnehmer wird den Auftraggeber darauf aufmerksam machen, wenn eine vom Auftraggeber erteilte Weisung seiner Meinung nach gegen gesetzliche Vorschriften verstößt. Der Auftragnehmer ist berechtigt, die Durchführung der entsprechenden Weisung so lange auszusetzen, bis sie durch den Verantwortlichen beim Auftraggeber bestätigt oder geändert wird.

11. Beendigung des Auftrags

11.1 Bei Beendigung des Auftragsverhältnisses oder jederzeit auf Verlangen des Auftraggebers hat der Auftragnehmer die im Auftrag verarbeiteten Daten nach Wahl des Auftraggebers entweder zu vernichten oder an den Auftraggeber zu übergeben. Ebenfalls zu vernichten sind sämtliche vorhandene Kopien der Daten. Die Vernichtung hat so zu erfolgen, dass eine Wiederherstellung auch von Restinformationen mit vertretbarem Aufwand nicht mehr möglich ist.

11.2 Der Auftragnehmer ist verpflichtet, die unverzügliche Rückgabe bzw. Löschung auch bei Subunternehmern herbeizuführen.

11.3 Dokumentationen, die dem Nachweis der ordnungsgemäßen Datenverarbeitung dienen, sind durch den Auftragnehmer den jeweiligen Aufbewahrungsfristen entsprechend auch über das Vertragsende hinaus aufzubewahren. Er kann sie zu seiner Entlastung dem Auftraggeber bei Vertragsende übergeben.

12. Vergütung

12.1 Die Vergütung des Auftragnehmers ist abschließend im Hauptvertrag geregelt.

13. Sonstiges

13.1 Die Parteien sind verpflichtet, alle im Rahmen des Vertragsverhältnisses erlangten Kenntnisse von Geschäftsgeheimnissen und Datensicherheitsmaßnahmen der jeweils anderen Partei auch über die Beendigung des Vertrages vertraulich zu behandeln. Bestehen Zweifel, ob eine Information der Geheimhaltungspflicht unterliegt, ist sie bis zur schriftlichen Freigabe durch die andere Partei als vertraulich zu behandeln.

13.2 Sollten einzelne Teile der gegenständlichen Allgemeinen Bedingungen zur Auftragsverarbeitung unwirksam sein, so berührt dies die Wirksamkeit der übrigen Teile nicht.

13.3 Die gegenständlichen Allgemeinen Bedingungen zur Auftragsverarbeitung stellen Allgemeine Geschäftsbedingungen der Vertical-Life GmbH laut Artikel 1341 Absatz 1 ZGB dar und sind gegenüber dem Auftraggeber wirksam, sofern dieser sie bei Vertragsschluss kannte oder unter Anwendung ordentlicher Sorgfalt kennen hätte müssen.

13.4 Die gegenständlichen Allgemeinen Bedingungen zur Auftragsverarbeitung unterliegen dem auf dem Gebiet der Italienischen Republik anzuwendenden Recht und werden nach diesem Recht ausgelegt und jegliche Rechtsstreitigkeiten, die sich aus dem Vertrag ergeben, unterliegen ausschließlich der Gerichtsbarkeit der Gerichte in Bozen.

Brixen, am _____

Ort, Datum: _____

Für den Auftragnehmer

Für den Auftraggeber

Vertical-Life GmbH

Matthias Polig

Anlage 1 – Derzeit bestehende Subdienstleister

Hosting, Network und Data Services:

Google Cloud ([GDPR](#))

Google Ireland Limited, Gordon House, Barrow Street, Dublin 4, Ireland

Standort der Datenverarbeitung: EU

Amazon Web Services ([GDPR](#))

Amazon Web Services EMEA SARL, 38 Avenue John F. Kennedy, Luxembourg City, 01855, Luxembourg

Standort der Datenverarbeitung: EU

Verwaltung kryptografischer Schlüssel:

Thales ([GDPR](#))

Thales corporate headquarters, Tour Carpe Diem, 31 Place des Corolles, CS 20001 - 92098 Paris La Défense, Frankreich

Standort der Datenverarbeitung: Europa

Web Application Firewall:

Cloudflare ([GDPR](#))

Cloudflare, Inc., 101 Townsend St, San Francisco, CA 94107, USA

Standort der Datenverarbeitung: Europa, USA

Garantie der DSGVO-konformen Verarbeitung: Zertifizierung ISO/IEC 27701:2019

Performance Monitoring:

App Signal ([GDPR](#))

AppSignal B.V., Rietwaard 4, 5236WC's Hertogenbosch, Niederlande

Standort der Datenverarbeitung: EU

E-Mail Service:

Mailgun ([GDPR](#))

Mailgun Technologies, Inc, 112 E. Pecan St. #1135, San Anonio, TX 78205, USA

Standort der Datenverarbeitung: EU

SMTPeter ([GDPR](#))

Copernica BV, De Ruijterkade 112, 1011 AB, Amsterdam, Niederlande

Standort der Datenverarbeitung: EU

Optionale Ergebnis-Übermittlung an die Corona-Warn-App:

Corona-Warn-App

T-Systems International GmbH, Hahnstraße 43d, 60528, Frankfurt am Main, Deutschland

Standort der Datenverarbeitung: EU

Druck und Versand der Immune-ID:

pml GmbH, Arthur-Piechler-Str. 1i, 86316 Friedberg, Deutschland
<http://www.pml-augsburg.de/impressum/>

VENDO Kommunikation + Druck GmbH, Johannes Gutenbergstraße 2, 4840
Vöcklabruck, Österreich
<https://vendo.at/impressum>

Anlage 2 – Weisungsberechtigte Personen

Folgende Personen sind zur Erteilung und Entgegennahme von Weisungen befugt:

Erteilung:

bitte ausfüllen

Entgegennahme:

Matthias Polig
Iiro Virtanen
Maria Hilber

Anlage 3 - Technisch-organisatorische Maßnahmen

1 Vertraulichkeit

- Zutrittskontrolle: Maßnahmen, die verhindern sollen, dass Unbefugte Zugang zu Datenträgern erhalten, die personenbezogene Daten verarbeiten oder verwenden: Schlüssel; einbruchsichere Fenster und Sicherheitstüren; Begleitung von Personen im Unternehmensgebäude;
- Zugangskontrolle: Maßnahmen, die eine unbefugte Systembenutzung verhindern sollen: Passwörter; Zweifaktor-Authentifizierung für Zugriffe auf Systemservices;
- Zugriffskontrolle: Kein unbefugtes Lesen, Kopieren, Verändern oder Entfernen innerhalb des Systems durch: Berechtigungsprofile, die eine differenzierte Steuerung des Datenzugriffs ermöglichen; Protokollierung von Zugriffen; sichere Aufbewahrung von Speichermedien; Clear-Desk/Clear-Screen Policy.

2 Datenintegrität

- Weitergabekontrolle: Kein unbefugtes Lesen, Kopieren, Verändern oder Entfernen bei elektronischer Übertragung oder Transport durch: Verschlüsselung von Dateien; sichere physische Speicherung von Daten durch Cloud Hosting;
- Sichere Speicherung: sichere physische Speicherung von Daten durch Cloud Hosting; Verschlüsselung von Datenbanken und deren Backups;
- Eingabekontrolle: Feststellung, ob und von wem personenbezogene Daten in Datenverarbeitungssysteme eingegeben, verändert oder entfernt worden sind durch: Protokollierung; Datenprotokolle, die auf verschiedenen Ebenen (z.B. Betriebssystem, Netzwerk, Firewall, Datenbank, Anwendung) erfolgen können; Dokumentenmanagement.

3 Verfügbar- und Belastbarkeit

- Verfügbarkeitskontrolle: Schutz gegen zufällige oder mutwillige Zerstörung bzw. Verlust durch: Backup Strategie (online/offline; on-site/off-site); Virenschutz; Firewall;
- Wiederherstellbarkeit: Daten werden täglich automatisch gesichert und können zu jedem Zeitpunkt wiederhergestellt werden.

4 Verfahren zur regelmäßigen Überprüfung, Bewertung und Evaluierung

- Datenschutzmanagement: Jährliche und regelmäßige Datenschutzbewertungen für alle unsere Dienstleistungen;.
- Incident-Response-Management: Unterstützung bei der Reaktion auf Sicherheitsverletzungen;.
- Datenschutzfreundliche Voreinstellungen: Privacy by design/privacy by default;
- Auftragskontrolle: Maßnahmen, die sicherstellen, dass personenbezogene Daten, die im Auftrag des Kunden verarbeitet werden, nur nach den Anweisungen des Kunden verarbeitet werden können. Alle unabhängigen

Auftragnehmer und/oder Berater halten sich an die definierten Datenverarbeitungsrichtlinien.