ANLAGE A ZUM HAUPTVERTRAG

Auftragsverarbeitungsvertrag nach Art. 28 Abs. 3 DSGVO

Die Parteien stimmen überein, dass dieser Auftragsverarbeitungsvertrag (kurz AVV) zu den Produkten und Services von No-Q ihre Verpflichtungen in Bezug auf die Verarbeitung und Sicherheit von personenbezogenen Daten im Zusammenhang mit den Produkten und Services festlegt. Wenn kein separater Vertrag zwischen No-Q und dem Kunden besteht, stimmen die Parteien außerdem zu, dass die Verarbeitung ebenfalls diesem AVV unterliegt.

Definitionen

Kunde: Nutzer der Software bzw. Verantwortlicher im Sinne der DSGVO

No-Q (No-Q): No-Q GmbH, Brennerstraße 32, I – 39042 Brixen

Hauptvertrag: Der mit dem Kunden abgeschlossene Lizenzvertrag

DSGVO: bezeichnet die Verordnung (EU) 2016/679 des Europäischen Parlaments und des Rates vom 27. April 2016 zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten, zum freien Datenverkehr und zur Aufhebung der Richtlinie 95/46/EG (Datenschutz-Grundverordnung).

Unterauftragsverarbeiter: bezeichnet sonstige Auftragsverarbeiter, die No-Q zur Verarbeitung von personenbezogenen Daten hinzuzieht, wie in Artikel 28 der DSGVO beschrieben.

Parteien: Der Kunde und No-Q

1. Gegenstand und Dauer der Vereinbarung

Zur Klarstellung wird angemerkt, dass diese AVV-Bestimmungen nur für die Verarbeitung von Daten in Umgebungen gelten, die von No-Q und den Unterauftragsverarbeitern von No-Q kontrolliert werden. Dies umfasst Daten, die von Produkten und Services an No-Q gesendet werden, jedoch keine Daten, die in den Räumlichkeiten des Kunden oder in vom Kunden ausgewählten Betriebsumgebungen von Drittanbietern verbleiben.

No-Q befolgt alle für die Bereitstellung der Produkte und Services geltenden Gesetze und Vorschriften, einschließlich Gesetzen zu Meldepflichten bei Sicherheitsverletzungen, sowie Datenschutzvorschriften. No-Q ist jedoch nicht für die Einhaltung von Gesetzen oder Regelungen verantwortlich, die für den Kunden oder seine Branche gelten (Bsp. Arztgeheimnis). No-Q ermittelt nicht, ob Personenbezogene Daten Informationen enthalten, die spezifischen Gesetzen oder Vorschriften unterliegen.

Diese Vereinbarung gilt mit Unterzeichnung des Hauptvertrages bzw. erster Nutzung der Software.

Der Kunde kann den AVV jederzeit ohne Einhaltung einer Frist kündigen, wenn ein schwerwiegender Verstoß von No-Q gegen Datenschutzvorschriften oder die Bestimmungen dieses Vertrages vorliegt, No-Q eine Weisung des Kundes nicht ausführen kann oder will oder No-Q Kontrollrechte des Kunden vertragswidrig verweigert. Insbesondere die Nichteinhaltung der in diesem Vertrag vereinbarten und aus Art. 28 DSGVO abgeleiteten Pflichten stellt einen schweren Verstoß dar.

2. Art und Zweck der Verarbeitung, Art der personenbezogenen Daten sowie Kategorien betroffener Personen

Die Art und Zweck der Verarbeitung, Art der personenbezogenen Daten sowie Kategorien betroffener Personen sind in der Anlage 1 zu diesem AVV beschrieben.

No-Q wird personenbezogene Daten nur wie nachstehend beschrieben verarbeiten:

(a) um dem Kunden die Produkte und Services in Übereinstimmung mit den dokumentierten Anweisungen des Kunden zur Verfügung zu stellen:

- Die Bereitstellung von Funktionen wie vom Kunden und dessen Benutzern lizenziert, konfiguriert und verwendet, einschließlich der Bereitstellung personalisierter Benutzererfahrungen,
- Die Fehlerbehebung (Verhinderung, Erkennung und Behebung von Problemen); und
- Produkte auf dem neuesten Stand und leistungsfähig zu halten und Förderung der Benutzerproduktivität, Zuverlässigkeit, Effektivität, Qualität und Sicherheit.

(b) für die Geschäftstätigkeiten, die durch die Bereitstellung der Produkte und Services an den Kunden veranlasst sind:

- Abrechnungs- und Kontoverwaltung;
- Der Kunde autorisiert No-Q zur Erstellung aggregierter statistischer, nicht personenbezogener Daten aus Daten, die pseudonymisierte Identifikatoren enthalten (wie etwa Nutzungsprotokolle, die eindeutige, pseudonymisierte Identifikatoren enthalten) und zur Berechnung von Statistiken

3. Rechte und Pflichten sowie Weisungsbefugnisse des Kunden

Für die Beurteilung der Zulässigkeit der Verarbeitung gemäß Art. 6 Abs. 1 DSGVO sowie für die Wahrung der Rechte der betroffenen Personen nach den Art. 12 bis 22 DSGVO ist allein der Kunde verantwortlich. Gleichwohl ist No-Q verpflichtet, alle solche Anfragen, sofern sie erkennbar ausschließlich an den Kunde gerichtet sind, unverzüglich an diesen weiterzuleiten.

Änderungen des Verarbeitungsgegenstandes und Verfahrensänderungen sind gemeinsam zwischen Kunde und No-Q abzustimmen und schriftlich oder in einem dokumentierten elektronischen Format festzulegen.

Der Kunde erteilt alle Aufträge, Teilaufträge und Weisungen in der Regel schriftlich oder in einem dokumentierten elektronischen Format. Mündliche Weisungen sind unverzüglich schriftlich oder in einem dokumentierten elektronischen Format zu bestätigen.

Der Kunde ist berechtigt, sich vor Beginn der Verarbeitung und sodann regelmäßig in angemessener Weise von der Einhaltung der bei No-Q getroffenen technischen und organisatorischen Maßnahmen sowie der in diesem Vertrag festgelegten Verpflichtungen zu überzeugen.

Der Kunde informiert No-Q unverzüglich, wenn er Fehler oder Unregelmäßigkeiten bei der Prüfung der Auftragsergebnisse feststellt.

Der Kunde ist verpflichtet, alle im Rahmen des Vertragsverhältnisses erlangten Kenntnisse von Geschäftsgeheimnissen und Datensicherheitsmaßnahmen von No-Q vertraulich zu behandeln. Diese Verpflichtung bleibt auch nach Beendigung dieses Vertrages bestehen.

4. Weisungsberechtigte des Kunden, Weisungsempfänger von No-Q

Der Kunde hat No-Q mit der Vertragsunterzeichnung bzw. vor der ersten Nutzung der Software schriftlich über die weisungsberechtigten Personen zu informieren.

Weisungsempfänger bei No-Q sind:

Maria Hilber: No-Q GmbH, Brennerstraße 32, I – 39042 Brixen, E-Mail: m.hilber@no-q.info

Matthias Polig: No-Q GmbH, Brennerstraße 32, I – 39042 Brixen, E-Mail: m.polig@no-q.info

Iiro Virtanen: No-Q GmbH, Brennerstraße 32, I – 39042 Brixen, E-Mail: i.virtanen@no-q.info

Für Weisung zu nutzende Kommunikationskanäle:

E-Mail, Post oder zertifizierte E-Mail (PEC).

Bei einem Wechsel oder einer längerfristigen Verhinderung der Ansprechpartner sind No-Q unverzüglich und grundsätzlich schriftlich oder elektronisch die Nachfolger bzw. die Vertreter mitzuteilen. Die Weisungen sind für ihre Geltungsdauer und anschließend noch für drei volle Kalenderjahre aufzubewahren.

5. Pflichten von No-Q

No-Q verarbeitet personenbezogene Daten ausschließlich im Rahmen der getroffenen Vereinbarungen und nach Weisungen des Kunden, sofern No-Q nicht zu einer anderen Verarbeitung durch das Recht der Union oder der Mitgliedstaaten, dem der Auftragsverarbeiter unterliegt, hierzu verpflichtet ist (z. B. Ermittlungen von Strafverfolgungs- oder Staatsschutzbehörden); in einem solchen Fall teilt No-Q dem Verantwortlichen diese rechtlichen Anforderungen vor der Verarbeitung mit, sofern das betreffende Recht eine solche Mitteilung nicht wegen eines wichtigen öffentlichen Interesses verbietet (Art. 28 Abs. 3 Satz 2 lit. a DSGVO).

No-Q verwendet die zur Verarbeitung überlassenen personenbezogenen Daten für keine anderen, insbesondere nicht für eigene Zwecke. Davon ausgenommen ist die unter Punkt 2 beschriebene Verwendung für statistische Zwecke. Kopien oder Duplikate der personenbezogenen Daten werden ohne Wissen des Kunden nicht erstellt. Davon jedenfalls ausgenommen sind die regelmäßigen Backups, welche No-Q im Kundenauftrag erstellt.

No-Q sichert im Bereich der auftragsgemäßen Verarbeitung von personenbezogenen Daten die vertragsgemäße Abwicklung aller vereinbarten Maßnahmen zu. No-Q sichert zu, dass die für den Kunden verarbeiteten Daten von sonstigen Datenbeständen strikt getrennt werden.

Die Datenträger, die vom Kunden stammen bzw. für den Kunden genutzt werden, werden besonders gekennzeichnet. Eingang und Ausgang sowie die laufende Verwendung werden dokumentiert.

Bei der Erfüllung der Rechte der betroffenen Personen nach Art. 12 bis 22 DSGVO durch den Kunden, an der Erstellung der Verzeichnisse von Verarbeitungstätigkeiten sowie bei erforderlichen Datenschutz-Folgeabschätzungen des Kunden hat No-Q im notwendigen Umfang mitzuwirken und den Kunde soweit möglich angemessen zu unterstützen (Art. 28 Abs. 3 Satz 2 lit e und f DSGVO).

No-Q wird den Kunden unverzüglich darauf aufmerksam machen, wenn eine vom Kunden erteilte Weisung seiner Meinung nach gegen gesetzliche Vorschriften verstößt (Art. 28 Abs. 3 Satz 3 DSGVO). No-Q ist berechtigt, die Durchführung der entsprechenden Weisung solange

auszusetzen, bis sie durch den Verantwortlichen beim Kunde nach Überprüfung bestätigt oder geändert wird.

No-Q hat personenbezogene Daten aus dem Auftragsverhältnis zu berichtigen, zu löschen oder deren Verarbeitung einzuschränken, wenn der Kunde dies mittels einer Weisung verlangt und berechtigte Interessen von No-Q dem nicht entgegenstehen.

Auskünfte über personenbezogene Daten aus dem Auftragsverhältnis an Dritte oder den Betroffenen darf No-Q nur nach vorheriger Weisung oder Zustimmung durch den Kunden erteilen.

No-Q erklärt sich damit einverstanden, dass der Kunde - grundsätzlich nach Terminvereinbarung - berechtigt ist, die Einhaltung der Vorschriften über Datenschutz und Datensicherheit sowie der vertraglichen Vereinbarungen im angemessenen und erforderlichen Umfang selbst oder durch vom Kunde beauftragte Dritte zu kontrollieren, insbesondere durch die Einholung von Auskünften und die Einsichtnahme in die gespeicherten Daten und die Datenverarbeitungsprogramme sowie durch Überprüfungen und Inspektionen vor Ort (Art. 28 Abs. 3 Satz 2 lit. h DSGVO).

No-Q sichert zu, dass sie, soweit erforderlich, bei diesen Kontrollen unterstützend mitwirkt.

No-Q bestätigt, dass die für die Auftragsverarbeitung einschlägigen datenschutzrechtlichen Vorschriften der DSGVO ihr bekannt sind. Sie verpflichtet sich, auch folgende für diesen Auftrag relevanten Geheimnisschutzregeln zu beachten, die dem Kunde obliegen:

Berufsgeheimnisse nach § 203 StGB

No-Q verpflichtet sich, bei der auftragsgemäßen Verarbeitung der personenbezogenen Daten des Kunden die Vertraulichkeit zu wahren. Diese besteht auch nach Beendigung des Vertrages fort.

Der No-Q sichert zu, dass er die bei der Durchführung der Arbeiten beschäftigten Mitarbeiter vor Aufnahme der Tätigkeit mit den für sie maßgebenden Bestimmungen des Datenschutzes vertraut macht und für die Zeit ihrer Tätigkeit wie auch nach Beendigung des Beschäftigungsverhältnisses in geeigneter Weise zur Verschwiegenheit verpflichtet (Art. 28 Abs. 3 Satz 2 lit. b und Art. 29 DSGVO). No-Q überwacht die Einhaltung der datenschutzrechtlichen Vorschriften in seinem Betrieb.

Beim No-Q ist als externer Beauftragte(r) für den Datenschutz:

PSY-LEX GmbH, Ansprechperson: Dott. Armin Wieser, E-Mail: psy-lex@legalmail.it, Tel. +39 3519933665

bestellt. Ein Wechsel des Datenschutzbeauftragten ist dem Kunde unverzüglich mitzuteilen.
oder

6. Mitteilungspflichten von No-Q bei Störungen der Verarbeitung und bei Verletzungen des Schutzes personenbezogener Daten

No-Q teilt dem Kunde unverzüglich Störungen, Verstöße bei No-Q oder der bei ihm beschäftigten Personen sowie gegen datenschutzrechtliche Bestimmungen oder die im Auftrag getroffenen Festlegungen sowie den Verdacht auf Datenschutzverletzungen oder Unregelmäßigkeiten bei der Verarbeitung personenbezogener Daten mit. Dies gilt vor allem auch im Hinblick auf eventuelle Melde- und Benachrichtigungspflichten des Kunden nach Art. 33 und Art. 34 DSGVO. No-Q sichert zu, den Kunden erforderlichenfalls bei seinen Pflichten

nach Art. 33 und 34 DSGVO angemessen zu unterstützen (Art. 28 Abs. 3 Satz 2 lit. f DSGVO). Meldungen nach Art. 33 oder 34 DSGVO für den Kunden darf No-Q nur nach vorheriger Weisung gem. Ziff. 4 dieses Vertrages durchführen.

7. Unterauftragsverarbeiter (Art. 28 Abs. 3 Satz 2 lit. d DSGVO)

Die Beauftragung von Unterauftragsverarbeitern mit der Verarbeitung von Daten des Kunden ist No-Q mit Genehmigung des Kunden gestattet.

Zurzeit sind für die No-Q Software die in Anlage 2 mit Namen, Anschrift und Auftragsinhalt bezeichneten Unterauftragsverarbeiter mit der Verarbeitung von personenbezogenen Daten in dem dort genannten Umfang beauftragt. Mit deren Beauftragung erklärt sich der Kunde einverstanden.

Der Auftragsverarbeiter informiert den Verantwortlichen immer über jede beabsichtigte Änderung in Bezug auf die Hinzuziehung neuer oder die Ersetzung bisheriger Unterauftragsverarbeiter, wodurch der Auftraggeber die Möglichkeit erhält, gegen derartige Änderungen Einspruch zu erheben (§ 28 Abs. 2 Satz 2 DSGVO).

Als genehmigt gelten jene Unterauftragsverarbeiter, welche dem Kunden mitgeteilt wurden und gegen die er innerhalb von 14 Tagen nach Erhalt der Mitteilung mittels E-Mail keinen Widerspruch eingelegt hat.

No-Q muss dafür Sorge tragen, dass es die Unterauftragsverarbeiter unter besonderer Berücksichtigung der Eignung der von diesen getroffenen technischen und organisatorischen Maßnahmen im Sinne von Art. 32 DSGVO sorgfältig auswählt. Die relevanten Prüfunterlagen dazu sind dem Kunden auf Anfrage zur Verfügung zu stellen.

Eine Beauftragung von Unterauftragsverarbeitern in Drittstaaten darf nur erfolgen, wenn die besonderen Voraussetzungen der Art. 44 ff. DSGVO erfüllt sind (z.B. Angemessenheitsbeschluss der Kommission, Standarddatenschutzklauseln, genehmigte Verhaltensregeln).

No-Q hat vertraglich sicherzustellen, dass die vereinbarten Regelungen zwischen Kunde und No-Q auch gegenüber Unterauftragsverarbeitern gelten. In dem Vertrag mit dem Unterauftragsverarbeiter sind die Angaben so konkret festzulegen, dass die Verantwortlichkeiten des Auftragnehmers und des Unterauftragsverarbeiters deutlich voneinander abgegrenzt werden. Werden mehrere Unterauftragsverarbeiter eingesetzt, so gilt dies auch für die Verantwortlichkeiten zwischen diesen Subunternehmern. Insbesondere muss der Kunde berechtigt sein, im Bedarfsfall angemessene Überprüfungen und Inspektionen, auch vor Ort, bei Unterauftragsverarbeitern durchzuführen oder durch von ihm beauftragte Dritte durchführen zu lassen.

Der Vertrag mit dem Unterauftragsverarbeiter muss schriftlich abgefasst werden, was auch in einem elektronischen Format erfolgen kann (Art. 28 Abs. 4 und Abs. 9 DSGVO).

Die Weiterleitung von Daten an den Unterauftragsverarbeiter ist erst zulässig, wenn der Unterauftragsverarbeiter die Verpflichtungen nach Art. 29 und Art. 32 Abs. 4 DSGVO bezüglich seiner Beschäftigten erfüllt hat.

No-Q haftet gegenüber dem Kunden dafür, dass der Unterauftragsverarbeiter den Datenschutzpflichten nachkommt, die ihm durch No-Q im Einklang mit dem vorliegenden Vertragsabschnitt vertraglich auferlegt wurden.

8. Technische und organisatorische Maßnahmen nach Art. 32 DSGVO (Art. 28 Abs. 3 Satz 2 lit. c DSGVO)

Es wird für die konkrete Auftragsverarbeitung ein dem Risiko für die Rechte und Freiheiten der von der Verarbeitung betroffenen natürlichen Personen angemessenes Schutzniveau gewährleistet. Dazu werden die Schutzziele von Art. 32 Abs. 1 DSGVO, wie Vertraulichkeit, Integrität und Verfügbarkeit der Systeme und Dienste sowie deren Belastbarkeit in Bezug auf Art, Umfang, Umstände und Zweck der Verarbeitungen derart berücksichtigt, dass durch geeignete technische und organisatorische Abhilfemaßnahmen das Risiko auf Dauer eingedämmt wird.

Das in Anlage 3 beschriebene Datenschutzkonzept stellt die Auswahl der technischen und organisatorischen Maßnahmen passend zum ermittelten Risiko unter Berücksichtigung der Schutzziele nach Stand der Technik detailliert und unter besonderer Berücksichtigung der eingesetzten IT- Systeme und Verarbeitungsprozesse beim Auftragnehmer dar.

9. Verpflichtungen des Auftragnehmers nach Beendigung des Auftrags, (Art. 28 Abs. 3 Satz 2 lit. g DSGVO)

Nach Abschluss der vertraglichen Arbeiten hat No-Q sämtliche in seinen Besitz sowie an Subunternehmen gelangte Daten, Unterlagen und erstellte Verarbeitungs- oder Nutzungsergebnisse, die im Zusammenhang mit dem Auftragsverhältnis stehen, dem Kunden auszuhändigen oder nach Anweisung desselben zu löschen bzw. zu vernichten/vernichten zu lassen.

Die Löschung bzw. Vernichtung ist dem Auftraggeber mit Datumsangabe schriftlich oder in einem dokumentierten elektronischen Format zu bestätigen.

10. Vergütung

Die Vergütung von No-Q auch für Tätigkeiten aus diesem AVV ist abschließend im Hauptvertrag geregelt.

11. Haftung

Auf Art. 82 DSGVO wird verwiesen.

12. Sonstiges

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.

Sollten einzelne Teile des gegenständlichen AVV unwirksam sein, so berührt dies die Wirksamkeit der übrigen Teile nicht.

Der gegenständliche AVV unterliegen dem auf dem Gebiet der Italienischen Republik anzuwendenden Recht und ist nach diesem Recht auszulegen. Jegliche Rechtsstreitigkeiten, die sich aus diesem AVV ergeben, unterliegen ausschließlich der Gerichtsbarkeit der Gerichte in Bozen.

ANLAGE 1

Art und Zweck der Verarbeitung, Art der personenbezogenen Daten sowie Kategorien betroffener Personen

Art der Verarbeitung (entsprechend der Definition von Art. 4 Nr. 2 DSGVO):
Die Verarbeitung ist folgender Art: Einsehen auf Anfrage, Speichern, Abänderung auf Anfrage, Übermittlung auf Anfrage, Anonymisieren laut Vorgaben des Kunden.
Art der personenbezogenen Daten (entsprechend der Definition von Art. 4 Nr. 1, 13, 14):

<table>
<tr>
<td>Daten der <u>Mitarbeiter</u>:
Vorname
Nachname
E-Mail-Adresse
Geburtsdatum
Adresse
Stadt
Postleitzahl
Telefon
Mobiltelefon
Log-Files
IBAN/BIC
Krankenkasse
Sozialversicherungsnummer</td>
<td rowspan="2">Daten der <u>Kunden</u>:
Vorname
Nachname
E-Mail-Adresse
Adresse
Stadt
Postleitzahl
Staatsangehörigkeit
Land (des Wohnsitzes)
Telefon
Mobiltelefon
Geburtsdatum
Steuernummer / Steueridentifikationsnummer
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
Zusätzliche Daten im Rahmen des Rezept Uploads: Fotos des Rezepts inkl. Inhalt (Krankenkasse, Wohnadresse, Datum, Kassen-Nr., Versicherten-Nr., Status, Betriebsstätten-Nr., Arzt-Nr., Verschriebene Medikamente und Einnahme, Unfalltag bei Arbeitsunfall und Arbeitgebernummer, Vertragsarztstempel und Unterschrift</td>
</tr>
<tr>
<td>Daten der <u>Ärzte (oder sonstiger Fachkräfte):</u>
Vorname, Nachname, gebuchte Termine, E-Mail-Adresse</td>
</tr>
</table>

	des Arztes, Informationen zu den Kosten der Medikamente, Informationen zur Abholung der Medikamente, ggf. Informationen zur Zustellung inkl. Adresse) ● Zusätzliche Daten für die Abwicklung sonstiger pharmazeutischer Dienstleistungen: Datum und Uhrzeit des gebuchten Termins, weitere individuell festgelegte abzufragende Informationen ● Zusätzliche Daten für die Buchung und Verlinkung der Videosprechstunden: Datum und Uhrzeit des gebuchten Termins, Gegenstand, gebuchter Arzt (oder sonstige Fachkraft)

Kategorien betroffener Personen (entsprechend der Definition von Art. 4 Nr. 1 DSGVO):

- Mitarbeiter
- Kunden
- Vertragsärzte
- Ärzte oder sonstige Fachkräfte

ANLAGE 2

Unterauftragsverarbeiter

Hosting, Network und Data Services:	T-Systems-Sovereign Cloud powered by Google GDPR T-Systems International GmbH, Hahnstrasse 43d, D-60528 Frankfurt am Main. E-Mail: info@t-systems.com, Telefon: +49 69 200 60-0 Standort der Datenverarbeitung: EU
Document Storage and Locators Hosting	Amazon Web Services EMEA SARL 38 Avenue John F. Kennedy, L-1855, Luxembourg (GPDR) Standort der Datenverarbeitung: Europa Garantie der DSGVO-konformen Verarbeitung: Zertifizierung ISO/IEC 27701:2019
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
Statistics, Notification and Billing Services	The Apache Software Foundation (GDPR) V. P. Data Privacy 1000 N West Street, Suite 1200 Wilmington, DE 19801 Standort der Datenverarbeitung: EU

ANLAGE 3

Technische und organisatorische Maßnahmen nach Art. 32 DSGVO

BEREICH	DETAILS
Organisation der IT-Sicherheit	☑ **Verantwortung für die Sicherheit.** No-Q hat einen oder mehrere Sicherheitsbeauftragte ernannt, die für die Koordination und Überwachung der Sicherheitsregeln und -verfahren verantwortlich sind. ☑ **Funktionen und Verantwortlichkeiten in Bezug auf Sicherheit.** No-Q-Mitarbeiter, die Zugang zu Personenbezogene Daten haben, sind zur Vertraulichkeit verpflichtet. ☑ **Risikomanagementprogramm.** No-Q hat vor der Verarbeitung der personenbezogenen Daten eine Risikobewertung durchgeführt.
Asset-Management	☑ **Anlagenbestand.** No-Q führt einen Bestand aller Datenträger, auf denen personenbezogene Daten gespeichert sind. Der Zugriff auf die Bestände solcher Medien ist auf No-Q-Mitarbeiter beschränkt, die schriftlich dazu berechtigt sind. ☑ **Asset-Handling** No-Q klassifiziert Personenbezogene Daten, um die Identifizierung zu erleichtern und eine angemessene Beschränkung des Zugriffs darauf zu ermöglichen. No-Q legt Einschränkungen für das Drucken von Personenbezogenen Daten fest und verfügt über Verfahren für die Entsorgung gedruckter Materialien, die solche Daten enthalten. Mitarbeiter von No-Q müssen eine Genehmigung von No-Q einholen, bevor sie personenbezogene Daten auf tragbaren Geräten speichern, remote auf solche Daten zugreifen oder solche Daten außerhalb der Einrichtungen von No-Q verarbeiten.
Personal-sicherheit	☑ **Sicherheitsschulungen.** No-Q informiert seine Mitarbeiter über relevante Sicherheitsverfahren und ihre jeweiligen Rollen. No-Q informiert seine Mitarbeiter auch über mögliche Folgen einer Verletzung der Sicherheitsregeln.
Physische und umgebungs-bezogene Sicherheit	☑ **Physischer Zugang zu Einrichtungen.** No-Q beschränkt den Zugang zu Einrichtungen, in denen sich Informationssysteme befinden, die personenbezogene Daten verarbeiten, auf identifizierte, autorisierte Personen. ☑ **Physischer Zugriff auf Komponenten.** No-Q führt Aufzeichnungen über die ein- und ausgehenden Medien, die personenbezogene Daten enthalten, einschließlich der Art der Medien, des zugelassenen Absenders/Empfängers, des Datums und der Uhrzeit, der Anzahl der Medien und der darin enthaltenen Arten von solchen Daten. ☑ **Schutz vor Unterbrechungen.** No-Q nutzt eine Vielzahl von branchenüblichen Systemen, um den Verlust von Daten durch Stromausfall oder Leitungsstörungen zu verhindern.

BEREICH	DETAILS
	☑ **Entsorgung von Komponenten.** No-Q nutzt branchenübliche Prozesse, um personenbezogene Daten zu löschen, wenn sie nicht mehr benötigt werden.
Kommunikations- und Betriebsmanagement	☑ **Betriebsrichtlinie.** No-Q führt Sicherheitsunterlagen, in denen die Sicherheitsmaßnahmen sowie die entsprechenden Verfahren und Verantwortlichkeiten der Mitarbeiter beschrieben sind, die Zugang zu personenbezogene Daten haben. ☑ **Datenwiederherstellungsverfahren** No-Q erstellt kontinuierlich, mindestens jedoch einmal pro Woche (es sei denn, es haben im betreffenden Zeitraum keine Aktualisierungen stattgefunden) mehrere Kopien von personenbezogenen Daten, aus denen solche Daten wiederhergestellt werden können. No-Q bewahrt Kopien von personenbezogenen Daten an einem anderen Ort als dem auf, an dem sich die primären Computergeräte befinden, von denen die Personenbezogene Daten und Professional Services-Daten verarbeitet werden. No-Q verfügt über bestimmte Verfahren, die den Zugriff auf Kopien von personenbezogenen Daten regeln. No-Q prüft die Datenwiederherstellungsverfahren mindestens einmal alle sechs Monate. No-Q protokolliert Datenwiederherstellungsmaßnahmen. Dabei werden Informationen zur verantwortlichen Person, die Beschreibung der wiederhergestellten Daten sowie gegebenenfalls Angaben zu den Daten, die bei der Datenwiederherstellung manuell eingegeben werden mussten, aufgezeichnet. ☑ **Malware.** No-Q nimmt Anti-Malware-Kontrollen vor, um zu verhindern, dass bösartige Software unbefugten Zugriff auf Personenbezogene Daten und Professional Services-Daten erhält, einschließlich bösartiger Software aus öffentlichen Netzwerken. ☑ **Daten außerhalb von Landesgrenzen** No-Q verschlüsselt personenbezogene Daten, die über öffentliche Netzwerke übermittelt werden, oder ermöglicht dem Kunden eine solche Verschlüsselung. No-Q schränkt den Zugriff auf personenbezogene Daten ein, die die Einrichtungen von No-Q verlassen. ☑ **Ereignisprotokollierung.** No-Q protokolliert den Zugriff und die Nutzung von Informationssystemen, die personenbezogene Daten enthalten, indem die Zugangs-ID, die Uhrzeit, die erteilte oder verweigerte Berechtigung und die entsprechende Aktivität registriert werden, oder ermöglicht dem Kunden eine Protokollierung.
Zugriffskontrolle	☑ **Zugriffsrichtlinie.** No-Q führt eine Aufzeichnung der Sicherheitsberechtigungen von Einzelpersonen, die Zugang zu personenbezogene Daten haben. ☑ **Zugriffsberechtigung**

BEREICH	DETAILS
	No-Q führt und aktualisiert Aufzeichnungen zu den Mitarbeitern, die zum Zugriff auf No-Q-Systeme autorisiert sind, die personenbezogene Daten oder Professional Services-Daten enthalten. No-Q deaktiviert Anmeldedaten, die über einen bestimmten Zeitraum, der sechs Monate nicht überschreiten darf, nicht verwendet wurden. No-Q benennt diejenigen Mitarbeiter, die berechtigt sind, den autorisierten Zugriff auf Daten und Ressourcen zu gewähren, zu ändern oder zu widerrufen. Wenn mehrere Personen Zugriff auf die Systeme haben, in denen personenbezogene Daten oder Professional Services-Daten enthalten sind, stellt No-Q sicher, dass diese Personen über separate Kennungen/Anmeldedaten verfügen. ☑ **Geringste Rechte** Technischen Supportmitarbeitern ist der Zugriff auf personenbezogene Daten nur gestattet, wenn dies erforderlich ist. No-Q schränkt den Zugriff auf personenbezogene Daten und auf solche Personen ein, die diesen Zugriff benötigen, um ihre berufliche Tätigkeit auszuführen. ☑ **Integrität und Vertraulichkeit** No-Q weist Mitarbeiter an, Administrationssitzungen zu deaktivieren, wenn sie Einrichtungen, die sich unter der Kontrolle von No-Q befinden, verlassen oder wenn Computer anderweitig unbeaufsichtigt sind. No-Q speichert Kennwörter so, dass sie während des Gültigkeitszeitraums nicht erkennbar sind. ☑ **Authentifizierung** No-Q verwendet Verfahren nach Branchenstandard, um Benutzer zu identifizieren und zu authentifizieren, die versuchen, auf Informationssysteme zuzugreifen. Wenn die Authentifizierungsverfahren auf Kennwörtern beruhen, schreibt No-Q vor, dass die Kennwörter regelmäßig erneuert werden müssen. Wenn die Authentifizierungsverfahren auf Kennwörtern beruhen, schreibt No-Q vor, dass das Kennwort mindestens acht Zeichen umfassen muss. No-Q stellt sicher, dass deaktivierte oder abgelaufene Kennungen an keine andere Person vergeben werden. No-Q überwacht wiederholte Versuche, sich mit ungültigen Kennwörtern Zugriff auf Informationssysteme zu verschaffen, oder ermöglicht dem Kunden eine solche Überwachung. No-Q unterhält Verfahren nach Branchenstandard zur Deaktivierung von Kennwörtern, die manipuliert oder versehentlich offengelegt wurden. No-Q verwendet Verfahren nach Branchenstandard zum Schutz von Kennwörtern, einschließlich Verfahren, die die Vertraulichkeit und Integrität von Kennwörtern während der Zuweisung und Verteilung sowie während der Speicherung wahren sollen. ☑ **Netzwerkdesign.** No-Q führt Kontrollen durch, um zu verhindern, dass Personen Zugriffsrechte erhalten, die ihnen nicht zugewiesen wurden, um Zugang zu Personenbezogenen Daten oder Professional Services-Daten zu erhalten, auf die sie nicht zugreifen dürfen.

BEREICH	DETAILS
Handhabung eines Informations-sicherheits-vorfalls	☑ **Vorfallreaktionsablauf** No-Q führt Unterlagen über Sicherheitsverletzungen unter Angabe einer Beschreibung der Verletzung, des Zeitraums, der Konsequenzen der Verletzung, des Namens der Person, die den Zwischenfall gemeldet hat, und der Person, der der Zwischenfall gemeldet wurde, sowie des Verfahrens für die Wiederherstellung von Daten. Für jede Sicherheitsverletzung, bei der es sich um einen Sicherheitsvorfall handelt, erfolgt (wie im Abschnitt „Meldung von Sicherheitsvorfällen“ weiter oben beschrieben) unverzüglich und auf jeden Fall innerhalb von 72 Stunden eine Benachrichtigung seitens No-Q. No-Q untersucht Offenlegungen von Personenbezogene Daten einschließlich der Fragen, welche Daten offengelegt wurden, gegenüber wem und zu welchem Zeitpunkt, oder versetzt den Kunden dazu in die Lage. ☑ **Dienstüberwachung.** Das No-Q-Personal überprüft die Protokolle mindestens alle sechs Monate, um gegebenenfalls Abhilfemaßnahmen vorzuschlagen.
Geschäfts-fortführungs-management	☑ No-Q unterhält Notfall- und Alternativpläne für die Einrichtungen, in denen sich No-Q-Informationssysteme befinden, die personenbezogene Daten verarbeiten. ☑ Bei No-Q sind redundante Speicherung und ihre Verfahren zur Datenwiederherstellung so konzipiert, dass versucht wird, personenbezogene Daten in ihrem ursprünglichen oder zuletzt replizierten Zustand vor dem Zeitpunkt des Verlusts oder der Vernichtung zu rekonstruieren.