Nutzungsbedingungen Corsign

Zwischen

innFactory GmbH, Eduard-Rüber-Str. 7, 83022 Rosenheim

nachfolgend: **„innFactory“, „wir“, „uns“ oder „Anbieter“**

und

dem Nutzer

werden folgende Nutzungsbedingungen vereinbart:

1. Vertragsgegenstand

Gegenstand dieser Vereinbarung ist die Bereitstellung der Web-App „Corsign“. Die Web-App dient der Erstellung eines Corona-Test-Zertifikats sowie der betrieblichen Dokumentation des Nachweises des erfüllten „G-Status“ des Personals.

2. Leistungen des Anbieters

Die Web-App „Corsign“ besteht aus den beiden Komponenten „CovCheck“ und „Corsign-Zertifikatserstellung“.

2.1 CovCheck

Über die Funktion CovCheck können Mitarbeiterinnen und Mitarbeiter, Dienstleister und Gäste des Nutzers über die Web-App ihren Nachweis des G-Status (Genesen, Geimpft, Getestet) gegenüber dem Nutzer erbringen. Auf der Startseite erscheint eine Checkbox, über die die einzucheckende Person ihre Erlaubnis erteilen kann, den G-Status länger als 24 bzw. 48 Stunden abzuspeichern. Dadurch wird die Erfüllung des G-Status über die jeweilige Gültigkeitsdauer abgespeichert, wodurch eine ständige Wiederholung des Einchecken-Prozesses vermieden wird. Mit Klick auf „Weiter“ gelangt der Nutzer auf den nächsten Screen, wo er zunächst je nach Browser bzw. Browsereinstellungen der Anwendung Zugriff auf die Kamera geben kann. Dadurch hat der Nutzer die Möglichkeit, seinen Genesenen- , Impf- oder Test-Nachweis in Form des jeweiligen QR-Codes in die Kamera zu halten, wodurch die Daten direkt erfasst werden. Alternativ kann der Nutzer über den Button „Foto/Screenshot verwenden“ direkt auf den Speicher seines Endgerätes zugreifen. Dadurch öffnet sich eine separate Maske, wo er die entsprechende Datei des Genesenen-, Impf- oder Testzertifikats ansteuern und auswählen kann. Mit Auswahl der Datei erhält der Nutzer eine Übersicht, ob die Erfassung des QR-Codes erfolgreich war, und wenn ja, mit welchen Daten er gleich im Rahmen der betrieblichen 3-G-Testung einchecken kann. Mit Klick auf „Jetzt Einchecken“ erscheint eine Bestätigung, dass der Nutzer eingecheckt hat, mit Angabe der jeweiligen Gültigkeit des benutzten Zertifikats.

Hat sich der Nutzer eingecheckt, erscheinen die relevanten Daten in Corsign mit Angabe des Gültigkeitsdatums des erbrachten Nachweises. Die Liste aller eingecheckten Mitarbeiter kann über die Funktion „Excel-Export“ exportiert und den Behörden als Nachweis für die Einhaltung der 3-G-Regelung am Arbeitsplatz vorgelegt werden.

2.2 Corsign-Zertifikatserstellung

Mit der Funktion Corsign ermöglichen wir dem Nutzer die Erstellung eines Corona-Test-Zertifikats zum Nachweis der betrieblichen Testung. Nach Registrierung erhalten Nutzer per E-Mail den Zugang zum Portal. Über den Reiter „Test erfassen“ auf der linken Seite hat der Nutzer die Möglichkeit, zunächst die Personendaten der zu testenden Person zu erfassen. Dies kann einerseits über die manuelle Eingabe der geforderten Daten geschehen oder andererseits über das Einscannen eines sog. Testprofils, welches z.B. über die Corona-Warn-App oder über https://www.corsign.de/guest erstellt werden kann. Das erzeugte Testprofil wird mittels eines QR-Codes ausgegeben. Über den Button „Daten von QR-Code übernehmen“ wird die Kamera des Endgeräts angesteuert. Sofern der Nutzer den Zugriff der Kamera erlaubt, kann der QR-Code durch Halten vor die Endgerätekamera ausgelesen und erfasst werden, wodurch die geforderten Personendaten vorbelegt werden. Ist die zu testende Person bereits erfasst, das Testergebnis liegt allerdings noch nicht vor und die nächste zu testende Person wartet bereits, kann über den Button „Getestete Person speichern & Testergebnis später erfassen“ eine ID (z.B. ID-100) vergeben werden und die Person landet im Bereich „Aktuell getestete Personen“ im linken Bereich der Anwendung. Liegt das Testergebnis schließlich vor, kann in diesem Bereich die angelegte Person mit Klick auf den Bearbeitungsstift in der Zeile neben den Personendaten wieder ausgewählt werden und das Testergebnis erfasst sowie das Zertifikat erstellt werden. Um dieses Zertifikat zu erstellen werden zunächst im Bereich „Test erfassen“ die Testinformationen benötigt. Dazu gibt der Nutzer die geforderten Daten, das Testergebnis und die Gültigkeit sowie den Ort des Tests ein. Nachdem alle Daten erfolgreich erfasst wurden, wird ein entsprechendes Test-Zertifikat erstellt, das dem Nutzer an seine angegebene E-Mailadresse gesendet wird. Zusätzlich besteht die Möglichkeit, das Test-Zertifikat direkt vor Ort auszudrucken. Über Corsign angelegte Personen landen bei Freischaltung der Funktion CovCheck (siehe 2.1 dieser Nutzungsvereinbarung) direkt im Bereich „Dokumentierte Personen“ in der Liste der eingecheckten Personen.

Die Parteien sind sich einig, dass das über Corsign erstellte Corona-Test-Zertifikat dem Nachweis der betrieblichen Testung im Sinne des § 28b Abs. 2 IfSG i.V.m. § 2 Nr. 7 lit. a und b COVID-19-Schutzmaßnahmen-Ausnahmenverordnung dienen soll und die Verwendbarkeit der Corona-Test-Zertifikate außerhalb einer betrieblichen Testung nicht geschuldet ist. Sollte dies gewünscht sein, ist es im Verantwortungsbereich des Nutzers, hier ggf. die erforderlichen Voraussetzungen herzustellen, etwa durch Aufnahme als Leistungserbringer nach § 6 Abs. 1 der Coronavirus-Testverordnung.

3. Verfügbarkeit

5.1 Verfügbarkeit der Web-App: Der Anbieter stellt die Funktionalitäten der Web-App über das Internet zur Verfügung, so dass die Erreichbarkeit naturgemäß Schwankungen unterworfen ist, auf welche der Anbieter zum Teil keinen Einfluss hat. Eine bestimmte Verfügbarkeit kann daher weder garantiert noch gewährleistet werden. Der Anbieter behält sich außerdem vor, einzelne Funktionalitäten der Web-App zum Zwecke von Wartungsarbeiten vorübergehend vom Netz zu nehmen.

5.2 Die Web-App wird laufend weiterentwickelt und ggf. um neue Funktionen ergänzt, ohne dass hierauf ein Anspruch des Nutzers besteht. Der Anbieter gewährleistet dabei aber immer die unter Ziffer 2 genannten Funktionen.

4. Urheberrecht

3.1 Die Web-App ist urheberrechtlich geschützt. : Sämtliche Bestandteile der Web-App, d.h. insbesondere alle Texte, Logos, Marken, Grafiken, Kunstwerke, Sounds, Musik und Software sind durch Urheberrechte, Persönlichkeitsrechte, Gebrauchsmuster, Patente, Marken, Designrechte, Datenbankrechte, Geschäftsgeheimnisse und andere ähnliche Rechte geschützt. Alle Rechte am geistigen Eigentum, die an der Web App und ihren Inhalten bestehen, sind entweder unser Eigentum oder an uns lizenziert. Alle Rechte bleiben uns oder, falls von einem Dritten bereitgestellt, dem Dritten vorbehalten (und selbst wenn ein solcher Inhalt oder Dienst nicht ausdrücklich als rechtlich geschützt oder registriert gekennzeichnet ist, bedeutet dies nicht, dass wir oder Dritte in Bezug auf einen solchen Inhalt oder Dienst ganz oder teilweise auf geltende geistige Eigentumsrechte verzichten). Der Nutzer darf keine Inhalte, Materialien oder Teile davon ohne unsere ausdrückliche vorherige schriftliche Zustimmung reproduzieren, kopieren, posten, neu veröffentlichen, versenden, aufzeichnen, übertragen oder bearbeiten, noch darf er etwas tun oder versuchen, das gegen unsere Rechte am geistigem Eigentum oder ein an uns lizenziertes oder im Eigentum Dritter stehendes geistiges Eigentum verstößt. Gleiches gilt für Ideen und Konzepte, auf denen die Web App oder ihr Inhalt beruhen, auch wenn sie nicht durch das Recht des geistigen Eigentums geschützt sind.

3.2 Nutzungslizenz für die Benutzung unserer Web App und ihrer Inhalte: Damit die Benutzung für den Nutzer trotz unserer umfassenden Rechte beim Besuch unserer Web-App nicht eingeschränkt ist, erhält der Nutzer von uns ein einfaches, nicht ausschließliches Nutzungsrecht für die bestimmungsgemäße Benutzung der Web-App und ihrer Inhalte im Rahmen dieser Nutzungsbedingungen. Die Nutzungslizenz ist nicht übertragbar mit Ausnahme der Nutzung der Funktion „CovCheck“ (Ziffer 2.1) für Mitarbeiter, Dienstleister und Gäste zur Erfassung im Betrieb des Nutzers. Die Nutzungslizenz ist beschränkt auf die Nutzung in dem Betrieb des Nutzers. Die Nutzungslizenz ist räumlich beschränkt auf die Standorte des Nutzers.

5. Haftungsbeschränkung

Schadensersatzansprüche jeglicher Art gegen den Anbieter sind ausgeschlossen, wenn nicht Vorsatz oder grobe Fahrlässigkeit vorliegt. Für leichte Fahrlässigkeit haftet der Anbieter im Fall der Verletzung einer wesentlichen Vertragspflicht. Wesentliche Vertragspflichten sind solche, deren Erfüllung die ordnungsgemäße Durchführung des Vertrages überhaupt erst ermöglicht und auf deren Einhaltung der Vertragspartner regelmäßig vertrauen darf. In diesem Fall ist die Haftung auf den vorhersehbaren, vertragstypischen Schaden beschränkt. Aufwendungsersatzansprüche anstelle der Leistung sind ausgeschlossen, soweit nach den vorstehenden Regelungen eine Haftung ausgeschlossen wäre. Die vorstehenden Regelungen zum Ausschluss oder zur Begrenzung der Haftung des Anbieters wirken auch für die persönliche Haftung ihrer gesetzlichen Vertreter, Angestellten und sonstigen Erfüllungsgehilfen. Die vorstehenden Haftungsbeschränkten gelten nicht für die Haftung aufgrund der Verletzung von Leben, Körper oder Gesundheit oder im Fall der Haftung nach dem deutschen Produkthaftungsgesetz.

6. Vertragslaufzeit

Der Vertrag wird für die Dauer der beauftragten Vertragslaufzeit geschlossen. Das Recht zur außerordentlichen Kündigung aus wichtigem Grund bleibt unberührt. Die Kündigung bedarf der Textform (§ 126b BGB, z.B. per E-Mail.)

7. Datenschutz

Die Parteien sind sich darüber einig, dass der Nutzer datenschutzrechtlich Verantwortlicher ist im Sinne des Art. 4 Nr. 7 DSGVO für die personenbezogenen Daten der Mitarbeiter, Dienstleister und Gäste. Er ist daher verantwortlich für die Prüfung, ob und unter welchen Voraussetzungen er diese Daten verarbeiten darf und hat die datenschutzrechtlichen Informationspflichten nach Art. 13, 14 DSGVO gegenüber den Betroffenen zu erfüllen.

innFactory ist Auftragsarbeiter im Sinne des Art. 28 DSGVO. **Die Parteien schließen den in der Anhang 1 dargestellten Auftragsverarbeitungsvertrag ab. Dieser ist ausdrücklich Gegenstand dieser Nutzungsbedingungen und wird mit Abschluss dieser Nutzungsbedingungen Vertragsbestandteil zwischen den Parteien.**

8. Änderung der Nutzungsbedingungen

Der Anbieter behält sich eine Änderung der Nutzungsbedingungen jederzeit vor und wird den Nutzer im Falle einer Änderung rechtzeitig informieren. Die Information wird per E-Mail verschickt oder dem Nutzer per Pop-up Fenster bei seinem nächsten Besuch auf der Website nach Aktualisierung der Nutzungsbedingungen mitgeteilt. Geht innerhalb von 4 (vier) Wochen nach Zugang der Änderungsmitteilung kein Widerspruch des Nutzers beim Anbieter ein, so gelten die geänderten Nutzungsbedingungen als vom Nutzer angenommen.

Der Anbieter wird den Nutzer im Rahmen der Änderungsmitteilung noch einmal gesondert auf sein Widerspruchsrecht hinweisen. Der Widerspruch kann schriftlich oder per E-Mail an den Anbieter geschickt werden.

9. Schlussbestimmungen

Es gelten ergänzend die Allgemeinen Geschäftsbedingungen des Anbieters. Die Regelungen dieser Nutzungsbedingungen gehen den Allgemeinen Geschäftsbedingungen vor.

Dieser Vertrag unterliegt ausschließlich deutschem Recht unter Ausschluss des UN-Kaufrechts über den internationalen Warenkauf (CISG).

Ausschließlicher Gerichtsstand für alle Streitigkeiten aus und im Zusammenhang mit diesem Vertrag ist Traunstein, sofern der Kunde Kaufmann, eine juristische Person des öffentlichen Rechts oder ein öffentlich-rechtliches Sondervermögen ist.

Erfüllungsort ist der Sitz des Anbieters. Der Kunde kann nur mit rechtskräftig festgestellten oder unbestrittenen Forderungen aufrechnen.

Ist eine oder mehrere Regelungen dieser Nutzungsbedingungen unwirksam, so bleibt der Vertrag im Übrigen wirksam. Soweit die Bestimmungen unwirksam sind, tritt an die Stelle der unwirksamen Regelung eine Regelung, die dem Willen der Parteien am besten entspricht.

Anhang 1

Vereinbarung zur Auftragsverarbeitung

nach Art. 28 EU Datenschutzgrundverordnung („DS-GVO“)

zwischen

dem Kunden der Software „Corsign – CovCheck“

- nachstehend „**Auftraggeberin“** oder **„Kunde**“ genannt -

und

innFactory GmbH
Eduard-Rüber-Straße 7, 83022 Rosenheim, Deutschland

- nachstehend „**Auftragnehmerin**“ genannt -

1. Gegenstand und Dauer dieser Vereinbarung

(1) Gegenstand der Vereinbarung

Der Gegenstand des Auftrags ergibt sich aus dem zwischen den Parteien geschlossenen Vertrag über die Nutzung von Corsign. (2) Dauer der Vereinbarung

Die Laufzeit dieser Vereinbarung richtet sich nach der Laufzeit des unter Ziffer 1 Abs. 1 genannten Vertrages.

2. Konkretisierung des Inhalts der Vereinbarung

(1) Umfang, Art und Zweck der vorgesehenen Verarbeitung von Daten durch die Auftragnehmerin für die Auftraggeberin sind in **Anlage 1** beschrieben.

(2) Die Arten der verarbeiteten personenbezogenen Daten sind in **Anlage 1** aufgeführt.

(3) Kategorien betroffener Personen

Die Kategorien der durch die Verarbeitung personenbezogener Daten im Rahmen dieser Vereinbarung betroffenen Personen sind die in **Anlage 1** aufgeführten Kategorien betroffener Personen.

(4) Die Erbringung der vertraglich vereinbarten Datenverarbeitung findet entweder in einem Mitgliedsstaat der Europäischen Union oder in einem anderen Vertragsstaat des Abkommens über den Europäischen Wirtschaftsraum statt oder in einem Drittland, welches die Voraussetzungen des Art. 44 ff. DSGVO erfüllt. 3. Technisch-organisatorische Maßnahmen

(1) Die Auftragnehmerin hat die Umsetzung der im Vorfeld der Auftragsvergabe dargelegten und erforderlichen technischen und organisatorischen Maßnahmen vor Beginn der Verarbeitung hinsichtlich der konkreten Auftragsdurchführung dokumentiert und der Auftraggeberin zur

Prüfung übergeben (**Anlage 2**). Die dokumentierten Maßnahmen werden Grundlage dieser Vereinbarung. Soweit ein Audit durch die Auftraggeberin einen Anpassungsbedarf ergibt, ist dieser einvernehmlich umzusetzen.

(2) Die Auftragnehmerin hat die Sicherheitsmaßnahmen gem. Artt. 28 Abs. 3 lit. c, 32 DS-GVO insbesondere in Verbindung mit Art. 5 Abs. 1, Abs. 2 DS-GVO umzusetzen und muss die Einhaltung dieser Vorgaben nachweisen können. Bei den zu treffenden Maßnahmen handelt es sich um Maßnahmen der Datensicherheit, die ein dem Risiko angemessenes Schutzniveaus hinsichtlich der Vertraulichkeit, der Integrität, der Verfügbarkeit sowie der Belastbarkeit der Systeme gewährleisten. Dabei sind der Stand der Technik, die Implementierungskosten und die Art, der Umfang, der Kontext 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. Die Auftragnehmerin muss als Mindestanforderung die technischen und organisatorischen Maßnahmen umsetzen, die in **Anlage 2** dokumentiert sind.

(3) Technische und organisatorische Maßnahmen unterliegen dem technischen Fortschritt und der Weiterentwicklung. Insoweit ist es der Auftragnehmerin gestattet, alternative angemessene Maßnahmen umzusetzen, wenn diese zumindest das Schutzniveau der in **Anlage 2** festgelegten Maßnahmen aufrechterhalten. Wesentliche Änderungen sind von der Auftragnehmerin zu dokumentieren und der Auftraggeberin zur Prüfung vorzulegen.

(4) Die Auftragnehmerin wird ihre internen Prozesse sowie ihre technischen und organisatorischen Maßnahmen regelmäßig überwachen und kontrollieren um zu gewährleisten, dass die Verarbeitung im Einklang mit den Anforderungen des geltenden Datenschutzrechts erfolgt und die Rechte und Freiheiten der betroffenen Person geschützt werden.

4. Berichtigung, Sperrung und Löschung von Daten, Anfragen betroffener Personen

(1) Die Auftragnehmerin darf personenbezogene Daten, die im Auftrag der Auftraggeberin verarbeitet werden, nicht eigenmächtig, sondern nur nach Erhalt einer dokumentierten Weisung der Auftraggeberin berichtigen, löschen oder deren Verarbeitung einschränken. Soweit sich eine betroffene Person unmittelbar an die Auftragnehmerin wendet und die Berichtigung, Löschung oder Einschränkung der Verarbeitung verlangt oder andere Betroffenenrechte geltend macht, wird die Auftragnehmerin dieses Ersuchen unverzüglich an die Auftraggeberin weiterleiten.

(2) *Soweit vom Leistungsumfang umfasst,* sind Löschkonzept, Berichtigung und Auskunft in Übereinstimmung mit entsprechenden dokumentierten Weisungen der Auftraggeberin durch die Auftragnehmerin sicherzustellen.

(3) Die Auftragnehmerin wird Ansprüche einer betroffenen Person ohne vorherige schriftliche Zustimmung der Auftraggeberin nicht anerkennen. Gleichfalls wird die Auftragnehmerin ohne vorherige schriftliche Zustimmung der Auftraggeberin keinen Vergleich mit einer betroffenen Person abschließen.

5. Qualitätssicherung durch die Auftragnehmerin

(1) Die Auftragnehmerin hat zusätzlich zu den Regelungen dieser Vereinbarung die gesetzlichen Pflichten gem. Artt. 28 bis 33 DS-GVO einzuhalten.

(2) Die Auftragnehmerin wird insbesondere:

a) die Wahrung der Vertraulichkeit gem. Artt. 28 Abs. 3 S. 2 lit. b, 29, 32 Abs. 4 DS-GVO gewährleisten. Die Auftragnehmerin wird bei der Durchführung der Arbeiten nur Beschäftigte einsetzen, die auf die Vertraulichkeit verpflichtet wurden oder die einer angemessenen gesetzlichen Verschwiegenheitspflicht unterliegen und die zuvor mit den für sie relevanten Bestimmungen zum Datenschutz vertraut gemacht wurden. Die Auftragnehmerin und jede der Auftragnehmerin unterstellte Person, die Zugang zu personenbezogenen Daten hat, dürfen diese Daten ausschließlich entsprechend der Weisungen der Auftraggeberin verarbeiten einschließlich der in dieser Vereinbarung eingeräumten Befugnisse, es sei denn, dass sie gesetzlich zur Verarbeitung verpflichtet sind. Die Vertraulichkeits-/Verschwiegenheitsverpflichtung besteht auch nach Beendigung der Vereinbarung fort. Die Auftragnehmerin schult ihre Mitarbeiter regelmäßig zum Datenschutz und wird sie in angemessenem Umfang über ihre Pflichten nach diesem Auftrag informieren.

b) schriftlich einen qualifizierten und kompetenten Datenschutzbeauftragten bestellen, soweit dies gesetzlich erforderlich ist (Art. 38 und 39 DS-GVO). Die Auftragnehmerin wird der Auftraggeberin die Kontaktdaten ihres Datenschutzbeauftragten sowie entsprechende Änderungen umgehend mitteilen.

c) regelmäßig die Umsetzung ihrer Verpflichtungen nach dieser Vereinbarung überprüfen, insbesondere die Einhaltung und ggf. notwendige Anpassung von Regelungen und Maßnahmen zur Durchführung der Vereinbarung.

6. Unterauftragsverhältnisse

(1) Als Unterauftragsverhältnisse im Sinne dieser Regelung sind solche Dienstleistungen von Unterauftragnehmern zu verstehen, die sich unmittelbar auf die Erbringung der Hauptleistung beziehen und im Auftrag für die Auftraggeberin verarbeite Daten betreffen. Nicht hierzu gehören Nebenleistungen wie z.B. Telekommunikationsleistungen, Post-/ Transportdienstleistungen und vergleichbare Leistungen. Die Auftragnehmerin ist jedoch verpflichtet, zur Gewährleistung des Datenschutzes und der Datensicherheit der im Auftrag von der Auftraggeberin verarbeiteten personenbezogenen Daten auch bei ausgelagerten Nebenleistungen angemessene und gesetzeskonforme vertragliche Vereinbarungen sowie angemessene Kontrollmaßnahmen zu ergreifen.

(2) Die Auftraggeberin stimmt zu, dass der Auftragnehmer Unterauftragnehmer hinzuzieht. Die derzeit eingesetzten Unterauftragnehmer werden in der **Anlage 3** dargestellt. Vor Hinzuziehung weiterer oder Ersetzung der bestehenden Unterauftragnehmer informiert die Auftragnehmerin die Auftraggeberin mindestens in Textform (z.B. per E-Mail). Die Auftraggeberin kann der Änderung – innerhalb einer Frist von 14 Tagen ab Zugang der Information – aus einem wichtigen datenschutzrechtlichen Grund – gegenüber der Auftragnehmerin widersprechen. Erfolgt kein Widerspruch innerhalb der Frist, gilt die Zustimmung zur Änderung als gegeben. Liegt ein wichtiger datenschutzrechtlicher Grund vor, und sofern eine einvernehmliche Lösungsfindung zwischen den Parteien nicht möglich ist, wird der Auftraggeberin und der Auftragnehmerin ein Sonderkündigungsrecht des unter Ziffer 1 Abs. 1 genannten Vertrages und dieses Vertrages eingeräumt.

(5) Erbringt der Unterauftragnehmer die vereinbarte Leistung außerhalb der EU/des EWR, stellt die Auftragnehmerin die datenschutzrechtliche Zulässigkeit durch entsprechende Maßnahmen sicher. Gleiches gilt, wenn Dienstleister im Sinne von Abs. 1 Satz 2 eingesetzt werden sollen.

(7) Die Auftragnehmerin hat die Einhaltung aller vertraglichen und gesetzlichen Datenschutzpflichten durch den Unterauftragnehmer angemessen zu kontrollieren und durchzusetzen, sowie die Ergebnisse dieser Kontrollen und etwaige Durchsetzungsmaßnahmen zu dokumentieren und der Auftraggeberin diese Dokumentation auf Nachfrage zur Verfügung zu stellen.

7. Kontrollrechte der Auftraggeberin

(1) Die Auftraggeberin hat das Recht, im Benehmen mit der Auftragnehmerin Überprüfungen durchzuführen oder durch im Einzelfall zu benennende Prüfer durchführen zu lassen. Die Auftraggeberin hat das Recht, sich durch Stichprobenkontrollen, die in der Regel rechtzeitig anzumelden sind, von der Einhaltung dieses Auftrags durch die Auftragnehmerin in deren Geschäftsbetrieb zu überzeugen. Die Auftragnehmerin ist verpflichtet, der Auftraggeberin oder den von der Auftraggeberin benannten Prüfern für diese Überprüfungen Zutritt zu ihrem Geschäftsbetrieb zu gewähren.

(2) Die Auftragnehmerin stellt sicher, dass die Auftraggeberin sich von der Einhaltung der Pflichten der Auftragnehmerin nach Art. 28 DS-GVO überzeugen kann, insbesondere bezüglich der von der Auftragnehmerin umzusetzenden angemessenen technischen und organisatorischen Maßnahmen zum Schutz personenbezogener Daten entsprechend des anwendbaren Datenschutzrechts und dieser Vereinbarung. Die Auftragnehmerin verpflichtet sich, Überprüfungen durch die Auftraggeberin oder von der Auftraggeberin benannte Prüfer vollumfänglich zu unterstützen, insbesondere kompetente Ansprechpartner sowie alle einschlägigen Informationen und Nachweise auf Anforderung bereit zu stellen.

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

☐ die Einhaltung genehmigter Verhaltensregeln gem. Art. 40 DS-GVO;

☐ die Zertifizierung nach einem genehmigten Zertifizierungsverfahren gem. Art. 42 DS-GVO;

☒ aktuelle Testate, Zertifizierungen, Berichte oder Berichtsauszüge unabhängiger Instanzen (z.B. Wirtschaftsprüfer, Revision, Datenschutzbeauftragter);

☒ eine geeignete Zertifizierung durch ein IT-Sicherheits- oder Datenschutzaudit (z.B. ISO 27K, ISAE 3402 Type II, SAS 70 Type II, SSAE16 Type II).

Das Recht der Auftraggeberin zur Durchführung von Überprüfungen und Kontrollen bleibt unberührt.

(4) Die Auftragnehmerin ist nicht berechtigt, im Zusammenhang mit der Durchführung von Überprüfungen oder Kontrollen eine Vergütung zu verlangen. Sollten durch Kontrollen der Auftraggeberin bei Rechenzentren von Unterauftragnehmern der Auftragnehmerin Kosten in Rechnung gestellt werden, so wird die Auftraggeberin geeignet nachgewiesene Kosten erstatten.

(5) Wenn durch eine Überprüfung oder Kontrolle ein Verstoß der Auftragnehmerin gegen vertragliche Pflichten nach dieser Vereinbarung oder gegen einschlägige Datenschutzvorschriften festgestellt wird, ist die Auftragnehmerin verpflichtet Kosten zu tragen, die die Auftraggeberin durch die Durchführung der Überprüfung oder Kontrolle entstanden sind.

8. Melde- und Mitwirkungspflichten der Auftragnehmerin

Die Auftragnehmerin hat der Auftraggeberin bei der Erfüllung ihrer Pflichten betreffend Anfragen und Ansprüche betroffener Personen gem. Kapitel III der DS-GVO sowie bei der Einhaltung der in den Artikeln 32 bis 36 der DS-GVO genannten Pflichten zur Sicherheit personenbezogener Daten, bei Meldepflichten bei Datenpannen, Datenschutz-Folgeabschätzungen und vorherigen Konsultationen mit Aufsichtsbehörden zu unterstützen. Hierzu gehören u.a.:

(1) die Verpflichtung, Verletzungen des Schutzes personenbezogener Daten unverzüglich an die Auftraggeberin zu melden und die Auftraggeberin bei der Erfüllung entsprechender Meldepflichten gegenüber einschlägigen Aufsichtsbehörden und Einzelpersonen zu unterstützen. Dies gilt auch im Fall von Anhaltspunkten für eine mögliche oder tatsächliche unrechtmäßige Übermittlung oder sonstige unrechtmäßige Offenlegung personenbezogener Daten gegenüber Dritten, im Fall erheblicher Leistungsunterbrechungen oder erheblicher Betriebsstörungen, in Verdachtsfällen sonstiger Verletzungen einschlägiger Datenschutzvorschriften sowie sonstiger Unregelmäßigkeiten im Zusammenhang mit der Verarbeitung personenbezogener Daten im Auftrag der Auftraggeberin. Im Fall einer Verletzung des Schutzes personenbezogener Daten hat die Auftragnehmerin in enger Abstimmung mit der Auftraggeberin angemessene Maßnahmen zum Schutz der personenbezogenen Daten und zur Begrenzung möglicher nachteiliger Auswirkungen auf die betroffenen Personen zu ergreifen.

(2) die Verpflichtung, die Auftraggeberin bei der Beantwortung von Auskunftsansprüchen betroffener Personen zu unterstützen und der Auftraggeberin alle erheblichen Informationen unverzüglich zur Verfügung zu stellen;

(3) die Unterstützung der Auftraggeberin nach Aufforderung bei Datenschutz-Folgenabschätzungen;

(4) die Unterstützung der Auftraggeberin nach Aufforderung bei Konsultationen der Aufsichtsbehörde;

(5) die unverzügliche Information der Auftraggeberin über Überprüfungen, Kontrollhandlungen und Maßnahmen der einschlägigen Aufsichtsbehörden, soweit sie im Zusammenhang mit personenbezogenen Daten stehen, die im Auftrag der Auftraggeberin verarbeitet werden. Dies gilt auch für behördliche Untersuchungen bei der Auftragnehmerin im Zusammenhang mit Ordnungswidrigkeiten- oder Strafverfahren;

(6) die Unterstützung der Auftraggeberin, soweit die Auftraggeberin ihrerseits von einer Überprüfung oder sonstigen Überwachungsmaßnahme einer Aufsichtsbehörde, von einem Ordnungswidrigkeits- oder Strafverfahren, von einem Haftungsanspruch einer betroffenen Person oder eines Dritten oder einem anderen Anspruch im Zusammenhang

mit der Verarbeitung personenbezogener Daten durch die Auftragnehmerin im Auftrag der Auftraggeberin ausgesetzt ist.

(7) Für Unterstützungsleistungen, die nicht auf ein Fehlverhalten der Auftragnehmerin zurückzuführen sind, kann die Auftragnehmerin eine angemessene Vergütung beanspruchen.

9. Weisungsbefugnisse der Auftraggeberin

(1) Die Auftragnehmerin wird die von der Auftraggeberin oder von Dritten im Auftrag der Auftraggeberin überlassenen Daten ausschließlich für die Auftraggeberin und nur im Rahmen dieser Vereinbarung sowie gemäß den dokumentierten Weisungen der Auftraggeberin verarbeiten, soweit sich nicht aus zwingenden gesetzlichen Vorgaben oder Anordnungen der zuständigen Aufsichtsbehörde etwas anderes ergibt. Jegliche anderweitige Nutzung dieser Daten, insbesondere für eigene Geschäftszwecke der Auftragnehmerin oder Dritter, ist der Auftragnehmerin untersagt.

(2) Die Weisungen werden anfänglich durch diese Vereinbarung festgelegt und können von der Auftraggeberin danach schriftlich oder elektronisch (Textform) geändert, ergänzt oder ersetzt werden (Einzelweisung). Weisungen, die im Vertrag nicht vorgesehen sind, werden als Antrag auf Leistungsänderung behandelt.

(3) Die Auftraggeberin behält sich im Rahmen dieser Vereinbarung ein umfassendes Weisungsrecht in Bezug auf Art, Umfang und Mittel der Datenverarbeitung vor, das die Auftraggeberin durch Einzelweisungen konkretisiert kann. Änderungen des Verarbeitungsgegenstandes und Verfahrensänderungen sind gemeinsam abzustimmen und zu dokumentieren. Die Auftragnehmerin darf nur nach vorheriger schriftlicher Zustimmung durch die Auftraggeberin Informationen an Dritte oder betroffene Personen weitergeben.

(4) Wenn die Auftragnehmerin der Meinung ist, eine Weisung der Auftraggeberin verstoße gegen Datenschutzvorschriften, hat sie die Auftraggeberin unverzüglich zu informieren. Die Auftragnehmerin ist berechtigt, die Durchführung der entsprechenden Weisung solange auszusetzen, bis sie durch die Auftraggeberin bestätigt oder geändert wird.

(5) Die weisungsberechtigten und weisungsempfangsberechtigten Personen sind in **Anlage 4** zu dieser Vereinbarung festgelegt, soweit im Hauptvertrag keine abweichende Vereinbarung getroffen wurde.

10. Löschung von Daten und Rückgabe von Datenträgern

(1) Die Auftragnehmerin wird die vertragsgegenständlichen Daten löschen, wenn die Auftraggeberin dies anweist. Ist eine datenschutzkonforme Löschung oder eine entsprechende Einschränkung der Datenverarbeitung nicht möglich, übernimmt die Auftragnehmerin die datenschutzkonforme Vernichtung von Datenträgern und sonstigen Materialien auf Grundlage einer Einzelweisung durch die Auftraggeberin oder gibt diese Datenträger an die Auftraggeberin zurück, soweit dazu keine Regelung im Hauptvertrag besteht.

(2) Kopien oder Duplikate der im Auftrag der Auftraggeberin verarbeiteten Daten dürfen ohne vorherige schriftliche Zustimmung der Auftraggeberin weder erstellt noch gegenüber Dritten offengelegt werden. Dies gilt nicht für Sicherheitskopien, soweit sie zur Gewährleistung einer angemessenen Sicherheit der Datenverarbeitung erforderlich sind.

(3) Nach Abschluss der vertraglich vereinbarten Arbeiten oder früher nach Aufforderung durch die Auftraggeberin - spätestens aber mit Beendigung des Hauptvertrags- hat die Auftragnehmerin sämtliche in ihren Besitz gelangte Dokumentationen, Ergebnisse der Verarbeitung personenbezogener Daten sowie Bestände personenbezogener Daten, die im Zusammenhang mit dem Auftragsverhältnis stehen, an die Auftraggeberin auszuhändigen oder nach vorheriger Zustimmung der Auftraggeberin datenschutzkonform zu vernichten. Gleiches gilt für Test- und Ausschussmaterial. Die Auftragnehmerin hat die Löschung zu protokollieren oder zu dokumentieren und wird der Auftraggeberin das Protokoll oder die Dokumentation zur Verfügung stellen.

(4) Dokumentationen, die dem Nachweis der auftrags- und ordnungsgemäßen Datenverarbeitung dienen, sind von der Auftragnehmerin entsprechend der jeweiligen Aufbewahrungsfristen über das Vertragsende hinaus aufzubewahren. Die Auftragnehmerin kann sie zu ihrer Entlastung bei Vertragsende an die Auftraggeberin übergeben.

Nach Artikel 29 DSGVO ist dieser Vertrag schriftlich abzufassen, was auch in einem elektronisch Format erfolgen kann und somit rechtskräftig erfolgt.

Anlage 1
Konkretisierung des Auftragsinhalts

Aufgaben

Bereitstellung einer Softwarelösung (SaaS) für das Erstellen von Corona-Testzertifikaten sowie die „G-Status“-Erfassung und deren Dokumentation..

Umfang, Art und Zweck der vorgesehenen Verarbeitung von Daten

- Erfassung von betrieblichen Corona-Testungen, Erstellung von Testzertifikaten bei negativer Testung, Weiterleitung positiver Fälle an das Gesundheitsamt sowie Übersendung des Testergebnisses an die getestete Person.
- Einchecken des Personals und der Unternehmensgäste durch Überprüfung des G-Status (Genesen, Getestet, Geimpft) mittels Auslesen des QR-Codes aus Impf-, Genesenen- oder Testzertifikat
- Dokumentation der eingecheckten Personen mit Angabe der Dauer der Gültigkeit des Zertifikats sowie Export-Funktion der Liste der eingecheckten Personen

Art und Kategorien der Daten und der betroffenen Personen

Gegenstand der Verarbeitung personenbezogener Daten sind folgende Arten/ Kategorien von Daten und betroffenen Personen:

Zutreffendes bitte ankreuzen	**Art der Daten**	**Kategorien der betroffenen Personen** **Bitte angeben:** **z. B. Kunden, Interessenten, Abonnenten, Mitarbeiter, Freelancer, Berater, Lieferanten, Handelsvertreter, Ansprechpartner, Website-Besucher, Anwender von IT-Systemen, [Sonstige]**
☒	Personenstammdaten	Mitarbeiter und vor Ort beschäftigte Dienstleister, Gäste
☒	Kommunikationsdaten (z.B. Telefon, E-Mail und Adressdaten)	Mitarbeiter und vor Ort beschäftigte Dienstleister, Gäste
☒	Testinformationen (Name des Tests, Hersteller, Art des Tests, Ort des Tests)	Mitarbeiter und vor Ort beschäftigte Dienstleister, Gäste
☐	Vertragsstammdaten (Vertragsbeziehung, Produkt- bzw. Vertragsinteresse)	------
☐	Kundenhistorie	------
☐	Vertragsabrechnungs- und Zahlungsdaten	------
☐	Auskunftsangaben (von Dritten, z.B. Auskunfteien, oder aus öffentlichen Verzeichnissen)	------
☐	Marketing-Daten	------
☒	Nutzungsdaten des Web-Portals (soweit automatisch erfasst wie z.B. Browserdaten)	Mitarbeiter und vor Ort beschäftigte Dienstleister, Gäste
☒	Protokolldaten von IT-Systemen (soweit automatisch erfasst)	Mitarbeiter und vor Ort beschäftigte Dienstleister, Gäste

☒	G-Status erfüllt Ja/Nein	Mitarbeiter und vor Ort beschäftigte Dienstleister, Gäste
☒	Dauer der Gültigkeit des G-Status (Nur nach expliziter Zustimmung des Mitarbeiters/ der Mitarbeiterin)	Mitarbeiter und vor Ort beschäftigte Dienstleister, Gäste

Anlage 2
Technische und organisatorische Maßnahmen nach Art. 32 DS-GVO

1. Vertraulichkeit (Art. 32 Abs. 1 lit. b DS-GVO)

- **Zutrittskontrolle**

Die Auftragnehmerin hat Maßnahmen zur Zutrittskontrolle umzusetzen, damit Unbefugte keinen Zutritt zu Datenverarbeitungsanlagen erlangen. Zu diesen Maßnahmen zählen z.B. Magnet- oder Chipkarten, Schlüssel, elektrische Türöffner, Werkschutz bzw. Pförtner, Alarmanlagen, Videoanlagen.

Die von der Auftragnehmerin ergriffenen Maßnahmen umfassen insbesondere:

☐ Empfang / Pförtner / Werkschutz

☐ Führung von Anwesenheitsaufzeichnungen

☐ Richtlinie hinsichtlich Begleitung von Gästen im Gebäude

☐ Foto-IDs / Mitarbeiterausweise

☐ Ausweisleser, Magnetkarte, Chipkarte

☐ Vereinzelungsschleusen

☐ Schlüssel / Schlüsselvergabe

☐ 24/7 Überwachungseinrichtung (z.B. Videoüberwachung)

☐ Alarmanlage

☐ verschlossene Türen zu Server-/IT-Räumen

☐ biometrische Maßnahmen

☒ Sonstiges, bitte erläutern:

- **Hosting der Daten in einem ISO/IEC 27001 zertifizierten Rechenzentrum**

- **Zugangskontrolle**

Die Auftragnehmerin hat Maßnahmen zur Zugangskontrolle umzusetzen, damit keine unbefugte Systembenutzung erfolgt, z.B. (sichere) Kennwörter, automatische Sperrmechanismen, Zwei-Faktor-Authentifizierung, Verschlüsselung von Datenträgern.

Die von der Auftragnehmerin ergriffenen Maßnahmen umfassen insbesondere:

☒ Berechtigungskonzept

☐ Protokollierung (Benutzung/Missbrauchsversuchen),

☐ Firewall

☐ Kennwortschutz im Einklang mit IT Security Regeln (Mindestlänge, Sonderzeichen, Gültigkeitsdauer, Rücksetzungsverfahren, Passworthistorie)

☐ Account-Sperrung bei mehrmaliger Eingabe eines falschen Passworts

☐ automatische Bildschirmsperrung bei Inaktivität

☐ Session Timeouts

☐ Chipkarte / PKI login

☐ biometrische Maßnahmen

☒ Sonstiges, bitte erläutern:

- **Hosting der Daten in einem ISO/IEC 27001 zertifizierten Rechenzentrum**

- **Zugriffskontrolle**

Die Auftragnehmerin hat Maßnahmen zur Zugriffskontrolle umzusetzen, damit unbefugtes Lesen, Kopieren, Verändern oder Entfernen innerhalb des Systems ausgeschlossen ist. Zu diesen Maßnahmen zählen z.B. Berechtigungskonzepte und bedarfsgerechte Zugriffsrechte, Protokollierung von Zugriffen.

Die von der Auftragnehmerin ergriffenen Maßnahmen umfassen insbesondere:

☒ differenziertes Rollen- und Berechtigungskonzept mit unterschiedlichen Rollen und Zugriffsgrenzen

☒ Zugriff wird auf “need to know” Basis gewährt

☐ eindeutige Identifikation jeder zugriffsberechtigten Person, z.B. durch PKI Login oder Ähnliches

☐ regelmäßige Kontrolle der Berechtigungen auf Gültigkeit (bitte Kontrollintervalle unter „Sonstiges“ angeben)

☒ sofortige Sperrung von Berechtigungen bei Funktionswechsel oder Ausscheiden eines Mitarbeiters

☒ Verschlüsselung

☐ Sonstiges, bitte erläutern:

- **Hosting der Daten in einem ISO/IEC 27001 zertifizierten Rechenzentrum**

- **Trennungskontrolle**

Die Auftragnehmerin hat Maßnahmen zur Trennungskontrolle umzusetzen, damit Daten, die zu unterschiedlichen Zwecken erhoben wurden, getrennt verarbeitet werden. Zu diesen Maßnahmen zählen z.B. Mandantenfähigkeit oder Sandboxing.

Die von der Auftragnehmerin ergriffenen Maßnahmen umfassen insbesondere:

☒ Trennung von Entwicklung-, Test- und Produktivsystem

☒ physische oder logische Mandantentrennung (interne Mandantenfähigkeit)

☐ Verarbeitung der Daten des Auftraggebers und der Daten anderer Kunden durch unterschiedliche Mitarbeiter

☐ Sandboxing

☐ Sonstiges, bitte erläutern:

- **Hosting der Daten in einem ISO/IEC 27001 zertifizierten Rechenzentrum**

- **Pseudonymisierung (Art. 32 Abs. 1 lit. a DS-GVO; Art. 25 Abs. 1 DS-GVO)**

Die Auftragnehmerin hat Maßnahmen zur Pseudonymisierung umzusetzen, damit die Daten ohne Hinzuziehung zusätzlicher Informationen nicht mehr einer spezifischen betroffenen Person zugeordnet werden können. Dies gilt dann, wenn diese zusätzlichen Informationen gesondert aufbewahrt werden und entsprechenden technischen und organisatorischen Maßnahmen unterliegen.

Die von der Auftragnehmerin ergriffenen Maßnahmen umfassen insbesondere:

Pseudonymisierung durch Verschlüsselung

2. Integrität (Art. 32 Abs. 1 lit. b DS-GVO)

- **Weitergabekontrolle**

Die Auftragnehmerin hat Maßnahmen zur Weitergabekontrolle umzusetzen, damit das unbefugte Lesen, Kopieren, Verändern oder Entfernen bei elektronischer Übertragung oder Transport ausgeschlossen ist. Zu diesen Maßnahmen zählen z.B. Verschlüsselung, Virtual Private Networks (VPN), elektronische Signatur.

Die von der Auftragnehmerin ergriffenen Maßnahmen umfassen insbesondere:

☒ Verschlüsselung aller Datenmedien

☐ Verschlüsselung von internen Emails

☐ Verschlüsselung von externen Emails

☐ Elektronische Signatur

☒ Verwendung sicherer Verbindungen für Datenübermittlungen (z.B. Tunnelverbindung – VPN)

☐ Lagerung von Datenträgern in Sicherheitsbereichen

☐ Einsatz sicherer Transportdienstleister für den Transport sensitiver Dokumente

☐ Protokollierung des Abrufs und Versands

☐ Sonstiges, bitte erläutern:

- **Hosting der Daten in einem ISO/IEC 27001 zertifizierten Rechenzentrum**

- **Eingabekontrolle**

Die Auftragnehmerin hat Maßnahmen zur Eingabekontrolle umzusetzen, damit festgestellt werden kann, ob und von wem personenbezogene Daten in Datenverarbeitungssysteme eingegeben, verändert oder entfernt worden sind. Zu diesen Maßnahmen zählen z.B. Protokollierung oder Dokumentenmanagement.

Die von der Auftragnehmerin ergriffenen Maßnahmen umfassen insbesondere:

☒ Logfiles / Protokollierungssysteme (Eingabe, Änderung, Löschung)

☐ Dokumentenmanagement

☐ Sonstiges, bitte erläutern:

3. Verfügbarkeit und Belastbarkeit (Art. 32 Abs. 1 lit. b DS-GVO)

- **Verfügbarkeitskontrolle**

Die Auftragnehmerin hat Maßnahmen zur Verfügbarkeitskontrolle umzusetzen, damit Daten gegen zufällige oder mutwillige Zerstörung bzw. Verlust geschützt sind. Zu diesen Maßnahmen zählen z.B. Backup-Strategie (on-line/offline; on-site/off-site), unterbrechungsfreie Stromversorgung (USV), Virenschutz, Firewall, Meldewege und Notfallpläne.

Die von der Auftragnehmerin ergriffenen Maßnahmen umfassen insbesondere:

☐ regelmäßige / tägliche Backups

☐ Festplattenspiegelung

☐ katastrophensichere Aufbewahrung der Datenträger

☐ Patch Management

☐ Viren- und Malwareschutz nach aktuellem Stand der Technik

☐ Firewall und Intrusionsschutz

☐ unterbrechungsfreie Stromversorgung

☐ regelmäßige Sicherheitsprüfungen mit simulierten Einbruchsversuchen in die Systeme

☐ Sonstiges, bitte erläutern:

- **Hosting der Daten in einem ISO/IEC 27001 zertifizierten Rechenzentrum**

- **Rasche Wiederherstellbarkeit (Art. 32 Abs. 1 lit. c DS-GVO);**

Die Auftragnehmerin hat Maßnahmen zur raschen Wiederherstellbarkeit umzusetzen, damit die Verfügbarkeit der personenbezogenen Daten und der Zugang zu ihnen bei einem physischen oder technischen Zwischenfall rasch wiederhergestellt werden können.

Die von der Auftragnehmerin ergriffenen Maßnahmen umfassen insbesondere:

☐ Ausweich-Rechenzentrum

☐ Notfallplan

☐ Sonstiges, bitte erläutern:

- **Hosting der Daten in einem ISO/IEC 27001 zertifizierten Rechenzentrum**

4. Verfahren zur regelmäßigen Überprüfung, Bewertung und Evaluierung (Art. 32 Abs. 1 lit. d DS-GVO; Art. 25 Abs. 1 DS-GVO) und zur Auftragskontrolle

- **Regelmäßige Überprüfung, Bewertung und Evaluierung**

Die Auftragnehmerin hat Maßnahmen zur regelmäßigen Überprüfung, Bewertung und Evaluierung der Wirksamkeit der technischen und organisatorischen Maßnahmen zur Gewährleistung der Sicherheit der Verarbeitung umzusetzen. Zu diesen Maßnahmen zählen z.B. Datenschutz-Management, Incident-Response-Management, datenschutzfreundliche Voreinstellungen (Art. 25 Abs. 2 DS-GVO).

Die von der Auftragnehmerin ergriffenen Maßnahmen umfassen insbesondere:

☒ Datenschutzmanagement

X☐ Incident Response Management

X☐ Privacy by design

X☐ Privacy by default

☐ Sonstiges, bitte erläutern:

- **Auftragskontrolle**

Die Auftragnehmerin hat außerdem Maßnahmen zur Auftragskontrolle umzusetzen, damit eine Auftragsverarbeitung im Sinne von Art. 28 DS-GVO ohne entsprechende Weisung des Auftraggebers ausgeschlossen ist. Zu diesen Maßnahmen zählen z.B. eindeutige Vertragsgestaltung, formalisiertes Auftragsmanagement, strenge Auswahl des Dienstleisters, Vorabüberzeugungspflicht, Nachkontrollen.

Die von der Auftragnehmerin ergriffenen Maßnahmen umfassen insbesondere:

☒ Klare und eindeutige Vertragsgestaltung

☐ Geregelter und formalisierter Einkaufsprozess

☐ Prozess zur Auswahl von Dienstleistern

☒ Dienstleisterprüfung vor Auftragsvergabe

☐ Nachkontrollen bei Dienstleistern

☒ regelmäßige Kontrolle der Einhaltung von Datenschutzbestimmungen

☒ regelmäßige Datenschutzinformation für Mitarbeiter des Auftragnehmers

☐ Vorlage geeigneter Prüfdokumente / Zertifikate / Auditberichte / Testate

☒ Abschluss eines gesetzeskonformen Auftragsdatenverarbeitungsvertrages (ADV)

☐ angemessene Audit- und Kontrollrechte gegenüber Unterauftragnehmern

☐ Sonstiges, bitte erläutern:

Anlage 3

Liste autorisierter Unterauftragnehmer

Auflistung aller im Zeitpunkt des Vertragsschlusses eingesetzter Unterauftragnehmer, mit voller Anschrift sowie unter Darstellung der erbrachten Leistungen:

	Unternehmensbezeichnung Unterauftragnehmer mit Unternehmenssitz	**Funktion (Umfang der Beauftragung durch die Auftragnehmerin**	**Ort der Datenverarbeitung**
1.	Google Ireland Limited Gordon House, Barrow Street Dublin 4, Irland	Hosting der Webseite und der Daten	Frankfurt
2.	Mailjet SAS (Global HQ) Büro- und Postadresse: Paris: 13-13 bis, rue de l'Aubrac, 75012 Paris, France	Mailservice (Versand des Testergebnisses)	Frankfurt (Deutschland) und Saint-Ghislain (Belgien)
3.			

Anlage 4
Weisungsberechtigte und weisungsempfangsberechtigte Personen

Bitte ausfüllen, soweit nicht bereits im Hauptvertrag geregelt bzw. soweit für datenschutzrechtliche Weisungen etwas vom Hauptvertrag Abweichendes gelten soll:

Weisungsberechtigte Person(en) beim Kunden	
Name, Vorname	
Funktion / Abteilung	
Email	
Telefon	
Mobiltelefon	
Name, Vorname	
Funktion / Abteilung	
Email	
Telefon	
Mobiltelefon	

Weisungsempfangsberechtigte Person(en) der Auftragnehmerin	
Name, Vorname	Tobias Jonas
Funktion / Abteilung	CEO
Email	t.jonas@innfactory.de
Telefon	+49 (0)8031 58193280
Mobiltelefon	
Name, Vorname	
Funktion / Abteilung	
Email	
Telefon	
Mobiltelefon	