Vereinbarung zur Auftragsverarbeitung gem. Art. 28 Datenschutz-Grundverordnung (DSGVO)

zwischen

_____

Name des datenschutzrechtlich Verantwortlichen (Auftraggeber)

_____

Straße Verantwortlicher

_____

PLZ, Ort Verantwortlicher

- nachfolgend **„Auftraggeber“** genannt -

und

free2pass GmbH
Hamburger Allee 2-4
30161 Hannover

- Als Auftragsverarbeiter, nachfolgend **„Auftragnehmer“** genannt -

- Auftraggeber und Auftragnehmer nachfolgend je einzeln „**Partei**“ und zusammen „**Parteien**“ genannt -

Präambel

Diese Vereinbarung zur Auftragsverarbeitung i. S. d. Art. 28 Abs. 3 DSGVO (nachfolgend „Vereinbarung“ genannt) konkretisiert die Verpflichtungen der Parteien zum Datenschutz, die sich bei der Nutzung von free2pass ergeben. Sie findet Anwendung auf alle Tätigkeiten, bei denen Beschäftigte des Auftragnehmers oder durch den Auftragnehmer Beauftragte personenbezogene Daten (nachfolgend auch „Daten“ genannt) des Auftraggebers verarbeiten.

§ 1 Gegenstand, Dauer und Spezifizierung der Auftragsverarbeitung

(1) Der Auftragnehmer verarbeitet personenbezogene Daten im Auftrag des Auftraggebers. Gegenstand des Auftrags sowie Art und Zweck der Verarbeitung sind im **Anhang 1** konkretisiert.

(2) Die Laufzeit dieser Vereinbarung richtet sich nach der auf dem Beauftragungsformular hinterlegten Laufzeit, sofern sich aus den Bestimmungen dieser Vereinbarung nicht darüberhinausgehende Verpflichtungen ergeben.

§ 2 Verantwortlichkeit, Weisungsbefugnis des Auftraggebers

(1) Der Auftraggeber ist im Rahmen dieser Vereinbarung für die Einhaltung der gesetzlichen Bestimmungen der Datenschutzgesetze, insbesondere für die Rechtmäßigkeit der Datenweitergabe an den Auftragnehmer sowie für die Rechtmäßigkeit der Datenverarbeitung allein verantwortlich („Verantwortlicher“ im Sinne des Art. 4 Nr. 7 DSGVO).

(2) Die Weisungen des Auftraggebers werden anfänglich im Rahmen der Auftragserteilung festgelegt und können vom Auftraggeber danach in schriftlicher Form oder in einem elektronischen Format (Textform) an die vom Auftragnehmer bezeichnete Stelle durch einzelne Weisungen geändert, ergänzt oder ersetzt werden (Einzelweisung). Weisungen, die im Rahmen der Auftragserteilung nicht vorgesehen sind, werden als Antrag auf Leistungsänderung behandelt; die Parteien werden die Leistungsänderung und deren kommerzielle Auswirkungen abstimmen und in einer entsprechenden schriftlichen Änderungsvereinbarung festlegen. Der Auftraggeber wird dem Auftragnehmer eine angemessene Frist zur Umsetzung der Weisungen setzen. Mündliche Weisungen sind unverzüglich schriftlich oder in Textform zu bestätigen.

(3) Der Auftragnehmer und der Auftraggeber benennen schriftlich oder in Textform jeweils einen Ansprechpartner, der zur Abgabe von (Einzel-)Weisungen bzw. für die Annahme von (Einzel-) Weisungen im Zusammenhang mit der vertragsgegenständlichen Datenverarbeitung berechtigt ist.

Bei einem Wechsel oder einer dauerhaften Verhinderung des verantwortlichen Ansprechpartners ist dies durch den jeweiligen Vertragspartner unverzüglich schriftlich oder in Textform unter Benennung eines Vertreters mitzuteilen.

(4) Es besteht keine materiell-rechtliche Prüfpflicht seitens des Auftragnehmers im Hinblick auf vom Auftraggeber erteilte Weisungen. Ist der Auftragnehmer jedoch der Auffassung, dass eine Weisung des Auftraggebers gegen anwendbare Gesetze verstößt, informiert er den

Auftraggeber unverzüglich. Der Auftragnehmer darf die Umsetzung der Weisung solange aussetzen, bis sie vom Auftraggeber bestätigt oder abgeändert wurde. Etwaig hierdurch entstehende Mehraufwände des Auftragnehmers trägt der Auftraggeber. Der Auftraggeber trägt die alleinige Verantwortung für die von ihm getroffene Entscheidung.

§ 3 Pflichten des Auftragnehmers

(1) Der Auftragnehmer darf Daten von betroffenen Personen nur im Rahmen des Auftrages und der Weisungen des Auftraggebers verarbeiten.

(2) Der Auftragnehmer wird in seinem Verantwortungsbereich die innerbetriebliche Organisation so gestalten, dass sie den besonderen Anforderungen des Datenschutzes gerecht wird. Er wird technische und organisatorische Maßnahmen zum angemessenen Schutz der Daten des Auftraggebers treffen, die den Anforderungen des Art. 32 DSGVO genügen. Weitere Regelungen hierzu sind in § 5 dieser Vereinbarung enthalten.

(3) Der Auftragnehmer unterrichtet den Auftraggeber unverzüglich, wenn ihm Verletzungen des Schutzes der Daten des Auftraggebers bekannt werden. Der Auftragnehmer kann in diesem Fall einstweilig und nach eigenem Ermessen in seinem Verantwortungsbereich angemessene Maßnahmen zum Schutze der Daten des Auftraggebers und zur Minderung möglicher nachteiliger Folgen treffen. Der Auftragnehmer informiert den Auftraggeber über etwaige von ihm getroffene Maßnahmen möglichst zeitnah.

(4) Der Auftragnehmer gewährleistet, dass es den mit der Verarbeitung der Daten des Auftraggebers befassten Mitarbeitern und anderen für den Auftragnehmer tätigen Personen untersagt ist, die Daten außerhalb der Weisung zu verarbeiten. Ferner gewährleistet der Auftragnehmer, dass sich die zur Verarbeitung der Daten befugten Personen zur Vertraulichkeit verpflichtet haben oder einer angemessenen gesetzlichen Verschwiegenheitspflicht unterliegen. Die Vertraulichkeits-/ Verschwiegenheitspflicht besteht auch nach Beendigung des Auftrages fort.

(5) Der Auftragnehmer gewährleistet die Einhaltung der Vorgaben zur schriftlichen Bestellung eines Datenschutzbeauftragten und teilt dem Auftraggeber auf Anfrage dessen Kontaktdaten mit. Sollte der Auftragnehmer gesetzlich nicht zur Bestellung eines Datenschutzbeauftragten verpflichtet sein, nennt er dem Auftraggeber auf Anfrage den Ansprechpartner für im Rahmen dieser Vereinbarung anfallende Datenschutzfragen.

(6) Auf Anfrage des Auftraggebers unterstützt der Auftragnehmer den Auftraggeber im Rahmen des Zumutbaren bei

a) der Einhaltung der in den Art. 32 bis 36 DSGVO geregelten Pflichten des Auftraggebers;

b) der Erfüllung der Anfragen und Ansprüche betroffener Personen gem. Kapitel III der DSGVO.

Der Auftragnehmer kann für diese Unterstützung eine angemessene Vergütung und die Erstattung von Aufwendungen verlangen, soweit diese nicht auf einer schuldhaften Verletzung dieser Vereinbarung oder des anwendbaren Datenschutzrechts durch den Auftragnehmer beruht.

(7) Im Falle einer Inanspruchnahme des Auftraggebers durch eine betroffene Person hinsichtlich etwaiger Ansprüche nach Art. 82 DSGVO, verpflichtet sich der Auftragnehmer den Auftraggeber bei der Abwehr des Anspruches im Rahmen seiner Möglichkeiten zu unterstützen

§ 4 Pflichten des Auftraggebers

(1) Der Auftraggeber hat den Auftragnehmer unverzüglich und vollständig zu informieren, wenn er in den Auftragsergebnissen Fehler oder Unregelmäßigkeiten bzgl. datenschutzrechtlicher Bestimmungen feststellt.

(2) Der Auftraggeber ist für die Erfüllung der in den Art. 33 bis 36 DSGVO geregelten Pflichten verantwortlich.

(3) Der Auftraggeber wird dem Auftragnehmer alle Informationen zur Verfügung stellen, die der Auftragnehmer zum Führen des Verzeichnisses nach Art. 30 Abs. 2 DSGVO benötigt.

(4) Im Falle einer Inanspruchnahme des Auftragnehmers durch eine betroffene Person hinsichtlich etwaiger Ansprüche nach Art. 82 DSGVO, verpflichtet sich der Auftraggeber den Auftragnehmer bei der Abwehr des Anspruches im Rahmen seiner Möglichkeiten zu unterstützen.

(5) Der Auftraggeber nennt dem Auftragnehmer den Ansprechpartner für im Rahmen dieser Vereinbarung anfallende Datenschutzfragen.

(6) Über die Aufbewahrung, Herausgabe oder Löschung der Daten des Auftraggebers nach Beendigung dieser Vereinbarung (vgl. § 9 dieser Vereinbarung) muss der Auftraggeber innerhalb einer vom Auftragnehmer gesetzten angemessenen Frist entscheiden. Geht dem Auftragnehmer innerhalb dieser Frist keine Entscheidung zu, ist der Auftragnehmer zur

Löschung dieser Daten berechtigt, soweit keine rechtlichen Verpflichtungen des Auftragnehmers zur Aufbewahrung dieser Daten bestehen.

§ 5 Technisch und organisatorische Maßnahmen

(1) Der Auftragnehmer wird in seinem Verantwortungsbereich technische und organisatorische Maßnahmen zum angemessenen Schutz der Daten des Auftraggebers treffen, die die Vertraulichkeit, Integrität, Verfügbarkeit und Belastbarkeit der Systeme und Dienste im Zusammenhang mit dieser Auftragsverarbeitung auf Dauer sicherstellen sowie die Fähigkeit haben, die Verfügbarkeit der personenbezogenen Daten und den Zugang zu ihnen bei einem physischen oder technischen Zwischenfall rasch wiederherzustellen. Die vom Auftragnehmer getroffenen technischen und organisatorischen Maßnahmen sind in **Anhang 2** niedergelegt (nachfolgend „TOMs“ genannt).

(2) Dem Auftraggeber obliegt die Evaluierung und Bewertung der Wirksamkeit der TOMs. Soweit diese aus Sicht des Auftraggebers nicht ausreichend sind, werden die Parteien entsprechende Änderungen und deren kommerzielle Auswirkungen abstimmen und auf Basis einer entsprechenden schriftlichen Änderungsvereinbarung umsetzen.

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

(4) Der Auftragnehmer hat ein Verfahren zur regelmäßigen Überprüfung der Wirksamkeit der technischen und organisatorischen Maßnahmen zur Gewährleistung der Sicherheit der Verarbeitung etabliert.

§ 6 Berichtigung, Einschränkung und Löschung von Daten

(1) Der Auftragnehmer darf die Daten, die im Auftrag verarbeitet werden, nicht eigenmächtig, sondern nur nach dokumentierter Weisung des Auftraggebers berichtigen, löschen oder deren Verarbeitung einschränken.

(2) Wendet sich eine betroffene Person mit Forderungen zur Berichtigung, Löschung oder Auskunft an den Auftragnehmer, wird der Auftragnehmer die betroffene Person an den Auftraggeber verweisen, sofern eine Zuordnung der Betroffenenanfrage an den Auftraggeber nach Angaben der betroffenen Person möglich ist. Der Auftragnehmer unterstützt den Auftraggeber im Rahmen seiner Möglichkeiten auf Weisung soweit vereinbart. Der Auftragnehmer haftet nicht, wenn das Ersuchen der betroffenen Person vom Auftraggeber nicht, nicht richtig oder nicht fristgerecht beantwortet wird.

§ 7 Nachweismöglichkeiten, Kontrollrechte des Auftraggebers

(1) Der Auftragnehmer weist dem Auftraggeber die Einhaltung der in dieser Vereinbarung niedergelegten Pflichten nach. Der Nachweis solcher Maßnahmen, die nicht nur den konkreten Auftrag betreffen, kann erfolgen durch

a) die Einhaltung genehmigter Verhaltensregeln gemäß Art. 40 DSGVO;

b) die Zertifizierung nach einem genehmigten Zertifizierungsverfahren gemäß Art. 42 DSGVO;

c) aktuelle Testate, Berichte oder Berichtsauszüge unabhängiger Instanzen (z.B. Wirtschaftsprüfer, Revision, Datenschutzbeauftragter, IT-Sicherheitsabteilung, Datenschutzauditoren, Qualitätsauditoren);

d) eine geeignete Zertifizierung durch IT-Sicherheits- oder Datenschutzaudit (z.B. nach BSI-Grundschutz).

(2) Sollten im Einzelfall datenschutzrechtlich gebotene Kontrollen oder Überprüfungen durch den Auftraggeber oder einen von diesem beauftragten unabhängigen externen Prüfer, dessen Namen dem Auftragnehmer rechtzeitig im Voraus mitgeteilt wird, erforderlich sein, werden diese im Beisein eines Mitarbeiters des Auftragnehmers zu den üblichen Geschäftszeiten sowie ohne Störung des Betriebsablaufs in der Betriebsstätte des Auftragnehmers nach Anmeldung unter Berücksichtigung einer angemessenen Vorlaufzeit durchgeführt. Der Auftragnehmer darf die Prüfer von der Unterzeichnung einer angemessenen Verschwiegenheitserklärung hinsichtlich der Daten anderer Kunden und der eingerichteten technischen und organisatorischen Maßnahmen abhängig machen.

(3) Der Auftragnehmer wird dem Auftraggeber auf Anforderung innerhalb einer angemessenen Frist alle Auskünfte geben, die zur Durchführung einer umfassenden Kontrolle erforderlich sind.

(4) Der Auftraggeber stellt dem Auftragnehmer eine Kopie des vollständigen Auditberichts in elektronischer Form zur Verfügung. Der Auftragnehmer darf den Auditbericht insbesondere auch seinen Subunternehmern überlassen.

§ 8 Subunternehmer (weitere Auftragsverarbeiter)

(1) Der Einsatz von Subunternehmern als weitere Auftragsverarbeiter ist nur zulässig, wenn der Auftraggeber vorher zugestimmt hat.

(2) Ein zustimmungspflichtiges Subunternehmerverhältnis liegt vor, wenn der Auftragnehmer weitere Auftragnehmer mit der ganzen oder einer Teilleistung der vereinbarten Leistung beauftragt. Der Auftragnehmer wird mit diesen Dritten im erforderlichen Umfang Vereinbarungen treffen, um angemessene Datenschutz- und Informationssicherheitsmaßnahmen zu gewährleisten.

(3) Der Auftraggeber stimmt hiermit zu, dass der Auftragnehmer, die in **Anhang 3** aufgeführten Subunternehmer hinzuzieht. Dem Auftragnehmer ist es gestattet weitere Subunternehmer zur Erfüllung seiner vertraglichen Pflichten hinzuzuziehen oder bestehende Subunternehmer zu ersetzen, sofern er den Auftraggeber rechtzeitig (grundsätzlich 6 Wochen) vor der Datenverarbeitung hierüber informiert (Art. 28 Abs. 2 DSGVO). Widerspricht der Auftraggeber nicht innerhalb von 4 Wochen nach Erhalt der Information, akzeptiert er die Einsetzung als genehmigt im Sinne dieses Vertrages.

(4) Erteilt der Auftragnehmer Aufträge an Subunternehmer, so obliegt es dem Auftragnehmer, seine datenschutzrechtlichen Pflichten aus dieser Vereinbarung dem Subunternehmer zu übertragen.

§ 9 Löschungen und Rückgabe von Daten

(1) Nach Beendigung dieser Vereinbarung wird der Auftragnehmer, sofern technisch möglich und vom Auftraggeber gemäß § 4 Abs. 6 dieser Vereinbarung gewünscht, die Daten des Auftraggebers herausgeben. Elektronisch gespeicherte Daten sind auf Wunsch entweder in einem marktüblichen Format auf Datenträgern herauszugeben oder verschlüsselt online dem Auftraggeber zu übermitteln.

(2) Der Auftragnehmer wird sämtliche elektronisch gespeicherten Daten des Auftraggebers, von denen der Auftraggeber keine Herausgabe gemäß vorstehendem Absatz 1 wünscht oder bei denen eine Herausgabe technisch nicht möglich ist, löschen. Der Auftragnehmer wird dem Auftraggeber die Löschung auf Wunsch in Textform bestätigen.

(3) Daten des Auftraggebers, die nicht in elektronischer Form gespeichert sind (z.B. Daten auf CDs, papierhafte Unterlagen) und von denen der Auftraggeber keine Herausgabe gemäß vorstehendem Absatz 1 wünscht, werden durch den Auftragnehmer datenschutzkonform vernichtet.

(4) Die Verpflichtung zur Herausgabe oder Löschung gemäß diesem § 9 besteht nicht, wenn der Auftragnehmer gesetzlich zur Aufbewahrung oder sonst zur Speicherung dieser Daten verpflichtet ist.

(5) Sofern der Auftraggeber eine Aufbewahrung seiner Daten über das Vertragsende hinaus wünscht, bedarf dies einer gesonderten Vereinbarung zwischen den Parteien. Die Parteien werden die entsprechenden Leistungen und kommerziellen Auswirkungen abstimmen und in einer entsprechenden schriftlichen Änderungsvereinbarung festlegen.

§ 10 Schlussbestimmungen

(1) Sollten die Daten des Auftraggebers beim Auftragnehmer durch Pfändung oder Beschlagnahme, durch ein Insolvenz- oder Vergleichsverfahren oder durch sonstige Ereignisse oder Maßnahmen Dritter gefährdet werden, so wird der Auftragnehmer den Auftraggeber hierüber unverzüglich informieren, sofern das betreffende Recht eine solche Mitteilung nicht wegen eines wichtigen öffentlichen Interesses verbietet. Der Auftragnehmer wird den Dritten unverzüglich darüber informieren, dass die Hoheit und das Eigentum an den Daten ausschließlich beim Auftraggeber als „Verantwortlicher“ im Sinne der DSGVO liegen.

(2) Änderungen und Ergänzungen dieser Vereinbarung und aller ihrer Bestandteile bedürfen der Schriftform. Dies gilt auch für den Verzicht auf dieses Formerfordernis.

(3) Sollte eine Bestimmung dieser Vereinbarung unwirksam sein oder werden oder sollte diese Vereinbarung eine Regelungslücke enthalten, so soll davon die Wirksamkeit der Vereinbarung im Übrigen nicht berührt werden. An die Stelle der unwirksamen Bestimmung tritt die gesetzlich zulässige Regelung, die demjenigen, was die Parteien bei Abschluss der Vereinbarung wollten, wirtschaftlich am nächsten kommt. An die Stelle einer Regelungslücke soll eine Bestimmung treten, die dem entspricht, was die Parteien nach Sinn und Zweck der Vereinbarung unter Berücksichtigung aller Umstände vereinbart hätten, wenn ihnen das Vorhandensein der Lücke bewusst gewesen wäre.

(4) Es gilt deutsches Recht.

(5) Gerichtsstand für alle sich aus oder im Zusammenhang mit dieser Vereinbarung ergebenden Streitigkeiten ist, soweit es sich bei dem Vertragspartner um einen Kaufmann im Sinne des Handelsgesetzbuchs, eine juristische Person des öffentlichen Rechts oder ein öffentlich-rechtliches Sondervermögen handelt, Hannover. Der Auftragnehmer ist in diesem Fall jedoch auch berechtigt, vor dem für den Auftraggeber örtlich zuständigen Gericht Klage zu erheben.

Anhang 1 Gegenstand und Spezifizierung der Auftragsverarbeitung

I. Gegenstand der Verarbeitung

Gegenstand der Verarbeitung ist die Nutzung der free2pass App, welche durch den Auftragnehmer als Software as a Service Leistung angeboten wird. Der Auftraggeber kann diese App nutzen, um es Bürger*innen, welche ebenfalls diese App nutzen, zu ermöglichen, das Ergebnis eines in einem Testzentrum durchgeführten Corona-Tests in der App erfassen zu lassen. Auf diese Weise können diese Büerger*innen bei einer Örtlichkeit (Restaurant, Einzelhandel, Veranstaltungsort) aufgrund negativem Testergebnis eingelassen werden (sog. Check-In). Der Auftraggeber kann diese App ferner nutzen, um im Falle eines positiven Testergebnisses die Gesundheitsämter umgehend mit Kontaktdaten der/des Getesteten in aufbereiteter digitaler Form zu versorgen. Nachfolgend wird erläutert, wie die Datenverarbeitung im Detail erfolgt.

II. Art und Zweck der Datenverarbeitung

Die free2pass App bietet Bürger*innen eine einfache Möglichkeit, nach Registrierung in der App, Identitätsprüfung im Testzentrum (Vorlage Lichtbildausweis zum Abgleich) und Durchführung eines Corona-Tests in einem Testzentrum das Testergebnis digital an das eigene Smartphone zugesandt zu bekommen. Zu Beginn generiert das Testzentrum für den konkreten Testvorgang einen QR-Code, der zur Verknüpfung mit den Identitätsdaten in die App gescannt wird. So kann nach Testdurchführung vom Testzentrum ein entsprechendes digitales Testzertifikat erstellt werden, welches an die App gesandt und dort hinterlegt wird.

Im Fall eines negativen Testergebnisses kann dieses Zertifikat zeitlich begrenzt und datenschutzfreundlich als Nachweis für die Teilhabe an Außenaktivitäten genutzt werden. Dies dann bei Stellen, die das digitale free2pass Testzertifikat zum Nachweis einer Infektionsfreiheit akzeptieren, wie etwa Restaurants, Geschäfte oder Veranstaltungen. Auf diese Weise kann bei den besagten Stellen eine Infektionsfreiheit nachgewiesen werden, um Einlass zu erhalten (sog. Check-In). Bürger*innen, die über kein Smartphone verfügen, können vom Testzentrum eine zeitlich begrenzte, aktive free2pass Checkkarte auf Papier erhalten, welches als Alternative zum digitalen Testzertifikat fungiert.

Im Fall eines positiven Testergebnisses sind die Testzentren verpflichtet, dieses Ergebnis an das zuständige Gesundheitsamt zu übermitteln, damit eine Kontaktnachverfolgung ermöglicht wird. Die free2pass App bietet in diesem Fall die Möglichkeit für das Testzentrum, diese Benachrichtigung sicher verschlüsselt durchzuführen.

III. Art der personenbezogenen Daten

Jede(r) Nutzer*in der App muss sich innerhalb der App registrieren. Bereits beim Installations- und Registrierungsvorgang wie auch später bei der Nutzung der App werden folgende Arten personenbezogener Daten verarbeitet:

- Handynummer
- Vorname
- Nachname
- Anschrift
- Profilbild
- QR-Code des Testzentrums, mithin Schlüssel und ID für einen konkreten Testvorgang. Dies verknüpft mit den Identitätsdaten aus dem Nutzerkonto
- Testergebnis eines durchgeführten Corona-Tests
- Nur bei Scannen des CR-Codes jeweils bei Check-In und/oder Check-out vor Ort bei Stellen, die free2pass zur Einlasskontrolle nutzen:
    - Standort,
    - Aktuelles Datum, Uhrzeit des Check-In (Einlass)
    - Aktuelles Datum, Uhrzeit eines Check-Out (Verlassen des Ortes)
    - Verweildauer bei Check-Out
- Erforderliche Metadaten in Logdateien für die Nutzung von free2pass:
    - IP-Adresse
    - Datum und Uhrzeit des Zugriffs
    - Angeforderte URL des Request
    - Apple Geräte-Token oder Google Registrations-ID für Push-Nachrichten

IV. Kategorien betroffener Personen

Kategorien betroffener Personen sind bei der Nutzung von free2pass:

- Bürger*innen, welche die App nutzen.
- Verwaltungsmitglieder (Administratoren) des Auftraggebers

Anhang 2 Technische und organisatorische Maßnahmen

I. Vertraulichkeit (Art. 32 Abs. 1 lit. b DSGVO)

Pseudonymisierung
Eine Pseudonymisierung von Daten kann nur nach vorheriger Vereinbarung erfolgen.

Verschlüsselung
Sämtliche Systeme werden anhand eines Krypto-Konzepts installiert, konfiguriert und administriert oder anhand konkreter Vorgabe durch den Kunden. Dies betrifft sowohl die Sowohl die Transportverschlüsselung, als auch die Verschlüsselung von Datenträgern, Verzeichnissen und Dateien.

Datenträgerversand
Physikalische Datenträger werden in der Regel nicht versendet, sollte dies vom Kunden gefordert werden, erfolgt dies unter Verwendung von effektiven Verschlüsselungsverfahren

Mehrfaktorauthentifizierung
Der Zutritt zu den Datenverarbeitungssystemen ist nur nach erfolgreicher Authentifizierung anhand von mindestens zwei Faktoren unterschiedlichen Typs (z. B. biometrisches Merkmal und PIN) möglich.

Zutrittsprotokollierung
Jeder Zutritt zu Sicherheitsbereichen, in denen sich Datenverarbeitungssysteme befinden, wird automatisch protokolliert und kann daher nachvollzogen werden.

Videoüberwachung
Sicherheitsbereiche, in denen sich Datenverarbeitungssysteme befinden, werden permanent von Videokameras überwacht. Die Aufnahmen werden gespeichert und für einen angemessenen Zeitraum aufbewahrt.

Versperrte Racks
Racks, in denen sich Datenverarbeitungssysteme befinden, sind versperrt. Die Schlüssel werden zentral verwaltet.

Fluchttüren
Sicherheitsbereiche dürfen ausschließlich durch die dafür vorgesehenen Eingänge betreten werden. Fluchttüren können von außen nicht als Eingang benutzt werden. Das Öffnen von Fluchttüren führt zu einer Alarmierung.

Genehmigungspflicht
Zutritts- oder Zugriffsberechtigungen zu den Sicherheitsbereichen oder Systemen unterliegen einem formalisierten Genehmigungsverfahren.

Reinigungs- und Wartungsarbeiten

In Sicherheitsbereichen finden keine unbegleiteten Wartungs- oder Reinigungsarbeiten durch Unberechtigte statt.

Passwörter

Der Zugang zu Datenverarbeitungssystemen ist nur nach vorheriger Authentifizierung anhand von Benutzernamen und Passwörtern möglich. Die Mindestanforderungen an Passwortlänge- und -komplexität sowie der Umgang mit Passwörtern sind in einer Richtlinie definiert und werden systemseitig unterstützt. Passwörter werden mit Zufallsgeneratoren erzeugt. Passwörter werden in Anmeldeverfahren verschlüsselt übertragen.

Zugriffsprotokollierung

Jede Anmeldung an einem Datenverarbeitungssystem wird protokolliert. Die Protokolle sind gegen Veränderung geschützt und werden für einen angemessenen Zeitraum aufbewahrt.

Klassifizierung

Eine Richtlinie regelt die Klassifizierung von Datenarten wie z. B. personenbezogenen Daten und damit verbundene Bestimmungen.

Mandantentrennung

Datenverarbeitungssysteme verschiedener Auftraggeber werden physisch oder logisch so voneinander getrennt, dass eine gegenseitige unberechtigte Einsichtnahme ausgeschlossen ist.

Mobile Datenträger

Personenbezogene Daten werden für den internen Gebrauch nicht auf mobilen Datenträgern wie z. B: USB-Sticks oder DVDs gespeichert.

Aufgabentrennung

An der Verwaltung der Datenverarbeitungssysteme und deren Infrastruktur sind verschiedene Mitarbeiter beteiligt, deren Verantwortlichkeiten und Berechtigungen in einem Rollenkonzept geregelt sein.

Regelmäßige Überprüfung

Im Rahmen von internen Audits werden regelmäßig Zugangsberechtigungen zu Datenverarbeitungssystemen kontrolliert und auf ihre Rechtmäßigkeit geprüft.

Entzug von Berechtigungen

Bei der Beendigung oder Veränderung der Anstellung von Mitarbeitern werden nicht mehr benötigte Zugriffsberechtigungen entzogen.

Bildschirmsperre

Arbeitsstationen der Mitarbeiter sind so konfiguriert, dass nach Ablauf eines Zeitintervalls die passwortgeschützte Bildschirmsperre aktiviert wird

II. Integrität (Art. 32 Abs. 1 lit. b DSGVO)

Genehmigungspflicht
Zugriffsberechtigungen zu den Datenverarbeitungssystemen unterliegen einem formalisierten Genehmigungsverfahren.

Protokollierung
Jeder Systemzugriff wird protokolliert. Die Protokolle sind gegen Veränderung geschützt und werden für einen angemessenen Zeitraum aufbewahrt.

III. Verfügbarkeit und Belastbarkeit (Art. 32 Abs. 1 lit. b DSGVO)

Brandschutz
Rechenzentren sind mit angemessenen Systemen zur Erkennung von Bränden und Alarmierungssystemen ausgestattet. In kritischen Sicherheitsbereichen stehen Löschanlagen zur Verfügung. Sicherheitsbereiche werden regelmäßig auf vermeidbare Brandlasten hin überprüft.

Stromversorgung
Die Rechenzentren verfügen über eine Anlage zur unterbrechungsfreien Stromversorgung (USV), die den Weiterbetrieb der Datenverarbeitungssysteme bei Ausfall der Stromzuführung gewährleistet. Kritische Sicherheitsbereiche sind darüber hinaus mit einer Netzersatzanlage (NEA) ausgestattet, die eine eigenständige Stromversorgung auch über längere Zeiträume hinweg gewährleistet.

Klimaversorgung
Die Gewährleistung der geeigneten Temperatur und Luftfeuchtigkeit in den Rechenzentren wird über redundante Klimageräte sichergestellt.

Netzwerkanbindung
Die vereinbarte Anbindung von Datenverarbeitungssystemen an vereinbarte Netzwerke erfolgt über redundante Leitungen verschiedener Anbieter.

Datensicherung
Kundensysteme werden gemäß den Vereinbarungen im Hauptvertrag gesichert. Interne Systeme werden gemäß einem Backupkonzept gesichert.

Sicherheitssysteme
Kritische Teile der Infrastruktur werden durch geeignete Systeme zur Vermeidung oder Reduzierung der Auswirkung von Angriffen oder Störungen (Sicherheitssysteme) geschützt.

Regelmäßige Überprüfung
Sicherheitssysteme werden regelmäßig auf ihre Angemessenheit und Wirksamkeit hin überprüft.

Notfallkonzepte
Für jeden Standort existieren Notfallkonzepte zur Notfallvorsorge und Notfallbehandlung

Regelmäßige Erprobung
Sämtliche Notfallkonzepte werden regelmäßig erprobt und die Ergebnisse dokumentiert.

IV. Regelmäßige Überprüfung, Bewertung und Evaluierung des Datenschutzes

AV-Vertrag
Kommt ein Unterauftragnehmer zum Einsatz, so werden Rechte und Pflichten in einem AV-Vertrag geregelt.

Überwachung
Alle datenschutzrelevanten Auftragnehmer der 1&1 IONOS GmbH werden regelmäßig auditiert, um die Einhaltung der vereinbarten Maßnahmen zu prüfen.

Audit
Sämtliche datenschutzrelevanten Prozesse und Dokumente werden regelmäßig auf Aktualität und Wirksamkeit geprüft.

V. Sonstige Maßnahmen

Datenschutzbeauftragter
Die 1&1 IONOS GmbH hat einen fachkundigen externen Datenschutzbeauftragten bestellt; Dieser ist unter datenschutz@IONOS.de erreichbar.

Datenschutzkonzept
Der Umgang mit personenbezogenen Daten ist in einem für alle Mitarbeiter verbindlichen Datenschutzkonzept geregelt.

Verpflichtungserklärung
Alle Mitarbeiter sind im Sinne der Datenschutzrechtlichen Gesetzgebung auf das Datengeheimnis verpflichtet.

Schulung
Alle Mitarbeiter werden regelmäßig von einem fachkundigen Datenschutzexperten im Umgang mit personenbezogenen Daten geschult.

Regelmäßige Überprüfung
Sämtliche Maßnahmen zum Datenschutz werden im Rahmen von internen Audits regelmäßig überprüft.

Anhang 3

Subunternehmer

Name und Geschäftssitz des Subunternehmers	Vom Subunternehmer durchgeführte Tätigkeit
1&1 IONOS SE Elgendorfer Str. 57 56410 Montabaur	Für die Bereitstellung eines Rechenzentrums (Webhosting, Content Delivery Network) sowie für den E-Mail-Versand mit Mailserver.
Twilio Inc., 375 Beale Street, Suite 300, San Francisco, CA 94105, USA	Für die Installations-Verifizierung per SMS.
Google, Inc. Mountain View, USA	Für den Dienst Firebase Cloud Messaging (FCM) zwecks Zustellung von Push-Nachrichten.

Ort, Datum

(Unterschrift des Auftraggebers)

Ort, Datum

(Unterschrift des Auftragsverarbeiters)