# Nutzungsbedingungen für Unternehmen

Die App bzw. Browseranwendung (nachfolgend zusammenfassend „Anwendung“) ist ein Service der unitverse GmbH, Christoph-Probst-Weg 4, 20251 Hamburg, Deutschland („*Twoogether*“). Für die Anwendung gelten gegenüber den Unternehmen, welche die Anwendung einsetzen („Unternehmen“), die nachfolgenden Nutzungsbedingungen.

**I. Nutzungsbedingungen**

1. Das Unternehmen erhält von Twoogether das Recht, die Anwendung für den bestimmungsgemäßen Gebrauch mit den dafür vorgesehenen Funktionen für die Dauer des Lizenzvertrags zu nutzen. Die Funktionen der Anwendung können sich zukünftig ändern. Twoogether ist in der Anpassung der Funktionen frei, soweit das Unternehmen nicht unangemessen benachteiligt wird. Weitere Rechte erhält das Unternehmen an der Anwendung nicht.

2. Twoogether überlässt dem Unternehmen die Anwendung grundsätzlich kostenfrei. Das Unternehmen hat die Möglichkeit, ergänzende Dienste durch gesonderte Buchung kostenpflichtig zu erwerben.

3. Das Unternehmen hat sich über die korrekte Bedienung der Anwendung und ihre technischen Anforderungen zu informieren. Das Unternehmen trägt das Risiko, dass die Anwendung seinen Wünschen entspricht und für seine Zwecke einsetzbar ist. Twoogether ist nicht dafür verantwortlich, dass die von den Endnutzern bei der Registrierung getätigten Angaben zutreffend sind.

4. Aufgrund der Vielgestaltigkeit von Endgeräten, der unterschiedlichen Versionierung von Betriebssystemen und deren unterschiedlichen Konfigurationen kann Twoogether keine Gewährleistung dafür übernehmen, dass die Anwendung auf den Endgeräten des Unternehmens, seinen Mitarbeitern / Beauftragten und/oder denen der Endkunden (fehlerfrei) funktioniert.

5. Dem Unternehmen ist es nicht gestattet, die Anwendung zu dekompilieren, zu bearbeiten oder außerhalb der bestimmungsgemäßen Nutzung zu vervielfältigen. Gesetzlich vorgesehene Rechte, eine Sicherungskopie anzufertigen, bleiben unberührt.

6. Das Unternehmen gewährleistet, dass die von seinen Mitarbeitern / Beauftragten in der Anwendung eingegebenen Daten korrekt und aktuell sind. Twoogether ist berechtigt, im Rahmen der datenschutzrechtlichen Zulässigkeit Daten der Nutzer der Anwendung einschließlich Daten der Endkunden zu Analyse- und Marketingzwecken zu nutzen. Sofern eine solche Nutzung erfolgt, wird Twoogether eine ggf. erforderliche ausdrückliche Einwilligung des Anwendung-Nutzers einholen und den Anwendung-Nutzer in der Datenschutzerklärung über den Umfang der Nutzung informieren.

7. Das Unternehmen darf die Daten der Endnutzer nur für gesetzlich vorgesehene Fälle herunterladen, insbesondere um seinen Verpflichtungen zur Weitergabe von Daten an Gesundheitsbehörden nachzukommen.

8. Twoogether haftet nach den gesetzlichen Bestimmungen bei grober Fahrlässigkeit, vorsätzlichem Handeln, Arglist oder einem Garantieversprechen sowie bei einer Verletzung des Lebens, des Körpers oder der Gesundheit. Auch eine Haftung nach dem Produkthaftungsrecht bleibt unberührt. In allen anderen Fällen haftet Twoogether nur bei fahrlässiger Verletzung einer wesentlichen Vertragspflicht; also einer Pflicht, die wesentlich für die Erreichung des Vertragszwecks ist (Kardinalpflicht). In letztgenanntem Fall bleibt die Haftung von Twoogether der Höhe nach begrenzt auf den Schaden, der nach der Art des Vertragsgegenstands vorhersehbar und typisch ist. Die Haftung von Twoogether ist für fahrlässiges Verhalten, unabhängig vom Rechtsgrund, der Höhe nach auf EUR 1.000,00 beschränkt. Twoogether haftet nicht für Folgeschäden einschließlich des entgangenen Gewinns. Twoogether haftet für den Verlust von Daten nur bis zu dem Betrag, der bei ordnungsgemäßer und regelmäßiger Sicherung der Daten zu deren Wiederherstellung angefallen wäre. Die Haftungsbeschränkung nach dieser Ziffer 8 gilt auch für die persönliche Haftung der Mitarbeiter, Vertreter und Organe von Twoogether.

9. Der Lizenzvertrag läuft auf unbestimmte Zeit. Sowohl das Unternehmen als auch Twoogether können den Lizenzvertrag jederzeit ohne Angaben von Gründen ordentlich kündigen. Ungeachtet aller sonstigen Rechte kann Twoogether den Lizenzvertrag außerordentlich fristlos kündigen, wenn das Unternehmen gegen die vorstehenden Nutzungsbedingungen verstößt.

10. Twoogether kann die Nutzungsbedingungen jederzeit ändern. Änderungen der Nutzungsbedingungen werden nach Wahl von Twoogether spätestens einen Monat vor dem vorgeschlagenen Zeitpunkt ihres Wirksamwerdens per E-Mail oder über die Anwendung angeboten. Das Unternehmen kann den Änderungen entweder zustimmen oder diese ablehnen. Die Zustimmung gilt als erteilt, wenn das Unternehmen die Ablehnung nicht vor dem vorgeschlagenen Zeitpunkt des Wirksamwerdens der Änderungen angezeigt hat. Auf die Genehmigungswirkung wird Twoogether das Unternehmen ausdrücklich in der E-Mail hinweisen. Bei Ablehnung der neuen Nutzungsbedingungen kann Twoogether den Lizenzvertrag ohne weitere Vorankündigung kündigen.

11. Anwendbares Recht ist deutsches Recht unter Ausschluss des UN-Kaufrechts. Für Streitigkeiten aus diesem Vertrag ist ausschließlicher Gerichtsstand der Geschäftssitz von Twoogether in Hamburg, soweit zulässig. Twoogether bleibt vorbehalten, das Unternehmen auch an dessen Geschäftssitz klageweise in Anspruch zu nehmen.

**II. Auftragsverarbeitungsvertrag gemäß Art. 28 DS-GVO**

1. Gegenstand und Dauer des Auftrags

   Dieser Auftragsverarbeitungsvertrag bezieht sich ausschließlich auf die pandemie-bedingte Datenverarbeitung (Erhebung von Kontaktdaten) zur Nachverfolgung von Infektionsketten.
   Art und Zweck der Verarbeitung: Die twoogether führt für den Auftraggeber die pandemie- bedingte Kontaktdatenerhebung durch.
   Art der Daten: Vorname, Nachname, Adresse, Telefonnummer, Aufenthaltszeitraum
   Kategorien betroffener Personen: User / Kunden
   Dieser Vertrag tritt – solange keine anderweitigen Regelungen vereinbart wurden – mit Zustimmung dieser Nutzungsbedingungen in Kraft und gilt, solange der Auftragnehmer für den Auftraggeber personenbezogene Daten verarbeitet.

   Die Erbringung der vertraglich vereinbarten Datenverarbeitung findet ausschließlich in einem Mitgliedsstaat der Europäischen Union oder in einem anderen Vertragsstaat des Abkommens über den Europäischen Wirtschaftsraum statt. Jede Verlagerung in ein Drittland bedarf der vorherigen Zustimmung des Auftraggebers.

2. Technisch-organisatorische Maßnahmen

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

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

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

3. Berichtigung, Einschränkung und Löschung von Daten

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

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

4. Qualitätssicherung und sonstige Pflichten des Auftragnehmers

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

Datenschutzbeauftragter: Sofern der Auftragnehmer gemäß Art. 37 DS-GVO bzw. § 38 BDSG-neu dazu verpflichtet ist einen Datenschutzbeauftragten zu bestellen, teilt er dem Auftraggeber dessen Kontaktdaten zum Zwecke der direkten Kontaktaufnahme mit. Ein Wechsel des Datenschutzbeauftragten wird dem Auftraggeber unverzüglich mitgeteilt. Die Kontaktdaten des Datenschutzbeauftragten des Auftraggebers und Auftragnehmers werden auf der Webseite dokumentiert.

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

Umsetzung und Einhaltung der technischen und organisatorischen Maßnahmen: Die Umsetzung und Einhaltung aller für diesen Auftrag erforderlichen technischen und organisatorischen Maßnahmen gemäß Artt. 28 Abs. 3 S. 2 lit. c, 32 DS-GVO. Der Auftragnehmer ist für die Nachweisbarkeit der getroffenen technischen und organisatorischen Maßnahmen gegenüber dem Auftraggeber im Rahmen seiner Kontrollbefugnisse nach Ziffer 6 dieses Vertrages verantwortlich.

Kontrolle durch die Aufsichtsbehörde: Der Auftraggeber und der Auftragnehmer arbeiten auf Anfrage mit der Aufsichtsbehörde bei der Erfüllung ihrer Aufgaben zusammen. Der Auftragnehmer hat den Auftraggeber unverzügliche über Kontrollhandlungen und Maßnahmen der Aufsichtsbehörde, soweit sie sich auf diesen Auftrag beziehen, zu informieren. Dies gilt auch, soweit eine zuständige Behörde im Rahmen eines Ordnungswidrigkeits- oder Strafverfahrens in Bezug auf die Verarbeitung personenbezogener Daten bei der Auftragsverarbeitung beim Auftragnehmer ermittelt. Soweit der Auftraggeber seinerseits einer Kontrolle der Aufsichtsbehörde, einem Ordnungswidrigkeits- oder Strafverfahren, dem Haftungsanspruch einer betroffenen Person oder eines Dritten oder einem anderen Anspruch im Zusammenhang mit der Auftragsverarbeitung beim Auftragnehmer ausgesetzt ist, hat ihn der Auftragnehmer nach besten Kräften zu unterstützen.

5. Unterauftragsverhältnisse

   Als Unterauftragsverhältnisse im Sinne dieser Regelung sind solche Dienstleistungen zu verstehen, die sich unmittelbar auf die Erbringung der Hauptleistung beziehen. Nicht hierzu gehören Nebenleistungen, die der Auftragnehmer z. B. als Telekommunikationsleistungen, Post- / Transportdienstleistungen, Wartungs- und Benutzerservice oder die Entsorgung von Datenträgern sowie sonstige Maßnahmen zur Sicherstellung der Vertraulichkeit, Verfügbarkeit, Integrität und Belastbarkeit der Hard- und Software von Datenverarbeitungsanlagen in Anspruch nimmt.

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

   Der Auftragnehmer darf Unterauftragnehmer (weitere Auftragsverarbeiter) nur nach vorheriger ausdrücklicher schriftlicher bzw. dokumentierter Zustimmung des Auftraggebers beauftragen. Die Zustimmung gilt als erteilt, sofern innerhalb von 14 Tagen nach Anzeige eines zusätzlich einzusetzenden Unterauftragnehmers kein Widerspruch gegen die Einbindung erfolgt.

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

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

   Die Verarbeitung bzw. Speicherung personenbezogener Daten erfolgt ausschließlich auf Servern, die sich in Deutschland befinden und gegen den Zugriff Dritter verschlüsselt sind.

6. Kontrollrechte des Auftraggebers

   Der Auftraggeber hat das Recht, im Benehmen mit dem Auftragnehmer Überprüfungen durchzuführen oder durch im Einzelfall zu benennende Prüfer durchführen zu lassen. Er hat das

Recht, sich durch Stichprobenkontrollen, die in der Regel rechtzeitig anzumelden sind, von der Einhaltung dieser Vereinbarung durch den Auftragnehmer in dessen Geschäftsbetrieb zu überzeugen.

Beauftragt der Auftraggeber einen Dritten mit der Durchführung der Kontrolle, hat der Auftraggeber den Dritten schriftlich gegenüber dem Auftragnehmer auf die Verschwiegenheit und Geheimhaltung zu verpflichten, es sei denn, dass der Dritte einer beruflichen Verschwiegenheitspflicht unterliegt. Auf Verlangen des Auftragnehmers wird ihm der Auftraggeber die Verschwiegenheitsverpflichtung unverzüglich vorlegen. Der Auftraggeber darf keinen Konkurrenten des Auftragnehmers mit der Kontrolle beauftragen. Der Auftragnehmer kann für seinen Aufwand bei der Durchführung der Kontrollen eine angemessene Vergütung verlangen.

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

Der Nachweis solcher Maßnahmen, die nicht nur den konkreten Auftrag betreffen, kann erfolgen durch: die Einhaltung genehmigter Verhaltensregeln gemäß Art. 40 DS-GVO; die Zertifizierung nach einem genehmigten Zertifizierungsverfahren gemäß Art. 42 DS-GVO; aktuelle Testate, Berichte oder Berichtsauszüge unabhängiger Instanzen (z. B. Wirtschaftsprüfer, Revision, Datenschutzbeauftragter, IT-Sicherheitsabteilung, Datenschutzauditoren, Qualitätsauditoren); eine geeignete Zertifizierung durch IT-Sicherheits- oder Datenschutzaudit (z. B. nach BSI-Grundschutz).

7. Mitteilung bei Verstößen des Auftragnehmers

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

   - die Sicherstellung eines angemessenen Schutzniveaus durch technische und organisatorische Maßnahmen, die die Umstände und Zwecke der Verarbeitung sowie die prognostizierte Wahrscheinlichkeit und Schwere einer möglichen Rechtsverletzung durch Sicherheitslücken berücksichtigen und eine sofortige Feststellung von relevanten Verletzungsereignissen ermöglichen;
   - die Verpflichtung, Verletzungen personenbezogener Daten unverzüglich an den Auftraggeber zu melden;
   - die Verpflichtung, den Auftraggeber im Rahmen seiner Informationspflicht gegenüber dem Betroffenen zu unterstützen und ihm in diesem Zusammenhang sämtliche relevante Informationen unverzüglich zur Verfügung zu stellen;
   - die Unterstützung des Auftraggebers für dessen Datenschutz-Folgenabschätzung;
   - die Unterstützung des Auftraggebers im Rahmen vorheriger Konsultationen mit der Aufsichtsbehörde.

8. Weisungsbefugnis des Auftraggebers

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

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

9. Löschung und Rückgabe von personenbezogenen Daten

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

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

   Dokumentationen, die dem Nachweis der auftrags- und ordnungsgemäßen Datenverarbeitung dienen, sind durch den Auftragnehmer entsprechend der jeweiligen Aufbewahrungsfristen über das

Vertragsende hinaus aufzubewahren. Er kann sie zu seiner Entlastung bei Vertragsende dem Auftraggeber übergeben.

## Anlage 1 – Technische und organisatorische Maßnahmen gemäß Art. 32 EU DS-GVO

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

| **Zutrittskontrolle:** | Maßnahmen, die geeignet sind, Unbefugten den Zutritt zu Datenverarbeitungsanlagen, mit denen personenbezogene Daten verarbeitet oder genutzt werden, zu verwehren. |
|---|---|
| ☒ Alarmanlage | ☒ Aufteilung der Gebäude in Sicherheitszonen |
| ☒ Automatische Zugangskontrolle | ☒ Videoüberwachung der Zugänge |
| ☒ Schließsystem mit Codesperre | ☒ Sicherheitsschlösser |
| ☒ Schlüsselregelung (Schlüsselausgabe etc.) | ☒ Personenkontrolle beim Pförtner / Empfang |
| ☒ Protokollierung der Besucher | ☒ Dokumentiere Regelungen für die Zutrittskontrolle |
| ☒ Sorgfältige Auswahl von Personal (Reinigung, Pförtner, etc.) | ☒ Personal Multi-Faktor-Authentifizierung |

| **Zugangskontrolle:** | Maßnahmen, die geeignet sind zu verhindern, dass Datenverarbeitungssysteme von Unbefugten genutzt werden können. |
|---|---|
| ☒ Zuordnung von Benutzerrechten | ☒ Auswertung von Log-Dateien |
| ☒ Passwortrichtlinie (komplexe Passwörter) | ☒ Zuordnung von Benutzerprofilen zu IT-Systemen |
| ☒ Authentifikation mit Benutzername / Passwort | ☒ Verschlüsselung von mobilen Datenträgern |
| ☒ Gehäuseverriegelung | ☒ Einsatz einer Software-Firewall |
| ☒ Sperrung von externen Schnittstellen | ☒ Regelmäßiger Passwortwechsel |
| ☒ Protokollierung der Besucher | ☒ Kontosperrung bei fehlerhaften Zugangsversuchen |
| ☒ Einsatz von Anti-Viren-Software | ☒ Bildschirmsperre nach definiertem Zeitintervall |
| ☒ Segmentierung von Netzwerken | |
| ☒ Protokollierung der Zugänge | |

| **Zugriffskontrolle:** | Maßnahmen, die gewährleisten, dass die zur Benutzung eines Datenverarbeitungssystems Berechtigten ausschließlich auf die ihrer Zugriffsberechtigung unterliegenden Daten zugreifen können, und dass personenbezogene Daten bei der Verarbeitung, Nutzung und nach der Speicherung nicht unbefugt gelesen, kopiert, verändert oder entfernt werden können. |
|---|---|
| ☒ Erstellen eines Berechtigungskonzepts | ☒ Verwaltung der Rechte durch Systemadministrator |
| ☒ Anzahl der Administratoren auf das Notwendigste beschränkt | ☒ Ordnungsgemäße Vernichtung von Datenträgern |
| ☒ Protokollierung von Zugriffen | |
| ☒ Verschlüsselung von Datenträgern | |

| **Trennungskontrolle:** | Maßnahmen, die gewährleisten, dass zu unterschiedlichen Zwecken erhobene Daten getrennt verarbeitet werden können. |
|---|---|
| ☒ Logische Mandantentrennung | ☒ Datensätze mit Zweckattributen |
| ☒ Trennung von Entwicklungs-, Test- und Produktivsystemen | |

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

| **Weitergabekontrolle:** | Maßnahmen, die gewährleisten, dass personenbezogene Daten bei der elektronischen Übertragung oder während ihres Transports oder ihrer Speicherung auf Datenträger nicht unbefugt gelesen, kopiert, verändert oder entfernt werden können, und dass überprüft und festgestellt werden kann, an welche Stellen eine Übermittlung personenbezogener Daten durch Einrichtungen zur Datenübertragung vorgesehen ist. |
|---|---|
| ☒ Weitergabe an Dritte nur nach Prüfung der Rechtsgrundlage | ☒ Beschränkung des zur Übermittlung befugten Personen-kreises |
| ☒ Sichere Übertragung von Datenlieferungen (TLS) | ☒ Protokollierung von Datenabruf oder –übermittlung |

| **Eingabekontrolle:** | Maßnahmen, die gewährleisten, dass nachträglich überprüft und festgestellt werden kann, ob und von wem personenbezogene Daten in Datenverarbeitungssysteme eingegeben, verändert oder entfernt worden sind. |
|---|---|
| ☒ Zuordnung der Logins zu datenverarbeitenden Mitarbeitern | ☒ Protokollierung der Eingabe, Änderung und Löschung personenbezogener Daten |
| ☒ automatische Löschung der Corona Kotaktlisten nach Ablauf der gesetzlichen Aufbewahrungsfrist | |

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

| **Verfügbarkeitskontrolle:** | Maßnahmen, die gewährleisten, dass personenbezogene Daten gegen zufällige Zerstörung oder Verlust geschützt sind. |
|---|---|
| ☒ Datensicherungskonzept mit regelmäßigem Backup | ☒ Überwachung der Betriebsparameter in Serverräumen |
| ☒ Sicherheitskonzept für Serverräume | ☒ Regelmäßiger Test der Rücksicherungsfähigkeit |
| ☒ Feuer- / Rauchmeldeanlage | ☒ Auslagerung von Datenträgern zur Datensicherung |
| ☒ Alarmanlage für Serverräume | ☒ Feuerlöschgeräte für Serverräume |
| ☒ Klimaanlage in Serverräume | |

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

| **Datenschutz-Management:** | Maßnahmen, die die Zulässigkeit, Angemessenheit und Wirksamkeit des Datenschutzes sicherstellen sollen. |
|---|---|
| ☒ Datenschutzbeauftragter bestellt<br>☒ Datenschutzfreundliche Voreinstellungen<br>☒ Meldewege für Sicherheitsvorfälle | ☒ Datenschutzschulung / -trainings<br>☒ Interne Überwachung der Ordnungsmäßigkeit |

| **Auftragskontrolle:** | Maßnahmen, die gewährleisten, dass personenbezogene Daten, die im Auftrag verarbeitet werden, nur entsprechend den Weisungen des Auftraggebers verarbeitet werden können. |
|---|---|
| ☒ Auswahl des Auftragnehmers unter Sorgfaltsgesichtspunkten (insbesondere hinsichtlich Datensicherheit)<br>☒ schriftliche Weisungen an den Auftragnehmer (z. B. durch Auftragsdatenverarbeitungsvertrag) i.S.d. Art. 28 DS-GVO<br>☒ Auftragnehmer hat Datenschutzbeauftragten bestellt<br>☒ Wirksame Kontrollrechte gegenüber dem Auftragnehmer vereinbart | ☒ Verpflichtung der Mitarbeiter des Auftragnehmers auf das Datengeheimnis /-geheimhaltung<br>☒ Sicherstellung der Vernichtung von Daten nach Beendigung des Auftrags |