KERKAPORTA
</IT SECURITY GMBH>

Allgemeine Geschäftsbedingungen

EASYTRACE – COVID19 Gästebuch

Kerkaporta IT Security GmbH
Anastasius-Grün-Gasse 17/17, 1180 Wien
www.kerkaporta.at | support@kerkaporta.at
FN: 521584 k | ATU: 74922818

1. Allgemeines

(1) Die Webanwendung EasyTrace.at wird von der Kerkaporta IT Security GmbH betrieben.
(2) EasyTrace ist ein COVID-19 Gästebuch, mit dem Personen, über einen QR-Code ihre Kontaktdaten eingeben und speichern können.
(3) Die Basisversion von EasyTrace ist kostenlos verwendbar. Ein Betrieb kann über den Button „HIER BEGINNEN“ einen QR-Code erstellen und diesen zum Erheben von Kontaktdaten verwenden.
(4) Es können maximal 10 QR-Codes pro Betrieb kostenlos verwendet werden.
(5) Mit der PRO-Version werden zusätzliche Features für einen oder mehrere QR-Codes freigeschaltet:
- Logo Upload
- Link für Speisekarte
- zentrale Verwaltung
- QR-Code bearbeiten (Name, Tischnummer, Logo, Speisekarte,...)
- GastroScreen
- Nachtragen von Gästen
(Weitere Features können jederzeit hinzugefügt werden)
(6) Die PRO-Version ist kostenpflichtig und kann per E-Mail über easytrace@kerkaporta.at bestellt werden.
(7) Im Gästebuch können Name, Adresse, Kontaktmöglichkeit (E-Mail bzw. Telefon) und die Tischnummer eingetragen werden. Diese Daten werden verschlüsselt und danach zum Server übertragen.
(8) Es werden keine Metadaten, wie IP-Adresse, User-Agent, usw. mitgeloggt.
(9) Eintragungen werden nach 28 Tagen automatisch vom System gelöscht.
(10) Das 4-Augen-Prinzip stellt sicher, dass der Ersteller des QR-Codes nur die verschlüsselten Daten erhält, wenn dieser eine Anordnung der Gesundheitsbehörde vorlegt.
(11) Kerkaporta hat zu keinem Zeitpunkt Zugriff auf unverschlüsselte Daten.
(12) Der Ersteller des QR-Codes stimmt mit der Generierung eines QR-Codes der Auftragsdatenverarbeitung mit der Kerkaporta IT Security GmbH zu. *(näheres siehe Seite 5)*

2. Ende-zu-Ende Verschlüsselung

(1) Beim Generieren eines QR-Codes wird am Client des Erstellers ein RSA Key-Pair generiert, dafür wird die Library Opencrypto verwendet. Danach wird ein Passwort, welches aus 10 zufälligen Bytes besteht, generiert. Mit diesem Passwort wird der Private Key verschlüsselt. 5 weitere zufällige Bytes bilden die geheime ID des QR-Codes.
(2) Diese ID wird verwendet um den Ersteller des QR-Codes zu identifizieren.
(3) Diese Berechnungen werden ausschließlich am Client des Erstellers beim Generieren eines QR-Codes ausgeführt.
(4) Nur die folgenden Daten werden zum Server übertragen:

- der Public Key
- der verschlüsselte Private Key
- die geheime ID
- der Name des Betriebes

(5) Als Antwort erhält der Ersteller einen QR-Code, über den sich Personen in das Gästebuch eintragen können.

(6) Scannt eine Person einen QR-Code, öffnet sich der Browser des Gerätes und ein Formular wird angezeigt. Darin kann die Person ihre persönlichen Daten eintragen.

(7) Beim Absenden verschlüsselt der Browser der Person die eingegebenen Daten mit dem Public Key des Erstellers. Dies geschieht ebenfalls am Gerät ohne Unterstützung des Servers. Wurden alle Daten verschlüsselt, werden diese zum Server gesendet.

3. Auslesen der Daten und das 4-Augen-Prinzip

(1) Muss der Ersteller des QR-Codes das Gästebuch aufgrund eines Covid-19-Falls auslesen, muss dieser die amtliche Bestätigung der Gesundheitsbehörde an Kerkaporta senden. Kerkaporta gibt nach einer Überprüfung der Bestätigung die verschlüsselten Daten frei, so dass der Ersteller des QR-Codes diese mit seinem geheimen Passwort entschlüsseln und der Gesundheitsbehörde weitergeben kann. Die Entschlüsselung der Daten findet ebenfalls am Client Browser statt.

(2) Somit ist es nur für den Ersteller des QR-Codes in Verbindung mit der Freigabe von Kerkaporta möglich, die Kundendaten auszulesen.

5. Haftung und Verfügbarkeit

(1) Kerkaporta ist bemüht, eine durchgängige Verfügbarkeit des Services zu gewährleisten, ist jedoch jederzeit zur Durchführung von Wartungsarbeiten berechtigt. Kerkaporta haftet nicht für Störungen und/oder Schäden, falls der Service nicht oder nur teilweise funktionsfähig bzw. erreichbar ist.

(2) Wartungsarbeiten werden wenn möglich, in den Nachtstunden, wo meist keine oder sehr wenige Personen den Service nutzen, durchgeführt.

(3) Als Auftragsverarbeiter ist die Kerkaporta IT Security GmbH nicht für die gesetzeskonforme Erfüllung der Registrierungspflicht verantwortlich. Diese liegt jederzeit beim Betreiber des jeweiligen (Gastro-)Betriebes.

(4) Für verlorene oder vergessene Zugangsdaten und/oder Passwörter wird ebenfalls keine Haftung übernommen.

(5) Die Haftung für Folgeschäden und für entgangenen Gewinn ist ausgeschlossen.

(6) Kerkaporta betreibt die Webanwendung auf Servern der Firma Hetzner Online GmbH in Deutschland. Diese befinden sich dementsprechend in einem Rechenzentrum in Nürnberg und sind physisch geschützt.

(7) Es werden stündliche Backups des Servers angefertigt, welche 10 Tage aufbewahrt werden. Somit ist auch sichergestellt, dass die Löschfristen ebenfalls beim Backupsystem eingehalten werden.
(8) Im Falle eines Komplettausfalls des Rechenzentrums der Firma Hetzner Online GmbH in Nürnberg kann der Server in einem zweiten Rechenzentrum in Falkenstein bzw. Helsinki hochgefahren werden.
(9) Die Leistung des Servers kann jederzeit erhöht werden, um die Verfügbarkeit bei hohen Belastungen sicherzustellen.
(10) Die Software selbst wird mit Hilfe einer Versionsverwaltung für Softwareprojekte (GITLAB) entwickelt und kann dadurch bei Fehlern jederzeit auf eine vorherige Version zurückgesetzt werden.
(11) Um Fehler im Vorhinein zu vermeiden, wird jeder Release mehrfach auf Testsystemen mit Testdaten automatisiert und teilweise manuell getestet und erst nach Freigabe in das Produktivsystem gespielt.

Auftragsverarbeitung zwischen

Kerkaporta IT Security GmbH
Anastasius-Grün-Gasse 17/17, 1180 Wien

(folgend Auftragnehmer)

und

Ersteller des QR-Codes

(folgend Auftraggeber)

1. GEGENSTAND DER VEREINBARUNG

(1) Beide Vertragspartner verpflichten sich, die geltenden datenschutzrechtlichen Bestimmungen, insbesondere die Vorschriften des Datenschutzgesetzes (DSG) und der Datenschutzgrundverordnung (DSGVO) einzuhalten.
(2) Gegenstand dieser Vereinbarung ist die Durchführung folgender Aufgaben: Verarbeitung von personenbezogenen Daten der Gäste des Betriebes zur Kontaktverfolgung eines Covid-19-Verdachtsfalles. (EasyTrace Covid-19 Gästebuch)
(3) Folgende Daten werden verarbeitet: Daten der Gäste: Name, Adresse, Kontaktdaten (E-Mail bzw. Telefon), Tischnummer, Zeitstempel, Ansprechperson, Kontaktdaten (E-Mail, Telefon)

2. ALLGEMEINES

(1) Das Gästebuch verwendet Ende-zu-Ende Verschlüsselung, um ein Maximum an Datenschutz zu gewährleisten.
(2) Die Daten der Gäste werden am Gerät des Gastes Ende-zu-Ende verschlüsselt und erst danach zum Auftragnehmer gesendet. Dieser speichert somit nur verschlüsselte Daten. Auf die unverschlüsselten Daten hat der Auftragnehmer keinen Zugriff.
(3) Nur der Zeitstempel der Eintragung wird unverschlüsselt gespeichert, um die Löschfrist von 28 Tagen gewährleisten zu können.
(4) Die verschlüsselten Daten der Gäste werden dem Auftraggeber nur freigegeben, wenn dieser nachweislich von der Gesundheitsbehörde aufgefordert wurde, die Daten der Gäste zum Zweck des Contact-Tracings den Behörden zu übermitteln.
(5) Der Auftragnehmer übernimmt keinerlei Verantwortung für die Richtigkeit der Daten, welche vom Gast eingetragen wurden.
(6) Die Daten der Gäste kann nur der Auftraggeber mit den generierten Passwörtern, nach Freigabe des Auftragnehmers, lesen. (nähere Informationen siehe: www.easytrace.at)

(7) Verliert oder vergisst der Auftraggeber die ihm zugewiesenen Passwörter, ist kein Zugriff auf die Daten möglich. Für etwaige Folgeschäden dadurch ist der Auftragnehmer nicht haftbar.

3. DAUER DER VEREINBARUNG

(1) Die Dauer dieser Vereinbarung entspricht der Laufzeit des abgeschlossenen Vertrages und endet mit Ende der gesetzlichen Verpflichtung der Erhebung von Kontaktdaten.

4. PFLICHTEN DES AUFTRAGNEHMERS

(1) Der Auftragnehmer verpflichtet sich, Daten und Verarbeitungsergebnisse ausschließlich im Rahmen dieser Vereinbarung zu verarbeiten. Erhält der Auftragnehmer einen behördlichen Auftrag, Daten des Auftraggebers herauszugeben, so hat er - sofern gesetzlich zulässig - den Auftraggeber unverzüglich darüber zu informieren und die Behörde an diesen zu verweisen. Desgleichen bedarf eine Verarbeitung der Daten für eigene Zwecke des Auftragnehmers eines schriftlichen Auftrages.

(2) Der Auftragnehmer erklärt rechtsverbindlich, dass er alle mit der Datenverarbeitung beauftragten Personen vor Aufnahme der Tätigkeit zur Vertraulichkeit verpflichtet hat oder diese einer angemessenen gesetzlichen Verschwiegenheitsverpflichtung unterliegen. Insbesondere bleibt die Verschwiegenheitsverpflichtung der mit der Datenverarbeitung beauftragten Personen auch nach Beendigung ihrer Tätigkeit und Ausscheiden beim Auftragnehmer aufrecht.

(3) Der Auftragnehmer erklärt rechtsverbindlich, dass er alle erforderlichen Maßnahmen zur Gewährleistung der Sicherheit der Verarbeitung nach Art 32 DSGVO ergriffen hat.

- Ende-zu-Ende Verschlüsselung der personenbezogenen Daten
- 4-Augen-Prinzip (nähere Informationen siehe: www.easytrace.at)
- Stündliche Backups der Daten
- Zugriffsberechtigungen am Server
- Sicherheitsüberprüfung der Anwendung (Pentest) von einer externen Firma
- TOMs Hetzner: https://docs.hetzner.com/de/general/general-terms-and-conditions/data-privacy-faq/

(4) Der Auftragnehmer unterstützt den Auftraggeber bei der Einhaltung der in den Art 32 bis 36 DSGVO genannten Pflichten (Datensicherheitsmaßnahmen, Meldungen von Verletzungen des Schutzes personenbezogener Daten an die Aufsichtsbehörde, Datenschutz-Folgeabschätzung, vorherige Konsultation). Benachrichtigung der von einer Verletzung des Schutzes personenbezogener Daten betroffenen Person ist dem Auftragnehmer alleine nicht möglich, da dieser die Daten ohne den Auftraggeber nicht entschlüsseln kann.

(5) Der Auftragnehmer ist nach Beendigung dieser Vereinbarung verpflichtet, alle Verarbeitungsergebnisse und Unterlagen, die Daten enthalten, zu vernichten.

(6) Der Auftragnehmer hat den Auftraggeber unverzüglich zu informieren, falls er der Ansicht ist, eine Weisung des Auftraggebers verstößt gegen Datenschutzbestimmungen der Union oder der Mitgliedstaaten.

4. ORT DER DURCHFÜHRUNG DER DATENVERARBEITUNG

(1) Alle Datenverarbeitungstätigkeiten werden ausschließlich innerhalb der EU bzw. des EWR durchgeführt.

5. UNTERAUFTRAGSVERHÄLTNISSE

(1) Der Auftragnehmer nimmt für die Verarbeitung von Daten im Auftrag des Auftraggebers Leistungen von Dritten in Anspruch, die in seinem Auftrag Daten verarbeiten („Unterauftragnehmer“).
(2) Der Auftragnehmer darf Unterauftragnehmer nur nach vorheriger ausdrücklicher schriftlicher bzw. dokumentierter Zustimmung des Auftraggebers beauftragen.
(3) Mit nachfolgenden Unternehmen bestehen bereits zum Vertragsschluss Unterauftragsverhältnisse:
    a. Hetzner Online GmbH, Industriestr. 25, 91710 Gunzenhausen, Deutschland – Server Hosting in Nürnberg und Falkenstein (Deutschland).

6. RÜCKGABE ODER LÖSCHUNG PERSONENBEZOGENER DATEN

(1) Die personenbezogenen Daten, welche im Zuge der Gästeregistrierung im EasyTrace Covid-19 Gästebuch verarbeitet werden, werden 28 Tage verschlüsselt gespeichert und danach automatisch gelöscht.
(2) Nach Abschluss der Erbringung der Verarbeitungsleistungen ist der Auftragnehmer verpflichtet, alle personenbezogenen Daten nach Wahl des Auftraggebers entweder zu löschen oder zurückzugeben, sofern nicht nach europäischen oder nationalen Vorschriften eine Verpflichtung zur Speicherung der personenbezogenen Daten besteht.
(3) 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.