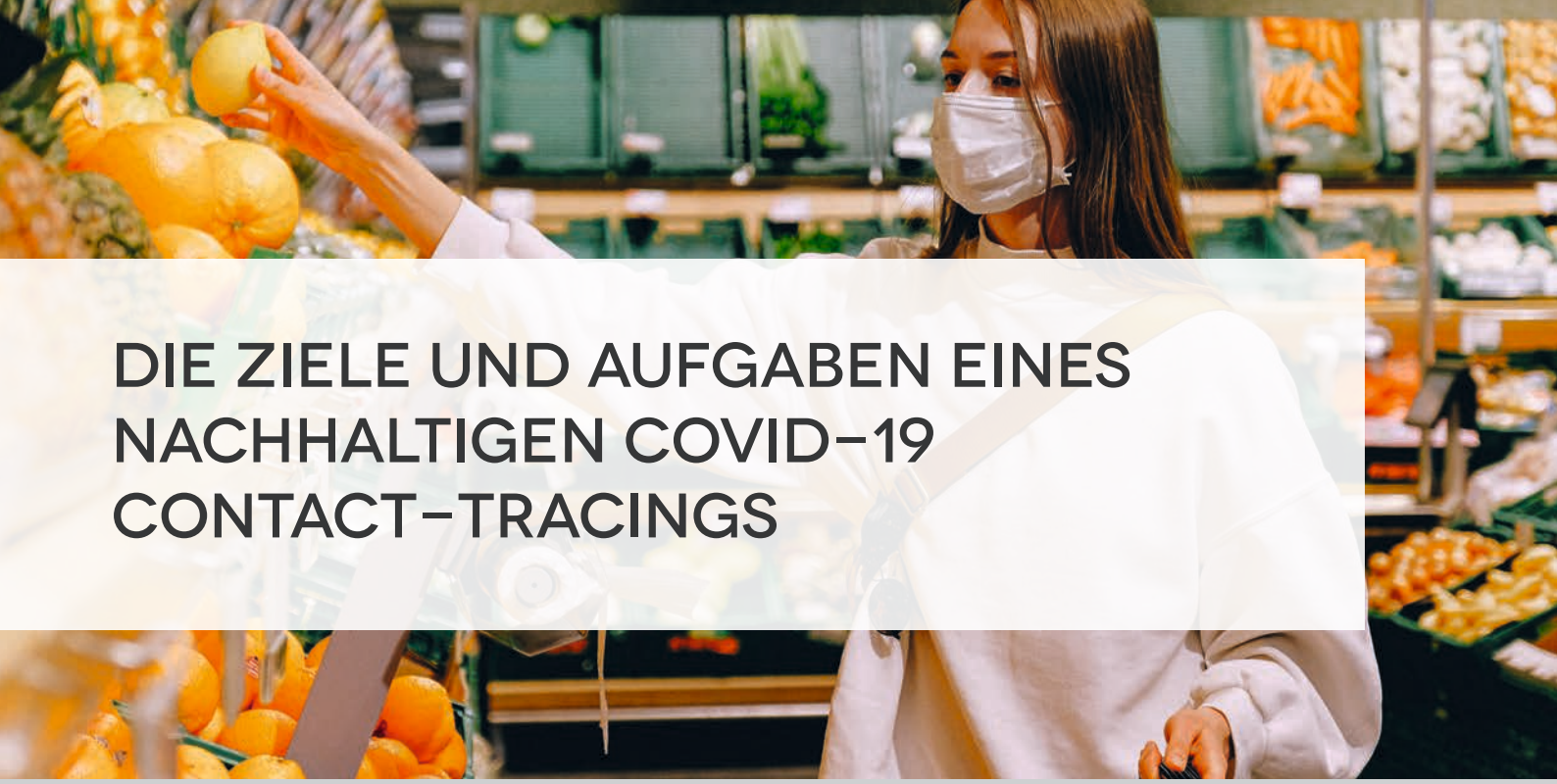
MSITEC

CONTACT-TRACING

BASIEREND AUF DEM DIGITALEN COVID-19 PASSPORT

MSITEC



DIE ZIELE UND AUFGABEN EINES NACHHALTIGEN COVID-19 CONTACT-TRACINGS

1. Die Registrierung der Gäste / Kunden muss unter klar definierten DSGVO-konformen Regeln durchgeführt werden. Hierbei stehen die Gäste- / Kundendaten nicht im Marketing Fokus der Betriebe, sondern NUR im Fokus der Pandemie-Bekämpfung.

2. Das Contact-Tracing muss eine effiziente Lösung zur Erfüllung der gesetzlichen Vorgaben bieten,

   aber

3. gleichzeitig eine optimierte und automatisierte Zusammenarbeit & Partnerschaft zwischen den Betrieben und den Gesundheitsbehörden ermöglichen.

4. Es bedarf einer Win-2-Win Konstellation für Betriebe, Behörden und vor allem den Gästen und Kunden.

5. Aufbau einer Plattform nach dem Prinzip „Eine für Alle“. Dies umfasst alle Betriebe aus Hotellerie, Gastronomie, Handel und Event-Veranstaltungen ***PLUS*** die Gesundheitsbehörden, die sich im Infektionsfall um das Contact-Tracing und die notwendigen Quarantäne-Maßnahmen kümmern müssen.

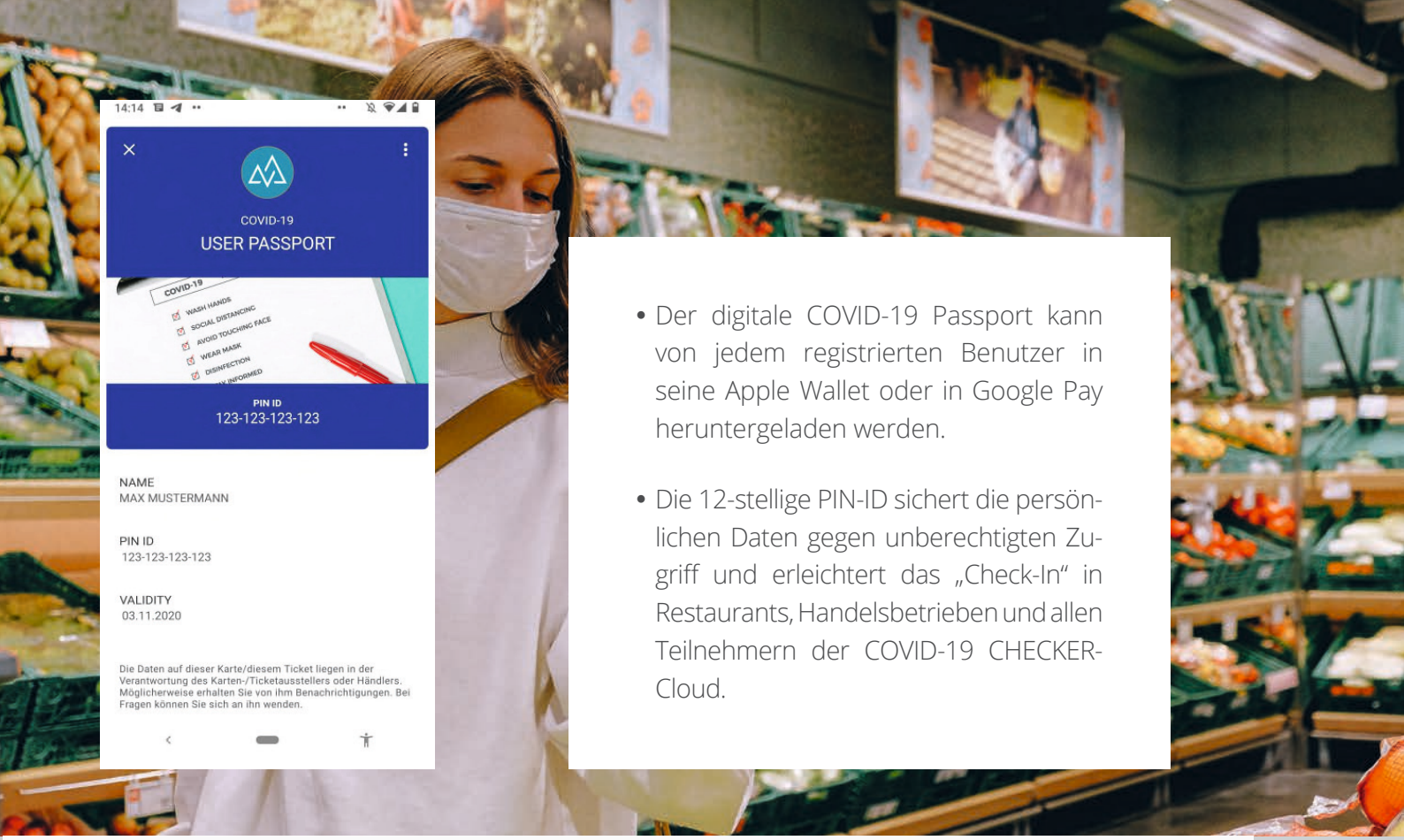
Die **Grundidee** ist, dass die Gesundheitsbehörde im Infektionsfall keine Listen (weder Papier noch Excel-Format) erhält und abtelefonieren muss.

Es muss auch kein aufwendiger Datenaustausch über teure Schnittstellen zwischen Betrieb und Behörde stattfinden, ist aber optional möglich wenn gewünscht.

Sobald der Betrieb Daten auf Anfrage freigegeben hat, greift die Gesundheitsbehörde mit eigenen gesicherten Benutzer-Accounts automatisch auf die Daten zu.

Die Erst-Benachrichtigung der Gäste/ Kunden erfolgt automatisiert durch den Betrieb.

Zeit ist nicht nur Geld
SONDERN rettet Leben!



- Der digitale COVID-19 Passport kann von jedem registrierten Benutzer in seine Apple Wallet oder in Google Pay heruntergeladen werden.
- Die 12-stellige PIN-ID sichert die persönlichen Daten gegen unberechtigten Zugriff und erleichtert das „Check-In“ in Restaurants, Handelsbetrieben und allen Teilnehmern der COVID-19 CHECKER-Cloud.

COVID-TRACING MIT DEM DIGITALEN COVID-19 PASSPORT

- Die Kombination aus PIN-ID und individueller Smartphone ID ermöglicht Check-In und Check-Out über den selben QR-Code und ist damit wesentlich leichter und sicherer zu verwenden als gängige Online-Apps, die auf Basis von Cookies die Re-Authentifizierung durchführen.
- Bei Vorab-Registrierung über PC oder Tablet kann der Benutzer den digitalen COVID-19 Passport auch in der analogen Variante auf Papier ausdrucken und somit wird das Check-In und Check-Out auch ohne Smartphone möglich.

COVID REGISTRIERUNG MIT HÖCHSTEM SICHERHEITSLEVEL DURCH PIN ID IM COVID-19 PASSPORT:

Kunde checkt mit Smartphone via QR-Code ein

Die datenschutzrechtlich relevante Authentifizierung erfolgt über die PIN-ID auf dem digitalen COVID-19 Passport, der im „Wallet“ des Smartphones hinterlegt wird.

DSGVO Konformität wird durch Registrierung und Verwendung eines persönlichen Pin-Codes sichergestellt.

Kein Cookie notwendig!

Erst-Registrierung wird empfohlen über eine dedizierte Registrierungsseite mit Double-Opt-In Bestätigung und Vergabe des digitalen COVID-19 Passports.

“Einmal” - Gäste/Kunden können sich auch beim ersten QR-Code Scan registrieren. Sie müssen den Double-Opt-In innerhalb von 48 Stunden nach Erstregistrierung nachholen über Ihre E-Mail-Adresse.

Zwangs-Logout nach Ende der sogenannten „Kill-time“, spätestens zu Betriebsschluss

Verlängerung individuell über den selben QR-Code wie beim Check-Out per Smart Phone möglich.

Reguläres Check-Out erfolgt am Ausgang / Verlassen des Betriebs über QR-Code und PIN-Eingabe.

Der Kunden-Record ist bei dem Betrieb für 30 Tage mit seiner Aufenthaltsdauer erfasst.
Der Aufenthalt wird gemäß DSGVO Erklärung automatisch nach Ablauf der Fristen gelöscht.

WARUM DER DIGITALE COVID-19 PASSPORT FÜR DAS CONTACT-TRACING SO WICHTIG IST.

1. Die Registrierung für den digitalen COVID-19 Passport mit Double-Opt-In Authentifizierung sichert damit einen geprüften Datenbestand der registrierten Besucher und Kunden schon vor dem ersten Check-In.

2. Der Gast/Kunde muss sich nur einmal für das „Contact-Tracing“ registrieren. Mit der PIN-ID des digitalen COVID-19 Passports ist eine “Beglaubigung“ seiner Identität jederzeit möglich.

3. Der digitale COVID-19 Passport in der Apple Wallet oder über Google Pay ist ein attraktives Medium um sich schnell, sicher und einfach zu identifizieren.

WIN-2-WIN KONZEPT FÜR BETRIEBE UND BEHÖRDEN

WIE PROFITIEREN DIE GESUNDHEITSBEHÖRDEN VON DER REGISTRIERUNG IN DEN BETRIEBEN ÜBER DEN DIGITALEN COVID-19 PASSPORT?

Das Gesundheitsamt erfasst über das Extranet der COVID-19 CHECKER-CLOUD die PIN-ID des Covid-19 infizierten Personen (= Patient 0) und schränkt dabei den Zeitraum der Suche ein.

Die Abfrage erfolgt an die zentrale Datenbank des COVID-19 CHECKERS standort-unabhägig.

Die Abfrage ermittelt Registrierungen für den abgefragten Zeitraum des Patienten 0. Diese Abfrage weist nur den Registrierungs-Status und die Anzahl der Registrierungen aus, nicht die Standorte oder die Betriebe.

Das Gesundheitsamt erhält alle Kontaktdaten der direkten Kontakte (Kontakt-Level A) und kann diese auswerten, weiterreichen (Zuständigkeitswechsel) bzw. direkt kontaktieren.

MANUELL MODUS

AUTO MODUS

Der Betrieb erhält die Aufforderung zur Datenfreigabe. Der Betrieb legt beim Setup seines Accounts fest, ob er Aufforderungen zur Datenfreigabe manuell/individuell beantwortet oder automatisch nach Eingang freigibt.

Jetzt erfolgt parallel zur Freigabe der Daten die E-Mail Benachrichtigung an den Kunden durch den Betrieb.

Der Betrieb legt beim Setup seines Accounts fest, ob er Kunden und Besucher manuell oder automatisiert über den Status eines Infektionsfalles informiert.

INFEKTIONSKETTEN VERFOLGUNG ÜBER E-MAIL (PHASE 2)

Direkte Kommunikation zwischen Betrieb und Kunden / Besucher ist die schnellste Option, die auch datenschutzrechtlich unproblematisch eingestuft wird:

ZERTIFIZIERUNGEN
UNSERER SICHEREN RECHENZENTREN

TÜV-27001
Zertifizierung für Informationssicherheit

Die internationale Norm ISO/IEC 27001 Information technology – Security techniques – Information security management systems – Requirements spezifiziert die Anforderungen für Herstellung, Einführung, Betrieb, Überwachung, Wartung und Verbesserung von Sicherheitsmechanismen sowie eines dokumentierten Informationssicherheits-Managementsystems unter Berücksichtigung der IT-Risiken innerhalb der gesamten Organisation.

TÜV- 9001
Zertifizierung für Qualitätsmanagement

Die Norm DIN ISO 9001 legt die Anforderungen an ein Qualitätsmanagementsystem fest, die von Unternehmen umzusetzen sind, um die Kundenanforderungen sowie weitere Anforderungen an die Produkt- bzw. Dienstleistungsqualität zu erfüllen.

Alle für den COVID-19 CHECKER freigegebenen Rechenzentren werden von dem MSITEC Partner Plutex GmbH in Bremen betrieben.

Die Plutex GmbH ist gemäß ISO 27001 und ISO 9001 vom TÜV Süd zertifiziert.

DSGVO KONFORME BEHANDLUNG DER PERSONENDATEN

CM STUDIO .COVID-19 CHECKER BIETET EINE SICHERE DATENÜBERMITTLUNG UND EINEN DSGVO-KONFORMEN WORKFLOW.

WIE WERDEN DIE DATEN IN DER CLOUD ABGELEGT?

1. Alle Registrierungsdaten der Benutzer werden verschlüsselt in der Datenbank abgelegt. Lediglich die anonyme PIN-ID ist für die Datenbankanfragen freigegeben.
2. Der Betrieb, der mit dem Kunden / Gast über eine Geschäftsbeziehung verfügt, kann die Daten im Rahmen der Besuchsverfolgung einsehen um somit die Korrektheit der Angaben überprüfen.
3. Die zuständige Gesundheitsbehörde sieht grundsätzlich keine Personendaten, ohne die vorherige Zustimmung des Betriebes erhalten zu haben. Die Identifizierung erfolgt über die PIN-ID des digitalen COVID-19 Passports.
4. Der CLOUD-Betreiber hat keinen Zugriff auf die Daten der Betriebe und kann lediglich bei einer Supportanfrage durch den anfragenden Betrieb temporär freigeschaltet werden.

WANN UND WIE KÖNNEN DIE DATEN EXPORTIERT WERDEN UND AN DRITTSYSTEME ÜBERGEBEN WERDEN?

1. Die Betriebe können Besucherdaten einsehen und protokolliert nach den Grundsätzen der Revisionssicherheit anpassen (z.B. bei falscher Namensangabe des Besuchers).
2. Die zuständige Gesundheitsbehörde kann Daten nach Freigabe des Betriebes exportieren mittels CSV- oder XML-Download. Hier findet die Authentifizierung über das Passwort des Benutzers in der Gesundheitsbehörde statt.
3. Bei einem automatisierten Datenaustausch via Schnittstelle zu Drittsystemen der Gesundheitsbehörden findet eine Verschlüsselung der Schnittstelle über ein Public-/Private-Key Verfahren statt, dass für jede einzelne Schnittstelle die jeweilige Gesundheitsbehörde identifiziert.

MSITEC – DIE ONLINE EXPERTEN

Schaarschmidt Hard- & Software e.K.

MSITEC

Paulinenweg 3
51149 Köln

T +49 (0)2203 911 33 100
F +49 (0)2203 911 33 99
www.msitec.de