Automatisches Einlassmanagement

Merkblatt Datenschutz für Anwender

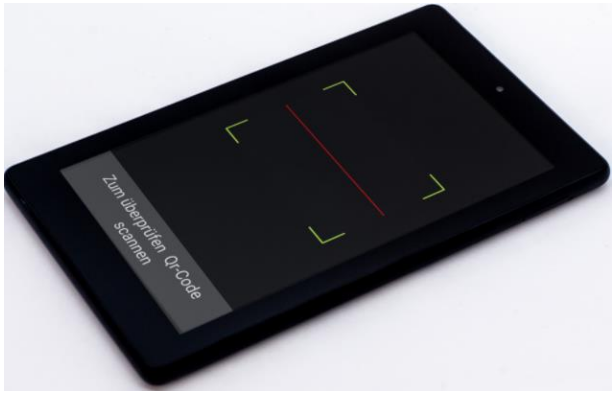
Inhalt

Die Anwendung - ‚2G-Ampel‘

Die von MyTech entwickelte Software Cov-Check (u. a. als 2G Ampel bekannt) bietet ein automatisiertes Einlassmanagement und ermöglicht eine schnelle und einfache Kontrolle von digitalen Impf-, Genesenen-, PCR- und Schnelltestzertifikaten, welche nach dem Greenpass-Standard erstellt wurden. Die dabei durchgeführte technische Prüfung ist durch die jeweilige Coronaverordnung der teilnehmenden Mitgliedsstaaten und insbesondere durch die Coronaverordnung der Bundesländer gefordert.

Ebenfalls besteht durch eine Dokumentationsfunktion die Möglichkeit der Kontaktnachverfolgung auf Basis der in den jeweiligen Zertifikaten enthaltenen Daten.

Die 2G-Ampel überprüft in Sekundenschnelle die Gültigkeit der Dokumente – kontaktlos, sicher und ohne zusätzlichen Personalbedarf. Gleichzeitig findet eine automatische Kontaktverfolgung statt, wodurch zusätzliche Arbeitsschritte und doppeltes Scannen entfallen.



Die Ampel erkennt alle europaweit geltenden Standards der **digitalen Test-, Impf- und Genesenen-Zertifikate**. Sie ist kompatibel mit dem digitalen Impfzertifikat, dem EU-Zertifikat sowie der Corona-Warn-App.

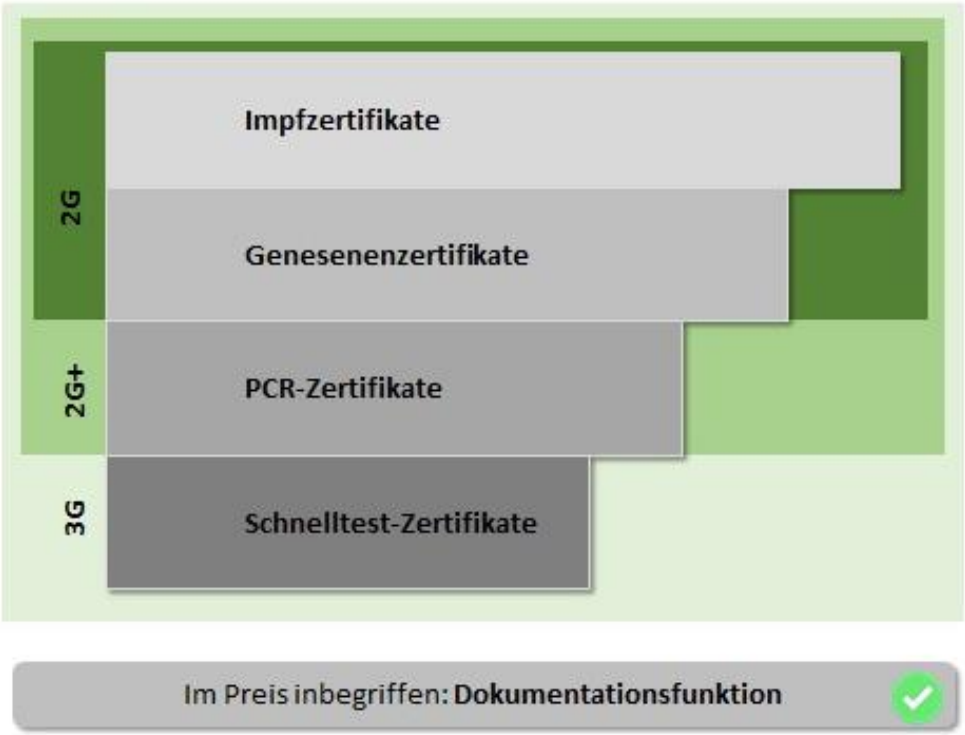
Wird ein gültiger QR-Code an das Lesegerät gehalten, schaltet die Ampel auf Grün und zeigt durch ein optisches und akustisches Signal die erfolgreiche Prüfung an.

Ein gelbes Signal erscheint, wenn der Nachweis nicht ausreichend ist oder wenn die Wartezeit bis zur vollständigen Immunisierung nicht eingehalten wurde.

Ein rotes Signal erscheint, wenn ein ungültiges oder abgelaufenes Zertifikat vorliegt.

Kundenindividuelle Anpassung

Um möglichst allen Anforderungen an ein Einlassmanagement gerecht werden zu können, hat der Anwender die Möglichkeit folgende Konfigurationen am System selbst vorzunehmen:



Ebenfalls können die jeweilige Landessprache sowie Dauer der Speicherung von Daten in den Einstellungen vorgenommen werden.

Alle auf Basis der COV-Check-Software entwickelten Produkte sind nur für den Einsatz im gewerblichen Umfeld vorgesehen und werden nicht an private Endkunden verkauft.

Datenschutzinformationen

Um den Kunden rechtliche Sicherheit beim Einsatz der Lösung zu geben, hat die MyTech GmbH die Erstellung dieser datenschutzrechtlichen Expertise beauftragt. Die Einschätzung wurde durch einen unabhängigen, externen und zertifizierten Datenschutzbeauftragten durchgeführt.

Ebenfalls wurde eine Empfehlung für die Anleitung und Information der Nutzer erarbeitet, die es ermöglichen, die ‚Scannenden' gemäß DS-GVO zu informieren und etwaige Unsicherheiten bei der Nutzung zu verringern.

Das digitale COVID-Zertifikat der EU

Das Zertifikat ist ein digitaler Nachweis dafür, dass eine Person gegen COVID-19 geimpft bzw. negativ auf Corona getestet wurde oder von Corona genesen ist.

Das digitale Zertifikat soll in erster Linie den sicheren und freien Personenverkehr in der EU erleichtern.

Die Mitgliedsstaaten können das COVID-Zertifikat aber auch für den Zutritt zu Veranstaltungen oder Einrichtungen einsetzen. Dafür gibt es jedoch keine EU-Vorschriften.

In solchen Fällen sollte das EU-Land sicherstellen, dass das digitale COVID-Zertifikat der EU anerkannt wird. So wird gewährleistet, dass EU-weit ein einziges Zertifikat genügt.

Beachtung sonstiger Verordnungen zur Datenerhebung

Die 2G-Ampel überprüft nur die Gültigkeit des entsprechenden Zertifikats (nicht die Identität der Person). Da es keine einheitliche Europa- oder auch nur deutschlandweite Verordnungen / Vorschriften gibt, müssen die jeweils gültigen Corona-Verordnungen der jeweiligen Region durch den Anwender selbst verfolgt und beachtet werden. Darüberhinausgehende Daten sind ggf. separat zu erfassen. Die Software führt keine Identitätsprüfung durch.

Welche Daten enthält das Zertifikat? Sind die Daten sicher?

Das digitale COVID-Zertifikat der EU enthält notwendige zentrale Informationen wie Name, Geburts- und Ausstellungsdatum sowie Angaben zu Impfstoff/Test/Genesung und ein individuelles Erkennungsmerkmal etc. Der Anwender muss in den Systemeinstellungen selbst festlegen, welche Daten er erheben bzw. speichern möchte und darf und wie lange diese gespeichert werden sollen.
Die Zertifikate enthalten nur eine begrenzte Anzahl notwendiger Daten, daher kann es im Anwendungsfall eventuell notwendig sein, Daten separat zu erheben. Das System überprüft lediglich die Gültigkeit des jeweiligen Zertifikates. Eine Identitätsprüfung kann daher nicht gewährleistet werden.

Anleitung und Datenschutzhinweise für den Nutzer

Da Daten gespeichert werden, die personenbezogen sind und auch Gesundheitsdaten beinhalten, ist die Information der Nutzer zum Datenschutz vorgeschrieben.
So empfiehlt es sich, **gut sichtbar** beim Lesegerät eine Nutzerinformation anzubringen, aus der die relevanten Informationen hervorgehen und es dem Nutzer ermöglicht wird, **VOR** der Benutzung der 2G-Ampel über die Nutzung zu entscheiden.

Beispiel:

PRÜFUNG DER GÜLTIGKEIT DES COVID-SCHUTZES
INFORMATION ZUR NUTZUNG DER 2G-AMPEL

Prüfung – Präsentieren Sie ihr Zertifikat der Ampel

WENN DIE AMPEL NICHT ‚GRÜN' WIRD, WENDEN SIE SICH AN EINEN MITARBEITER

Datenschutzrechtlich verantwortlich

Firmenname / Institution
Anschrift 1
Anschrift 2
Anschrift 3

Vertreten durch:
Verantwortlicher (Geschäftsführer/-in, Inhaber, Vorstand, etc)

Kontakt:
T: +49 (00000) 66666666
F: +49 (00000) 77777777
vorne@hinten.de
www.website.de

Zweck der Datenerfassung
Einhaltung der Coronaverordnung von z.B. des Landes Baden-Württemberg

Berechtigung der Datenerfassung
DSGVO Art. 6 Abs. 1 lit. B) und §4 BDSG (neu) – berechtigtes Interesse
DSGVO Art. 9 Abs. 2 lit. b) erhebliches öffentliches Interesse

Erfasste Daten
Vorname, Nachname, Geburtsdatum, Status, Datum / Uhrzeit von Check-In und Check-Out, Ausstellungs- und Gültigkeitsdatum des Zertifikats, bei Schnell- und PCR-Tests zusätzlich Email, Telefon, Testergebnis, Uhrzeit und Datum des Tests,

Speicherdauer der Daten
werden nach dem Erreichen der gemäß Coronaverordnung vorgeschriebenen Speicherdauer automatisch gelöscht.

LUCA CHECK-IN

DAS-ITSEC.DE

Dieses Beispiel muss auf die entsprechenden örtlichen Gegebenheiten und regionalen Vorschriften angepasst werden.

Datenschutzrechtliche Bewertung

Nach der detaillierten Analyse des Verfahrens und der nachfolgenden Verfahrensdokumentation mit Riskobewertung bestehen bei der Anwendung der auf Cov-Check basierenden Produkte aus Sicht der Verfasser keine datenschutzrechtlichen Bedenken.

Da die Daten nur zum Zwecke des rechtlich vorgeschriebenen Nachweises genutzt werden und auch nur in diesem Rahmen eine Übertragung/Weiterleitung erfolgt, ist hier keine Beeinträchtigung der Betroffenen zu erwarten.

Verfahrensbeschreibung

Zwecke der Verarbeitung (Art. 30 Abs. 1 S. 2 lit b))	Erleichterung / Beschleunigung der Kontrolle der Gültigkeit von **digitalen Test-, Impf- und Genesenen-Zertifikate** im Rahmen von COVID19
Name des eingesetzten Verfahrens / der Software	2G-Ampel Appliance auf Android-Basis mit der Applikation COV-CHECK
Rechtmäßigkeit der Verarbeitung	Einhaltung der Pandemie- und Corona-Verordnungen in Verbindung mit der DS-GVO Art. 6 Abs. 1 lit. f) berechtigtes Interesse Gesundheitsschutz: die Verarbeitung ist zur **Wahrung der berechtigten Interessen des Verantwortlichen oder eines Dritten erforderlich**, sofern nicht die Interessen oder Grundrechte und Grundfreiheiten der betroffenen Person, die den Schutz personenbezogener Daten erfordern, überwiegen, insbesondere dann, wenn es sich bei der betroffenen Person um ein Kind handelt. Art. 9 Abs. 2 lit. b) erhebliches öffentliches Interesse Die Verarbeitung ist auf der Grundlage des Unionsrechts oder des Rechts eines Mitgliedsstaates, das in angemessenem Verhältnis zu dem verfolgten Ziel steht, den Wesensgehalt des Rechts auf Datenschutz wahrt und angemessene und spezifische Maßnahmen zur Wahrung der Grundrechte und Interessen der betroffenen Person vorsieht, **aus Gründen eines erheblichen öffentlichen Interesses erforderlich**

Beschreibung der Kategorien betroffener Personen (Art. 30 Abs. 1 S. 2 lit. c) und Schutzbedarfs-feststellung	**Betroffene Personen** alle Nutzer der auf COV-CHECK basierenden Produkte **Erhobene Daten** Persönliche Daten – Daten des Zertifikats: Vorname, Nachname, Geburtsdatum, Impf- bzw. Genesenenstatus, Datum / Uhrzeit von Check-In und Check-Out, Ausstellungs- und Gültigkeitsdatum des Zertifikats, bei Schnell- und PCR-Tests zusätzlich E-Mail, Telefon, Testergebnis, Uhrzeit und Datum des Tests, Adresse **Schutzbedarfsfeststellung** Da die Daten nach Art. 9 der DS-GVO Gesundheitsdaten umfassen, haben sie einen hohen Schutzbedarf.
Risikobewertung	☐ kein oder geringes Risiko der Verarbeitung: normaler Schutzbedarf für von der Verarbeitung betroffene Personen ☐ normales Risiko der Verarbeitung: normaler Schutzbedarf für von der Verarbeitung betroffene Personen ☒ hohes Risiko der Verarbeitung: hoher Schutzbedarf für von der Verarbeitung betroffene Personen ☐ sehr hohes Risiko der Verarbeitung: sehr hoher Schutzbedarf für von der Verarbeitung betroffene Personen Personenbezogene Daten, deren unsachgemäße Handhabung eine betroffene Person in ihrer gesellschaftlichen Stellung oder in ihren wirtschaftlichen Verhältnissen beeinträchtigen könnte („Ansehen“)

<table>
<tr><td>Beurteilung der Eintrittswahrscheinlichkeit</td><td>☐ Vernachlässigbar: Für die ausgewählte Risikoquelle scheint es nicht sehr wahrscheinlich zu sein, eine Schwachstelle eines unterstützenden Wertes auszunutzen, um eine Bedrohung eintreten zu lassen

☒ Eingeschränkt: Für die ausgewählte Risikoquelle scheint es schwierig zu sein, eine Schwachstelle eines unterstützenden Wertes auszunutzen, um eine Bedrohung eintreten zu lassen

☐ Signifikant: Für die ausgewählte Risikoquelle scheint es möglich zu sein, eine Schwachstelle eines unterstützenden Werts auszunutzen, um eine Bedrohung eintreten zu lassen

☐ Maximal: Für die ausgewählte Risikoquelle scheint es einfach zu sein, eine Schwachstelle eines unterstützenden Wertes auszunutzen, um eine Bedrohung eintreten zu lassen</td></tr>
<tr><td>Erforderlichkeit einer Datenschutz-folgeabschätzung</td><td>Abgleich mit Einstufung der Datenschutzkonferenz (DSK, Positivliste Version 1.1 vom 17.10.2018):

<table>
<tr><td>Vertrauliche oder höchst persönliche Daten (Bildaufzeichnung)</td><td>nicht betroffen</td></tr>
<tr><td>Daten zu schutzbedürftigen Betroffenen</td><td>betroffen</td></tr>
<tr><td>Datenverarbeitung in großem Umfang</td><td>betroffen</td></tr>
<tr><td>Systematische Überwachung</td><td>nicht betroffen</td></tr>
<tr><td>Innovative Nutzung oder Anwendung neuer technologischer oder organisatorischer Lösungen</td><td>nicht betroffen</td></tr>
<tr><td>Bewerten oder Einstufen (Scoring)</td><td>findet nicht statt</td></tr>
<tr><td>Abgleichen oder Zusammenführen von Datensätzen</td><td>erfolgt nicht</td></tr>
<tr><td>Automatisierte Entscheidungsfindung mit Rechtswirkung oder ähnlich bedeutsamer Wirkung</td><td>findet statt – Zutrittsgewährung oder -ablehnung</td></tr>
<tr><td>Betroffene werden an der Ausübung eines Rechts oder der Nutzung einer Dienstleistung bzw. Durchführung eines Vertrags gehindert</td><td>trifft nicht zu</td></tr>
</table>

Vorgabe der DSK zur Erstellung einer DSFA:
Eine DSFA ist immer erforderlich bei hohem oder sehr hohem Risiko in Verbindung mit einer signifikanten oder maximalen Eintrittswahrscheinlichkeit. Eine DSFA ist in separatem Dokument unter Einbindung des DSB zu erstellen.</td></tr>
</table>

	Beurteilung: ☒ DSFA nicht erforderlich ☐ DSFA erforderlich **Begründung:** Es besteht insgesamt ein vernachlässigbares/geringes Risiko eines Zugriffs auf die Daten durch unbefugte Dritte, da folgende Schutzmechanismen eingesetzt werden: - Die Endgeräte sind durch eine Passwort-/PIN-Eingabe vor unbefugtem Zugriff geschützt - Die Geräte sind an kein Netzwerk angebunden - Die Daten werden nach Erreichen der Speicherdauer automatisch gelöscht - Die Geräte sind gegen Diebstahl durch eine Fixierung in der Halterung mit einem Schloss gesichert.
Kategorien von Empfängern, gegenüber denen die personen-bezogenen Daten offengelegt worden sind oder noch werden (Art. 30 Abs. 1 S. 2 lit. d))	☐ Datenübermittlung findet nicht statt und ist auch nicht geplant ☒ Datenübermittlung findet statt
	Die Daten können mittels Exportfunktion extrahiert werden, um sie gemäß der gültigen Coronaregelungen den Kontrollbehörden zur Verfügung zu stellen.
	☒ intern (Zugriffsberechtigte)
	Verantwortliche der anwendenden Institution bzw. von ihnen beauftragte Mitarbeiter
	☒ extern
	Institution/Kontrollbehörden gemäß den jeweils regional gültigen rechtlichen Regelungen / Gesetzen / Corona-Verordnungen (z.B. Ortspolizeibehörde, Gesundheitsamt, …)

Fristen für die Löschung der verschiedenen Datenkategorien (Art. 30 Abs. 1 S. 2 lit. f))	Die Daten werden entsprechend der regional vorgeschriebenen Löschfristen automatisch aus dem System entfernt. Diese müssen in der Anwendung entsprechend erfasst werden. Voreinstellung ist 30 Tage.
Durchführung der Löschung	Automatisch durch die Software
Angewendete technische und organisatorische Maßnahmen	• Passwort-/PIN-Schutz • Automatische Datenlöschung • Keine Netzwerkanbindung (AirGap) • Schutz vor Diebstahl durch integriertes Schloss

Disclaimer / Haftungsausschluss

Die im Dokument hinterlegten Informationen dienen lediglich als Leitfaden für die Integration in das „Datenschutz Management System“. Es wird kein Anspruch auf Vollständigkeit sowie Richtigkeit erhoben. Auch können Änderungen externer Vorgaben (Pandemiebestimmungen, Änderungen datenschutzrechtlicher Vorgaben oder Rechtsprechung etc.) auf die Richtigkeit der in diesem Dokument hinterlegten Informationen Auswirkungen haben. Dafür übernehmen weder der Systemhersteller noch der Datenschutzbeauftragte eine Haftung oder Gewährleistung.

Der Verantwortliche des die Lösung anwendenden Unternehmens hat im Kontext seines Umfelds die Gültigkeit der hier aufgeführten datenschutzrechtlichen Bewertungen zu prüfen und ggf. weiterführende Maßnahmen durchzuführen.

Impressum

Dieses Dokument wurde erstellt von DAS-ITSEC – Klaus Leukert im Auftrag der MyTech GmbH.

Verantwortlich für den Inhalt:

MyTech GmbH - Vertreten durch Geschäftsführer Kilian Brauchle
Registernummer: HRB 779592 Registergericht: Amtsgericht Stuttgart

Kontakt

MyTech GmbH

Ziegelweg 1/1 Telefon +49 7121 1378657 E-Mail: info@2g-ampel.de
72764 Reutlingen Web www.2g-ampel.de

DAS-ITSEC DATENSCHUTZ UND IT-SECURITY

Klaus Leukert Telefon +49 7123 9435254 E-Mail klle@das-itsec.de
Carl-Benz-Str. 6 Fax +49 7123 9435255 Web www.das-itsec.de
72555 Metzingen Mobil +49 171 8330134

DAS-ITSEC.DE