Factsheet Datenschutz und Datensicherheit

- Datensparsame Erhebung: Digitale Visitenkarte wird auf dem mobilen Endgerät erfasst und verbleibt dort. Für den Check-in werden die je nach Allgemeinverfügung der Bundesländer festgelegten persönlichen Daten ausgewählt und nach Interaktion mit dem Nutzer verschlüsselt übertragen.
- Keine Aktivität im Hintergrund: pass4all arbeitet ausschließlich, wenn der Nutzer dies veranlasst (zum Beispiel durch Klick beim Check-in). Danach kann die App wieder geschlossen werden.
- Schneller und kontaktloser Check-in (Infektionsschutz: weniger Warteschlangen, keine Stifte usw.)
- Verschlüsselte und anonymisierte Speicherung der Daten auf Servern in Deutschland.
- Betreiber erhalten keinerlei Zugriff auf Kundendaten.
- Verifizierte Daten und fälschungssicherer Check-in.
- Durch Anonymisierung ist es nicht möglich, Bewegungsprofile zu erstellen oder Nutzerverhalten zu analysieren.
- Durch Verschlüsselung und Zerlegung des privaten Schlüssels ist es weder für die Veranstalter / Gastronomen (Betreiber) noch für pass4all technisch möglich, die Daten zu entschlüsseln.
- Genaueste Eingrenzung der zu übermittelnden Daten: Die Betreiber grenzen die Daten über Metadaten des Ortes / der Veranstaltung ein (Reihe, Sitzplatz, Tischnummer usw.). Dadurch werden ausschließlich betroffene Datensätze für die Übermittlung ausgewählt. (datensparsam)
- Keinerlei technische Möglichkeit der Datenweitergabe an Dritte (durch Verschlüsselung und Zerlegung des privaten Schlüssels)
- Automatische Löschung der Daten auf dem Server nach Ablauf der Fristen.

Verschlüsselung

- Sichere asymmetrische Verschlüsselung der Nutzerdaten nach Empfehlung des Bundesamtes für Sicherheit in der Informationstechnik (BSI)
  Verschlüsselung: RSA OAEP SHA-512, Schlüssellänge: 4096 Bit / 8192 Bit
- Zusätzlich: Vier-Augen-Prinzip durch Zerlegung des privaten Schlüssels
  Einen Schlüsselteil erhält der jeweilige Betreiber, einen zweiten Teil wird für das Gesundheitsamt verwahrt. Dadurch ist es weder den Betreibern noch pass4all einem anderen Dritten technisch möglich, die Daten zu entschlüsseln. Dies geschieht erst durch Zusammenführung der Schlüsselteile beim Gesundheitsamt.
- Entschlüsselung direkt beim Gesundheitsamt (auf interner Infrastruktur).

Entlastung der Gesundheitsämter

- Direkte digitale Schnittstelle zu den Gesundheitsämtern. (OctoWare TN, CSV-Datei usw.)
- Verifizierte Kontaktdaten (E-Mail-Adresse).
- Es werden durch die o.g. Eingrenzung nur direkt betroffene Nutzerdaten übermittelt.
- Persönliches Kontakttagebuch (Historie) lokal in der App.

pass4all / Betreiber können technisch niemals …

- Persönliche Daten entschlüsseln
- Bewegungsprofile erstellen oder das Nutzerverhalten analysieren
- Daten für andere Zwecke verwenden (kein Zugriff, Daten sind verschlüsselt)

Deutschlandweit im Einsatz seit Anfang September 2020.

pass4all GmbH * Löbtauer Str. 71 * 01159 Dresden * www.pass4all.de * 0351 48 28 70 10