Uniqor UG (haftungsbeschränkt)
Alter Weg 5 · 31199 Diekholzen
Tel. +49 5121 9570590
E-Mail info@uniqor.de
Web www.uniqor.de

Datenschutzerklärung

Fassung 2026-12.23 · gültig ab 05.11.2026 · Prüfsumme 566bdb29f1a4e45f

Diese Datenschutzerklärung gilt einheitlich für alle Angebote der Uniqor UG (haftungsbeschränkt):

- die Website www.uniqor.de mit Kontakt-, Kündigungs- und Widerrufsformular,
- Uniqinvoice (uniqinvoice.de) einschließlich der Unterschrifts-, Zahl- und Freigabeseiten,
- Uniqscreen (www.uniqscreen.de) mit Webanwendung, Player-Apps für Displays und den Apps für iPhone, iPad und Android,
- StampBy (stampby.de) mit Händler-Dashboard, Kundenkarten, Scan-Anwendung und den Apps für iPhone und Android,
- unsere IT-Dienstleistungen wie Betreuung, Fernwartung, Hosting und Datensicherung.

Teil A gilt für alle Angebote. Teil B enthält Ergänzungen für die einzelnen Anwendungen. Teil C fasst Empfänger, Speicherdauer und Ihre Rechte zusammen. Teil D enthält die Hinweise für Karteninhaber von StampBy auf Englisch. Alle Anwendungen verweisen auf diese Fassung unter www.uniqor.de/datenschutz/.

Teil A – Für alle Angebote

1. Verantwortlicher

Uniqor UG (haftungsbeschränkt), vertreten durch den Geschäftsführer Sascha Schöning, Alter Weg 5, 31199 Diekholzen, Deutschland · Amtsgericht Hildesheim HRB 210232 · Telefon +49 5121 9570590 · E-Mail info@uniqor.de · Website www.uniqor.de

Ein Datenschutzbeauftragter ist nicht benannt, weil die Voraussetzungen des § 38 BDSG und des Art. 37 DSGVO nicht vorliegen. Für alle Fragen zum Datenschutz erreichen Sie uns unter den oben genannten Kontaktdaten.

2. Wer ist wofür verantwortlich?

Für unsere Website, für die Konten unserer Kundinnen und Kunden, für Vertrag und Abrechnung sowie für den technischen Betrieb unserer Anwendungen einschließlich der Server- und Sicherheitsprotokolle sind wir Verantwortlicher im Sinne der DSGVO.

Für die Inhalte, die ein Kundenbetrieb in unseren Anwendungen verarbeitet, ist dieser Betrieb Verantwortlicher. Das sind etwa seine Kunden, Belege und Unterschriften in Uniqinvoice, seine Bildschirminhalte in Uniqscreen oder die Kundenkarten seines Geschäfts in StampBy. Dasselbe gilt für Daten auf Systemen, die wir für Kunden betreuen oder hosten. Wir verarbeiten diese Daten als Auftragsverarbeiter nach Art. 28 DSGVO auf Grundlage unserer Vereinbarung zur Auftragsverarbeitung (Anlage zu unseren AGB unter www.uniqor.de/agb/).

Erhalten Sie also eine Rechnung, die mit Uniqinvoice erstellt wurde, unterschreiben Sie ein Angebot über einen Unterschriftslink oder nutzen Sie die Kundenkarte eines Geschäfts, richten Sie Auskunfts- oder Löschwünsche bitte an diesen Betrieb. Er wird Ihnen auf dem Dokument, der Unterschriftsseite oder der Karte genannt. Wir unterstützen ihn bei der Beantwortung und leiten Anfragen, die uns erreichen, unverzüglich weiter.

3. Hosting und Standorte

Unsere Website und Anwendungen laufen auf eigenen Servern, die wir bei der netcup GmbH, Emmy-Noether-Straße 10, 76131 Karlsruhe, angemietet haben und selbst betreiben und administrieren. netcup stellt Hardware, Strom und Netzanbindung bereit und verarbeitet dabei als Auftragsverarbeiter die auf den Servern gespeicherten Daten. Mit netcup besteht ein Vertrag über die Auftragsverarbeitung nach Art. 28 DSGVO.

- Rechenzentrum Wien, Österreich (EU): Website www.uniqor.de, Uniqinvoice, StampBy
- Rechenzentrum Nürnberg, Deutschland (EU): Uniqscreen
- Systeme, die wir für Kunden hosten, je nach Vereinbarung an einem dieser beiden Standorte

Die laufende Datenhaltung findet damit ausschließlich in der Europäischen Union statt. Datenbanken, Zwischenspeicher und Dateispeicher sind von außen nicht unmittelbar erreichbar. Rechtsgrundlage ist Art. 6 Abs. 1 lit. f DSGVO; unser berechtigtes Interesse ist eine sichere, schnelle und effiziente Bereitstellung unserer Angebote. Welche Dienstleister außerhalb der EU einzelne Daten erhalten können, steht in den Ziffern 18 und 19.

4. Server-Protokolle und Schutz vor Angriffen

Beim Aufruf unserer Website und Anwendungen übermittelt Ihr Browser oder Ihre App automatisch Verbindungsdaten. Unsere Webserver verarbeiten dabei IP-Adresse, Datum und Uhrzeit, aufgerufene Adresse, Statuscode, übertragene Datenmenge, Referrer sowie Browser- und Betriebssystemkennung. Das ist nötig, um die Seiten auszuliefern, Fehler zu beheben und Angriffe zu erkennen und abzuwehren. Geheime Kennungen in Adressen, etwa aus Unterschrifts-, Zahl- oder Kartenlinks, entfernen wir vor der Speicherung aus den Protokollen.

- Server in Wien (Website, Uniqinvoice, StampBy): Das Sicherheitsprotokoll enthält die vollständige IP-Adresse und wird spätestens nach 14 Tagen gelöscht. Für die Website führen wir zusätzlich ein Zugriffsprotokoll mit gekürzter IP-Adresse (bei IPv4 ohne die letzten 8 Bit, bei IPv6 ohne die letzten 80 Bit), das ebenfalls nach spätestens 14 Tagen gelöscht wird.
- Server in Nürnberg (Uniqscreen): Im Zugriffsprotokoll wird die IP-Adresse nur gekürzt gespeichert (bei IPv4 die ersten beiden Blöcke, bei IPv6 die ersten 32 Bit). Zugriffs- und Systemprotokolle werden nach spätestens 14 Tagen gelöscht.

Schutzdienst CrowdSec. Auf unseren Servern wertet die Software CrowdSec die Sicherheitsprotokolle aus, um Angriffsmuster wie massenhafte Anmeldeversuche oder Schwachstellensuchen zu erkennen. Auffällige IP-Adressen werden vorübergehend gesperrt. Erkennt CrowdSec einen Angriff, übermittelt der Server die angreifende IP-Adresse, die Art des erkannten Angriffs und den Zeitpunkt an die CrowdSec SAS, Paris, Frankreich. Im Gegenzug erhalten wir eine gemeinsame Sperrliste bekannter Angreifer. Inhalte von Anfragen, Formulardaten oder Zugangsdaten werden nicht übermittelt. Erkannte Angriffe speichert CrowdSec auf unserem Server höchstens 7 Tage. Rechtsgrundlage ist Art. 6 Abs. 1 lit. f DSGVO; unser berechtigtes Interesse ist der Schutz unserer Systeme und der Daten unserer Kundinnen und Kunden vor Angriffen.

Eine Zusammenführung der Protokolle mit anderen Datenquellen findet nicht statt. Rechtsgrundlage der Protokollierung ist Art. 6 Abs. 1 lit. f DSGVO; unser berechtigtes Interesse ist der sichere und stabile Betrieb.

5. Cookies und Speicherung auf Ihrem Endgerät

Wir setzen keine Cookies oder vergleichbaren Techniken zur Analyse, Reichweitenmessung, Werbung oder zum Tracking ein und binden keine solchen Dienste Dritter ein. Ein Cookie-Banner ist deshalb nicht erforderlich. Unsere Website www.uniqor.de setzt überhaupt keine Cookies und speichert nichts auf Ihrem Endgerät.

Die Anwendungen speichern nur, was für ihre Nutzung technisch erforderlich ist, etwa ein Sitzungs-Cookie nach der Anmeldung. Das ist nach § 25 Abs. 2 Nr. 2 TDDDG ohne Einwilligung zulässig. Welche Einträge das im Einzelnen sind, steht in Teil B bei der jeweiligen Anwendung. Sollten wir künftig einwilligungsbedürftige Techniken einsetzen, holen wir vorher Ihre Einwilligung ein (§ 25 Abs. 1 TDDDG, Art. 6 Abs. 1 lit. a DSGVO).

6. Kontakt per Formular, E-Mail, Telefon und WhatsApp

Wenn Sie uns kontaktieren, verarbeiten wir die von Ihnen mitgeteilten Daten, etwa Name, E-Mail-Adresse, gegebenenfalls Telefonnummer, Firma und den Inhalt Ihrer Nachricht, ausschließlich zur Bearbeitung und Beantwortung Ihrer Anfrage. Die in Formularen als Pflichtfeld gekennzeichneten Angaben brauchen wir, um antworten zu können; alle weiteren Angaben sind freiwillig. Rechtsgrundlage ist Art. 6 Abs. 1 lit. b DSGVO, soweit Ihre Anfrage auf einen Vertrag gerichtet ist, im Übrigen Art. 6 Abs. 1 lit. f DSGVO auf Grundlage unseres berechtigten Interesses an der Beantwortung von Anfragen.

Formulare auf unseren Websites senden Ihre Angaben transportverschlüsselt per E-Mail an unser Postfach; auf dem Webserver werden die Nachrichten nicht gespeichert. Das Formular in Uniqscreen übermittelt zusätzlich Ihre IP-Adresse und, wenn Sie angemeldet über „Hilfe & Kontakt“ schreiben, die E-Mail-Adresse Ihres Kontos und den Namen Ihrer Organisation.

Zum Schutz vor Spam und Missbrauch begrenzen wir die Zahl der Absendungen. Auf www.uniqor.de speichern wir dafür einen mit einem geheimen Zufallswert gebildeten, nicht rückrechenbaren Prüfwert Ihrer IP-Adresse (bei IPv6 des Netzbereichs) und den Zeitpunkt, höchstens 15 Minuten nach der letzten Absendung. Die Anwendungen zählen Anfragen je IP-Adresse für höchstens eine Stunde. Rechtsgrundlage ist Art. 6 Abs. 1 lit. f DSGVO.

WhatsApp. Sie können uns auch über WhatsApp schreiben. Dann verarbeitet die WhatsApp Ireland Limited, 4 Grand Canal Square, Grand Canal Harbour, Dublin 2, Irland, Ihre Telefonnummer, Ihren Profilnamen und die Inhalte Ihrer Nachricht; dabei kann es zu einer Übermittlung an die Meta Platforms, Inc. in den USA kommen (Ziffer 19). Rechtsgrundlage für unsere Verarbeitung ist Art. 6 Abs. 1 lit. b bzw. lit. f DSGVO. Die Nutzung ist freiwillig. Wenn Sie das vermeiden möchten, nutzen Sie bitte Telefon, E-Mail oder unsere Formulare. Hinweise von WhatsApp: whatsapp.com/legal/privacy-policy-eea

Wir löschen Anfragen, sobald sie abschließend bearbeitet sind und keine gesetzlichen Aufbewahrungspflichten entgegenstehen. Entsteht aus einer Anfrage ein Vertrag, gelten die Fristen nach Ziffer 20.

7. Kündigung und Widerruf über unsere Website

Kündigung. Über die Kündigungsschaltfläche unter www.uniqor.de/kuendigung/ verarbeiten wir die eingegebenen Angaben (Art der Kündigung, Bezeichnung des Vertrags, gegebenenfalls Vertrags- oder Kundennummer, gewünschter Beendigungszeitpunkt, Name, Anschrift, E-Mail-Adresse, freiwillige Mitteilung) sowie Datum und Uhrzeit des Eingangs, um die Kündigung zu bearbeiten und ihren Zugang zu bestätigen. Rechtsgrundlage ist Art. 6 Abs. 1 lit. b DSGVO und Art. 6 Abs. 1 lit. c DSGVO in Verbindung mit § 312k BGB.

Widerruf. Über die Widerrufsfunktion unter www.uniqor.de/widerruf/ verarbeiten wir die eingegebenen Angaben (Name, Bezeichnung des Vertrags, gegebenenfalls Vertrags- oder Kundennummer und Datum des Vertragsschlusses, E-Mail-Adresse für die Eingangsbestätigung, freiwillig Anschrift und Mitteilung) sowie Datum und Uhrzeit des Eingangs. Rechtsgrundlage ist Art. 6 Abs. 1 lit. c DSGVO in Verbindung mit § 356a BGB und Art. 6 Abs. 1 lit. b DSGVO (Rückabwicklung des Vertrags).

Die Angaben werden per E-Mail an uns übermittelt. Für beide Formulare gilt dieselbe Ratenbegrenzung wie beim Kontaktformular (Ziffer 6). Damit die Formulare nicht zum Versand von E-Mails an fremde Adressen missbraucht werden, speichern wir zusätzlich einen nicht rückrechenbaren Prüfwert der angegebenen E-Mail-Adresse für 24 Stunden; an dieselbe Adresse gehen höchstens drei Bestätigungen am Tag. Scheitert die Übermittlung an uns, wird die Erklärung ausnahmsweise auf dem Server zwischengespeichert, automatisch erneut zugestellt und danach gelöscht, spätestens nach 30 Tagen. Rechtsgrundlage für diese Schutzmaßnahmen ist Art. 6 Abs. 1 lit. f DSGVO. Kündigungs- und Widerrufserklärungen bewahren wir bis zum Ablauf der gesetzlichen Verjährungs- und Aufbewahrungsfristen auf.

8. Kundinnen und Kunden: Vertrag, Konto und Abrechnung

Zur Anbahnung, Begründung und Durchführung eines Vertrags verarbeiten wir Bestands- und Kontaktdaten (Name, Firma, Anschrift, E-Mail-Adresse, Telefonnummer, USt-IdNr.), Angebote, Aufträge, die bei Vertragsschluss akzeptierte Fassung von AGB und AVV mit Zeitpunkt, Zugangsdaten der Benutzerkonten sowie Nutzungs-, Abrechnungs- und Zahlungsdaten. Rechtsgrundlage ist Art. 6 Abs. 1 lit. b DSGVO; für die Aufbewahrung von Rechnungen und Buchungsbelegen Art. 6 Abs. 1 lit. c DSGVO in Verbindung mit § 147 AO und § 257 HGB.

Unsere Rechnungen erstellen wir mit unserer eigenen Anwendung Uniqinvoice; Uniqscreen und StampBy übermitteln ihr dafür die Rechnungsdaten, StampBy bei Händler-Stempeln auch die Bestell- und Versanddaten (Ziffer 15). Eine Weitergabe an Dritte findet dabei nicht statt; für den Versand von Händler-Stempeln gilt Ziffer 15.

Zahlungen. Soweit Zahlungen über Stripe abgewickelt werden (Stripe Payments Europe, Ltd., 1 Grand Canal Street Lower, Dublin 2, Irland), übermitteln wir die dafür erforderlichen Daten an Stripe, insbesondere Name bzw. Firma, E-Mail-Adresse, Rechnungsanschrift, Betrag, Leistungsbezeichnung und eine interne Kennung. Karten- oder Kontodaten geben Sie unmittelbar bei Stripe ein; wir sehen davon nur Art und Endziffern. Wählen Sie auf der Zahlungsseite von Stripe PayPal (PayPal (Europe) S.à r.l. et Cie, S.C.A., Luxemburg), Klarna (Klarna Bank AB, Schweden) oder Amazon Pay (Amazon Payments Europe S.C.A., Luxemburg), erhält dieser Anbieter die für die Zahlung nötigen Angaben. Die Zahlungsdienste verarbeiten die Daten als eigene Verantwortliche, auch zur Betrugsvorbeugung und zur Erfüllung gesetzlicher Pflichten. Rechtsgrundlage ist Art. 6 Abs. 1 lit. b DSGVO. Informationen von Stripe: stripe.com/de/privacy

Ohne die für den Vertrag erforderlichen Angaben können wir keinen Vertrag schließen und kein Konto anlegen. Eine gesetzliche Pflicht zur Angabe besteht nicht.

9. E-Mail-Postfächer und Versand

Unsere E-Mail-Postfächer betreibt die ALL-INKL.COM – Neue Medien Münnich, Inhaber René Münnich, Hauptstraße 68, 02742 Friedersdorf, Deutschland. Über deren Mailserver versenden wir auch die Nachrichten aus unseren Formularen und die System-E-Mails unserer Anwendungen, etwa Bestätigungen, Einladungen, Kartenlinks und Hinweise (Absender donotreply@uniqor.de). Mit All-Inkl besteht ein Vertrag über die Auftragsverarbeitung nach Art. 28 DSGVO; die Verarbeitung erfolgt auf Servern in Deutschland.

Von E-Mails aus Uniqscreen und StampBy zu Bestellungen, Verträgen und Zahlungen legen wir eine Kopie in einem eigenen Archivpostfach bei All-Inkl ab, weil sie als Handels- und Geschäftsbriefe sechs Jahre aufzubewahren sind (Art. 6 Abs. 1 lit. c DSGVO in Verbindung mit § 257 HGB, § 147 AO). E-Mails mit Anmelde-, Bestätigungs- oder Kartenlinks archivieren wir nicht. Damit diese Vorgangsmails zuverlässig ankommen, legen Uniqscreen und StampBy sie zunächst in einem Postausgang ab (Empfänger, Betreff, Inhalt, Versandstatus) und wiederholen einen gescheiterten Versand automatisch; die Einträge löschen wir nach 180 Tagen, zusammen mit dem Konto bzw. Geschäft auch früher. Rechtsgrundlage ist Art. 6 Abs. 1 lit. b und f DSGVO.

E-Mails, die ein Kundenbetrieb aus Uniqinvoice an seine eigenen Kunden sendet, laufen über das Postfach, das dieser Betrieb selbst hinterlegt hat.

10. Datensicherung

Damit Daten nach einem Ausfall wiederhergestellt werden können, sichern wir unsere Server regelmäßig. Gesichert werden Datenbanken, hochgeladene Dateien und Einstellungen. Auf dem Server liegen die Sicherungen in geschützten Verzeichnissen. Bevor sie den Server verlassen, werden sie verschlüsselt und nur in dieser Form kopiert: in einen Speicher bei Google Drive (Google Ireland Limited, Gordon House, Barrow Street, Dublin 4, Irland) und, für den Server in Wien, zusätzlich per verschlüsselter Verbindung auf ein eigenes Speichersystem (NAS) in unseren Geschäftsräumen in Deutschland. Den Schlüssel hat nur Uniqor; Google kann die Inhalte nicht lesen. Die Sicherungen werden ausschließlich zur Wiederherstellung verwendet und nach Ablauf der Vorhaltezeit automatisch gelöscht:

- Server in Wien (Website, Uniqinvoice, StampBy, dort gehostete Kundensysteme): täglich; auf dem Server bis zu 30 Tage, bei Google Drive 7 Tage, auf dem NAS 30 Tage
- Server in Nürnberg (Uniqscreen): alle sechs Stunden; auf dem Server und bei Google Drive bis zu 14 Tage
- Systeme, die wir für Kunden hosten oder sichern: nach der im Vertrag vereinbarten Vorhaltezeit

Gelöschte Daten können bis zum Ablauf dieser Fristen in den Sicherungen fortbestehen. Rechtsgrundlage ist Art. 6 Abs. 1 lit. f DSGVO; unser berechtigtes Interesse ist die Ausfallsicherheit. Zur möglichen Übermittlung an Google LLC in den USA siehe Ziffer 19.

11. IT-Dienstleistungen, Fernwartung und KI-Unterstützung

Fernwartung. Für Fernwartung setzen wir AnyDesk ein (AnyDesk Software GmbH, Türlenstraße 2, 70191 Stuttgart). Die Verbindungen sind Ende-zu-Ende verschlüsselt; AnyDesk vermittelt sie, erhält aber keinen Zugriff auf Bildschirminhalte. Verarbeitet werden dabei die AnyDesk-Kennungen der Geräte, Zeitpunkte und die IP-Adressen der Verbindung. Zugriffe erfolgen nur mit Ihrer Zustimmung oder über vereinbarte, abgesicherte Zugänge und werden protokolliert. Für Daten auf Ihren Systemen sind Sie Verantwortlicher; es gilt unsere AVV.

KI-Unterstützung. Für Wartung, Fehlersuche und Programmierung unserer Server und Anwendungen sowie für Auswertungen und Texterstellung nutzen wir Claude von Anthropic PBC, San Francisco, USA, in der geschäftlichen Version ohne Nutzung der Daten zum Training. Dabei können Protokoll- und Konfigurationsdaten einsehbar sein, etwa IP-Adressen oder E-Mail-Adressen in Fehlermeldungen, im Einzelfall auch einzelne Datensätze. Anthropic handelt als unser Auftragsverarbeiter. Rechtsgrundlage ist Art. 6 Abs. 1 lit. f DSGVO; unser berechtigtes Interesse ist ein sicherer und fehlerfreier Betrieb. Zur Übermittlung in die USA siehe Ziffer 19.

12. Links und soziale Medien

Unsere Websites verlinken unser Unternehmensprofil auf Instagram, unsere Produkt-Websites und im Bereich „Referenzen“ die Websites von Kundinnen und Kunden. Das sind einfache Links: Daten werden erst übertragen, wenn Sie sie anklicken und unsere Seite verlassen. Für die Verarbeitung dort ist der jeweilige Betreiber verantwortlich, bei Instagram die Meta Platforms Ireland Limited, Merrion Road, Dublin 4, Irland (privacycenter.instagram.com/policy). Vorschaubilder, Schriften, Skripte und Icons liefern wir von unseren eigenen Servern aus; Verbindungen zu Servern Dritter baut unsere Website nicht auf. Die Startseite von stampby.de enthält einen Hinweis für Safari auf dem iPhone und iPad auf die StampBy-App im App Store. Safari

kann daraufhin selbst ein Banner einblenden und lädt die Angaben zur App dafür direkt bei Apple (Apple Distribution International Ltd., Cork, Irland). Das App-Store-Abzeichen liefern wir selbst aus; es ist ein einfacher Link.

Teil B – Ergänzungen für die einzelnen Anwendungen

13. Uniqinvoice

Anmeldung. Für die Anmeldung verarbeiten wir Benutzername und Passwort; das Passwort speichern wir ausschließlich als bcrypt-Hash. Nach der Anmeldung setzen wir ein technisch notwendiges Sitzungscookie (connect.sid, Laufzeit sieben Tage, httpOnly, SameSite=Strict). Rechtsgrundlage ist Art. 6 Abs. 1 lit. b DSGVO und § 25 Abs. 2 Nr. 2 TDDDG.

Systemprotokoll. Ändernde Zugriffe protokollieren wir mit Benutzername, IP-Adresse, Zeitpunkt, Aktion und Antwortstatus. Das dient der Nachvollziehbarkeit, der Erkennung von Missbrauch und den Anforderungen an eine ordnungsmäßige Buchführung (GoBD). Geheime Kennungen aus Links werden dabei maskiert. Einträge werden nach 90 Tagen gelöscht; unveränderbare Belegprotokolle, die zur Buchführung gehören, bleiben für die gesetzliche Aufbewahrungsfrist erhalten. Rechtsgrundlage ist Art. 6 Abs. 1 lit. f DSGVO und, soweit Buchführungsdaten betroffen sind, Art. 6 Abs. 1 lit. c DSGVO in Verbindung mit § 147 AO.

Daten in der Anwendung. Kunden, Angebote, Aufträge, Rechnungen, Zahlungen, Artikel, Belege und Mitarbeiterdaten verarbeiten wir ausschließlich weisungsgebunden für den jeweiligen Betrieb (Ziffer 2). Die Daten der Betriebe sind streng voneinander getrennt. Ruft ein Betrieb Zahlungsdaten über sein eigenes PayPal-Konto oder Kontoauszüge per EBICS bei seiner Bank ab, geschieht das mit seinen eigenen Zugängen.

KI-gestützte Belegerkennung. Lädt ein Betrieb einen Beleg hoch und nutzt die automatische Erkennung, übermitteln wir den Beleg an Anthropic PBC (USA), um Betrag, Datum, Lieferant und Positionen auszulesen. Anthropic nutzt die Daten nicht zum Training. Die Erkennung schlägt nur Werte vor; der Betrieb prüft und bestätigt sie. Wir handeln dabei als Auftragsverarbeiter des Betriebs, Anthropic als unser Unterauftragnehmer (Ziffer 19).

Digitale Unterschrift. Wird Ihnen ein Angebot oder Auftrag zur Unterschrift geschickt, verarbeiten wir im Auftrag des absendenden Betriebs Ihren Namen, Ihre Unterschrift (als Bild oder Schriftzug), die Zeitpunkte von Versand, Öffnen und Unterschrift, Ihre IP-Adresse, die Browserkennung, die Ihnen vorgelegten Texte und das versiegelte Dokument. Das dient dem Vertragsschluss und dem Nachweis Ihrer Erklärung. Verantwortlicher ist der absendende Betrieb. Die Unterschriftsseite setzt keine Cookies, speichert nichts in Ihrem Browser und lädt keine Inhalte von Dritten.

Versand eigener Warenbestellungen. Bestellungen aus unseren eigenen Anwendungen, derzeit Händler-Stempel aus StampBy, wickeln wir in Uniqinvoice als Verantwortlicher selbst ab, mit Auftrag, Versand über DHL und Rechnung. Einzelheiten stehen in Ziffer 15.

Wetter und Wechselkurse. Für die Wetteranzeige ruft unser Server bei Open-Meteo Wetterdaten für den eingestellten Ort ab; übermittelt wird nur der Ortsname bzw. dessen Koordinaten. Wechselkurse ruft der Server bei der Europäischen Zentralbank ab. Personenbezogene Daten werden dabei nicht übermittelt.

14. Uniqscreen

Konto und Vertrag. Für ein Konto verarbeiten wir Name, E-Mail-Adresse und Passwort (nur als bcrypt-Hash), für die Organisation Firmierung, Anschrift, USt-IdNr., Kontaktangaben und, soweit für den Einzug erforderlich, die Bankverbindung. Uniqscreen richtet sich ausschließlich an Unternehmen. Bei der Buchung speichern wir die akzeptierte Fassung von AGB und AVV und den Zeitpunkt Ihrer Bestätigung, als Unternehmer zu buchen. Endet der Vertrag, löschen wir die Organisation mit Displays, Medien, Playlisten und Einstellungen frühestens 30 Tage nach Vertragsende und nicht früher als 14 Tage nach einem Hinweis an den Inhaber auf den Datenexport. Nach einem Datenexport oder einem Verlangen nach Anbieterwechsel (§ 50 AGB) verschiebt sich die Löschung entsprechend. Dazu speichern wir den Zeitpunkt eines Wechselverlangens und protokollieren Datenexporte mit handelnder Person und Zeitpunkt. Konten ohne Organisation löschen wir 30 Tage nach Wegfall der letzten Mitgliedschaft.

Cookies und lokale Speicherung. Uniqscreen setzt nur technisch notwendige Cookies: __Secure-authjs.session-token (Anmeldung, bis zu 12 Monate, beim Demo-Zugang 2 Stunden), __Host-authjs.csrf-token (Schutz vor gefälschten Anfragen, bis zum Schließen des Browsers), __Secure-authjs.callback-url (Zielseite nach der Anmeldung, bis zum Schließen des Browsers) und uniqscreen_active_org (ausgewählte Organisation bei Konten mit mehreren Organisationen, 30 Tage bzw. 24 Stunden bei Öffnung durch die Plattform-Verwaltung). Alle sind httpOnly und werden nur verschlüsselt übertragen. Im Browser, in der App bzw. auf dem Display gespeichert werden außerdem der Kopplungs-Token des Players, zuletzt geladene Inhalte für den Betrieb bei Netzausfall, Anzeigeeinstellungen und in der App das Push-Token und die Einstellung der App-Sperre.

Zwei-Faktor-Anmeldung und Passkeys. Bei der Zwei-Faktor-Anmeldung (für Verwaltungskonten Pflicht) speichern wir das gemeinsame Geheimnis verschlüsselt (AES-256-GCM) sowie die Zeitpunkte von Einrichtung und letztem Code; von den Wiederherstellungscodes nur Hashwerte. Bei Passkeys speichern wir nur den öffentlichen Schlüssel, die Kennung, einen Signaturzähler, Ihre Bezeichnung, die Typkennung des Geräts bzw. Passwortmanagers (AAGUID), ob der Passkey synchronisiert wird, und die Zeitpunkte von Erstellung und letzter Nutzung. Biometrische Merkmale erhalten wir nie. Die Einmal-Abfrage für die Anmeldung wird höchstens 5 Minuten vorgehalten.

Demo-Zugang. Über „Demo ansehen“ können Sie eine Beispiel-Organisation ohne Konto ansehen. Die Demo ist rein lesend und endet nach 2 Stunden. Gegen Missbrauch zählen wir Demo-Anmeldungen über einen gekürzten Hashwert Ihrer IP-Adresse, der nach einer Stunde gelöscht wird; im Anmeldeprotokoll steht bei Demo-Anmeldungen keine IP-Adresse.

Betrieb der Displays. Ein gekoppeltes Display meldet Gerätekennung, Online-Status, App- und Systemversion, Auflösung, laufendes Layout, Fehlermeldungen und bei ferngesteuert eingerichtetem WLAN den Netznamen (SSID). Zur Fehlersuche übermittelt der Player technische Geräteangaben wie Hersteller, Modell, Seriennummer, Android-ID, Firmware-Kennung, Browserkennung, Speicherbelegung, lokale IP- und MAC-Adresse, Netzwerktyp, Zeitzone und Sprache; aus der Verbindung speichern wir die öffentliche IP-Adresse des Anschlusses. Wir halten davon nur den aktuellen Stand vor. Wird ein Display gelöscht, entfernen wir Netz- und Gerätekennungen sofort. Zusätzlich halten wir fest, welcher Inhalt wie lange lief (Wiedergabenachweis). Auf Anforderung der Organisation kann ein Display ein Bildschirmfoto der aktuellen Anzeige an unseren Server senden (derzeit mit der App für Samsung-Displays). Es kann die angezeigten Inhalte einschließlich personenbezogener Daten zeigen, ist nur für die Organisation sichtbar und wird nach 24 Stunden gelöscht. WLAN-Passwörter speichern wir nur verschlüsselt (AES-256-GCM, gebunden an die Gerätekennung). Uniqscreen verwendet keine Kameras, Sensoren, Gesichts- oder Personenerkennung und erfasst keine Zuschauer.

Hochgeladene Dateien. Bilder werden neu berechnet; eingebettete Metadaten wie Aufnahmeort werden dabei entfernt. Damit Displays Dateien ohne Anmeldung abspielen können, ist jede Datei über ihre eigene, nicht erratbare Adresse abrufbar; ein Verzeichnis wird nicht ausgegeben. Wer eine Adresse kennt, kann die Datei öffnen. Laden Sie deshalb keine vertraulichen Unterlagen und keine besonderen Kategorien personenbezogener Daten (Art. 9 DSGVO) hoch.

Sicherheitsprotokolle. Wir protokollieren jeden Anmeldeversuch (E-Mail-Adresse, Erfolg, Anmeldeart, Zeitpunkt, IP-Adresse) und sicherheits- und abrechnungsrelevante Änderungen einschließlich Fernzugriffen auf Displays und des Öffnens einer Organisation durch unseren Support (handelnde Person, Vorgang, Datensatz, Zeitpunkt, IP-Adresse). Gehört eine eingegebene Adresse zu keinem Konto, speichern wir nur einen nicht umkehrbaren Prüfwert. Nach 30 Tagen kürzen wir die IP-Adressen, nach 12 Monaten werden die Einträge gelöscht. Zur Begrenzung automatisierter Angriffe zählt der Server Versuche je IP-Adresse bzw. Konto für 5 Minuten bis 1 Stunde.

Apps für iPhone, iPad und Android. Die App zeigt die Anwendung von www.uniqscreen.de an; für Konto und Inhalte gilt alles oben Gesagte. Mitteilungen (etwa „Display offline“) sendet die App nur, wenn Sie sie erlauben; zugestellt werden sie über den Apple Push Notification Service bzw. Firebase Cloud Messaging von Google, die dabei das Push-Token und den Text der Mitteilung erhalten. Wir speichern dafür Push-Token, Plattform, App-Version, Sprache und letzte Nutzung sowie versendete Mitteilungen 90 Tage gegen Doppelzustellung. Beim Abmelden wird das Push-Token gelöscht, als ungültig gemeldete nach 30 Tagen, unbenutzte nach 12 Monaten. Kamera, Fotos und Mikrofon nutzt die App erst nach Ihrer Freigabe und nur, wenn Sie selbst eine Aufnahme starten, ein Bild auswählen oder einen QR-Code scannen; das Kamerabild beim Scannen wird nur auf dem Gerät ausgewertet. Unter Android übernimmt das die Bibliothek ML Kit von Google, die nach Angaben von Google technische Nutzungsdaten ohne Bilder an Google senden kann. Face ID, Touch ID und Fingerabdruck prüft allein das Gerät. Die App enthält kein Tracking, keine Werbung und keine Analyse- oder Absturzdienste Dritter. Rechtsgrundlage für Mitteilungen ist Ihre Einwilligung (Art. 6 Abs. 1 lit. a DSGVO, § 25

Abs. 1 TDDDG), die Sie unter Einstellungen → Mitteilungen oder in den Systemeinstellungen jederzeit widerrufen können.

Meldung rechtswidriger Inhalte. Über die Seite „Inhalt melden“ gehen Name, E-Mail-Adresse, Angaben zum Inhalt, Begründung und IP-Adresse per E-Mail an unsere Kontaktstelle. Bei Meldungen zu Darstellungen sexuellen Missbrauchs von Kindern sind Name und E-Mail-Adresse freiwillig. Gegen Missbrauch zählt der Server Meldungen je IP-Adresse eine Stunde und je gehashter E-Mail-Adresse einen Tag. Rechtsgrundlage ist Art. 6 Abs. 1 lit. c DSGVO in Verbindung mit Art. 16 der Verordnung (EU) 2022/2065 (Digital Services Act).

Eingebundene Inhalte. Wetterdaten (Open-Meteo) und XML-Nachrichten-Feeds ruft unser Server ab; übermittelt wird nur der eingestellte Ort bzw. die Feed-Adresse. Feed-Bilder, HTML5-Feeds und HTML-Inhalte mit einer selbst eingetragenen Adresse lädt dagegen das Display direkt beim Anbieter; dieser erhält dabei die IP-Adresse des Anschlusses und die Browserkennung des Displays. Bei der Ortssuche in den Einstellungen eines Bestell-Boards ruft Ihr Browser Open-Meteo direkt ab und übermittelt dabei den Suchbegriff und Ihre IP-Adresse.

Konto löschen. Sie können Ihr Konto in der App und im Browser unter Einstellungen → Konto selbst löschen. Konto, Push-Anmeldungen, Passkeys, Zwei-Faktor-Daten und Mitteilungen werden sofort entfernt. Sind Sie alleiniger Inhaber einer Organisation ohne weitere Mitglieder, wird auch die Organisation gelöscht; ein laufender Vertrag gilt dann als zum nächstmöglichen Termin gekündigt. Rechnungsunterlagen, Protokolleinträge bis zum Ablauf ihrer Frist und Sicherungen (Ziffer 10) bleiben bestehen. Ohne Zugang genügt eine E-Mail von der Adresse Ihres Kontos an info@uniqor.de.

Rechtsgrundlagen für Uniqscreen: Konto, Displays, Inhalte, App-Funktionen und Anmeldung Art. 6 Abs. 1 lit. b DSGVO; Sicherheits- und Anmeldeprotokolle, Ratenbegrenzung und Demo-Zugang Art. 6 Abs. 1 lit. f DSGVO.

15. StampBy

Händlerkonto. Für Registrierung und Dashboard verarbeiten wir Name, E-Mail-Adresse, Telefon, ein Passwort (nur als scrypt-Hash), auf Wunsch das Geheimnis der Zwei-Faktor-Anmeldung (verschlüsselt) und, wenn Sie bei der Anmeldung „Code per E-Mail senden“ wählen, einen einmaligen sechsstelligen Code an die E-Mail-Adresse des Kontos (10 Minuten gültig, höchstens 5 Versuche, nur als Prüfwert gespeichert), Angaben zum Geschäft (Name, Anschrift, Kontakt, USt-IdNr.), Fotos und Inhalte der Karten, Rollen im Team, die gewählte Sprache des Dashboards sowie Karten- und Standortkonfiguration. Zu jeder Anmeldesitzung speichern wir die gekürzte IP-Adresse (IPv4 ohne das letzte Oktett, IPv6 nur die ersten 48 Bit) und die Browserkennung. Änderungen im Dashboard protokollieren wir mit handelnder Person, Vorgang, Zeitpunkt und gekürzter IP-Adresse, etwa bei Tarif, Stammdaten, Annahme der AVV, Datenexport, Kartenlöschung, Support-Zugriff und Plattformverwaltung; vollständige IP-Adressen speichert StampBy nicht. Bearbeiter-Namen stehen in den Stempel- und Einlösebewegungen. Für Passkeys speichern wir den öffentlichen Schlüssel, die Kennung, einen Zähler, Gerätetyp, Sicherungsstatus, Transportwege, die Typkennung (AAGUID) und eine Gerätebezeichnung. StampBy richtet sich nur an Unternehmer; das wird bei der Registrierung, beim Abschluss eines Abos und bei der Bestellung von Händler-Stempeln bestätigt. Die Bestätigung speichern wir jeweils mit Zeitpunkt, bei der Registrierung zusammen mit der akzeptierten Fassung der AGB. Rechtsgrundlage ist Art. 6 Abs. 1 lit. b DSGVO, für die Protokolle Art. 6 Abs. 1 lit. f DSGVO; Zwei-Faktor-Anmeldung, E-Mail-Code und Passkeys dienen zudem der Sicherheit der Verarbeitung (Art. 32 DSGVO).

Händler-Stempel. Für Händler-Stempel mit NFC-Chip speichern wir Kennung und Bezeichnung des Chips, seine Zuordnung zu Standort oder Programm, die Zahl der Nutzungen und die letzte Nutzung sowie die Schlüssel des Chips (verschlüsselt). Bei einer Bestellung speichern wir Menge, Lieferanschrift, die bestellende Person, Zahlungsstatus und Kennung der Zahlung bei Stripe (Ziffer 8) sowie Paketdienst und Sendungsnummer. Nach der Zahlung übermittelt StampBy die Bestellung an unsere Anwendung Uniqinvoice (Ziffer 8): Menge, Nettobetrag, Rechnungsanschrift, E-Mail-Adresse und USt-IdNr. des Geschäfts, Lieferanschrift, Zahlungsart und Kennungen der Zahlung bei Stripe. Dort entstehen ein Auftrag und ein Versandeintrag, beim Versand die Rechnung. Das Versandetikett erstellt Uniqinvoice über die Schnittstelle von DHL. Die DHL Paket GmbH, Bonn, erhält dafür Name, gegebenenfalls Firma und Lieferanschrift und verarbeitet sie als eigener Verantwortlicher für die Zustellung; E-Mail-Adresse und Telefonnummer übermitteln wir nicht. Versenden wir ausnahmsweise mit einem anderen Paketdienst (DPD, Hermes, GLS oder Deutsche Post), erhält dieser dieselben Angaben. Uniqinvoice meldet Paketdienst und Sendungsnummer an StampBy zurück; StampBy schickt der bestellenden Person eine Versandbestätigung mit einem Link zur Sendungsverfolgung des Paketdienstes. In Uniqinvoice steht die Lieferanschrift im Versandeintrag und als interner Hinweis auf dem Auftrag, nicht auf der Rechnung. Die Lieferanschrift löschen wir in StampBy und in Uniqinvoice (Versandeintrag, Hinweis auf dem Auftrag und Versandetikett) 180 Tage nach dem Versand, bei

abgebrochenen oder stornierten Bestellungen nach 30 Tagen; in Uniqinvoice bleiben danach nur Postleitzahl und Ort, Paketdienst und Sendungsnummer. Die übrigen Bestellangaben bleiben bis zur Löschung des Geschäfts, die Rechnung mit Name und Anschrift des Geschäfts als Rechnungsempfänger nach den gesetzlichen Fristen. Rechtsgrundlage ist Art. 6 Abs. 1 lit. b DSGVO, für Rechnungen und ihre Aufbewahrung lit. c in Verbindung mit § 147 AO und § 257 HGB.

Konto löschen und Vertragsende. Im Dashboard und in den Apps können Sie Ihr Konto selbst löschen (in den Apps unter „Mehr → Konto löschen"); wie das geht, steht auch ohne Anmeldung unter stampby.de/konto-loeschen. Es wird sofort gelöscht; sind Sie alleiniger Inhaber, wird das Geschäft mit Karten, Fotos und Team mitgelöscht. Endet der Vertrag, löschen wir das Geschäft 30 Tage nach Vertragsende; 7 Tage vorher erhält der Inhaber eine Warnung. Damit Kundenkarten auch in Apple Wallet entwertet werden, bleibt in beiden Fällen bis zu 7 Tage eine Hülle ohne Angaben zum Geschäft und ohne Personendaten bestehen (anonymisierte Karten mit ihrem Wallet-Zugang); sie ist nicht nutzbar und wird danach endgültig gelöscht. Rechnungen bleiben in Uniqinvoice nach den gesetzlichen Fristen erhalten. Mit dem Geschäft wird auch sein Änderungsprotokoll gelöscht; es bleibt nur ein Vermerk über die Löschung ohne Namen (Nachweis, Ziffer 20). Bleibt das Geschäft bestehen, weil es weitere Inhaber gibt, bleiben Ihre bisherigen Einträge im Änderungsprotokoll bis zum Ablauf seiner Frist (Ziffer 20). In Sicherungen können gelöschte Daten bis zu 30 Tage fortbestehen (Ziffer 10).

Testzugang. Für einen kostenlosen Testzugang verarbeiten wir die Angaben aus dem Antrag (Name, E-Mail-Adresse, Firma, Anschrift, Telefon, freiwillig USt-IdNr.). Um Mehrfachanträge zu erkennen, speichern wir nicht umkehrbare Prüfwerte von E-Mail-Adresse, Firma mit Postleitzahl und gegebenenfalls USt-IdNr.; sie werden nach 24 Monaten gelöscht. Der Test endet automatisch und ohne Zahlungspflicht; Zahlungsdaten fragen wir dafür nicht ab. Ohne Abschluss werden Testgeschäft und Antragsdaten 60 Tage nach Testende gelöscht, mit einer Warnung 7 Tage vorher. Informationen zu Angeboten senden wir nur mit Ihrer gesonderten Einwilligung (Art. 6 Abs. 1 lit. a DSGVO), die Sie über den Abmeldelink in jeder E-Mail oder an info@uniqor.de widerrufen können.

Händler werben Händler. Jedes Geschäft hat einen persönlichen Empfehlungslink (stampby.de/r/…), den es selbst weitergibt; StampBy versendet keine Einladungen und liest keine Kontakte aus. Die Seite hinter dem Link und die Registrierung zeigen den Namen des empfehlenden Geschäfts. Der Code wird nur über die Adresse und das Formular weitergegeben, ohne Cookie. Registriert sich ein Geschäft darüber, speichern wir den Code bis zur Anlage des Geschäfts am Benutzerkonto und danach die Verknüpfung beider Geschäfte mit Status, Zeitpunkten und gegebenenfalls dem Gratiszeitraum. Um eigene oder verbundene Geschäfte und bestehende Kunden auszuschließen, gleichen wir vorhandene Daten ab: E-Mail-Adressen der Teammitglieder, Firma mit Postleitzahl und USt-IdNr.; zusätzliche Daten erheben wir dafür nicht. Das empfehlende Geschäft sieht nur die Zahl seiner offenen, gutgeschriebenen und eingelösten Empfehlungen, nicht die Namen der geworbenen Geschäfte, und erhält bei einer Gutschrift eine E-Mail ohne diesen Namen. Rechtsgrundlage ist die Teilnahme an der Aktion (Art. 6 Abs. 1 lit. b DSGVO), für den Abgleich unser berechtigtes Interesse an einer fairen Aktion (Art. 6 Abs. 1 lit. f DSGVO). Wird eines der beiden Geschäfte gelöscht, löschen wir die Verknüpfung.

Enterprise-Anfrage. Über das Formular unter stampby.de/enterprise können Sie ein Angebot für den Tarif Enterprise anfragen. Wir erhalten Firma, Ansprechpartner, E-Mail-Adresse, freiwillig Telefonnummer, Zahl der Standorte und Kunden sowie Ihre Nachricht per E-Mail; StampBy speichert die Anfrage nicht. An die angegebene Adresse geht eine Eingangsbestätigung, die Ihre Eingaben nicht enthält. Gegen Missbrauch lässt der Server je IP-Adresse höchstens drei Anfragen pro Stunde und je E-Mail-Adresse höchstens drei am Tag zu; dafür speichert er einen nicht rückrechenbaren Prüfwert der E-Mail-Adresse für 24 Stunden. Im Übrigen gilt Ziffer 6.

Karteninhaber. Für die Daten der Kundenkarten ist das Geschäft verantwortlich, das die Karte ausgibt (Ziffer 2). Wer eine Karte über den QR-Code anlegt, gibt freiwillig einen Namen an (ein Vorname genügt) und eine E-Mail-Adresse, wenn das Geschäft sie verlangt, sonst ebenfalls freiwillig. Rechtsgrundlage ist die Nutzung der Karte, die Sie beim Geschäft holen (Art. 6 Abs. 1 lit. b DSGVO); eine Einwilligung ist dafür nicht nötig. Ohne die Angaben, die das Geschäft verlangt, kann keine Karte angelegt werden. Die Karten sind für Personen ab 16 Jahren bestimmt. Gespeichert werden außerdem Kundennummer und Zeitpunkt des Beitritts, Stempel- und Einlösebewegungen mit Zeitpunkt, Standort und Quelle, Geschenke und Gutscheine, ein persönlicher Empfehlungscode und gegebenenfalls die Verknüpfung mit der werbenden Karte, auf Wunsch ein Hintergrundfoto, freiwillige Rückmeldungen an das Geschäft, Mitteilungstexte, ein Protokoll automatischer Aktionen und technische Kennungen der Wallet-Registrierung. Ein Geschäft kann zusätzlich eine Telefonnummer erfassen. Schaltet es Kundennotizen ein, kann sein Team zu Ihrer Karte eine kurze Notiz (höchstens 500 Zeichen) speichern und die Karte Kundengruppen zuordnen, um Sie persönlicher zu bedienen oder Aktionsnachrichten an eine Gruppe zu richten; diese gehen weiterhin nur an Karten mit Einwilligung (Art. 6 Abs. 1 lit. f DSGVO). Notizen und Gruppen sieht nur das Team des Geschäfts; sie erscheinen nie auf der Wallet-

Karte, sind in der Datenauskunft enthalten und werden mit der Karte gelöscht. Angaben zur Gesundheit, zur Religion oder andere sensible Daten darf das Geschäft dort nicht eintragen. Die E-Mail-Adresse dient dazu, Ihnen einen persönlichen Link zur Karte zu senden. Kartenseiten, Wallet-Karte, Mitteilungen und E-Mails zur Karte gibt es auf Deutsch und Englisch; die Sprache richtet sich nach der Spracheinstellung Ihres Geräts oder Ihrer Auswahl und wird an der Karte gespeichert, damit E-Mails zur Karte in dieser Sprache kommen. Jedes Geschäft führt Ihre Karte getrennt; wir verknüpfen Karten verschiedener Geschäfte nicht, auch wenn Sie dieselbe E-Mail-Adresse verwenden.

Beitritt ohne Anmeldung. Bietet ein Geschäft „nur scannen“ an, legt das Scannen die Karte ohne Name, E-Mail-Adresse oder Geburtstag an (Art. 6 Abs. 1 lit. b DSGVO). Damit je Programm nur eine Karte entsteht, setzen wir ein technisch erforderliches Cookie mit einer zufälligen Geräte-Kennung; in der Datenbank liegt davon nur ein Prüfwert, der außerdem der Missbrauchsprüfung bei Empfehlungsaktionen dient (Art. 6 Abs. 1 lit. b und f DSGVO). Die Zuordnung gilt je Gerät und Browser: Wer das Cookie löscht oder ein zweites Gerät nutzt, kann eine weitere Karte erhalten. Ohne E-Mail-Adresse können wir Ihnen bei Verlust des Geräts keinen Kartenlink senden. Aktionsnachrichten erhalten Sie in diesem Modus nur, wenn Sie den freiwilligen Haken „Aktionen erhalten“ setzen (siehe „Aktionsnachrichten“). Karten, die so angelegt und nie genutzt wurden, löschen wir nach 30 Tagen.

Gedruckte Mitgliedskarten. Manche Geschäfte geben statt einer Karte auf dem Handy eine gedruckte Karte (etwa aus Plastik) mit Kartennummer und QR-Code aus, die sie in StampBy erzeugen. Zu einer solchen Karte speichern wir weder Name noch E-Mail-Adresse oder Telefonnummer, sondern nur Kartennummer, Stempel- bzw. Punktestand, Belohnungen und Geschenke sowie die Buchungen mit Zeitpunkt, Standort und Quelle, für das Geschäft als Verantwortlichen (Ziffer 2, Art. 6 Abs. 1 lit. b DSGVO). Das Team des Geschäfts scannt die Karte; Sie brauchen dafür weder App noch Wallet. Geht eine Karte verloren, kann das Geschäft Stand, Belohnungen und Verlauf auf eine neue gedruckte Karte übertragen; die alte Karte wird gesperrt. Noch nie gestempelte gedruckte Karten löschen wir nicht automatisch, weil sie bis zur Ausgabe beim Geschäft liegen; ab der ersten Buchung gelten dieselben Fristen wie für andere Karten (Ziffer 20).

Karten nur auf Einladung. Manche Karten gibt ein Geschäft nur mit persönlicher Einladung aus. Die Einladung ist ein Link oder QR-Code, den das Geschäft selbst weitergibt; StampBy verschickt keine Einladungen. Wir speichern einen Prüfwert des Links, seine Gültigkeit (14 Tage), ob und wann er genutzt wurde, die damit angelegte Karte und, wenn das Geschäft ihn angibt, den Namen der eingeladenen Person. Ein Link ist nur einmal nutzbar; bis zur Bestätigung der E-Mail-Adresse liegt er höchstens 24 Stunden beim Beitrittswunsch. Das Geschäft kann neue Karten dabei automatisch einer Kundengruppe zuordnen. Einladungen samt Name löschen wir 30 Tage nach Ablauf ihrer Gültigkeit, bei Löschung der Karte sofort. Rechtsgrundlage ist die Ausgabe der Karte (Art. 6 Abs. 1 lit. b DSGVO), für den Namen das berechtigte Interesse des Geschäfts, seine Einladungen zuzuordnen (Art. 6 Abs. 1 lit. f DSGVO).

E-Mail-Bestätigung beim Beitritt. Hat das Geschäft sie eingeschaltet, senden wir in seinem Auftrag eine E-Mail ohne Werbung mit einem Bestätigungslink (Art. 6 Abs. 1 lit. b DSGVO). Erst nach Ihrem Klick wird die Karte angelegt; bis dahin speichern wir die Angaben höchstens 24 Stunden. Der Link wird nur als Prüfwert gespeichert, ist einmalig verwendbar und läuft nach 24 Stunden ab.

Aktionsnachrichten. Nur wenn Sie beim Beitritt den freiwilligen, nicht vorangekreuzten Haken für Aktionsnachrichten setzen, kann das Geschäft Ihnen Aktionsnachrichten auf die Karte senden, etwa Angebote oder einen Bonusstempel zum Geburtstag (Einwilligung, Art. 6 Abs. 1 lit. a DSGVO). Dazu gehört auch eine einmalige Bitte um eine Bewertung bei Google mit dem Bewertungslink des Geschäfts, frühestens drei Stunden nach einem Besuch und nicht nachts; dafür speichern wir an der Karte, wann die Bitte fällig ist und wann sie gesendet wurde. Sie wird nur gesendet, wenn der Wortlaut Ihrer Einwilligung sie ausdrücklich nennt; sonst verfällt eine vorgemerkte Bitte nach 30 Tagen. Ob und wie Sie bewerten, erfahren weder wir noch das Geschäft über StampBy; für die Bewertung selbst gelten die Bestimmungen von Google. Als Nachweis speichern wir Zeitpunkt, Wortlaut und Sprache sowie die gekürzte IP-Adresse der Einwilligung; die IP-Adresse wird nach 90 Tagen gelöscht. Bestellen Sie Aktionsnachrichten ab, bleiben Wortlaut und Datum der Einwilligung als Nachweis bis zur Löschung der Karte gespeichert. Tag und Monat Ihres Geburtstags erfragen und speichern wir nur mit dieser Einwilligung und nur, wenn das Geschäft einen Geburtstagsbonus anbietet; Sie können ihn auch später auf Ihrer Kartenseite eintragen. Sie können Aktionsnachrichten jederzeit auf Ihrer Kartenseite unter „Meine Daten“ abbestellen; das ist ein Widerruf mit Wirkung für die Zukunft, Ihre Karte bleibt bestehen. Eine Aktionsnachricht erscheint als Mitteilung und auf der Karte, bis sie abläuft oder das Geschäft sie löscht; bestellen Sie Aktionsnachrichten ab, verschwindet eine angezeigte Nachricht sofort von Ihrer Karte. Wer bedacht wird, richtet sich nach einfachen Regeln wie der Zeit seit dem letzten Besuch oder dem Stempelstand; eine Entscheidung mit rechtlicher Wirkung nach Art. 22 DSGVO findet nicht statt. Ein Geschäft kann einen Teil der Karten bewusst nicht bedenken, um die Wirkung einer Aktion zu messen (Art. 6 Abs. 1 lit. f

DSGVO).

Hinweise ohne Werbung. Unabhängig von einer Einwilligung kann Ihre Karte kurze Hinweise zur Karte selbst anzeigen (Art. 6 Abs. 1 lit. b DSGVO): eine einmalige Begrüßung nach dem ersten Hinzufügen zur Wallet und, wenn das Geschäft einen Verfall gesammelter Stempel vorsieht, eine Erinnerung 14 Tage vor dem Verfall sowie die Mitteilung, dass Stempel verfallen sind. Die Regel steht in den Teilnahmebedingungen; jeder Besuch setzt die Frist neu, und ohne vorherige Erinnerung verfallen keine Stempel. Dafür speichern wir, dass die Begrüßung gesendet wurde (im Protokoll automatischer Aktionen), und den Zeitpunkt der Erinnerung an der Karte. Bietet ein Geschäft Doppelstempel-Zeiten an, stehen sie auf der Karte; der zusätzliche Stempel wird als eigene Buchung im Stempelverlauf gespeichert.

Kunden werben Kunden. Bietet ein Geschäft eine Empfehlungsaktion an, enthält Ihre Karte einen persönlichen Einladungslink mit einem zufälligen Code, auch auf der Rückseite der Wallet-Karte. Der Link enthält weder Ihren Namen noch Ihre Kundennummer, und Werbende und Geworbene sehen ihre Namen gegenseitig nicht. Legt jemand über den Link eine Karte an, speichern wir die Verknüpfung beider Karten mit Code und Zeitpunkten. Die neue Karte erhält ihren Bonus beim Anlegen, die werbende Karte nach dem ersten Stempel der neuen Karte im Geschäft. Das Geschäft sieht in seinem Dashboard, welche Karte welche eingeladen hat und wie viele Einladungen eine Karte erfolgreich ausgesprochen hat. Um Missbrauch zu verhindern, prüfen wir mit bereits vorhandenen Daten, ob die neue Karte dieselbe E-Mail-Adresse oder denselben Prüfwert der Geräte-Kennung (Beitritt ohne Anmeldung) hat wie die werbende Karte, ob die werbende Karte mindestens 24 Stunden alt ist und ob die vom Geschäft festgelegte Obergrenze erreicht ist; zusätzliche Daten erheben oder speichern wir dafür nicht. Trifft eines davon zu, wird die Karte ohne Verknüpfung und ohne Bonus angelegt. Die Teilnahmebedingungen legt das Geschäft fest; sie sind über die Einladungsseite und Ihre Kartenseite abrufbar. Rechtsgrundlage ist die Teilnahme an der Aktion (Art. 6 Abs. 1 lit. b DSGVO), für die Missbrauchsprüfung das berechtigte Interesse des Geschäfts an einer fairen Aktion (Art. 6 Abs. 1 lit. f DSGVO).

Stempeln mit dem Händler-Stempel (NFC). Hat ein Geschäft einen Händler-Stempel mit NFC-Chip, stempelt es Ihre Karte, indem es den Stempel an Ihr Smartphone hält (Display eingeschaltet). Ihr Gerät öffnet dann eine Adresse mit der Kennung des Stempels und einem verschlüsselten, nur einmal gültigen Prüfwert. Damit Ihr Gerät die richtige Karte findet, speichert Ihr Browser beim Beitritt, beim Hinzufügen der Karte zu einer Wallet und beim Öffnen Ihrer Kartenseite bei einem solchen Geschäft (etwa über „Karte neu laden“ in der Wallet-Karte) den Link dieser Karte in einem Cookie, das er nur an die Stempeladresse sendet. Beim nächsten Antippen fasst der Server diese Cookies in einem Cookie mit den Links von bis zu 12 Karten zusammen; sie gelten höchstens 365 Tage ab ihrer letzten Speicherung. Es ist für das Stempeln Ihrer Karte mit dem Händler-Stempel unbedingt erforderlich und deshalb ohne Einwilligung zulässig (§ 25 Abs. 2 Nr. 2 TDDDG); die Kartenseite weist darauf hin. Der Server prüft die Links darin nur auf Gültigkeit und sucht die Karte des Geschäfts, zu dem der Stempel gehört; die Links Ihrer Karten bei anderen Geschäften werden weder gespeichert noch protokolliert noch miteinander verknüpft. Hat Ihr Gerät mehrere Karten desselben Geschäfts gespeichert, wird nur eine gestempelt: vorrangig eine, die in einer Wallet liegt, sonst die zuletzt genutzte; zusätzliche Daten speichern wir dafür nicht. Gespeichert wird nur die Stempelbuchung mit dem Hinweis auf den Händler-Stempel. Auf dem Chip liegen keine Daten zu Karten oder Personen. Ist eine Karte gelöscht, sind ihre Kundendaten gelöscht oder wurde ihr Link erneuert, entfernt der Server den alten Link beim nächsten Antippen eines Händler-Stempels aus dem Cookie und zeigt statt eines Stempels den Hinweis, sich eine neue Karte zu holen; eine gesperrte Karte wird beim Stempeln nicht gefunden. Sie können das Cookie jederzeit in Ihrem Browser löschen; Stempeln per NFC ist dann erst nach dem nächsten Öffnen der Kartenseite wieder möglich, Stempeln per QR-Code jederzeit. Rechtsgrundlage ist die Bereitstellung der Karte (Art. 6 Abs. 1 lit. b DSGVO).

Hintergrundfoto. Ein hochgeladenes Foto ist für Sie, das Team des Geschäfts und als Teil der Karte für Apple bzw. Google sichtbar. Metadaten wie der Aufnahmeort werden entfernt. Sie können das Foto jederzeit selbst löschen. Hochgeladene Bilder, die nicht verwendet werden, löschen wir nach 24 Stunden.

Hinweis in der Nähe. Hinterlegt ein Geschäft Standorte, enthält Ihre Karte deren Koordinaten, und Ihr Gerät kann die Karte in der Nähe vorschlagen (Apple Wallet) oder Sie benachrichtigen (Google Wallet). Die Ortung führt ausschließlich Ihr Gerät bzw. dessen Wallet durch. Wir und das Geschäft erhalten Ihren Standort nicht. Der Hinweis zeigt Ihren Stempelstand bzw. Mitgliedsstatus und enthält keine Werbung; eigene Texte des Geschäfts, etwa zu Aktionen, erscheinen dort nur, wenn Sie in Aktionsnachrichten eingewilligt haben. Google erhält nur die Koordinaten und legt den Text selbst fest. Bei neuen Karten ist der Hinweis Teil der Karte (Art. 6 Abs. 1 lit. b DSGVO); die Koordinaten stehen in der Karte, die Sie selbst in Ihre Wallet legen (§ 25 Abs. 2 Nr. 2 TDDDG). Bei Google sind höchstens etwa vier Benachrichtigungen pro Tag möglich; Radius und Zeitpunkt legen die Wallets fest. Sie können die Hinweise jederzeit in der Wallet bei der Karte oder in den Einstellungen Ihres Geräts abschalten. Bei älteren Karten ohne diese Einstellung zeigt Apple Wallet vor Ort nur einen

neutralen Text, und Google benachrichtigt nicht; Sie können den Hinweis auf Ihrer Kartenseite einschalten, gespeichert wird dann der Zeitpunkt.

Apple Wallet und Google Wallet. Erst wenn Sie „Zu Apple Wallet“ bzw. „Zu Google Wallet“ antippen, gehen Daten an Apple (Apple Distribution International Ltd., Cork, Irland; Apple Inc., USA) bzw. Google (Google Ireland Limited). Dorthin gelangen die Inhalte der Karte (Name und Logo des Geschäfts, Stand, Ihr Name, Kundennummer, Barcode, Adresse, Öffnungszeiten und Koordinaten des Geschäfts, gewähltes Hintergrundfoto, Geschenke, Mitteilungstexte, die letzten Bewegungen, Ihr persönlicher Kartenlink und gegebenenfalls Ihr Einladungslink) sowie technische Kennungen und Push-Token für Aktualisierungen. Google verarbeitet die an Google übermittelten Daten in eigener Verantwortung; Apple lädt die Karte direkt von unserem Server und erhält über den Push-Dienst technische Kennungen. Für die Verarbeitung durch Apple und Google gelten deren Datenschutzbestimmungen. Sie können eine Karte jederzeit in der Wallet löschen. Entfernen Sie eine Karte aus Apple Wallet auf allen Geräten oder schalten Sie dort „Automatische Updates“ für sie aus, meldet Apple das Gerät bei uns ab; liegt die Karte dann in keiner Wallet mehr, löschen wir sie wie bei einer Löschung über „Meine Daten“ (siehe „Ihre Karte verwalten“), gesammelte Stempel verfallen. Darauf weisen Beitritts- und Kartenseite beim Hinzufügen zu Apple Wallet sowie die Rückseite der Karte in Apple Wallet hin. Rechtsgrundlage ist die Bereitstellung der Karte in der von Ihnen gewählten Wallet (Art. 6 Abs. 1 lit. b DSGVO).

Ihre Karte verwalten. Auf Ihrer Kartenseite unter „Meine Daten“ können Sie Ihre Daten als Datei (JSON) abrufen, Aktionsnachrichten abbestellen und Ihre Karte samt Daten selbst löschen; alternativ wenden Sie sich an das Geschäft. Ebenso gelöscht wird eine Karte, die Sie aus Apple Wallet entfernen (siehe „Apple Wallet und Google Wallet“). Name, Kontaktdaten, Geburtstag, Foto, Rückmeldungen und Geschenke werden dann gelöscht, ebenso Stempelverlauf und Belohnungen der Karte; sie zählen danach auch in den Auswertungen des Geschäfts nicht mehr mit. Inaktive Karten löscht StampBy automatisch nach der vom Geschäft eingestellten Frist (mindestens 6 Monate, Voreinstellung 24 Monate); das Geschäft kann diese automatische Löschung auch abschalten. Gelöscht werden dabei die Daten der Karte samt Stempelverlauf und Belohnungen. Wird eine Karte gelöscht, ist ihr Link sofort ungültig. Liegt sie in Google Wallet, wird sie dort sofort entwertet. Liegt sie in Apple Wallet, holt Ihr Gerät in den folgenden Tagen eine entwertete Fassung ohne QR-Code, Standorte und Personendaten ab; dafür bewahren wir Wallet-Zugang und Geräteregistrierung noch bis zu 7 Tage auf und löschen sie danach. Löscht ein Geschäft eine Karte (ein Programm) mit allen Kundenkarten, werden diese ebenso entwertet und nach 7 Tagen mit allen Stempelbewegungen endgültig gelöscht. Wird das gesamte Händlerkonto gelöscht, gilt dasselbe. In beiden Fällen überschreiben wir außerdem die Kartenvorlage bei Google neutral, ohne Name und Logo des Geschäfts.

Webhooks. Im Tarif Enterprise kann ein Geschäft Ereignisse an Dienste senden lassen, die es selbst auswählt, etwa Zapier oder Make. Übermittelt werden Kartennummer, Karten-ID, Stand, Belohnung und Gutschein. Diese Dienste handeln im Auftrag und nach Weisung des Geschäfts, nicht als Unterauftragnehmer von Uniqor, und können ihren Sitz außerhalb der EU haben, etwa in den USA.

Cookies und lokale Speicherung. StampBy setzt nur technisch erforderliche Einträge: ein Sitzungs-Cookie im Händler-Dashboard (30 Tage ab der letzten Nutzung) und kurzlebige Hilfs-Cookies bei Zwei-Faktor- und Passkey-Anmeldung; für Karteninhaber bei Beitritt ohne Anmeldung ein Cookie mit einer zufälligen Geräte-Kennung (bis zu 90 Tage) und beim Beitritt, beim Hinzufügen zur Wallet und beim Öffnen der Kartenseite eines Geschäfts mit Händler-Stempel ein Cookie mit dem Link der Karte, das nur an die Stempeladresse gesendet und dort mit den übrigen zu einem Cookie mit den Links von bis zu 12 Karten zusammengefasst wird (bis zu 365 Tage ab der letzten Speicherung) und, wenn Sie die Sprache über den Umschalter DE | EN wählen, ein Cookie „sprache“ mit dieser Wahl (bis zu 1 Jahr); im lokalen Speicher des Browsers bei der Registrierung die gewünschte Tarifart (Basis oder Enterprise) bis zum ersten Aufruf des Dashboards im Dashboard, ob der Installationshinweis ausgeblendet wurde, und auf der Kartenseite, wann die Karte zuletzt für „Stempeln per NFC“ gespeichert wurde (damit das höchstens einmal täglich geschieht); in der Scan-Anwendung einen Zwischenspeicher für den Betrieb ohne Verbindung mit vorgemerkten Buchungen und zuletzt gescannten Karten (Kundennummer, Name, Stand, keine E-Mail-Adressen) bis zum Senden bzw. zur Abmeldung.

Adresssuche für Standorte. Lässt ein Geschäft die Koordinaten eines Standorts ermitteln, senden wir nur die Geschäftsadresse an den Dienst Nominatim der OpenStreetMap Foundation, St John’s Innovation Centre, Cowley Road, Cambridge, CB4 0WS, Vereinigtes Königreich (Angemessenheitsbeschluss nach Art. 45 DSGVO; Rechtsgrundlage Art. 6 Abs. 1 lit. b DSGVO). Die Emoji-Grafiken der Kartengestaltung lädt unser Server einmalig von jsDelivr und speichert sie lokal; dabei wird nur die IP-Adresse unseres Servers übermittelt.

Apps „StampBy“ für iPhone und Android. Die Apps sind für Geschäfte und ihr Team. Sie nutzen dasselbe Konto wie das Dashboard (Anmeldung mit E-Mail-Adresse und Passwort, Zwei-Faktor-Anmeldung oder Passkey), zeigen die Verwaltung von stampby.de an und verarbeiten dieselben Kontodaten (Name, E-Mail-Adresse, Telefon, Anschrift, Fotos und Inhalte). Die Kamera dient nur zum Scannen der QR-Codes von Kundenkarten; die Erlaubnis dafür erfragt die App erst, wenn Sie die Kamera aktivieren. Das Bild wird auf dem Gerät ausgewertet (unter Android mit der quelloffenen Bibliothek ZXing, ohne Google-Dienste) und nicht gespeichert, übertragen wird nur der erkannte Karten-Code. Face ID und Touch ID unter iOS bzw. die biometrische App-Sperre unter Android (Fingerabdruck, Gesicht oder Geräte-PIN) prüft allein das Betriebssystem; biometrische Daten erhalten die Apps nicht. Melden Sie sich in den Apps mit einem Passkey an, verwaltet ihn der Schlüsselbund bzw. Passwortmanager Ihres Geräts (unter iOS der iCloud-Schlüsselbund, unter Android der Passwortmanager von Google oder des Geräts); StampBy erhält wie auf der Website nur den öffentlichen Schlüssel. Den Code für die Zwei-Faktor-Anmeldung können Sie sich auch in den Apps per E-Mail schicken lassen. Das Sitzungsmerkmal liegt unter iOS im geschützten Schlüsselbund, unter Android im privaten Speicher der App; beim Abmelden wird die Sitzung beendet. Ohne Netz vorgemerkte Buchungen und die zuletzt gesehenen Karten (Kundennummer, Name, Stand) liegen bis zum Senden im geschützten App-Speicher, werden beim Abmelden gelöscht und sind nicht Teil der Gerätesicherung; unter iOS sind sie nur bei entsperrtem Gerät lesbar. Die Android-App schließt ihre Daten von Cloud-Sicherung und Geräteübertragung aus. Die Apps verbinden sich nur verschlüsselt mit stampby.de. Sie lesen keine Werbe- oder Gerätekennungen aus und enthalten keine Dienste zur Analyse, Werbung oder zum Tracking und keine Software-Bausteine Dritter, die Daten erheben; die Android-App nutzt keinen Push-Dienst. Absturzberichte erhalten wir nur, wenn Sie das Teilen mit App-Entwicklern in iOS bzw. das Senden von Nutzungs- und Diagnosedaten in Android erlaubt haben; Apple bzw. Google erheben diese Daten in eigener Verantwortung. Rechtsgrundlage ist Art. 6 Abs. 1 lit. b DSGVO.

Support-Zugriff. Auf Bitte eines Geschäfts oder zur Störungsbehebung können Mitarbeiter von Uniqor mit eigener Zwei-Faktor-Anmeldung vorübergehend auf das Dashboard eines Geschäfts zugreifen. Jeder Zugriff wird mit Grund und Zeitpunkt protokolliert, der Inhaber wird per E-Mail informiert, und der Zugriff endet nach spätestens vier Stunden. Grundlage ist die AVV mit dem Geschäft (Art. 28 DSGVO).

Digitale Visitenkarten von Uniqor. Die Visitenkarten unserer Mitarbeiterinnen und Mitarbeiter (Name, Position, Telefon, E-Mail-Adresse, Anschrift und Foto) sind über einen geheimen Link als vCard oder Wallet-Karte abrufbar. Fügen Sie eine solche Karte zu Apple Wallet oder Google Wallet hinzu, erhalten Apple bzw. Google diese Angaben. Den geheimen Teil des Links entfernen wir aus den Server-Protokollen.

Technische Anwendungsprotokolle. Start- und Fehlermeldungen ohne Passwörter und Nachrichteninhalte halten wir bis zu 90 Tage vor.

Teil C – Empfänger, Speicherdauer und Ihre Rechte

16. Datensicherheit

Alle Verbindungen sind verschlüsselt (TLS, HSTS). Passwörter speichern wir nur als Hash (bcrypt bzw. scrypt), besonders schutzwürdige Geheimnisse wie Zwei-Faktor-Schlüssel, WLAN-Passwörter oder Bankschlüssel zusätzlich verschlüsselt (AES-256-GCM bzw. XChaCha20-Poly1305). Sicherungen verlassen die Server nur verschlüsselt. Die Daten verschiedener Kundenbetriebe sind getrennt, Zugriffe über Rollen abgestuft. Administrative Zugänge zu den Servern sind nur mit Schlüssel und für einen kleinen Personenkreis möglich.

17. Keine automatisierte Entscheidungsfindung

Eine automatisierte Entscheidungsfindung einschließlich Profiling nach Art. 22 DSGVO findet nicht statt.

18. Empfänger und Auftragsverarbeiter

Wir geben Daten nur weiter, soweit das für den jeweiligen Zweck erforderlich ist. Mit Auftragsverarbeitern bestehen Verträge nach Art. 28 DSGVO.

Auftragsverarbeiter:

- netcup GmbH, Karlsruhe: Betrieb der Server in Wien und Nürnberg (Ziffer 3); Ort: EU
- ALL-INKL.COM – Neue Medien Münnich, Friedersdorf: E-Mail-Postfächer und Versand (Ziffer 9); Ort: Deutschland
- Google Ireland Limited, Dublin: verschlüsselte Kopie der Sicherungen bei Google Drive (Ziffer 10) und Zustellung von Mitteilungen an die Uniqscreen-App für Android (Ziffer 14); Ort: EU, ggf. USA

- Apple Distribution International Ltd., Cork: Zustellung von Mitteilungen an die Uniqscreen-App für iPhone und iPad (Ziffer 14) und Aktualisierungen von Karten in Apple Wallet (Ziffer 15); Ort: EU, ggf. USA
- Anthropic PBC, San Francisco: KI-Unterstützung bei Betrieb und Programmierung (Ziffer 11) und KI-gestützte Belegerkennung in Uniqinvoice (Ziffer 13); Ort: USA
- AnyDesk Software GmbH, Stuttgart: Vermittlung von Fernwartungsverbindungen (Ziffer 11); Ort: Deutschland

Empfänger in eigener Verantwortung:

- CrowdSec SAS, Paris: angreifende IP-Adressen (Ziffer 4); Ort: Frankreich
- Stripe Payments Europe, Ltd., Dublin, und die dort gewählten Zahlungsdienste PayPal, Klarna und Amazon Pay (Ziffer 8); Ort: EU, je Anbieter auch USA
- DHL Paket GmbH, Bonn: Name, gegebenenfalls Firma und Lieferanschrift beim Versand von Händler-Stempeln (Ziffer 15), ausnahmsweise auch ein anderer Paketdienst; Ort: Deutschland
- Google Ireland Limited (Google Wallet), wenn Sie eine StampBy-Karte oder eine Visitenkarte zu Google Wallet hinzufügen (Ziffer 15); Ort: EU, ggf. USA
- Dienste, die ein Geschäft per Webhook an StampBy anbindet, etwa Zapier oder Make, im Auftrag des Geschäfts (Ziffer 15); Ort: je Dienst, auch USA
- jsDelivr: nur die IP-Adresse unseres Servers beim einmaligen Laden von Grafiken (Ziffer 15)
- WhatsApp Ireland Limited, Dublin, wenn Sie uns über WhatsApp schreiben (Ziffer 6); Ort: EU, ggf. USA
- OpenStreetMap Foundation (Nominatim), Cambridge: nur Geschäftsadressen (Ziffer 15); Ort: Vereinigtes Königreich
- Open-Meteo: nur Orte für die Wetteranzeige, bei der Ortssuche in Uniqscreen auch Ihre IP-Adresse (Ziffern 13 und 14); Ort: Europa
- Anbieter von Nachrichten-Feeds und Webinhalten, die ein Uniqscreen-Kunde einbindet (Ziffer 14)
- Behörden, Gerichte und Berater, soweit wir gesetzlich dazu verpflichtet sind oder es zur Geltendmachung, Ausübung oder Verteidigung von Rechtsansprüchen erforderlich ist (Art. 6 Abs. 1 lit. c bzw. f DSGVO)

Systeme in unseren eigenen Geschäftsräumen (NAS für Sicherungen) betreiben wir selbst; dabei findet keine Übermittlung an Dritte statt.

19. Übermittlung in Drittländer

Die laufende Datenhaltung findet in der EU statt (Ziffer 3). Eine Übermittlung in Drittländer außerhalb der EU bzw. des EWR kommt nur in folgenden Fällen in Betracht:

- bei der KI-Unterstützung und der Belegerkennung durch Anthropic PBC (USA),
- bei der verschlüsselten Kopie der Sicherungen und bei Mitteilungen an die Android-App über Google (ggf. Google LLC, USA),
- bei Mitteilungen an die iOS-App und bei Apple-Wallet-Karten über Apple (ggf. Apple Inc., USA),
- bei Zahlungen über Stripe und die dort gewählte Zahlart, bei Google Wallet und bei WhatsApp, soweit Sie diese Wege nutzen,
- bei Webhooks, die ein StampBy-Geschäft selbst an Dienste außerhalb der EU anbindet (in dessen Verantwortung),
- bei der Adresssuche über Nominatim (Vereinigtes Königreich).

Wir stützen die Übermittlung auf einen Angemessenheitsbeschluss der EU-Kommission (Art. 45 DSGVO), für die USA auf das EU-US Data Privacy Framework, soweit der Empfänger danach zertifiziert ist, und im Übrigen auf die Standardvertragsklauseln der EU-Kommission (Art. 46 Abs. 2 lit. c DSGVO). Ein dem europäischen Recht vollständig entsprechendes Datenschutzniveau kann in Drittländern gleichwohl nicht in jedem Fall gewährleistet werden. Eine Kopie der Garantien erhalten Sie auf Anfrage.

20. Speicherdauer im Überblick

Wir löschen Daten, sobald ihr Zweck entfällt und keine Aufbewahrungspflicht entgegensteht. Im Einzelnen:

Für alle Angebote:

- Sicherheitsprotokoll mit vollständiger IP-Adresse (Server in Wien): höchstens 14 Tage
- Zugriffsprotokolle mit gekürzter IP-Adresse: höchstens 14 Tage
- von CrowdSec erkannte Angriffe auf dem Server: höchstens 7 Tage

- Prüfwerte zur Ratenbegrenzung von Formularen: 15 Minuten bis 24 Stunden
- Zwischenspeicherung bei gescheiterter Formularübermittlung: bis zur Zustellung, höchstens 30 Tage
- Anfragen: bis zur abschließenden Bearbeitung, bei Vertragsbezug nach den gesetzlichen Fristen
- Kündigungs- und Widerrufserklärungen: bis zum Ablauf der Verjährungsfrist, in der Regel drei Jahre ab Jahresende
- Vertrags- und Abrechnungsdaten, Rechnungen und Buchungsbelege: für die gesetzliche Aufbewahrungsfrist (§ 147 AO, § 257 HGB), je nach Art sechs Jahre (Handels- und Geschäftsbriefe), acht Jahre (Buchungsbelege) oder zehn Jahre (Bücher und Abschlüsse)
- Sicherungen: Server in Wien bis zu 30 Tage, Server in Nürnberg bis zu 14 Tage, Kundensysteme nach Vertrag

Uniqinvoice:

- Systemprotokoll: 90 Tage
- Belege, Rechnungen und unterschriebene Dokumente der Betriebe: für die Dauer des Vertrags, solange der Betrieb sie nicht selbst löscht; die gesetzliche Aufbewahrung (§ 147 AO, § 257 HGB) obliegt dem Betrieb als Verantwortlichem. Nach Vertragsende stehen die Daten noch 30 Tage zum Export bereit und werden danach gelöscht (§ 51 AGB)
- nicht unterschriebene Unterschriftsvorgänge: Löschung der Vorlage 30 Tage nach Ablauf
- Freitexte aus Ablehnungen und Widerrufen: drei Jahre
- Zugangsdaten: bis zur Löschung des Benutzerkontos

Uniqscreen:

- Zustandsmeldungen der Displays: 14 Tage
- Wiedergabenachweise und versendete Mitteilungen: 90 Tage
- Anmelde- und Prüfprotokoll: 12 Monate, IP-Adressen nach 30 Tagen gekürzt
- ausgeführte Gerätebefehle: 30 Tage
- abgelaufene Kopplungsvorgänge und -codes: 1 Tag
- abgelaufene oder benutzte Links (Passwort zurücksetzen, Einladung): 7 Tage
- Abholnummern der Bestell-Boards: 2 Tage
- gelöschte Displays, Standorte, Medien, Inhalte, Playlisten, Kampagnen, Feeds und Bestell-Boards: 30 Tage nach dem Löschen (Netz- und Gerätekennungen sofort)
- Zähler gegen Missbrauch: 5 Minuten bis 1 Stunde, Meldeformular je E-Mail-Adresse 1 Tag
- Demo-Sitzung: 2 Stunden
- Push-Anmeldungen: bis zur Abmeldung, ungültige nach 30 Tagen, unbenutzte nach 12 Monaten
- Konto, Inhalte, Passkeys und Zwei-Faktor-Daten: bis zur Löschung des Kontos
- Organisation nach Vertragsende: frühestens 30 Tage und mindestens 14 Tage nach dem Hinweis; nach Datenexport oder Wechselverlangen später
- Bildschirmfotos von Displays: 24 Stunden

StampBy:

- Prüfwerte zur Ratenbegrenzung: nur im Arbeitsspeicher, höchstens 24 Stunden
- Konto- und Vertragsdaten der Händler und Bearbeiter-Namen: für die Dauer des Vertrags; 30 Tage nach Vertragsende werden Geschäft, Karten, Fotos und Team gelöscht (Warnung 7 Tage vorher), Rechnungen nach den gesetzlichen Fristen
- Änderungsprotokoll: 12 Monate; Nachweise zu AVV-Annahme, Support-Zugriffen, Löschungen und Testzugängen: 36 Monate
- Anmelde-Sitzungen: 30 Tage ab der letzten Nutzung; Bestätigungs- und Einladungsdaten: bis zum Ablauf, danach höchstens 30 Tage
- unbestätigte Händlerkonten: 7 Tage
- Wallet-Aufträge: 30 Tage, Erinnerungs-Protokolle: 90 Tage
- Testzugang ohne Abschluss: 60 Tage; Prüfwerte gegen Mehrfachanträge: 24 Monate
- Empfehlungen zwischen Geschäften (Händler werben Händler): bis zur Löschung eines der beiden Geschäfte; Empfehlungscode am Benutzerkonto bis zur Anlage des Geschäfts

• Kartendaten einschließlich Stempelverlauf, Belohnungen, Notizen und Gruppenzuordnung: bis zur Löschung durch das Geschäft oder den Karteninhaber, inaktive Karten nach der vom Geschäft eingestellten Frist (mindestens 6, Voreinstellung 24 Monate, abschaltbar)

• gekürzte IP-Adresse der Einwilligung von Karteninhabern in Aktionsnachrichten: 90 Tage

• unbestätigter Beitrittswunsch: höchstens 24 Stunden, technisch gelöscht nach spätestens rund 25 Stunden

• Einladungen zu Karten nur auf Einladung (mit optionalem Namen): 30 Tage nach Ablauf ihrer Gültigkeit von 14 Tagen, bei Löschung der Karte sofort

• nie genutzte Karten aus Beitritt ohne Anmeldung: 30 Tage

• gedruckte Mitgliedskarten: wie Kartendaten; noch nie gestempelte bis zur Löschung durch das Geschäft

• Geräte-Kennung bei Beitritt ohne Anmeldung: bis zur Löschung der Karte, Cookie höchstens 90 Tage

• Cookie „sprache“ (gewählte Sprache auf Beitritts- und Kartenseite): höchstens 1 Jahr

• Cookie „Stempeln per NFC“: höchstens 365 Tage ab der letzten Speicherung (beim Öffnen der Kartenseite, in der Regel höchstens einmal täglich), jederzeit im Browser löschbar

• Wallet-Zugang und Apple-Geräteregistrierungen gelöschter Karten: bis zu 7 Tage nach dem Löschen (Entwertung in der Wallet); Karten eines gelöschten Programms bzw. Händlerkontos samt Bewegungen: 7 Tage

• Lieferanschrift bei Bestellungen von Händler-Stempeln (in StampBy und in Uniqinvoice einschließlich Hinweis auf dem Auftrag und Versandetikett): 180 Tage nach dem Versand, bei abgebrochenen oder stornierten Bestellungen 30 Tage; in Uniqinvoice bleiben danach nur Postleitzahl und Ort, Paketdienst und Sendungsnummer

• nicht verwendete hochgeladene Bilder: 24 Stunden

• technische Anwendungsprotokolle: bis zu 90 Tage

21. Ihre Rechte

Soweit wir Verantwortliche sind, haben Sie das Recht auf Auskunft (Art. 15 DSGVO), Berichtigung (Art. 16), Löschung (Art. 17), Einschränkung der Verarbeitung (Art. 18) und Datenübertragbarkeit (Art. 20). Eine erteilte Einwilligung können Sie jederzeit mit Wirkung für die Zukunft widerrufen (Art. 7 Abs. 3 DSGVO). Gesetzliche Aufbewahrungspflichten gehen einem Löschverlangen vor (Art. 17 Abs. 3 lit. b DSGVO). Betreffen Ihre Daten die Inhalte eines Kundenbetriebs, etwa eine Kundenkarte oder eine Rechnung, wenden Sie sich bitte an diesen Betrieb (Ziffer 2).

Widerspruchsrecht (Art. 21 DSGVO). Verarbeiten wir Daten auf Grundlage eines berechtigten Interesses (Art. 6 Abs. 1 lit. f DSGVO), etwa Server- und Sicherheitsprotokolle, Sicherungen oder die Beantwortung allgemeiner Anfragen, können Sie dem aus Gründen, die sich aus Ihrer besonderen Situation ergeben, jederzeit widersprechen. Wir verarbeiten die Daten dann nicht mehr, es sei denn, wir können zwingende schutzwürdige Gründe nachweisen, die Ihre Interessen, Rechte und Freiheiten überwiegen, oder die Verarbeitung dient der Geltendmachung, Ausübung oder Verteidigung von Rechtsansprüchen.

Zur Ausübung Ihrer Rechte genügt eine formlose Nachricht an info@uniqor.de oder an unsere Postanschrift. In Uniqscreen können Sie eine Kopie Ihrer Kontodaten unter Einstellungen → Konto selbst herunterladen. Auskunft und Datenkopie stellen wir innerhalb eines Monats bereit.

22. Beschwerderecht bei der Aufsichtsbehörde

Unbeschadet anderweitiger Rechtsbehelfe haben Sie das Recht auf Beschwerde bei einer Datenschutz-Aufsichtsbehörde, insbesondere in dem Mitgliedstaat Ihres Aufenthaltsorts, Ihres Arbeitsplatzes oder des Orts des mutmaßlichen Verstoßes (Art. 77 DSGVO). Für uns zuständig ist die Landesbeauftragte für den Datenschutz Niedersachsen, Prinzenstraße 5, 30159 Hannover, Telefon +49 511 120-4500, E-Mail poststelle@lfd.niedersachsen.de, Website lfd.niedersachsen.de.

23. Änderungen dieser Datenschutzerklärung

Wir passen diese Erklärung an, wenn sich unsere Angebote oder die Rechtslage ändern. Es gilt die jeweils unter www.uniqor.de/datenschutz/ veröffentlichte Fassung; Versionsangabe und Gültigkeitsdatum stehen auf der Seite. Alle Anwendungen verweisen auf diese Fassung.

Teil D – Privacy notice for StampBy card holders (English)

This part is for people who use a customer card ("card") that a shop issues with StampBy. It gives the information from Parts A to C that applies to card holders in English. If the two versions differ, the German text above prevails.

D1. Who is responsible?

The shop that issues your card is the controller of your card data. Its name, address and contact details are shown on the join page, at the bottom of your card page and on the back of the card in your wallet. Uniqor UG (haftungsbeschränkt), Alter Weg 5, 31199 Diekholzen, Germany, info@uniqor.de, operates StampBy and processes card data on behalf of the shop as a processor (Art. 28 GDPR). Uniqor is the controller only for the technical operation, including server and security logs (D5). Please send requests about your card, such as access, correction or deletion, to the shop. We support the shop and forward requests that reach us without delay.

D2. What data is processed and why?

Your card. When you join, you enter a name (a first name is enough) and an email address if the shop requires one; otherwise the email address is optional. We also store your customer number and the time you joined, stamps and redemptions with time, location and source, rewards, gifts and vouchers, a personal referral code, a background photo if you upload one, feedback you send to the shop, notification texts, a log of automatic actions, technical identifiers of your wallet registration and the language of your card (German or English), so that emails about your card come in that language. The shop may also record a phone number. Legal basis is providing the card you ask for (Art. 6(1)(b) GDPR). Without the details the shop requires, no card can be created. Cards are intended for people aged 16 and over. Each shop keeps your card separately; we do not link cards from different shops, even if you use the same email address.

Joining without sign-up. If a shop offers "scan only", scanning creates the card without name, email address or birthday. To make sure there is only one card per programme, we set a strictly necessary cookie with a random device ID (up to 90 days); the database holds only a hash of it, which is also used to check referral abuse. Cards created this way and never used are deleted after 30 days.

Email confirmation. If the shop has switched it on, we send an email without advertising with a confirmation link. The card is only created after you click; until then we keep your details for at most 24 hours.

Promotions (only with your consent). Only if you tick the optional box "Receive promotions" when joining or later on your card page can the shop send promotions to your card, for example offers, a birthday bonus or a one-time request to review the shop on Google (at the earliest three hours after a visit and not at night; only if the wording of your consent expressly mentions it). Legal basis is your consent (Art. 6(1)(a) GDPR). As proof we store the time, wording and language of your consent and a shortened IP address, which is deleted after 90 days. If you unsubscribe, the wording and date remain as proof until the card is deleted. We only ask for and store the day and month of your birthday with this consent and only if the shop offers a birthday bonus. You can unsubscribe at any time on your card page under "My data"; this withdraws your consent for the future, and your card remains. Who receives a promotion follows simple rules, such as the time since the last visit or the number of stamps; no decision with legal effect is made (Art. 22 GDPR). A shop can deliberately leave out some cards to measure the effect of a promotion (Art. 6(1)(f) GDPR). Neither we nor the shop learn through StampBy whether or how you review the shop; Google's terms apply to the review itself.

Notices without advertising. Regardless of consent, your card can show short notices about the card itself (Art. 6(1)(b) GDPR): a one-time welcome after you first add it to your wallet and, if the shop lets collected stamps expire, a reminder 14 days before they expire and a notice once stamps have expired. The rule is part of the terms of participation; every visit restarts the period, and no stamps expire without a prior reminder. Bonus stamps during "double stamp" hours are recorded as a separate entry. Notifications about stamps, rewards and gifts are part of the card; you can switch them off for the card in your wallet.

Notes and customer groups. If the shop switches this on, its team can add a short note (up to 500 characters) to your card and assign the card to customer groups, to serve you more personally or to address promotions to a group; promotions still only go to cards with consent. Only the shop's team sees notes and groups. They never appear on the wallet card, are included in your data download and are deleted with the card. The shop must not enter health information, religion or other sensitive data. Legal basis is the shop's legitimate interest in personal service (Art. 6(1)(f) GDPR).

Cards by invitation only. Some cards are only available with a personal invitation, a link or QR code that the shop passes on itself; StampBy does not send invitations. We store a hash of the link, its validity (14 days), whether and when it was used, the card created with it and, if the shop enters it, the name of the invited person. Invitations, including the name, are deleted 30 days after they expire, or immediately when the card is deleted (Art. 6(1)(b) and (f) GDPR).

Refer a friend. If a shop offers a referral promotion, your card contains a personal invitation link with a random code that contains neither your name nor your customer number. If someone creates a card with it, we store the link between both cards with code and timestamps, and the shop sees which card invited which. To prevent abuse, we use existing data only to check whether the new card has the same email address or device-ID hash as the inviting card, whether the inviting card is at least 24 hours old and whether the shop's limit has been reached. Legal basis is taking part in the promotion (Art. 6(1)(b) GDPR) and, for the abuse check, the shop's legitimate interest in a fair promotion (Art. 6(1)(f) GDPR).

Stamping with the shop's NFC stamp. So that your phone finds the right card when the shop holds its NFC stamp to it, your browser stores the link of your card in a cookie that is only sent to the stamping address; the cookie holds the links of up to 12 cards for up to 365 days after they were last stored. It is strictly necessary for stamping (§ 25(2) no. 2 TDDDG). No data about cards or people is stored on the chip.

Printed member cards. Some shops hand out a printed card (for example a plastic card) with a card number and QR code that they create in StampBy instead of a card on your phone. For such a card we store no name, email address or phone number, only the card number, the stamp or points balance, rewards and gifts and the bookings with time, location and source, on behalf of the shop as controller (Art. 6(1)(b) GDPR). The shop's team scans the card; you need neither an app nor a wallet. If a card is lost, the shop can transfer balance, rewards and history to a new printed card; the old card is blocked. Printed cards that have never been stamped are not deleted automatically, because they stay with the shop until they are handed out; from the first booking on, the same periods apply as for other cards.

Nearby notice. If the shop has stored locations, your card contains their coordinates, and your phone can suggest the card nearby. Only your device determines your location; neither we nor the shop receive it. You can switch the notice off in your wallet or in your phone's settings.

Background photo. A photo you upload is visible to you, to the shop's team and, as part of the card, to Apple or Google. Metadata such as the place where it was taken are removed. You can delete it at any time; uploaded images that are not used are deleted after 24 hours.

D3. Apple Wallet and Google Wallet

Data only goes to Apple (Apple Distribution International Ltd., Cork, Ireland; Apple Inc., USA) or Google (Google Ireland Limited) when you tap "Add to Apple Wallet" or "Add to Google Wallet". They receive the contents of the card (name and logo of the shop, balance, your name, customer number, barcode, address, opening hours and coordinates of the shop, background photo, gifts, notification texts, recent activity, your personal card link and, if applicable, your invitation link) as well as technical identifiers and push tokens for updates. Google processes this data under its own responsibility; Apple loads the card directly from our server and receives technical identifiers via its push service. Their privacy policies apply. If you remove the card from Apple Wallet on all your devices, or switch off "Automatic Updates" for it there, and it is then in no wallet any more, we delete the card as if you had deleted it yourself; collected stamps are lost. Legal basis is providing the card in the wallet you chose (Art. 6(1)(b) GDPR).

D4. Cookies and local storage

StampBy only uses entries that are strictly necessary (§ 25(2) no. 2 TDDDG): the device-ID cookie for joining without sign-up (up to 90 days), the cookie for stamping with the NFC stamp (up to 365 days), the cookie "sprache" with the language you choose with the DE | EN switch (up to 1 year) and, in your browser's local storage, when the card was last stored for NFC stamping. There are no cookies for analytics, advertising or tracking.

D5. Hosting, logs and recipients

StampBy runs on our own servers, rented from netcup GmbH, Karlsruhe, in the data centre in Vienna, Austria (EU). Web server security logs contain the full IP address and are deleted after 14 days at the latest; secret parts of card links are removed from the logs. To fend off attacks, the CrowdSec software may send attacking IP addresses to CrowdSec SAS, Paris, France. Emails about your card are sent via ALL-INKL.COM – Neue Medien Münnich, Friedersdorf, Germany. Apple delivers updates to Apple Wallet cards on our behalf. If the shop connects other services via webhooks, for example Zapier or Make, the shop is responsible for them; card number, card ID, balance, reward and voucher are transmitted. Data can only be transferred to countries outside the EU (in particular the USA) with Apple, Google and such webhooks; we rely on the EU-US Data Privacy Framework where the recipient is certified and otherwise on the EU standard contractual clauses.

D6. How long is data kept?

- Card data, including stamp history, rewards, notes and groups: until the shop or you delete the card; inactive cards are deleted after the period set by the shop (at least 6 months, 24 months by default; the shop can switch this off).
- After a card is deleted: wallet access and Apple device registration for up to 7 days, so that the card can be invalidated in Apple Wallet; in backups for up to 30 days.
- Shortened IP address of your consent: 90 days.
- Unconfirmed join requests: 24 hours. Cards from joining without sign-up that were never used: 30 days.
- Printed member cards: like card data; cards that have never been stamped until the shop deletes them.
- Invitations to cards by invitation only: 30 days after they expire.
- Unused uploaded images: 24 hours. Server logs: 14 days.

D7. Your rights

You have the right of access (Art. 15 GDPR), rectification (Art. 16), erasure (Art. 17), restriction of processing (Art. 18) and data portability (Art. 20), and you can object to processing based on legitimate interests on grounds relating to your particular situation (Art. 21). You can withdraw a consent at any time with effect for the future (Art. 7(3)). On your card page under "My data" you can download your data as a file (JSON), unsubscribe from promotions and delete your card yourself. Otherwise, please contact the shop, or us at info@uniqor.de; we forward your request. You have the right to lodge a complaint with a data protection supervisory authority, in particular in the EU member state where you live or work (Art. 77 GDPR). The authority responsible for Uniqor is the Landesbeauftragte für den Datenschutz Niedersachsen, Prinzenstraße 5, 30159 Hannover, Germany, poststelle@lfd.niedersachsen.de.