Ticket-Unterlagen

KTCards · Datenschutz
Datenschutzhinweise zur KTCards-Kunden-App

Stand: 08.11.2026

Diese Hinweise gelten für die Kunden-App auf ktcards-app.de und die zugehörige Kundenverwaltung im KTCards-Portal. Für den Onlineshop und die Videoüberwachung im Store gelten eigene ergänzende Informationen.

Spielhilfen und Event-Timer

Nach dem sichtbaren Rundenende können in beiden Spieleransichten wechselnde Hinweise zu eigenen Spiel- und Store-Events sowie Store-Angeboten erscheinen. Regelmäßige Local-Zeiten stammen aus der zentralen Filialplanung. Die Auswahl folgt Spiel und Filiale des bereits geöffneten Timers, ohne Werbeprofil, Klickmessung, zusätzliche Gerätekennung oder externe Werbedienste. Bei laufender Spielzeit und vorrangigen betrieblichen Meldungen werden diese Hinweise ausgeblendet. Sie dienen der Information über das eigene Angebot (Art. 6 Abs. 1 Buchst. f DSGVO); gegen Direktwerbung kannst du jederzeit widersprechen. Die Hinweise lassen sich vor dem Öffnen der Spielhilfe über die entsprechende Auswahl abschalten. Die Spielhilfe ist auch ohne Eventverbindung nutzbar. Es werden weiterhin keine Spielstände gespeichert.

Die freiwillig verwendbaren Spielhilfen für Palworld, Lorcana, Magic und Flesh & Blood rechnen Zählerstände ausschließlich im Arbeitsspeicher der geöffneten Ansicht. Diese Werte werden nicht an KTCards oder Dritte übermittelt, nicht in Cookies, Local Storage oder Session Storage abgelegt und nicht archiviert. Schließen oder Neuladen der Ansicht verwirft den Stand; bei Unterbrechungen kann das Gerät ihn ebenfalls verwerfen. Es erfolgt keine Auswertung eures Spielverlaufs.

Bei einer ausdrücklich geöffneten Eventverbindung prüft das Portal anhand deiner vorhandenen Anmeldung, Filial- und Teilnahmezuordnung, ob du den Timer sehen darfst. Die App ruft dann den aktuellen Timerstatus, Rundennummer und gegebenenfalls betriebliche Hinweise ab. An die Timerabfrage werden keine Zählerstände oder Mitspielerangaben angehängt. Die Verarbeitung dient der von dir gewählten App-Funktion (Artikel 6 Absatz 1 Buchstabe b DSGVO); erforderliche Zugriffssicherheit und technische Betriebsprotokolle bleiben nach den unten erläuterten Regeln bestehen. Auf Wunsch versucht die App während der geöffneten Spielhilfe das Display wach zu halten; die Gerätefunktion überträgt keine Spielwerte.

Adventskalender: derzeit nur interne Vorbereitung

In diesem Versionsstand ist der Adventskalender nicht für Kunden freigegeben. Es gibt keine Türchenöffnungszählung, Gewinnermittlung oder Gutscheinvergabe. Vor einer späteren Freigabe werden Teilnahmebedingungen und diese Hinweise um die tatsächlich umgesetzte Verarbeitung ergänzt. Die interne Redaktion ist kein Kunden-Tracking.

1. Verantwortlicher

KTCards – Tobias Schultz

Am Markt 9
24568 Kaltenkirchen

, Deutschland

E-Mail: info@ktcards.de

2. Daten, Zwecke und Rechtsgrundlagen

Wir verarbeiten die für dein Kundenkonto und deine angefragten Leistungen erforderlichen Daten: Name und Kontaktdaten, Kundennummer und Kartenkennung, sichere Anmeldedaten, Spiele und Spieler-IDs sowie je nach Nutzung Teilnahme, Check-ins, Reservierungen, Wartelisten, Wünsche, Nachrichten, Gutscheine, Bestellungen, Zahlungen und Grading-Aufträge einschließlich erforderlicher Fotos und Unterlagen. Freiwillige Angaben sind im jeweiligen Zusammenhang erkennbar. Ohne erforderliche Angaben lässt sich die jeweilige Leistung nicht anbieten; freiwillige Zusatzfunktionen sind keine Voraussetzung für das übrige Kundenkonto.

Kundenkonto, Kundenkarte und angefragte Leistungen: Art. 6 Abs. 1 Buchst. b DSGVO, soweit für ein Vertragsverhältnis oder vorvertragliche Maßnahmen erforderlich.

Gesetzlich erforderliche Buchführungs-, Aufbewahrungs- und Betroffenenrechtsverfahren: Art. 6 Abs. 1 Buchst. c DSGVO.

Sicherer Betrieb, Missbrauchsabwehr und erforderliche Anspruchsabwehr: Art. 6 Abs. 1 Buchst. f DSGVO. Unsere Interessen sind zuverlässige Systeme, Schutz vor unberechtigtem Zugriff und die Klärung offener Ansprüche; überwiegende Interessen Betroffener werden berücksichtigt.

Freiwillige Service-Push-Mitteilungen und einwilligungsbedürftige Zusatzfunktionen: Art. 6 Abs. 1 Buchst. a DSGVO. Einwilligungen sind für die Zukunft widerrufbar.

Bestell- und Zahlungsinformationen können auch aus der Warenwirtschaft oder vom jeweiligen Zahlungsdienstleister kommen. Bei Store-Vorgängen erfassen Mitarbeitende deine Angaben. Der Stammkunden-/Stammspielerstatus kann aus Käufen und Teilnahmen nach unseren Store-Regeln berechnet werden. Bei Fragen oder Fehlern kannst du eine Prüfung und Korrektur durch den Store verlangen.

In „Meine Dokumente“ werden die dir bereits zugeordneten und bereitgestellten Originaldokumente gesammelt angezeigt. Die Links in Nachrichten und Dokumentübersicht greifen auf dieselben gespeicherten Dateien zu; die Übersicht erzeugt keine zusätzliche Rechnungsfassung. Suche und Filter verwenden vorhandene Zuordnungsdaten. Die neue Übersicht führt keine zusätzliche Weitergabe an Dienstleister und keine neue dauerhafte Browserspeicherung ein. Bestehende Aufbewahrungsfristen und Zugriffsberechtigungen bleiben maßgeblich.

Manga-Wunschlisten und Bearbeitungsstand

Wenn du eine Manga-Wunschliste übermittelst, speichern wir deinen Originaltext, die Zuordnung zu deinem Kundenkonto, eine Listennummer und den Bearbeitungsstand. Das Store-Team kann daraus einzelne Titel und Bände mit Mengen und Bestellständen erfassen, auch wenn ein Titel noch nicht im Artikelstamm vorhanden ist. In deiner App siehst du den Gesamtstatus, Kundenhinweise und vom Team geprüfte, für dich freigegebene Positionen. Interne Arbeitsnotizen werden dort nicht angezeigt. Die Verarbeitung dient deiner Anfrage und gegebenenfalls der Vorbereitung oder Abwicklung deiner Bestellung (Art. 6 Abs. 1 Buchst. b DSGVO).

Berechtigte Mitarbeitende können die Liste als Arbeitsunterlage ausdrucken. Ihr QR-Code enthält einen Verweis auf den geschützten Portalvorgang und dessen Bearbeitungsstand, keine Namen, E-Mail-Adressen oder Wunschtitel. Er ersetzt keine Mitarbeiteranmeldung. Listen und interne Bearbeitungsdaten unterliegen den unten beschriebenen Erforderlichkeits-, Lösch- und Aufbewahrungsregeln. Eine Wunschliste allein wird nicht dadurch zu einem Buchungsbeleg, dass sie gedruckt wird; getrennt entstandene Bestell- und Rechnungsunterlagen werden nach ihrer eigenen rechtlichen Einordnung behandelt.

Judge-Zuordnung und Hilferufe

Für ein Event können mehrere Judges eingeteilt sein. Nur die jeweils berechtigten Personen erhalten Zugriff auf die zugeordneten Timer, Hilferufe und gegebenenfalls erforderlichen Decklisten. Bei einem Hilferuf werden Teilnehmerzuordnung, optionaler Tisch, Runde, Zeitpunkt, Bearbeitungsstatus und übernehmender Judge gespeichert, damit der Ruf nicht doppelt bearbeitet wird. Auf dem Store-Bildschirm werden für eingeteilte Judges Vornamen angezeigt. Die Zuordnung kann vom Team aufgehoben werden. Dies dient der Betreuung des angefragten Events (Art. 6 Abs. 1 Buchst. b DSGVO) und der sicheren, geordneten Bearbeitung (Art. 6 Abs. 1 Buchst. f DSGVO). Push-Mitteilungen erfordern weiterhin die bestehende Freigabe.

Gast-Warteliste für Events

Du kannst eine freigegebene Event-Warteliste ohne App-Konto nutzen. Wir verarbeiten dafür deinen Namen, deine E-Mail-Adresse, das gewählte Event sowie Bestätigungs-, Angebots- und Bearbeitungszeitpunkte und Status zur Bearbeitung deiner angefragten Teilnahme (Art. 6 Abs. 1 Buchst. b DSGVO). Ein Eintrag garantiert keinen Startplatz. Es wird kein Kundenkonto angelegt und keine Zahlung ausgelöst. App-Nutzer verwenden ihr Konto mit bestätigter E-Mail-Adresse.

Erst nach E-Mail-Bestätigung und deiner Bestätigung auf der Seite wird der Gasteintrag aktiv. Für doppelte aktive Einträge verwenden wir eine zweckgebundene, schlüsselbasierte E-Mail-Kennung; diese ist kein öffentliches Adressverzeichnis. Namen, E-Mail-Adressen und Mailinhalte werden verschlüsselt gespeichert. Technische Eventzuordnung, Status, Zeiten und Prüfkennungen bleiben für den Ablauf erforderlich. Ein privater Link erlaubt den Zugriff auf deinen eigenen Gasteintrag; bitte nicht weitergeben. Der Link wird im URL-Fragment übergeben und nach dem Öffnen aus der Adresszeile entfernt. Die Freigabe erfolgt bewusst über einen Button und gilt in dieser Sitzung höchstens 30 Minuten.

Unbestätigte Gastanfragen verfallen spätestens nach 24 Stunden oder bei Eventstart. Neue bestätigte Gasteinträge einschließlich zugehöriger Wartelistenmails werden sieben Tage nach Eventende bei der nächsten regelmäßig ausgeführten Wartung gelöscht; danach funktionieren die Zugangslinks nicht mehr. Diese besondere Frist gilt für den Gast-Wartelisteneintrag, nicht für unabhängig entstandene Geschäftsunterlagen. Für Missbrauchsbegrenzung werden

zweckgebundene Hash-Kennungen zu IP-Adresse bzw. E-Mail und Anfragezähler vorübergehend verwendet und durch die bestehende Bereinigung entfernt. Notwendige Serverprotokolle unterliegen den unten erläuterten Regeln. Grundlage der Missbrauchsabwehr ist unser berechtigtes Interesse am sicheren Betrieb (Art. 6 Abs. 1 Buchst. f DSGVO).

Für Bestätigungen und Platzangebote wird unser bestehender E-Mail-Dienst genutzt; keine Übermittlung an JTL oder einen Zahlungsdienst durch den bloßen Wartelisteneintrag. Auf der Gastseite wird das notwendige Sitzungscookie für Formularschutz und zeitlich begrenzten Zugriff verwendet (§ 25 Abs. 2 Nr. 2 TDDDG). Der im Shop eingebundene Auslastungs-/Wartelistenbaustein setzt selbst keine Cookies, zeigt keine personenbezogenen Teilnehmerdaten und verwendet keine Werbeauswertung.

3. Anmeldung und Speicherung auf deinem Gerät

Für die Anmeldung wird das notwendige Sitzungscookie ktcards_customer verwendet. Nur bei Auswahl von „30 Tage angemeldet bleiben“ kommt ktcards_remember hinzu; der Zugang kann durch Abmelden widerrufen werden. Notwendige Speicherzugriffe dienen der von dir angeforderten Funktion (§ 25 Abs. 2 Nr. 2 TDDDG); einwilligungsbedürftige Zugriffe erfolgen erst nach deiner Auswahl (§ 25 Abs. 1 TDDDG).

Eine angebotene Formular-Zwischenspeicherung ist standardmäßig aus. Nach bewusster Auswahl können Texte und Auswahlfelder, auch Namen und Anschriften, im Sitzungsspeicher dieses Tabs bis zu zwei Stunden für die Wiederherstellung bereitliegen. Passwörter, Dateien und Unterschriften werden dadurch nicht gespeichert. Abwählen entfernt die bekannten Entwürfe. Ein angehaltener Browser kann die tatsächliche Entfernung bis zum nächsten Seitenaufruf verzögern. Weitere Sitzungsdaten unterstützen Navigation und Bedienung. Öffentliche statische Dateien können im Browsercache liegen; persönliche Seiten werden vom App-Service-Worker nicht als Offlinekopie gespeichert.

Die Kunden-App enthält kein Google Analytics, keinen Google Tag Manager, kein Meta Pixel und kein Werbe- oder Reichweitentracking.

Freiwillige Passkeys und Wiederherstellung

Du kannst weiterhin ein Passwort verwenden. Passwörter werden als dafür vorgesehene sichere Hashwerte gespeichert, nicht als lesbarer Text oder rückentschlüsselbares Passwort. Unterstützt die Serverumgebung Argon2id, wird es für neue Hashwerte und eine sichere Aktualisierung nach erfolgreicher Anmeldung verwendet; andernfalls wird bcrypt eingesetzt.

Nach bestätigter E-Mail kannst du freiwillig Passkeys hinzufügen. Face ID, Fingerabdruck oder Geräte-PIN werden durch dein Gerät beziehungsweise deinen Passkey-Anbieter geprüft. KTCards erhält keine biometrischen Merkmale und keinen privaten Passkey-Schlüssel. Gespeichert werden der öffentliche Prüfschlüssel, eine technische Kennung, Sicherheitszähler und der Anlagezeitpunkt. Bei Nutzung eines synchronisierten Passkeys gelten ergänzend die Bedingungen deines Geräte- oder Passkey-Anbieters.

Ein Passwort-Wiederherstellungslink gilt 30 Minuten, ist nur einmal verwendbar und wird nur an eine bereits bestätigte Konto-E-Mail versendet. Eine erfolgreiche Wiederherstellung sperrt bisherige Sitzungen und Passkeys. Hast du keinen Zugriff auf die bestätigte E-Mail, hilft der Store nach Identitätsprüfung. Aus Sicherheitsgründen geben Anforderungsseiten nicht bekannt, ob eine fremde E-Mail registriert ist.

4. Freiwillige Service-Push-Mitteilungen

Service-Push wird erst nach ausdrücklicher Bestätigung der Service-Hinweise und der Browserberechtigung eingerichtet. Volljährige können Service-Push nach Bestätigung selbst am Gerät aktivieren. Eine ausdrückliche Sperre oder eine notwendige Minderjährigenfreigabe bleibt zu beachten. Die Aktivierung ist erst nach bestätigter Speicherung abgeschlossen; eine Browsererlaubnis allein genügt nicht. Wir speichern technische Abonnementadresse und Schlüssel, Zeitpunkt und Version der bestätigten Hinweise. Eine ältere Browsererlaubnis allein genügt nicht.

Die Mitteilungen betreffen bestehende Servicevorgänge, etwa Reservierungen, ausgewählte Events, Grading und abholbereite Promos. Allgemeine Werbe- und automatische Umfrage-Pushs sind ausgeschlossen. Die Benachrichtigung enthält einen allgemeinen Hinweis, keine Kundenakte oder Auftragsdetails. Der Nachrichteninhalt wird vor Übergabe an den Pushdienst verschlüsselt; technische Verbindungs- und Zustellungsdaten bleiben für den Transport erforderlich.

Je nach Browser läuft die Zustellung über Apple, Google oder Mozilla. Dabei können unter anderem die technische Geräte-/Browserzuordnung, IP-Adresse, Zeitpunkt und Zustellungsdaten bei diesen Anbietern verarbeitet werden, auch außerhalb des EWR, insbesondere in den USA. Es wird kein Firebase-Analyse-SDK in die App eingebunden. Für die browserseitigen Dienste gelten zusätzlich die Hinweise des von dir verwendeten Browseranbieters. Informationen zu deren Verarbeitung und internationalen Übermittlungen einschließlich der dort beschriebenen Garantien und Anforderung von Standardvertragsklauseln findest du bei Apple, Google und Mozilla. Du kannst nähere Informationen zum konkreten KTCards-Vorgang auch unter info@ktcards.de anfordern.

„Push auf allen Geräten deaktivieren“ entfernt die serverseitigen Abonnements und aktiven Bestätigungen. Zusätzlich kannst du die Browserberechtigung entziehen. Die übrige App bleibt ohne Push nutzbar.

Instagram-Direktnachrichten

Wenn du uns über Instagram schreibst und die Verbindung eingerichtet ist, übernehmen wir neue Direktnachrichten in unser geschütztes CRM und können dir von dort antworten. Verarbeitet werden Nachrichteninhalt, Instagram-Konto- und Kontaktkennungen, Zeitpunkte, interne Bearbeitungsinformationen und Versandstatus. Die Bearbeitung deiner vertraglichen oder vorvertraglichen Anfrage beruht auf Art. 6 Abs. 1 Buchst. b DSGVO; bei sonstigen Anfragen auf unserem berechtigten Interesse an ihrer Bearbeitung nach Art. 6 Abs. 1 Buchst. f DSGVO. Eine Zuordnung zu einem Kundenkonto erfolgt nicht automatisch. Likes, Follower-Meldungen und Reaktionen werden nicht für CRM-Tickets übernommen. Bei Anhängen speichern wir einen Hinweis; Medien werden nicht automatisch abgerufen. Für Instagram gelten außerdem die Datenschutzhinweise von Meta Platforms Ireland Limited. Die von uns abgesendete Antwort und die zu ihrer Zustellung erforderlichen Kennungen werden an Meta übertragen.

Instagram-Verläufe unterliegen im Portal denselben zweckbezogenen Aufbewahrungs-, Archivierungs- und Löschprüfungen wie andere CRM-Anfragen. Geschäftlich aufbewahrungspflichtige Inhalte und offene Rechtsansprüche werden entsprechend Abschnitt 7 gesondert behandelt. Das Entfernen einer Portal-Kopie löscht keine bei Instagram gespeicherten Nachrichten. Für Betroffenenrechte gegenüber KTCards kannst du dich an die oben angegebene Kontaktadresse wenden.

Monatsunterlagen für die Steuerberatung enthalten erforderliche Gutscheinbewegungen sowie abgeschlossene

Kassenformulare und deren notwendige Anlagen. Einlösbare Gutscheincodes werden in den neuen PDF-/CSV-Exporten nicht ausgegeben. Monatsfassungen werden im Portal geschützt archiviert; berechtigte Mitarbeitende können sie für die gesonderte Weitergabe an die Steuerberatung herunterladen.

5. Kundenkarte, Veranstaltungen und Servicevorgänge

Karte und QR-Code ordnen dich deinem Kundenkonto zu. Bei Locals und Events werden erforderliche Teilnahme-, Spiel-, Spieler-ID- und gegebenenfalls Altersklassenangaben verarbeitet. Externe Turnierangebote, die du separat nutzt, unterliegen deren eigenen Informationen. Wünsche, Wartelisten, Reservierungen, Promonachlieferungen und Nachrichten werden zur Bearbeitung des jeweiligen Anliegens gespeichert. Neue Wartelisteneinträge erfolgen für eine Person mit einem Platz pro aktivem Eintrag; Begleitpersonen werden nicht neu erfasst. Bestehende gemeinsame Einträge bleiben bis zur gesonderten Bearbeitung erhalten.

Eine von dir ausgelöste Gutscheinprüfung kann den Code über JTL-Vouchers prüfen; sie ist keine Einlösung. Bestehende Guthabenansprüche entfallen durch die Löschung des App-Zugangs nicht. Bei Bestell- oder Zahlungsvorgängen werden erforderliche Angaben mit JTL beziehungsweise Mollie verarbeitet. Mollie verarbeitet die eigentliche Zahlung in eigener Verantwortung. Vollständige Kreditkartendaten werden nicht als App-Profilangabe benötigt.

Für einen beauftragten Grading-Vorgang erhält GSG im Paket einen Einreichungsbogen mit erforderlichem Namen, Anschrift, Kartendaten und KTCards-Auftragsnummer. Der Portalablauf überträgt diese Kundendaten nicht automatisch elektronisch an GSG. Erforderliche Versand- und Empfangsnachweise werden dem Vorgang zugeordnet.

Digitale Kassenbelege und Zahlungen im Store

Bei Retouren, Korrekturen der Zahlungsart und besonderen Zahlungsvorgängen am Tresen erfassen wir die für den Vorgang erforderlichen Angaben. Dazu gehören je nach Vorgang Datum, Betrag, Kasse und Bonnummer, die Zahlungs- oder Erstattungsart, der Grund, gegebenenfalls eine Unterschrift und Fotos oder Kopien der benötigten Belege. Die Angaben dienen der Durchführung des jeweiligen Geschäfts und der Buchführung (Art. 6 Abs. 1 Buchst. b beziehungsweise c DSGVO). Für die Klärung von Zahlungsabweichungen und Ansprüchen verarbeiten wir erforderliche Angaben auch im berechtigten Interesse an einer nachvollziehbaren Abwicklung (Art. 6 Abs. 1 Buchst. f DSGVO).

Berechtigte Mitarbeitende bearbeiten Entwürfe im Portal. Abgeschlossene Vorgänge werden mit den benötigten Anlagen als Buchungsbelege archiviert und können in die Monatsunterlagen übernommen werden. Die Aufbewahrung richtet sich nach der Art des Belegs und den in Abschnitt 7 genannten Kriterien.

Bei einer Mollie-Zahlung am Tresen übermitteln wir Betrag und technische Vorgangsreferenzen an Mollie und rufen den Zahlungsstatus ab. Die Zahlungsdaten gibst du bei Mollie ein. Bei einer PayPal-Zahlung verarbeitet PayPal die eigentliche Zahlung. Wir erfassen für die Zuordnung zum Kassenbeleg nur die erforderlichen Zahlungsangaben.

6. Empfänger

Berechtigte Mitarbeitende erhalten Zugriff nach ihrer Aufgabe. Je nach genutzter Leistung können Daten an folgende Empfängerkategorien gelangen: ALL-INKL für Hosting von App und Portal; ecomDATA für die eingesetzten IT-/Warenwirtschaftsleistungen und die Mailpostfächer; JTL/JTL-Vouchers für Warenwirtschaft und Gutscheine; Mollie und PayPal für die jeweils gewählte Zahlung; Amazon Web Services für Schlüsselverwaltung und externe Sicherungen; GSG für beauftragtes Grading; erforderliche Versanddienstleister für eine vereinbarte Versendung; die in Abschnitt 4 genannten Browser-Pushdienste. Gesetzlich erforderliche Übermittlungen an Behörden, Gerichte oder zur konkreten Rechtsverfolgung bleiben vorbehalten.

WhatsApp, Discord, Instagram, Google-Bewertungen, YouTube und der Shop können verlinkt sein. Erst das Öffnen eines Links führt zum jeweiligen externen Angebot. Der App-Ablauf bettet solche Videos nicht automatisch ein. Eine konfigurierte serverseitige Livestream-Abfrage übernimmt keine Kundenprofile in die Abfrage.

Geschützte Dokumentablage und AWS KMS

Kundenunterlagen, Auftrags-PDFs und zugeordnete Dateien werden im Portal geschützt abgelegt. Nach Freischaltung der Kunden-KMS-Verschlüsselung erhält jede neue Datei einen zufälligen Dokumentenschlüssel. AWS Key Management Service schützt diesen Schlüssel mit einem vom Personalschlüssel getrennten Kundenschlüssel in der gewählten Region Frankfurt (eu-central-1). AWS erhält dafür die zufälligen Schlüssel und technische Zugriffs- und Kontextinformationen; Dokumentinhalte werden für diese Schlüsselverarbeitung nicht an AWS übertragen. Die Anmeldung erfolgt mit kurzlebigen Berechtigungen über IAM Roles Anywhere.

Vorhandene Dateien werden erst nach ausdrücklich gestarteter, geprüfter Umstellung in dieses Verfahren übernommen. Alte Sicherungskopien werden dadurch nicht automatisch nachverschlüsselt. Rechteprüfung und geschützte Übertragung bleiben zusätzlich erforderlich. Für AWS-Verarbeitung und gegebenenfalls internationale Zugriffe gelten die vereinbarten Auftragsverarbeitungs- und Übermittlungsregelungen. Näheres: AWS-Datenschutz und auf Anfrage bei KTCards.

7. Löschung und Aufbewahrung

Daten werden nach Wegfall ihres Zwecks gelöscht oder auf das noch erforderliche Maß beschränkt. Offene Vorgänge, Ansprüche und gesetzliche Nachweispflichten werden vor einer Löschung einzeln geprüft. Die Kontolöschung umfasst deshalb nicht automatisch alle geschäftlichen Originalunterlagen.

BereichFrist oder maßgebliches Kriterium
Inaktiver App-ZugangHinweis nach elf Monaten ohne App-Nutzung oder Local-Check-in; anschließend 30 Tage Bedenkzeit ab Übergabe des Hinweises an den Mailserver. Offene Fälle werden gesondert geprüft.
Local-Teilnahmen / eigene SaisonwertungenLocal-Check-ins grundsätzlich zwölf Monate; personenbezogene eigene Turnier-/Saisondaten grundsätzlich 90 Tage nach Saisonende.
Abgeschlossene Wünsche, Wartelisten, Reservierungen und PromonachlieferungenGrundsätzlich 30 Tage nach endgültigem Abschluss, sofern keine offenen Ansprüche oder anderen Nachweiszwecke bestehen.
Umfragen / BewertungenPersonenbezogene Umfrageantworten grundsätzlich 30 Tage nach Ende, Bewertungen grundsätzlich 90 Tage nach Eingang; gegebenenfalls bleibt eine anonyme Auswertung.
Push-ZustellprotokolleGrundsätzlich 14 Tage nach endgültiger Verarbeitung und Ablauf der Nachricht.
Grading-FotosNach bestätigter Abholung bzw. Rückgabe und Prüfung, dass kein weiterer Foto- oder Anspruchsnachweis nötig ist. Geschäftsbelege werden getrennt behandelt.
GeschäftsunterlagenJe nach Einordnung regelmäßig sechs Jahre für Geschäftsbriefe, acht Jahre für Buchungsbelege und

zehn Jahre für Bücher/Abschlüsse, gerechnet ab dem einschlägigen Jahresende (§ 257 HGB, § 147 AO). Besondere Pflichten und offene Verfahren können längere Speicherung erfordern.
Digitale Kassenbelege und MonatsarchivDigitale Buchungsbelege einschließlich notwendiger Anlagen und Retourenunterschrift grundsätzlich acht Jahre. Zusammengefasste Monatsunterlagen mit Buchführungsauswertungen grundsätzlich zehn Jahre. Die Fristen beginnen am maßgeblichen Jahresende; offene steuerliche oder rechtliche Verfahren können sie verlängern. Nach Ablauf werden freigegebene Daten und Dateien im Wartungslauf gelöscht. Korrekturketten, offene Zahlungen, Klärungen und begründete Sperren werden vorab geprüft. Kopien beim Steuerberater oder DATEV werden getrennt verwaltet. Grundlage der gesetzlichen Aufbewahrung ist Art. 6 Abs. 1 Buchst. c DSGVO in Verbindung mit den anwendbaren Aufbewahrungsvorschriften.
Registrierungs- und BestätigungslinksRegistrierungs- und E-Mail-Bestätigungslinks 24 Stunden, Wiederherstellungslinks 30 Minuten. Abgelaufene oder ersetzte offene Link-E-Mails werden vor Versand aus der Warteschlange entfernt; verbleibende technische Link-E-Mail-Nachweise werden nach 30 Tagen bereinigt.AuskunftspaketeFreigegebene Downloadpakete sind sieben Tage abrufbar. Vorbereitete Arbeitskopien werden grundsätzlich 30 Tage nach dokumentiertem Abschluss entfernt, sofern keine begründete Aufbewahrungssperre besteht. Bei Ablauf, Widerruf oder endgültiger Zugangssperre werden Inhalt und Empfängeradresse in den vorgesehenen Bereinigungsläufen entfernt. Technische Bereitstellungsnachweise werden grundsätzlich nach 30 Tagen bereinigt.
Datenschutz-FallnachweiseNur soweit für Bearbeitung und erforderliche Anspruchsabwehr nötig: grundsätzlich bis Ende des dritten Folgejahres nach dokumentierter Antwort, früher bei Zweckwegfall. Das ist keine allgemeine gesetzliche Mindestaufbewahrung; offene Fälle und begründete Sperren werden gesondert geprüft.

Technische Bereinigungen laufen in begrenzten Arbeitsschritten; offene Sperren oder Fehler erfordern eine Nachbearbeitung. Sicherheits- und Zugriffsprotokolle werden nur soweit und solange für den sicheren Betrieb oder einen konkreten Vorfall erforderlich verarbeitet. Technische Lösch-/Sperrmarker dienen dazu, gelöschte Zugänge und Daten nicht unbeabsichtigt wieder zu übernehmen; ihre Notwendigkeit wird in Zusammenhang mit offenen Vorgängen und verfügbaren Altsicherungen überprüft.

Native JTL-POS-Kassensicherungen können die in der Kasse gespeicherten Kunden-, Vorgangs- und Zahlungsdaten enthalten. Sie werden aus dem dafür eingerichteten Kassenpostfach nach Absender- und Kassenzuordnung verschlüsselt übernommen. Eine Mail wird erst nach vollständiger Speicherung und erfolgreicher Rückleseprüfung aller Anhänge gelöscht. Die Originaldateien sind nur für berechtigte Administratoren zur Wiederherstellung abrufbar. Technische Kassensicherungen werden grundsätzlich 30 Tage aufbewahrt; die letzte geprüfte Sicherung jeder Kasse bleibt bis zu einer erfolgreichen Folgesicherung erhalten. Kopien in vollständigen Portal-Sicherungspaketen unterliegen zusätzlich deren eigenem Sicherungszyklus. Zur Prüfung zurückgestellte Mails bleiben im Postfach, bis ihre Verarbeitung oder Entfernung geklärt wurde. Technische Prüfnotizen enthalten Grund und Anhangsmetadaten, keine Mailtexte; sie werden nach 30 Tagen beim Wartungslauf entfernt.

Hoster-Sicherungen dienen der Wiederherstellung und stehen nicht als normale Kundenakte zur Verfügung. Daten in Sicherungen und externen Postfächern werden getrennt vom aktiven Portalbestand behandelt. Bei Wiederherstellung muss der jüngere Lösch-/Sperrstand vor erneutem Betrieb berücksichtigt werden. Die Löschung im Portal allein entfernt keine externe Mail- oder Sicherungskopie.

Zur Wiederherstellung nach technischen Störungen erstellen wir verschlüsselte Sicherungen. Bei aktiviertem vollständigem Sicherungsjob umfassen sie die Portal-Datenbank und separate Dokumentdateien. Bei aktivierter externer Sicherung werden die verschlüsselten Pakete nach Amazon S3 in Frankfurt (eu-central-1) übertragen und beim Rücklesen geprüft. Ein separat verschlüsseltes Wiederherstellungspaket enthält die Portal-Konfiguration; der private Wiederherstellungsschlüssel wird getrennt aufbewahrt. Die Verarbeitung dient unserem berechtigten Interesse, Datenverluste zu vermeiden und den Betrieb wiederherstellen zu können (Art. 6 Abs. 1 Buchst. f DSGVO). Vom vollständigen Sicherungsjob verwaltete Pakete werden

grundsätzlich sieben Tage aufbewahrt. Die letzte geprüfte Sicherung bleibt bis zu einer erfolgreichen Folgesicherung erhalten. Alte Pilotkopien, Hoster-Sicherungen und gegebenenfalls vorhandene S3-Objektversionen werden gesondert bereinigt. Nach einer Wiederherstellung wird vor erneutem Betrieb der aktuelle Lösch- und Sperrstand berücksichtigt.

8. Minderjährige

Nach unserer Store-Regel ist die Online-Registrierung ab 18 Jahren möglich. Du bestätigst die Volljährigkeit; dafür wird bei Erwachsenen kein zusätzliches Geburtsdatum verlangt. Neue Konten werden erst nach Bestätigung eines einmaligen, 24 Stunden gültigen E-Mail-Links erstellt. Nicht bestätigte Registrierungsentwürfe werden nach Ablauf in den Bereinigungsläufen entfernt. Eine vorhandene Kundenkarte wird nicht allein wegen eines gleichen Namens automatisch verknüpft; die Zuordnung erfolgt im Store nach Prüfung.

Für Personen von 7 bis 17 Jahren prüfen Mitarbeitende im Store Sorgeberechtigung und Zustimmung und verknüpfen das Minderjährigenkonto mit einem Elternkonto. Ein Elternkonto reicht. Für die Altersprüfung wird beim Minderjährigenkonto das Geburtsdatum geschützt gespeichert. Die Zuordnung endet mit Volljährigkeit bei der automatischen Altersprüfung; die Prüfungen erfolgen bei Nutzung und im eingerichteten Wartungslauf. Die bloße Verknüpfung gewährt keinen pauschalen Zugriff auf sämtliche Vorgänge des anderen Kontos. Anlegen, Ändern und Aufheben erfolgen durch berechtigte Mitarbeitende. Nach Aufhebung einer Zuordnung bleibt die erforderliche Altersbegrenzung bis zur Volljährigkeit erhalten.

Service-Push für ein Minderjährigenkonto setzt zusätzlich eine geprüfte sorgeberechtigte Person und gesonderte Freigabe voraus. Zustimmung und Berechtigung werden im Store dokumentiert; die freiwillige Geräteaktivierung kommt hinzu. Es erfolgt keine pauschale Freigabe unbekannter Minderjährigenkonten durch eine Erwachsenenbestätigung in der App.

9. Deine Rechte

Du hast nach Maßgabe der DSGVO Rechte auf Auskunft, Berichtigung, Löschung, Einschränkung und Datenübertragbarkeit. Einwilligungen kannst du jederzeit für die Zukunft widerrufen. Bei einer Verarbeitung aufgrund berechtigter Interessen kannst du aus Gründen deiner besonderen Situation widersprechen; gegen Direktwerbung kannst du jederzeit widersprechen. Wende dich an info@ktcards.de.

Der App-Selbstauszug ist eine Teilauskunft. Für eine vollständige Auskunft prüfen wir auch zugehörige Geschäftsunterlagen und weitere Quellen. Anfragen auf Datenauskunft und Kontoschließung können in der App oder auf anderem Weg eingehen und werden gemeinsam im Portal bearbeitet. Eine Kontoschließungsanfrage beendet den Zugang nicht sofort; die Administration prüft zunächst Identität, Antwortweg, offene Vorgänge und Aufbewahrung. Bei gleichzeitig gewünschter Auskunft wird diese vor der Schließung bereitgestellt. Die Schließung entfernt App-Anmeldedaten und sperrt die Karte, bestätigt aber keine vollständige Löschung aller Geschäftsunterlagen. Eine getrennt geschützte Antwortadresse dient der Bearbeitung und wird nach dokumentierter Antwort aus dieser Ablage entfernt. Eine geprüfte Auskunft wird als PDF, bei beigefügten Unterlagen als ZIP mit Haupt-PDF, über einen eigenen befristeten Link und getrennten Zugangscode bereitgestellt. Der Abruf ist auch nach Kontoschließung möglich. Der Code wird über einen gesondert geprüften sicheren Weg übergeben; ein Store-Besuch ist dafür nicht zwingend. Die Antwort ersetzt nicht die Prüfung aller verbleibenden Daten. Bei begründeten Zweifeln können wir eine angemessene Identitäts-/Vertretungsprüfung verlangen. Wir antworten grundsätzlich unverzüglich und spätestens innerhalb eines Monats; zulässige Verlängerungen werden begründet mitgeteilt.

Du kannst dich bei einer Datenschutzaufsichtsbehörde beschweren, insbesondere beim Unabhängigen Landeszentrum für Datenschutz Schleswig-Holstein.

Event-Decklisten

Bei entsprechend gekennzeichneten Events kannst du bis zum Eventstart eine Deckliste als PDF oder Foto übermitteln, auch als Gast ohne App-Konto. Erforderlich sind Name und Spieler-Tag, bei Pokémon stattdessen Spieler-ID und Geburtsjahr. Die Angaben dienen der Durchführung und regelgerechten Organisation des Events (Art. 6 Abs. 1 Buchst. b DSGVO). Fehlende Spielerangaben eines angemeldeten Kontos werden aus der Abgabe in dessen Profil ergänzt; vorhandene Angaben werden nicht stillschweigend ersetzt. Weitere bewusste Abgaben bleiben zur Klärung nebeneinander erhalten.

Die Dateien werden normalisiert und mit dem eingerichteten AWS-KMS-Schutz gespeichert. Berechtigte Store-Mitarbeitende und dem Event zugewiesene Judges können sie einsehen. Teilnehmerlisten und Druckausgaben sind ebenfalls auf diese Berechtigungen beschränkt. Decklisten sind keine öffentlich zugänglichen Dokumente. Bitte keine zusätzlichen Kontaktdaten oder sonstigen unnötigen Angaben hochladen. Ähnliche Namen und Spielerkennungen werden nur als Prüfhinweis verwendet und führen nicht automatisch zur Zusammenführung von Personen.

24 Stunden nach Eventende endet der Zugriff; Dateien und zugehörige Angaben werden im regelmäßigen Wartungslauf entfernt. Sicherungskopien unterliegen dem gesonderten Sicherungs- und Löschverfahren. Zum Schutz des Uploads werden zeitlich begrenzte, pseudonymisierte Sitzungs- und Netzwerkzähler verwendet; sie werden nach einem Tag bereinigt. Kalenderexporte enthalten Eventdaten, keine Teilnehmerdaten.

Öffentlicher Shop-Kalender

Der eingebettete Kalender stellt ausschließlich freigegebene Eventdaten und Spiellogos bereit. Der Aufruf benötigt keine App-Anmeldung und setzt durch die Kalenderfunktion kein Anmelde- oder Trackingcookie. Die technische Bereitstellung verarbeitet die üblichen Verbindungsdaten wie IP-Adresse im Rahmen des Hostings. Es werden keine Teilnehmernamen oder Decklisten veröffentlicht. Freiwillige App-Aktionen öffnen die Kunden-App; Anmeldung und Kontorechte werden dort geprüft. Kalenderexporte sind einmalige Kopien und kein automatisch aktualisierter Kalender. Für den früher eingebetteten Google-Kalender gelten bis zu dessen tatsächlicher Entfernung die bisherigen Hinweise des Onlineshops weiter.

10. Änderungen

Diese Hinweise werden bei Änderungen der Funktionen oder Datenverarbeitung aktualisiert. Die aktuelle Fassung ist in der App erreichbar.

Einmal-Freigabe zur Registrierung im Store

Für eine neue Kundenkarte erhalten volljährige Personen am Tresen einen zufällig erzeugten Einmal-QR-Code. Er erlaubt den Start fünf Minuten lang. Beim bewussten Start wird er einmalig an die aktuelle Browsersitzung gebunden; für die Angaben bleiben 30 Minuten. Anschließend bestätigt die Person ihre E-Mail-Adresse mit dem gesonderten Bestätigungslink. Der QR-Code enthält keine Kundendaten. Gespeichert werden sein Prüfwert, ausgebender Mitarbeiter, Filiale, Gültigkeit und Verwendungsstatus. Abgelaufene Freigabedatensätze werden spätestens im nächsten Wartungslauf nach einer zusätzlichen

technischen Nachweisfrist von 24 Stunden bereinigt. Eine Freigabe ist kein Alters- oder Identitätsnachweis; bestehende Kundenkarten werden weiterhin im Store zugeordnet.

Die Sitzungsbindung dient der angeforderten Kontoerstellung und dem Schutz vor mehrfacher Verwendung. Rechtsgrundlagen sind Art. 6 Abs. 1 Buchst. b DSGVO für die angeforderte Kontoerstellung und Art. 6 Abs. 1 Buchst. f DSGVO für die Missbrauchsabwehr. Ein erhaltener Code kann vor seiner ersten Verwendung weitergegeben werden; deshalb wird er pro Person erst am Tresen ausgegeben.

Check-in bei vorübergehendem Internetausfall

Das Team kann Kundenkarten für einen zuvor online vorbereiteten Local-Tag offline scannen. Auf dem Mitarbeitergerät werden nur verschlüsselte Kartencodes mit Scanzeit und Zuordnung zu Spiel oder Store-Event vorgemerkt. Es wird keine Kundenkartei auf das Gerät heruntergeladen. Die Vormerkung enthält keine Bestätigung der Kartenidentität und zählt erst nach Prüfung auf dem Server als Teilnahme. Die normalen Check-in-Zwecke und Rechtsgrundlagen gelten auch für diesen Übertragungsweg.

Die Erfassung gilt nur für den vorbereiteten Tag. Ein Abgleich ist bis 24 Stunden nach Ende dieses Tages möglich, nur mit dem ursprünglichen berechtigten Mitarbeiterkonto und in derselben Filiale. Bestätigte Vormerkungen werden vom Gerät entfernt. Abgelaufene Vormerkungen werden beim nächsten Aufruf oder laufender Offline-Seite nach Ablauf entfernt; dabei wird zur manuellen Nachprüfung nur eine Anzahl für höchstens sieben weitere Tage angezeigt. Browser, die gerade geschlossen sind, können keine aktive Bereinigung ausführen. Serverseitige Vorbereitungsschlüssel und technische Wiederholungsbelege werden beim nächsten Wartungslauf nach Ende der Abgleichfrist entfernt. Die Gerätedaten dienen ausschließlich der zuverlässigen Übertragung im ausdrücklich genutzten Check-in; es findet damit kein Tracking statt.

Registrierung und erste Local-Teilnahme

Neue Registrierungen werden vom Store freigegeben. Nach Freigabe gilt: Innerhalb von 30 Tagen nach bestätigter Kontoerstellung muss mindestens ein tatsächlich erfasster, nicht stornierter Local-Check-in vorliegen, sofern KTCards keine begründete Ausnahme hinterlegt. Für bei Einführung vorhandene Beta-Konten beginnt eine neue Frist von 30 Tagen am Einführungstag. Es gibt keine Erinnerungsmail. Bei Fristablauf werden App-Anmeldedaten, Passkeys und Sitzungszugänge gelöscht beziehungsweise unwirksam gemacht. Die Kundenkarte, offene Geschäftsvorgänge und aufzubewahrende Unterlagen werden gesondert behandelt. Auskunft oder Überprüfung einer fehlerhaften Zuordnung kann über den Store verlangt werden.

Für Prüfung und sichere Zugangsverwaltung werden Kontoerstellungsdatum, gültige Teilnahmen, Frist und gegebenenfalls eine begründete Ausnahme verarbeitet. Rechtsgrundlage ist die Durchführung der vereinbarten App-Zugangsbedingungen (Art. 6 Abs. 1 Buchst. b DSGVO), für Sicherheits- und Nachweiszwecke das berechtigte Interesse am sicheren Betrieb (Art. 6 Abs. 1 Buchst. f DSGVO). Lokale technische Datenbanksicherungen werden verschlüsselt sieben Tage vorgehalten; die letzte erfolgreiche Sicherung bleibt bei ausbleibender Folgesicherung erhalten. Eine Wiederherstellung darf gelöschte Zugänge nicht unbeabsichtigt reaktivieren; bestehende Wiederherstellungssperren und Löschabgleiche sind anzuwenden.

Datenschutzhinweise zum Ticketkauf · Stand 08.11.2026
KTCards · Tobias Schultz · Am Markt 9 · 24568 Kaltenkirchen · Telefon 04191 2748564 · info@ktcards.de

Für Bestellung, Zahlung, Dokumentversand und Einlass verarbeiten wir Käufername, Rechnungsanschrift, E-Mail, gebuchte Veranstaltung, Ticketnummer und Zahlungsreferenz (Art. 6 Abs. 1 lit. b DSGVO). Mollie verarbeitet die zur Zahlung

notwendigen Angaben; vollständige Zahlungsinstrumente werden nicht im Portal gespeichert. JTL-Wawi erhält die zur Auftrags- und Rechnungserstellung nötigen Daten über JTL-Ameise auf unserem geschützten Windows-Rechner. Die Übertragung erfolgt verschlüsselt. Temporäre Importdateien werden nach dem Lauf entfernt. Lokale Diagnoseberichte werden benutzergebunden verschlüsselt und nach 30 Tagen beim nächsten Lauf gelöscht. Ein ungeklärter Import bleibt bis zur Klärung vorgemerkt. Die Auftrags- und Belegaufbewahrung bleibt davon unberührt. Auftragsbezogene Nachrichten gehen an die angegebene E-Mail und bei Kontonutzung in dein App-Postfach.

Gastkauf ist ohne Kundenkonto möglich. Begleitpersonen werden nicht durch eine Namenssuche mit bestehenden Konten verbunden. Ein eigenes Konto wird erst beim persönlichen Vorzeigen der Kundenkarte zugeordnet. Ticketcodes sind zufällige Zugangskennungen ohne Namen im Code. Behandle Ticket und Buchungslink vertraulich.

Aufbewahrung: Buchungs- und Zahlungsbelege grundsätzlich acht Jahre, empfangene und abgesandte Geschäftsbriefe grundsätzlich sechs Jahre, jeweils ab Ende des maßgeblichen Kalenderjahrs. Gesetzlich erforderliche längere Bindungen und dokumentierte Aufbewahrungssperren werden berücksichtigt (Art. 6 Abs. 1 lit. c DSGVO). Erfolglos beendete, unbezahlte Vorgänge ohne offene Geldbewegung werden nach 30 Tagen gelöscht. Saisonberechtigungen und ihre Prüflisten bleiben bis zwei Jahre nach Saisonende intern abrufbar (Art. 6 Abs. 1 lit. f DSGVO: nachvollziehbare Saisonfreigabe); sie erscheinen nur während ihrer Gültigkeit in der App.

Weitere Empfänger, Hosting, verschlüsselte Sicherungen sowie deine Rechte auf Auskunft, Berichtigung, Löschung, Einschränkung, Datenübertragbarkeit, Widerspruch und Beschwerde bei der Datenschutzaufsicht sind in den ergänzenden allgemeinen Datenschutzhinweisen der KTCards-App beschrieben. Diese Hinweise sind vor Bestellung abrufbar und werden der Vertragsbestätigung beigefügt.