

Besondere Datenschutzhinweise des FC Ingolstadt 04 GmbH gemäß Artikel 13, 14 DSGVO im Rahmen der Abwicklung von Kreditkarten-Zahlungen

Name und Kontaktdaten des Verantwortlichen

FC Ingolstadt 04 Fussball GmbH

Am Sportpark 1b 85053
Ingolstadt
DEUTSCHLAND
Postfach 100404
85004 Ingolstadt
DEUTSCHLAND
Tel: +49 841 88 55 7-0
Fax: +49 841 88 55 7-126
E-Mail: info@fcingolstadt.de
Internetseite: www.fcingolstadt.de

Kontakt Daten des Datenschutzbeauftragten

Mümtaz Kilic

Rechtsanwalt | udis zert DSB

Rechtsanwaltskanzlei Kilic
Neidhartstraße 20 86159
Augsburg
DEUTSCHLAND
Telefon: +49 821 4552265
Telefax: +49 821 4552266
E-Mail: mk@ra-kilic.de
Internetseite: www.kanzlei-kilic.de

Zwecke, für die die personenbezogenen Daten verarbeitet werden sollen, sowie die Rechtsgrundlage für die Verarbeitung

Vertragsdurchführung.

Als unser Kunde haben Sie mit FC Ingolstadt 04 Fussball GmbH (im Folgenden auch „FCI“ genannt) zahlungspflichtig einen Vertrag abgeschlossen und beim Check Out bewusst eine bestimmte Zahlungsart gewählt, wobei für die Durchführung dieser Zahlung die Übermittlung bestimmter Daten erforderlich ist.

Rechtsgrundlage:

Bei der Verarbeitung von personenbezogenen Daten, die zur Erfüllung eines Vertrages, dessen Vertragspartei die betroffene Person ist, erforderlich ist, dient uns Art. 6 Abs. 1 lit. b DSGVO als Rechtsgrundlage.

Durchführung der starken Kundenauthentifizierung nach der Richtlinie EU 2015/2366 (PSD 2) bzw. dem Zahlungsdienstenaufsichtsgesetz (ZAG).

Rechtsgrundlage:

Soweit eine Verarbeitung personenbezogener Daten zur Erfüllung einer rechtlichen Verpflichtung erforderlich ist, der unser Unternehmen unterliegt, dient Art. 6 Abs. 1 lit. c DSGVO i.V.m. mit den entsprechenden Regelungen der Richtlinie EU 2015/2366 (PSD 2) bzw. des Zahlungsdiensteaufsichtsgesetzes (ZAG). als Rechtsgrundlage.

Frictionless Flow / Optimierung von Konversionsraten / Benutzerfreundlichkeit

Rechtsgrundlage:

Ist die Verarbeitung zur Wahrung eines berechtigten Interesses unseres Unternehmens oder eines Dritten erforderlich und überwiegen die Interessen, Grundrechte und Grundfreiheiten des Betroffenen das erstgenannte Interesse nicht, so dient Art. 6 Abs. 1 lit. f DSGVO als Rechtsgrundlage für die Verarbeitung.

Betrugsprävention

Rechtsgrundlage:

Bei Verträgen, die ein kreditorisches Risiko enthalten bzw. bei denen der Vertragspartner potenziell einen Zahlungsausfall befürchten muss, kann ein berechtigtes Interesse gemäß Artikel 6 Absatz 1 Satz 1 lit. f DSGVO im Regelfall angenommen werden.

Kategorien personenbezogener Daten, die verarbeitet werden

- Informationen über den Kunden (z.B. Vor- und Nachname, Anschrift, E-Mail-Adresse, Geburtsdatum, IP Adresse);
- Informationen zu der gewählten Zahlungskarte sowie Zahlungsinformationen des Kunden (z.B. Kreditkartennummer, Status einer Zahlung);
- Informationen zur Transaktion (z.B. Ware, Artikelnummer, Kaufpreis und ähnliche Informationen);
- Informationen zum vom Kunden verwendeten Endgerät (z.B. auf dem Endgerät eingestellte Sprache);
- Informationen über aktuelle und vergangene Transaktionen des Kunden, sofern eine Bonitätsprüfung vorgenommen wird;
- Bonitätsdaten, die von Finanzinformationsdienstleistern eingeholt werden, die Aufschluss über die Bonität des Kunden geben (z.B. titulierte Forderungen gegen den Kunden).

Empfänger oder Kategorien von Empfängern der personenbezogenen Daten

Computop Wirtschaftsinformatik GmbH, welche von uns als Auftragsverarbeiter nach Artikel 28 DSGVO für die technische Steuerung von Zahlungstransaktionen einschließlich der Durchführung des 3D Secure 2.0 Verfahrens beauftragt wurde. Weitere Empfänger sind die involvierten Banken (zum einen die kartenausgebende Bank - der Issuer – und zum anderen die kreditkartenakzeptierende Bank des FCI - der Acquirer).

Datenübermittlung an ein Drittland oder an eine internationale Organisation

Die Datenverarbeitung im Computop Paygate, der Zahlungsplattform der Computop Wirtschaftsinformatik GmbH, findet in zwei Rechenzentren in Deutschland statt. Zu einem Datentransfer in Drittländer kann es potenziell in Fällen kommen, in denen die involvierten Banken in Drittländern ansässig sind.

Dauer, für die die personenbezogenen Daten gespeichert werden

FCI verarbeitet und speichert Ihre personenbezogenen Daten, solange es für die Erfüllung der vertraglichen und gesetzlichen Pflichten erforderlich ist.

Darüber hinaus unterliegt FCI verschiedenen Aufbewahrungs- und Dokumentationspflichten, die sich unter anderem aus dem Handelsgesetzbuch (HGB) und der Abgabenordnung (AO) ergeben. Die dort vorgegebenen Fristen zur Aufbewahrung bzw. Dokumentation betragen zwei bis zehn Jahre.

Schließlich beurteilt sich die Speicherdauer auch nach den gesetzlichen Verjährungsfristen, die zum Beispiel nach den §§ 195 ff. des Bürgerlichen Gesetzbuches (BGB) in der Regel drei Jahre, in gewissen Fällen aber auch bis zu dreißig Jahre betragen können, wobei die regelmäßige Verjährungsfrist drei Jahre beträgt.

Das Computop Paygate setzt standardmäßig folgende Löschfristen für Zahlungstransaktionen einschließlich 3DS 2.0 Prüfungen um:

- Computop Paygate Datenbank und Computop Analytics: Löschung von Zahlungstransaktionen nach Ablauf von 12 Monaten.
- Computop Reporter Datenbank: Löschung von Zahlungstransaktionen nach Ablauf von 24 Monaten.
- Aufbewahrung von Backups der Datenbanken für die Dauer (und Löschung dieser Backups nach Ablauf) von weiteren 12 Monaten.

Datenschutzrechte der betroffenen Person

Jede betroffene Person hat das Recht auf Auskunft nach Art. 15 DSGVO, das Recht auf Berichtigung nach Art. 16 DSGVO, das Recht auf Löschung nach Art. 17 DSGVO, das Recht auf Einschränkung der Verarbeitung nach Art. 18 DSGVO, das Recht auf Widerspruch aus Art. 21 DSGVO sowie das Recht auf Datenübertragbarkeit aus Art. 20 DSGVO. Beim Auskunftsrecht und beim Löschungsrecht gelten die Einschränkungen nach §§ 34 und 35 BDSG. Darüber hinaus besteht ein Beschwerderecht bei einer zuständigen Datenschutzaufsichtsbehörde (Art. 77 DSGVO i.V.m. § 19 BDSG).

Pflicht zur Bereitstellung von Daten

Im Rahmen der Geschäftsbeziehung müssen Sie diejenigen personenbezogenen Daten bereitstellen, die für die Aufnahme und Durchführung einer Geschäftsbeziehung und der Erfüllung der damit verbundenen vertraglichen Pflichten erforderlich sind oder zu deren Erhebung wir gesetzlich verpflichtet sind. Ohne diese Daten werden wir in der Regel den Abschluss des Vertrages oder die Ausführung des Auftrages ablehnen müssen oder einen bestehenden Vertrag nicht mehr durchführen können und ggf. beenden müssen.

Bestehen einer automatisierten Entscheidungsfindung einschließlich Profiling

Es findet eine automatisierte Authentifizierungs- bzw. Risikoprüfung statt. Auswirkung kann potenziell sein, dass die Authentifizierung möglicherweise nicht erfolgreich ist und die gewählte Zahlungsart im konkreten Fall nicht genutzt werden kann.