

Häufige Fragen & Antworten für Ihren Datenschutzbeauftragten

Hinweise zum Datenschutz von appack-Apps

Wir freuen uns über Ihr Interesse an unserem Produkt. Beim Einsatz von moderner Software und Apps ist das Thema Datenschutz ein wichtiger Aspekt. Datenschutz und Datensicherheit haben im Betrieb unserer Lösungen für uns höchste Priorität. Die Wahrung der Persönlichkeitsrechte der App-Nutzer und der Schutz bei der Verarbeitung personenbezogener Daten ist für uns eine Selbstverständlichkeit. Dieses Dokument gibt einen Überblick und beantwortet häufige Fragen zum Datenschutz, welche Sie als Herausgeber Ihrer App möglicherweise haben oder welche Sie Ihr Datenschutzbeauftragter zu Ihrer App möglicherweise fragen wird.

Rechtgrundlage DSGVO, Herausgeber und Betreiber der IT-Infrastruktur

Als Kunde von appack sind Sie der **Herausgeber** Ihrer App und für den Einsatz Ihrer App verantwortlich. Als Dienstleister helfen wir Ihnen im Auftrag Ihre App zu entwickeln und betreiben für Sie die notwendige IT-Infrastruktur (die App-Plattform appack) u.a. ein CMS und i.d.R. zwei native Apps für iOS und Android. Als **Betreiber** der IT für Ihre App sind wir gemäß DSGVO ebenso wie Sie der DSGVO verpflichtet.

Welche Module und Funktionen Sie in Ihrer App nutzen obliegt Ihnen als Herausgeber. Sie können über das CMS der App selbst, Module, Funktionen ergänzen, ändern und damit ohne unser Wissen und zutun mit Ihrer App als Werkzeug arbeiten. Daraus ergibt sich, dass Sie ggf. auch personenbezogene Daten erheben oder bearbeiten, je nachdem welche Module oder Funktionen Sie einsetzen. Ihre Datenschutzerklärung Ihrer App muss dies stets berücksichtigen.

Datenerhebung und –Verarbeitung

Identifikation eines Nutzers in einer (appack-)App

Damit eine native App auf einem Smartphone technisch funktionieren kann, muss diese Zugriff auf den Speicher des mobilen Endgerätes (Smartphone, Tablets, etc.) erhalten, den Inhalt des Speichers ggf. ändern und löschen (z.B. bei der Installation der App aus dem App Store) und bei Änderungen von App-Inhalten Daten von unserem Server abrufen können (z.B. damit die Inhalte Ihrer App stets auf dem neuesten Stand bleiben). Sämtliche Datenerhebungen und -verarbeitung erfolgt zu bestimmten Zwecken, die sich aus technischen oder vertraglichen Erfordernissen oder aus Ihren Wünschen als Herausgeber der App ergeben.

Welche Daten werden verarbeitet / ggf. optional Aufgrund von Nutzer-Eingaben erfasst?

Bei Aufruf und Nutzung einer appack App folgende Zugriffsdaten:

- App-ID (von Apple und Google – anonyme ID)
- Name des Smartphones
- Modellbezeichnung
- Betriebssystemversion
- IP-Adresse (wenn i.d.R. pseudonymisiert)
- Zeitstempel des Zugriffs
- abgefragte Ressource
- Übertragene Datenmenge und
- Dauer der Datenübertragung
- Name und Version der Browsersoftware

Die hier aufgeführten Daten werden max. 30 Tage in den Server-Log-Dateien gespeichert. Die App kann, ohne weitere personenbezogene Daten zu verarbeiten, genutzt werden.

Die App kann, sofern Sie als Herausgeber dies wünschen oder Sie Funktionen nutzen, welche einen Datenaustausch implizieren, weitere Daten erheben, z.B. Eingaben zur Nutzerauthentifizierung oder Formularfelder oder z.B. eine Anmeldung für einen Termin. Häufig sind das dann:

- Vorname
- Name
- E-Mail-Adresse

Darüber hinaus werden je nach Anwendungsfall und eingesetztem Modul ggf. weitere Informationen abgefragt. Dies können z.B. sein:

- Bilder
- Audiodaten
- Videodaten

Welche personenbezogenen Daten dabei anzugeben sind, ergibt sich aus der jeweiligen Eingabemaske. Welche das in ihrem Fall sind prüfen Sie, indem Sie entsprechende Eingabefelder in Ihrer App identifizieren. Typische Module in denen personenbezogene Daten erfasst werden sind das Profilmodul, ein Feedbackmodul, ein Terminmodul in dem die Anmeldefunktion genutzt wird.

Serverstandort / Datenspeicherung

Die Server für die IT-Infrastruktur der App werden in Deutschland betrieben. Wir beauftragen dazu spezialisierte Subunternehmer, welche ebenfalls der DSGVO unterworfen sind und vereinbarte Leistungen / Teilleistungen für Serverhosting und Object Storage gemäß DSGVO erbringen:

Subunternehmer	Beschreibung der Teilleistungen	Serverstandort / Physikalische Speicherung
IONOS SE (ehem. 1&1 Internet SE)	Serverhosting	Baden-Baden
Akenes SA (Exoscale)	Object Storage (Datenspeicher)	Frankfurt

Verschlüsselung der Datenkommunikation

Die Datenkommunikation zwischen Apps, Server und CMS findet verschlüsselt (SSL) statt. Auch mögliche App-Nutzer-Profile (sofern diese überhaupt erfasst und verarbeitet werden) werden auf der Festplatte des Servers verschlüsselt. Sie können theoretisch nur von berechtigten internen Mitarbeitern (z.B. im Supportfall) gelesen werden, welche Administratorrechte für die Datenbank besitzen.

Findet ein Nutzer-Tracking statt?

Sofern Sie uns nicht explizit dazu beauftragen, tracken wir kein Nutzerverhalten.

Auf welche Weise werden Daten erhoben?

Im Rahmen des Zugriffs auf die App oder in der App eingebundene Webseiten werden die Zugriffsdaten ggf. automatisiert protokolliert. Ansonsten werden alle weiteren Daten durch Eingaben der Nutzer erhoben.

Wofür werden Daten genutzt?

Zur Bereitstellung der Funktionen und Dienstleistungen in Ihrer App sowie zur Optimierung und zum Schutz der App und Webservices. Mit der Einwilligung der Nutzer nutzen wir Eingaben, um auf Supportanfragen/Nachrichten zu reagieren. Nur in besonderen Ausnahmen oder wenn Sie dazu eingewilligt haben, erfolgt eine Weitergabe Ihrer Daten an Dritte, z.B. zur strafrechtlichen Verfolgung bei Missbrauch oder Angriff auf unsere IT-Systeme.

Inhalte

Werblicher Informationen

Ob in der App werbliche Informationen ausgespielt werden, obliegt dem inhaltlich verantwortlichen Herausgeber der App. Personenbezogene Daten der App Nutzer werden von appack ohne ausdrückliche Einwilligung des Nutzers weder an Werbepartner noch an sonstige Dritte weitergegeben.

Verantwortung für Inhalte und Verbot illegaler Nutzung der App und der App-Plattform

a) Der Herausgeber der App (Kunde von appack) ist dafür verantwortlich, die Rechte Dritter zu wahren.

b) Für die Inhalte der App ist ausschließlich der Herausgeber verantwortlich.

c) Jede Nutzung von appack für rechtswidrige Zwecke ist untersagt. Bei jeder Nutzung sind die geltenden Gesetze, insbesondere Urheberrecht, Wettbewerbsrecht, Datenschutzrecht, Strafrecht etc. zu beachten. Jeder Verstoß kann zur sofortigen Kündigung des Vertragsverhältnisses zwischen dem Betreiber appack dem Herausgeber der App führen.

d) Es ist nicht zulässig, Inhalte einzustellen oder zu verwenden, die obszön, beleidigend, verleumderisch, gewalttätig, gewaltverherrlichend, rassistisch, fremdenfeindlich, pornographisch oder eindeutig sexuell sind oder so verstanden werden können.

e) Es ist ausdrücklich untersagt, Viren, Würmer oder anderen schädlichen Code auf appack hochzuladen oder über die App-Plattform per E-Mail zu versenden.

Social Plug-ins / Möglicher Einsatz von Plugins von Drittanbietern in einer App

Ggf. werden in der App durch den Herausgeber sog. Social Plug-ins ("Plug-ins") z.B. von sozialen Netzwerken angeboten. Mit Hilfe dieser Plug-ins können App-Nutzer beispielsweise einem Freund Inhalte weiterempfehlen oder Sharing Funktionen nutzen. In den Apps können u.a. folgende externe Plug-ins verbaut werden: Facebook, Twitter, LinkedIn, Google+, Pinterest, Youtube etc. ggf. das Geräte eigene E-Mail System für das Betriebssystem iOS oder Android. Für manche dieser Dienste muss sich der App-Nutzer ggf. bei dem Dienstleister registrieren. Zweck und Umfang der Datenerhebung durch die verschiedenen sozialen Netzwerke sowie die dortige weitere Verarbeitung und Nutzung der Daten wie auch diesbezügliche Rechte und Einstellungsmöglichkeiten zum Schutz der persönlichen Privatsphäre entnehmen Sie bitte den Datenschutzhinweisen der Drittanbieter Facebook, Google+, Twitter sowie aller weiteren Plug-in Dienste. Social Plug-ins sind nicht Teil des Produkts und der Dienstleistung von appack. Der Herausgeber der App ist verpflichtet die Nutzungsbedingungen und Datenschutzerfordernungen zu prüfen und seine App-Nutzer darüber aufzuklären.

Datensicherheit

Wir setzen technische und organisatorische Sicherheitsmaßnahmen ein, um zu gewährleisten, dass Nutzerdaten (ggf. auch persönlichen Daten) vor Verlust, unrichtigen Veränderungen oder unberechtigten Zugriffen Dritter geschützt sind. In jedem Fall haben zur Wartung, Weiterentwicklung und Pflege der appack-Plattform und einzelner Apps nur berechnigte Personen Zugriff auf personenbezogene Daten, und dies auch nur insoweit, als es im Rahmen der oben genannten Zwecke erforderlich ist. Die Sicherheitsmaßnahmen werden ständig den verbesserten technischen Möglichkeiten angepasst.

Sonstiges

Vertrag zur Auftragsdatenverarbeitung

Sollten Sie uns als Betreiber Ihrer App personenbezogene Daten zur Auftragsverarbeitung überlassen oder überlassen haben, fordert die DSGVO, dass Sie mit uns einen Vertrag zur Auftragsdatenverarbeitung schließen. [Hier](#) finden Sie weitere Informationen sowie den Vertrag dazu. Als Herausgeber der App füllen Sie diesen bitte aus, unterschreiben diesen und schicken ihn an support@appack.de

Erstellen einer Datenschutzerklärung für Ihre App

Gerne dürfen Sie sich unserer Mustervorlage für eine typ. Datenschutzerklärung bedienen. Diese Vorlage finden Sie im CMS der App bei [Seiten](#) siehe *Datenschutzerklärung Mustervorlage (kommentiert)*.

Sollten Sie Fragen oder Hinweise zum Datenschutz haben, wenden Sie sich gerne an uns: support@appack.de Bitte haben Sie Verständnis, dafür, dass wir als Softwaredienstleister keine Rechtsberatung leisten.

Appack: Eckpunkte zum Datenschutz

- Appack Apps können ohne die Erfassung von für appack oder den Herausgeber authentifizierbaren personenbezogenen Daten genutzt und betrieben werden. Wir empfehlen den Herausgebern von appack Apps -wo immer möglich- nur dort personenbezogene Daten zu erfassen, wo dies der konkrete Anwendungsfall zwingend verlangt.
- Appack betreibt seine Server in Deutschland. Es gilt die DSGVO.
- Appack nutzt einschlägige Sicherheitsstandards um Inhalte der Apps, Nutzerdaten zu sichern. Die Datenübertragung zwischen App und Server erfolgt insb. via HTTPS.
- Datenschutzerklärungen sind durch die Herausgeber der Apps an geeigneter Stelle leicht auffindbar sichtbar zu machen (z.B. im Menü der App, dem Impressum, ggf. vor der Installation der App im App-Store)
- Benötigt die App funktional Zugriffsberechtigungen des Geräts wird der Nutzer dazu gefragt und kann über das Betriebssystem der App diese Berechtigung jederzeit wieder entziehen.
- Für die Inhalte und ggf. externe Links oder Plugins von Drittanbietern in der App ist der jeweilige Herausgeber der App selbst verantwortlich und sollte diese Angebote den Nutzern entsprechend kenntlich machen.
- Das Nutzerverhalten der App-Nutzer (Bewegungsprofile) wird durch appack grundsätzlich nicht aufgezeichnet. Sie können uns dazu bei Bedarf explizit beauftragen für Sie einen ext. Dienst (wir nutzen häufig Matomo) zu betreiben.