

ÜBERSICHT NACH ART. 32 DSGVO

Technische und organisatorische Maßnahmen (TOM)

Dokumentierte Schutzmaßnahmen für die Apps, die Website und die Server von PedalArrow:
Umsetzung, Datenwege und Nachweisgrundlagen im Überblick.

Stand: 16. Oktober 2026

HTTPS verschlüsselte Verbindungen zu den Diensten	Max. 120 Sekunden Speicherdauer eines Standorts	Ende-zu-Ende verschlüsselte Gruppenfahrten	14 Tage Protokolle nur mit gekürzter IP-Adresse	2 offene Ports 80 und 443, nur für Cloudflare
---	---	--	---	---

GELTUNGSBEREICH

PedalArrow-Apps	Android und iOS
live.pedalarrow.com	Gruppenfahrten, Offline-Karten, Termine, Begriffshilfe
routing.pedalarrow.com	Routenberechnung
www.pedalarrow.com	Website, Einladungsseite
pedalarrow.de	Weiterleitung, E-Mail
pedal-arrow.com, .de	Weiterleitung auf www.pedalarrow.com

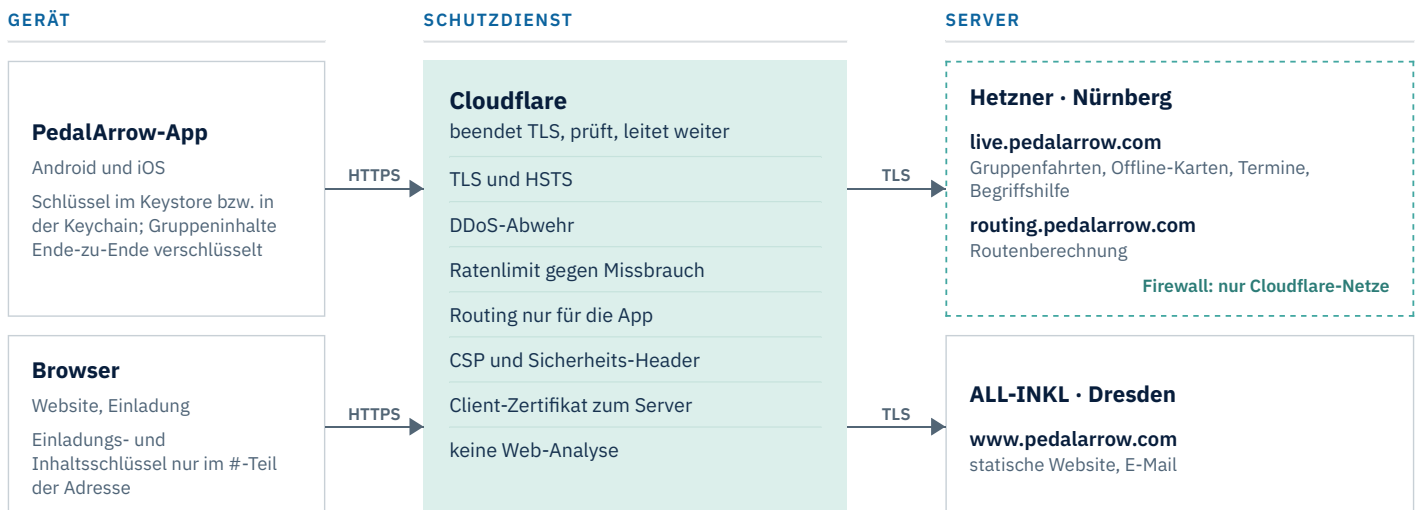
Verantwortlicher (Art. 4 Nr. 7 DSGVO): Khashayar Nivipour, München ·
info@pedalarrow.com · Anschrift im Impressum unter
www.pedalarrow.com/Impressum/

HOSTING UND ZUSÄTZLICHE DIENSTLEISTER

Cloudflare, Inc. (USA)	Schutzdienst vor Servern und Website
Hetzner Online GmbH	Server in Nürnberg
ALL-INKL.COM	Webhosting, E-Mail, DNS für pedalarrow.de; Rechenzentrum in Dresden
DeepL API	Übersetzung festgelegter Katalogbegriffe über den PedalArrow-Dienst

Betreiber von ALL-INKL.COM: Neue Medien Münnich, Friedersdorf. Rollen, Vertrags- und Übermittlungsgrundlagen sind in der Datenschutzerklärung erläutert.

Datenwege und Schutzschichten



Karten, ADFC-Bilder, Ersatz-Routing, Suche, Wetter und MVV werden direkt bei den Anbietern abgerufen. Öffentliche Termine liefert vorrangig der eigene Termindienst. Die Begriffshilfe sendet nur feste Katalogwörter vom Server an DeepL; freie Texte und Nutzer-IP bleiben ausgeschlossen. pedalarrow.de und E-Mail laufen direkt bei ALL-INKL.

41 MASSNAHMEN IN NEUN BEREICHEN

1	Zugang und Berechtigungen	4	2	Transport und Netz	5	3	Gruppenfahrt-Dienst	6
4	Apps auf dem Gerät	5	5	Website und Webhosting	4	6	Datensparsamkeit und Transparenz	7
7	Verfügbarkeit und Wartung	3	8	Entwicklung und Freigabe	3	9	E-Mail und DNS	4

So sind die Maßnahmen belegt

Die rechte Spalte nennt die Nachweise: dokumentierte Einstellungen, frühere Live-Tests oder Quellcode.

■ **Einstellung**

Dokumentierte Einstellungen der Anbieter, etwa zur Server-Firewall.

■ **Live-Test**

Vorliegende externe Prüfungen, etwa von TLS, DNS und Sicherheits-Headern.

■ **Quellcode**

Implementierung und Konfiguration der Apps und Server.

Der Stand bezeichnet die inhaltliche Aktualisierung anhand des Hauptzweigs und der Datenschutz- und Betriebsdokumentation. Frühere Einstellungs- und Live-Prüfungen werden als Nachweise übernommen; sie wurden hierfür nicht vollständig wiederholt. Das Factsheet ist keine Zertifizierung und kein Penetrationstest. Regelmäßige Wirksamkeitsprüfungen bleiben erforderlich.

1 Zugang und Berechtigungen

Art. 32 Abs. 1 lit. b DSGVO · Vertraulichkeit

MASSNAHME	UMSETZUNG	GRUNDLAGE
Zwei-Faktor-Anmeldung	Cloudflare mit TOTP, für das Konto erzwungen; Hetzner, GitHub, ALL-INKL, Google Play Console und Apple Developer (App Store Connect) ebenfalls mit zweitem Faktor.	■ Einstellung
Minimale Zugänge	Zugänge bei Cloudflare, Hetzner und in der GitHub-Organisation auf das Nötigste beschränkt; keine API-Tokens bei Cloudflare und Hetzner.	■ Einstellung
Serverzugang	SSH-Port per Firewall geschlossen, SSH nur mit Schlüssel; Verwaltung ausschließlich über die Hetzner-Konsole (Konto mit zweitem Faktor).	■ Einstellung
Webspace-Zugang	SSH-Zugang bei ALL-INKL deaktiviert; Website-Pflege über einen FTP-Nutzer mit TLS-Verschlüsselung (FTPS), der nur das Website-Verzeichnis erreicht.	■ Einstellung

2 Transport und Netz

Art. 32 Abs. 1 lit. b DSGVO · Vertraulichkeit und Integrität

MASSNAHME	UMSETZUNG	GRUNDLAGE
Verschlüsselte Verbindungen	TLS für alle Verbindungen. Dokumentierter SSL-Labs-Befund: A+ für www, live und routing, A für pedalarrow.de und mta-sts. HTTP wird auf HTTPS umgeleitet.	■ Live-Test
HSTS	Ein Jahr, mit Subdomains und Preload-Kennzeichnung.	■ Live-Test
Cloudflare bis zum Server	Modus „Full (strict)“, fest eingestellt; Cloudflare weist sich beim Server mit einem Client-Zertifikat aus eigener CA aus (Authenticated Origin Pulls). 0-RTT abgeschaltet.	■ Einstellung
Server-Firewall	Eingehend nur 80 und 443 aus den Cloudflare-Netzen und von den eigenen Servern. Ausgehend nur die für Namensauflösung, Zeitabgleich und Updates nötigen Verbindungen. Beide Regelwerke aktiv angewendet.	■ Einstellung
Zertifikatskontrolle	CAA-Einträge beschränken die Ausstellung auf die genutzten Zertifizierungsstellen; Certificate-Transparency-Überwachung aktiv; CT-Logs zeigen nur erwartete Zertifikate.	■ Live-Test ■ Einstellung

3 Gruppenfahrt-Dienst

Art. 32 Abs. 1 lit. a DSGVO · Verschlüsselung und Pseudonymisierung

MASSNAHME	UMSETZUNG	GRUNDLAGE
Pseudonyme Kennungen	Gruppenfahrten ohne Benutzerkonto; zufällige, temporäre Mitgliedskennung und frei gewählter Anzeigename.	■ Quellcode
Geheimnisse nur als Prüfwert	256-Bit-Schlüssel; der Server speichert nur BLAKE2b-Prüfwerte und vergleicht zeitkonstant (hash_equals).	■ Quellcode
Ende-zu-Ende-Verschlüsselung	Fahrtnamen, Anzeigenamen, Standort und Treffpunkt mit AES-256-GCM verschlüsselt. Inhaltsschlüssel nur in Apps und im #-Teil der Einladung, für Server und Cloudflare unlesbar. Serverseitig zusätzlich XChaCha20-Poly1305; Standorte spätestens nach 120 s gelöscht.	■ Quellcode ■ Live-Test
Flüchtige Speicherung	Daten nur in einem RAM-Dateisystem ohne Auslagerung; keine Zugriffsprotokolle; Systemjournal flüchtig, höchstens ein Tag.	■ Quellcode
Einladungsschlüssel	Nur im #-Teil des Links, nie in Serverprotokollen; beim Beitritt TLS-geschützt gesendet, gespeichert nur als Prüfwert. Sitzung in der App nur im Arbeitsspeicher.	■ Quellcode
Begrenzte Schnittstellen	Begrenzte Schnittstellen für Gruppenfahrten, Status, Offline-Karten, Termine und Begriffshilfe; feste Fehlercodes. Die Begriffshilfe akzeptiert nur geprüfte Begriff-IDs.	■ Quellcode

4 Apps auf dem Gerät

Art. 32 Abs. 1 lit. a und b DSGVO · Vertraulichkeit

MASSNAHME	UMSETZUNG	GRUNDLAGE
Android	Kein Backup, kein unverschlüsseltes HTTP, nur System-CAs; Schlüssel im Keystore (AES-GCM); Bildschirmschutz (FLAG_SECURE); R8; Kartenbibliothek nur zu den geprüften Kartendiensten; keine Hintergrund-Standortberechtigung; nur notwendige Aktivitäten exportiert.	 Quellcode
iOS	App Transport Security ohne Ausnahmen; Keychain „WhenUnlockedThisDeviceOnly“; vollständiger Dateischutz; vom Backup ausgenommen; flüchtige Netzwerksitzungen ohne Cookies; Kartenbibliothek nur zu den geprüften Kartendiensten; gewähltes Offline-Gebiet mit gerätegebundenem Schlüssel versiegelt.	 Quellcode
Sparsame Berechtigungen	Kein Zugriff auf Adressbuch oder Fotomediathek: Kontakte werden über die Systemkarte angelegt, der Einladungscode gelangt nicht in die Fotomediathek. Keine Rechte für Herzfrequenz, Trittfrequenz und Leistung; Übertragung an Health Connect oder Apple Health nur nach gesonderter Einwilligung.	 Quellcode
Kein eigenes Tracking	Keine Werbe-, Tracking- oder eigenen Crash-SDKs. Google ML Kit verarbeitet Termintexte lokal; Modellabruf und SDK-Betrieb können technische Nutzungs- und Diagnosedaten an Google übermitteln.	 Quellcode
Bestätigte App-Links	Einladungslinks öffnen die App direkt; die Zuordnungsdateien für App Links und Universal Links sind veröffentlicht und von Google und Apple bestätigt.	 Live-Test

5 Website und Webhosting

Art. 32 Abs. 1 lit. b DSGVO · Integrität

MASSNAHME	UMSETZUNG	GRUNDLAGE
Statische Seiten	Keine Formulare, keine externen Ressourcen, keine Cookies der Website selbst; Content Security Policy ohne Drittanbieter, zusätzlich am Webserver.	 Live-Test
Einladungsseite /gruppe/	Eigene, strengere Header: default-src 'none', Referrer-Policy: no-referrer, no-store; jeder Header genau einmal.	 Live-Test
Gespernte Dateien	.env, .htaccess und PHP-Dateien liefern 403; alte Schnittstellen liefern 404.	 Live-Test
Sicherheitskontakt	/.well-known/security.txt veröffentlicht.	 Live-Test

6 Datensparsamkeit und Transparenz

Art. 5, 13, 25 und 28 DSGVO · Datenminimierung und Transparenz

MASSNAHME	UMSETZUNG	GRUNDLAGE
Webserver-Protokolle	ALL-INKL speichert nur gekürzte IP-Adressen (bei IPv4 ohne die letzten beiden Blöcke) und löscht nach 14 Tagen; die Zugriffsstatistik ist passwortgeschützt.	 Einstellung  Live-Test
Keine Web-Analyse	Cloudflare Web Analytics abgeschaltet; kein Messskript auf Website und Einladungsseite.	 Einstellung  Live-Test
Keine Zugriffsprotokolle	Die Konfigurationen von Gruppenfahrt-, Karten-, Termin-, Routing- und Begriffsdienst deaktivieren Zugriffsprotokolle. Das schließt die Verarbeitung von Verbindungsdaten bei Cloudflare und externen Anbietern nicht aus.	 Quellcode
Gerundete Standortabfragen	Umgebungssuche mit einem auf vier Nachkommastellen gerundeten Punkt (rund 10 m, zuzüglich 8 m Radiuszuschlag) statt der vollen GPS-Genauigkeit; Suche entlang der Route mit höchstens 120 gerundeten Punkten der geplanten Route.	 Quellcode
Begrenzte Begriffshilfe	Nach lokalem Fehler nur eine feste ID aus zwölf Begriffen an den eigenen Dienst; nur Katalogwort und Sprachrichtung an DeepL. Keine freien Texte, Standortdaten oder Nutzer-IP an DeepL. Schlüssel nur serverseitig; Cache 30 Tage ohne Nutzerzuordnung, feste Kontingente und Ratenlimits.	 Quellcode
Datenschutzerklärung	Deutsch und Englisch: Empfänger, Zwecke, Speicherfristen und Freigaben einschließlich ML Kit, Begriffshilfe über DeepL und lokaler Standortsortierung. Maßgeblich sind die Hinweise der installierten App und die aktuelle Website.	 Live-Test
Auftragsverarbeitung	Dokumentierte AV-Verträge mit Hetzner und ALL-INKL sowie das Cloudflare Data Processing Addendum. Die Datenschutzerklärung erläutert Rollen und Übermittlungsgrundlagen. Cloudflare beendet TLS und verarbeitet Verbindungsdaten; Gruppeninhalte bleiben Ende-zu-Ende-verschlüsselt.	 Einstellung

7 Verfügbarkeit und Wartung

Art. 32 Abs. 1 lit. b und c DSGVO · Verfügbarkeit, Belastbarkeit, Wiederherstellung

MASSNAHME	UMSETZUNG	GRUNDLAGE
Schutz vor Überlast	DDoS-Abwehr durch Cloudflare; gegen Missbrauch ein Ratenlimit für das Routing, das nur der App antwortet.	☒ Einstellung ☒ Live-Test
Sicherheitsupdates	Beide Server installieren Sicherheitsupdates täglich automatisch (unattended-upgrades). Neustarts: Routing-Server bei Bedarf nachts, Gruppenfahrt-Server gezielt außerhalb laufender Fahrten, da ein Neustart sie beenden würde.	☒ Einstellung
Sicherung und Löschschutz	Tägliche Backups beider Server, bis zu sieben Stände; Löschschutz aktiv.	☒ Einstellung

8 Entwicklung und Freigabe

Art. 25 und Art. 32 Abs. 1 lit. b DSGVO · Integrität

MASSNAHME	UMSETZUNG	GRUNDLAGE
Geschützter Hauptzweig	Änderungen per Pull Request mit den Pflichtprüfungen der CI. Fachliche Freigaben und ausdrücklich erteilte Ausnahmen werden getrennt dokumentiert.	☒ Einstellung
Sichere Build-Kette	Actions per Commit-Hash gebunden, Standardrechte nur lesend; Signierung in geschützten Umgebungen. Herkunft, Prüfsummen, Signaturen und App-Kennungen werden vor dem Upload geprüft.	☒ Quellcode ☒ Einstellung
Store-Angaben	Datensicherheit, Datenschutzhinweise und Review-Unterlagen müssen die tatsächlichen Datenflüsse einschließlich ML Kit und Begriffshilfe abbilden. Store-Freigabe und Geräteabnahme sind getrennte Nachweise; dieses Factsheet bestätigt keine Veröffentlichung.	☒ Einstellung

9 E-Mail und DNS

Art. 32 Abs. 1 lit. b DSGVO · Integrität

MASSNAHME	UMSETZUNG	GRUNDLAGE
Absenderschutz	SPF mit „-all“, DKIM für beide Domains, DMARC p=reject mit Berichten.	☒ Live-Test
Transportschutz	TLS-Berichte (TLS-RPT) und MTA-STX veröffentlicht.	☒ Live-Test
DNSSEC	pedalarrow.com ist signiert und über die .com-Registry abgesichert; validierende Resolver weisen gefälschte DNS-Antworten ab.	☒ Live-Test
Aufgeräumte Zonen	pedalarrow.de ohne Wildcard-Eintrag, unbekannte Subdomains lösen nicht auf; CAA nur für Let's Encrypt. pedal-arrow.com und pedal-arrow.de leiten über Cloudflare auf www.pedalarrow.com um, ohne Webspace-Inhalte.	☒ Live-Test

APP LADEN

PedalArrow für Android und iPhone

QR-Code mit der Kamera scannen oder den Link öffnen - ohne Konto und Anmeldung direkt nutzbar.



ANDROID
Google Play
play.google.com/store/apps/details?id=de.KhashayarN.PedalArrow
für Android-Smartphones



IPHONE
App Store
apps.apple.com/de/app/pedalarrow/id6800365475
für iPhone

VERANTWORTLICHER

Khashayar Nivipour, München

info@pedalarrow.com · www.pedalarrow.com

Anschrift im Impressum: www.pedalarrow.com/Impressum/

WEITERE UNTERLAGEN

Datenschutzerklärung und Fachinformation

Datenschutzerklärung: www.pedalarrow.com/Datenschutz/

„PedalArrow für den Radverkehr im Landkreis München“: PDF auf www.pedalarrow.com