



DevDeliver

Security Architecture & EU GDPR Assessment

Multilingual technical report | Mehrsprachiger technischer Bericht | Çok dilli teknik rapor

ASSESSMENT UPDATE - VERSION 2.0

Credential hashing, login throttling, security headers, cross-site mutation protection and verified database TLS are now active. Privacy-by-default and company isolation remain core controls. Organisational GDPR duties are identified separately from software safeguards.

Scope	Reviewed state
Application	DevDeliver web platform, API, route import, account and delivery-GPS workflows
Infrastructure	DigitalOcean application deployment and PostgreSQL/Supabase connection model
Security baseline	Commits 954c39d and f89dd0c; 123 automated tests passed
Languages	Deutsch, Türkçe, English, Español, Dansk, Svenska, Français

This report is a technical assessment, not legal advice, an audit opinion or a GDPR certification. Controllers and processors retain their own legal and organisational responsibilities.

Language index / Sprachindex / Dil indeksi

Each language section contains the same two-page assessment: current architecture and controls, followed by data categories, GDPR mapping and remaining responsibilities.

Language	Section	Pages
Deutsch	Sicherheitsarchitektur und EU-DSGVO-Bewertung	3-4
Türkçe	Güvenlik Mimarisi ve AB GDPR Değerlendirmesi	5-6
English	Security Architecture and EU GDPR Assessment	7-8
Español	Arquitectura de seguridad y evaluación del RGPD de la UE	9-10
Dansk	Sikkerhedsarkitektur og EU GDPR-vurdering	11-12
Svenska	Säkerhetsarkitektur och EU GDPR-bedömning	13-14
Français	Architecture de sécurité et évaluation du RGPD de l'UE	15-16

DOCUMENT CONTROL

Version 2.0 | Assessment date: 19 September 2026 | Public document URL:
<https://devdeliver.app/documents/devdeliver-security-gdpr-report.pdf> | Review basis: production code and security configuration.

Reading guide

Green callouts describe safeguards confirmed in the implementation. Amber callouts identify governance or legal work that must be completed by DevDeliver and each deploying company. No section claims automatic or universal GDPR compliance.

DE | Sicherheitsarchitektur und EU-DSGVO-Bewertung

Management-Zusammenfassung

DevDeliver verarbeitet standardmäßig nur die für Routenplanung und Navigation erforderlichen Betriebsdaten. Personenbezogene Kunden- und Produktfelder werden im Standardimport verworfen. Die aktuelle Version verstärkt Authentifizierung, Mandantentrennung, Browser-Schutz und die verifizierte TLS-Verbindung zur Datenbank.

Aktueller Stand

Wesentliche technische Schwachstellen des ersten Berichts wurden behoben. Das System unterstützt eine DSGVO-konforme Nutzung, stellt jedoch weder eine rechtliche Zertifizierung dar noch ersetzt es Verträge, Informationspflichten, Aufbewahrungsregeln oder Risikobewertungen des Verantwortlichen.

Datenfluss und Zweckbindung

Stufe	Verarbeitung	Schutz
1. Import	Routenquelle wird im Browser verarbeitet.	Standardmäßig nur Adresse, Koordinaten, Route, Reihenfolge und Betriebsstatus.
2. Datenschutzfilter	Browser und Server wenden eine Positivliste an.	Rohdatei sowie Kunden- und Produktdetails werden standardmäßig nicht gespeichert.
3. Anwendung	API prüft Sitzung, Rolle und Unternehmen.	Jeder Zugriff wird auf companyId und zulässige Rolle begrenzt.
4. Speicherung	Bereinigter Betriebszustand in PostgreSQL.	RLS, entzogene öffentliche Rechte und TLS mit CA- und Hostprüfung.

Aktive technische Kontrollen

Bereich	Umgesetzte Kontrolle
Zugangsdaten	6-stellige PINs werden mit individuellem Salt und scrypt gehasht; Vergleich erfolgt zeitkonstant. PINs sind nach Erstellung nicht einsehbar.
Sitzungen	HttpOnly-, SameSite- und HTTPS-Secure-Cookies; PIN-Zurücksetzung macht bestehende Sitzungen ungültig.
Missbrauchsschutz	Kontobezogene Anmeldebegrenzung, Turnstile-Prüfung bei Registrierung und Blockierung standortfremder Schreib Anfragen.
Browser	CSP, HSTS, DENY-Framing, nosniff, Referrer- und Berechtigungsrichtlinien.
Berechtigung	Rollenbasierter Zugriff für Account Manager, Manager und Courier mit Unternehmensgrenzen.
Datenbank	TLS mit verifizierter Supabase-CA und Hostname; öffentliche Rollen haben keinen Tabellenzugriff.

DE | Verarbeitete Daten und Aufbewahrung

Kategorie	Standardzweck	Hinweis
Adresse und Koordinaten	Routenplanung und Navigation	Kann trotz fehlendem Namen personenbezogen sein; Frist festlegen.
Route und Status	Ablauf und Fortschritt	Betriebliche Aufbewahrungsfrist dokumentieren.
Kurierkonto	Zugang, Rolle, Zuordnung	Austritts- und Deaktivierungsprozess erforderlich.
Liefer-GPS	Qualitätsgesicherte gemeinsame Position	Transparenz und begrenzte Aufbewahrung sind wichtig.
Problemfoto	Optionaler Nachweis	Binärbild wird nach 48 Stunden gelöscht; Metadaten können verbleiben.
Optionale Felder	Nur nach Manager-Freigabe	Erweiterter Umfang braucht Zweck, Rechtsgrundlage und Frist.

DSGVO-Zuordnung und Verantwortlichkeiten

Thema	Bewertung
Art. 5 - Minimierung	Standard-Positivliste und keine dauerhafte Rohdatei unterstützen Datenminimierung und Zweckbindung.
Art. 25 - Datenschutz durch Technik	Datenschutzfilter, sichere Standardwerte und Managerfreigaben sind in den Ablauf eingebaut.
Art. 28 - Auftragsverarbeitung	Rollen, Weisungen, Unterauftragsverarbeiter und Löschung müssen vertraglich festgelegt werden.
Art. 32 - Sicherheit	Hashing, Zugriffskontrolle, TLS, Sicherheitsheader und Tests sind umgesetzt; Wirksamkeit muss regelmäßig geprüft werden.

Noch organisatorisch zu erledigen

DPA/AV-Vertrag und Unterauftragsverarbeiterliste; konkrete Aufbewahrungs- und Löschfristen für Routen, GPS und Protokolle; Verfahren für Betroffenenrechte; dokumentierter Vorfallprozess; Wiederherstellungstest; MFA oder stärkere Anmeldung für privilegierte Konten; Freigabeprozess für optionale Importfelder.

Dieses Dokument ist eine technische Bewertung, keine Rechtsberatung oder Zertifizierung. Der jeweilige Verantwortliche muss Rechtsgrundlage, Transparenz, DPIA-Bedarf und nationale Anforderungen selbst bewerten.

Quellen und Prüfgrundlage

EU GDPR, Regulation (EU) 2016/679, Articles 5, 25, 28 and 32: eur-lex.europa.eu

EDPB Guidelines 4/2019, Data Protection by Design and by Default: edpb.europa.eu

Danish Data Protection Authority, controller obligations and security: datatilsynet.dk

Supabase documentation, verified SSL database connections: supabase.com/docs

Cloudflare Turnstile, mandatory server-side token validation: developers.cloudflare.com

DevDeliver code and live configuration review, commits 954c39d and f89dd0c, verified by 123 automated tests.

TR | Güvenlik Mimarisi ve AB GDPR Değerlendirmesi

Yönetici özeti

DevDeliver varsayılan olarak yalnızca rota oluşturma ve navigasyon için gerekli operasyon verilerini işler. Müşteri kimliği ve ürün alanları standart içe aktarmada elenir. Güncel sürüm kimlik doğrulamayı, şirket ayırımını, tarayıcı korumalarını ve doğrulanmış TLS veritabanı bağlantısını güçlendirmiştir.

Güncel durum

İlk rapordaki önemli teknik açıklar kapatılmıştır. Sistem GDPR uyumlu kullanımı destekleyen kontroller sunar; ancak hukuki sertifika değildir ve veri sorumlusunun sözleşme, aydınlatma, saklama ve risk değerlendirmesi yükümlülüklerinin yerini almaz.

Veri akışı ve amaçla sınırlılık

Aşama	İşlem	Koruma
1. İçe aktarma	Rota kaynağı tarayıcıda işlenir.	Varsayılan alanlar: adres, koordinat, rota, sıra ve operasyon durumu.
2. Gizlilik filtresi	Tarayıcı ve sunucu izinli alan listesini uygular.	Ham dosya ile müşteri ve ürün ayrıntıları varsayılan olarak saklanmaz.
3. Uygulama	API oturumu, rolü ve şirketi kontrol eder.	Her erişim companyId ve izin verilen rolle sınırlandırılır.
4. Saklama	Temizlenmiş operasyon durumu PostgreSQL'e yazılır.	RLS, kaldırılmış public yetkiler ve CA/hostname doğrulamalı TLS.

Aktif teknik kontroller

Alan	Uygulanan kontrol
Kimlik bilgisi	6 haneli PIN'ler benzersiz salt ve scrypt ile hashlenir; karşılaştırma sabit zamanlıdır. Oluşturulduktan sonra PIN görüntülenmez.
Oturum	HttpOnly, SameSite ve HTTPS Secure cookie; PIN sıfırlanınca mevcut oturumlar geçersiz olur.
Kötüye kullanım	Hesap bazlı giriş deneme sınırı, kayıta Turnstile ve siteler arası değişiklik isteklerinin engellenmesi.
Tarayıcı	CSP, HSTS, frame engeli, nosniff, referrer ve permission policy başlıkları.
Yetkilendirme	Account Manager, Manager ve Courier için rol tabanlı erişim; şirket sınırı uygulanır.
Veritabanı	Supabase CA ve hostname doğrulamalı TLS; public rollerin tablo erişimi kaldırılmıştır.

TR | İşlenen veri ve saklama

Kategori	Varsayılan amaç	Not
Adres ve koordinat	Rotalama ve navigasyon	İsim olmasa da kişisel veri olabilir; süre belirlenmelidir.
Rota ve durum	İş akışı ve ilerleme	Operasyonel saklama süresi yazılı olmalıdır.
Kurye hesabı	Erişim, rol ve atama	İşten ayrılma ve hesap kapatma süreci gerekir.
Teslim GPS'i	Onaylı ortak teslim noktası	Şeffaflık ve sınırlı saklama önemlidir.
Sorun fotoğrafı	İsteğe bağlı kanıt	Fotoğraf 48 saatte silinir; metadata kalabilir.
İsteğe bağlı alanlar	Yalnızca Manager seçerse	Geniş kapsam için amaç, hukuki dayanak ve süre gerekir.

GDPR eşlemesi ve sorumluluklar

Konu	Değerlendirme
Madde 5 - Minimizasyon	Varsayılan izinli alan listesi ve ham dosyanın saklanmaması veri minimizasyonunu destekler.
Madde 25 - Tasarımla gizlilik	Gizlilik filtresi, güvenli varsayılanlar ve yönetici onayı akışa gömülmüştür.
Madde 28 - Veri işleyen	Roller, talimatlar, alt işleyenler ve silme sözleşmeyle düzenlenmelidir.
Madde 32 - Güvenlik	Hash, erişim kontrolü, TLS, güvenlik başlıkları ve testler uygulanmıştır; etkinlik düzenli ölçülmelidir.

Organizasyonel olarak tamamlanması gerekenler

DPA/veri işleme sözleşmesi ve alt işleyen listesi; rota, GPS ve loglar için somut saklama-silme süreleri; veri sahibi talep prosedürü; olay müdahale planı; geri yükleme testi; ayrıcalıklı hesaplarda MFA veya daha güçlü giriş; isteğe bağlı içe aktarma alanları için onay süreci.

Bu belge teknik değerlendirmedir; hukuki görüş veya sertifika değildir. Hukuki dayanak, aydınlatma, DPIA gereksinimi ve ulusal yükümlülükler veri sorumlusu tarafından değerlendirilmelidir.

Kaynaklar ve inceleme temeli

EU GDPR, Regulation (EU) 2016/679, Articles 5, 25, 28 and 32: eur-lex.europa.eu

EDPB Guidelines 4/2019, Data Protection by Design and by Default: edpb.europa.eu

Danish Data Protection Authority, controller obligations and security: datatilsynet.dk

Supabase documentation, verified SSL database connections: supabase.com/docs

Cloudflare Turnstile, mandatory server-side token validation: developers.cloudflare.com

DevDeliver code and live configuration review, commits 954c39d and f89dd0c, verified by 123 automated tests.

EN | Security Architecture and EU GDPR Assessment

Executive summary

By default, DevDeliver processes only the operational data required to build routes and navigate deliveries. Customer identity and product fields are excluded from the standard import. The current release strengthens authentication, tenant isolation, browser protections and verified TLS database connectivity.

Current position

The material technical gaps identified in the first report have been addressed. The system provides controls that support GDPR-compliant use, but it is not a legal certification and does not replace the controller's contracts, notices, retention rules or risk assessment.

Data flow and purpose limitation

Stage	Processing	Safeguard
1. Import	The route source is processed in the browser.	Default fields are address, coordinates, route, sequence and operational status.
2. Privacy filter	Browser and server enforce an allowlist.	The raw file and customer or product details are not retained by default.
3. Application	The API checks session, role and company.	Every request is limited by companyId and the permitted role.
4. Storage	Sanitised operational state is written to PostgreSQL.	RLS, revoked public grants and TLS with CA and hostname verification.

Active technical controls

Area	Implemented control
Credentials	Six-digit PINs use unique salts and scrypt hashes with constant-time comparison. PINs cannot be viewed after creation.
Sessions	HttpOnly, SameSite and HTTPS Secure cookies; resetting a PIN invalidates existing sessions.
Abuse protection	Account-scoped login throttling, Turnstile registration checks and blocking of cross-site mutation requests.
Browser	CSP, HSTS, frame denial, nosniff, referrer and permissions policies.
Authorisation	Role-based access for Account Managers, Managers and Couriers with company boundaries.
Database	TLS with verified Supabase CA and hostname; public database roles have no table access.

EN | Processed data and retention

Category	Default purpose	Note
Address and coordinates	Routing and navigation	May remain personal data without a name; define a retention period.
Route and status	Workflow and progress	Document an operational retention period.
Courier account	Access, role and assignment	Requires offboarding and deactivation rules.
Delivered GPS	Approved shared delivery position	Transparency and limited retention are important.
Issue photo	Optional evidence	Binary image is deleted after 48 hours; metadata may remain.
Optional fields	Only when enabled by a Manager	Expanded scope needs purpose, legal basis and retention.

GDPR mapping and responsibilities

Topic	Assessment
Article 5 - minimisation	The default allowlist and non-retention of raw files support minimisation and purpose limitation.
Article 25 - data protection by design	Privacy filtering, safe defaults and Manager approvals are built into the workflow.
Article 28 - processor terms	Roles, instructions, subprocessors and deletion must be defined contractually.
Article 32 - security	Hashing, access control, TLS, security headers and tests are implemented; effectiveness must be reviewed.

Remaining organisational work

DPA and subprocessor list; concrete retention and deletion periods for routes, GPS and logs; data-subject request procedure; documented incident response; restore testing; MFA or stronger authentication for privileged accounts; approval process for optional import fields.

This is a technical assessment, not legal advice or certification. The relevant controller must assess legal basis, transparency, DPIA need and applicable national requirements.

Sources and review basis

EU GDPR, Regulation (EU) 2016/679, Articles 5, 25, 28 and 32: eur-lex.europa.eu

EDPB Guidelines 4/2019, Data Protection by Design and by Default: edpb.europa.eu

Danish Data Protection Authority, controller obligations and security: datatilsynet.dk

Supabase documentation, verified SSL database connections: supabase.com/docs

Cloudflare Turnstile, mandatory server-side token validation: developers.cloudflare.com

DevDeliver code and live configuration review, commits 954c39d and f89dd0c, verified by 123 automated tests.

ES | Arquitectura de seguridad y evaluación del RGPD de la UE

Resumen ejecutivo

De forma predeterminada, DevDeliver solo trata los datos operativos necesarios para crear rutas y navegar entregas. La identidad del cliente y los campos de producto se excluyen de la importación estándar. La versión actual refuerza la autenticación, el aislamiento entre empresas, la protección del navegador y la conexión TLS verificada con la base de datos.

Situación actual

Se han corregido las carencias técnicas relevantes del primer informe. El sistema aporta controles que respaldan un uso conforme al RGPD, pero no constituye una certificación jurídica ni sustituye contratos, avisos, normas de conservación o evaluaciones de riesgo del responsable.

Flujo de datos y limitación de la finalidad

Etapa	Tratamiento	Protección
1. Importación	La fuente de rutas se procesa en el navegador.	Campos por defecto: dirección, coordenadas, ruta, secuencia y estado operativo.
2. Filtro de privacidad	Navegador y servidor aplican una lista permitida.	El archivo original y los datos de clientes o productos no se conservan por defecto.
3. Aplicación	La API valida sesión, rol y empresa.	Cada solicitud se limita por companyld y rol autorizado.
4. Almacenamiento	El estado operativo depurado se guarda en PostgreSQL.	RLS, permisos públicos revocados y TLS con CA y hostname verificados.

Controles técnicos activos

Área	Control implantado
Credenciales	Los PIN de seis dígitos usan salt único y hash scrypt con comparación en tiempo constante. No pueden verse tras crearse.
Sesiones	Cookies HttpOnly, SameSite y Secure por HTTPS; restablecer el PIN invalida las sesiones existentes.
Abuso	Límite de intentos por cuenta, Turnstile en el registro y bloqueo de modificaciones entre sitios.
Navegador	CSP, HSTS, bloqueo de marcos, nosniff y políticas de referencia y permisos.
Autorización	Acceso por roles para Account Manager, Manager y Courier con límites por empresa.
Base de datos	TLS con CA de Supabase y hostname verificados; los roles públicos no acceden a tablas.

ES | Datos tratados y conservación

Categoría	Finalidad estándar	Nota
Dirección y coordenadas	Rutas y navegación	Puede seguir siendo dato personal sin nombre; definir plazo.
Ruta y estado	Flujo y progreso	Documentar un plazo operativo.
Cuenta del repartidor	Acceso, rol y asignación	Requiere baja y desactivación.
GPS de entrega	Posición compartida aprobada	La transparencia y la limitación temporal son importantes.
Foto de incidencia	Prueba opcional	La imagen se elimina en 48 horas; pueden quedar metadatos.
Campos opcionales	Solo si Manager los activa	El alcance ampliado exige finalidad, base legal y plazo.

Correspondencia RGPD y responsabilidades

Tema	Evaluación
Art. 5 - minimización	La lista permitida y no conservar archivos originales respaldan minimización y finalidad.
Art. 25 - privacidad desde el diseño	Filtros, valores seguros y aprobaciones de Manager están integrados.
Art. 28 - encargado	Roles, instrucciones, subencargados y borrado deben quedar en contrato.
Art. 32 - seguridad	Hash, control de acceso, TLS, cabeceras y pruebas están implantados; debe revisarse su eficacia.

Trabajo organizativo pendiente

DPA y lista de subencargados; plazos concretos para rutas, GPS y registros; procedimiento de derechos; respuesta a incidentes; prueba de restauración; MFA o autenticación reforzada para cuentas privilegiadas; aprobación de campos opcionales.

Esta es una evaluación técnica, no asesoramiento jurídico ni certificación. El responsable debe evaluar la base legal, transparencia, necesidad de EIPD y requisitos nacionales.

Fuentes y base de revisión

EU GDPR, Regulation (EU) 2016/679, Articles 5, 25, 28 and 32: eur-lex.europa.eu

EDPB Guidelines 4/2019, Data Protection by Design and by Default: edpb.europa.eu

Danish Data Protection Authority, controller obligations and security: datatilsynet.dk

Supabase documentation, verified SSL database connections: supabase.com/docs

Cloudflare Turnstile, mandatory server-side token validation: developers.cloudflare.com

DevDeliver code and live configuration review, commits 954c39d and f89dd0c, verified by 123 automated tests.

DA | Sikkerhedsarkitektur og EU GDPR-vurdering

Ledelsesresumé

DevDeliver behandler som standard kun de driftsdata, der er nødvendige for at opbygge ruter og navigere leveringer. Kundeidentitet og produktfelter er udeladt fra standardimporten. Den aktuelle version styrker godkendelse, virksomhedsadskillelse, browserbeskyttelse og verificeret TLS-forbindelse til databasen.

Aktuel status

De væsentlige tekniske mangler fra den første rapport er rettet. Systemet indeholder kontroller, der understøtter GDPR-kompatibel brug, men er ikke en juridisk certificering og erstatter ikke den dataansvarliges aftaler, information, opbevaringsregler eller risikovurdering.

Dataflow og formålsbegrænsning

Trin	Behandling	Beskyttelse
1. Import	Rutekilden behandles i browseren.	Standardfelter: adresse, koordinater, rute, rækkefølge og driftstatus.
2. Privatlivsfilter	Browser og server håndhæver en positivliste.	Råfil samt kunde- og produktoplysninger gemmes ikke som standard.
3. Applikation	API kontrollerer session, rolle og virksomhed.	Hver adgang begrænses af companyId og tilladt rolle.
4. Lagring	Renset driftstilstand gemmes i PostgreSQL.	RLS, fjernede offentlige rettigheder og TLS med CA- og hostnavnkontrol.

Aktive tekniske kontroller

Område	Implementeret kontrol
Legitimationsoplysninger	Seks-cifrede PIN-koder hashes med unik salt og scrypt; sammenligning er tidskonstant. PIN kan ikke vises efter oprettelse.
Sessioner	HttpOnly-, SameSite- og HTTPS Secure-cookies; nulstilling af PIN ugyldiggør eksisterende sessioner.
Misbrug	Loginbegrænsning pr. konto, Turnstile ved registrering og blokering af cross-site ændringsanmodninger.
Browser	CSP, HSTS, frame-blokering, nosniff samt referrer- og permission-politikker.
Adgang	Rollebaseret adgang for Account Manager, Manager og Courier med virksomhedsgrænser.
Database	TLS med verificeret Supabase-CA og hostnavn; offentlige roller har ingen tabeladgang.

DA | Behandlede data og opbevaring

Kategori	Standardformål	Bemærkning
Adresse og koordinater	Rute og navigation	Kan være personoplysninger uden navn; fastsæt periode.
Rute og status	Arbejdsgang og fremdrift	Dokumentér driftsmæssig opbevaring.
Kurérkonto	Adgang, rolle og tildeling	Kræver fratrædelses- og deaktiveringsproces.
Leverings-GPS	Godkendt fælles position	Gennemsigtighed og begrænset opbevaring er vigtig.
Hændelsesfoto	Valgfri dokumentation	Billedet slettes efter 48 timer; metadata kan bestå.
Valgfrie felter	Kun når Manager aktiverer	Udvidet omfang kræver formål, hjemmel og periode.

GDPR-kobling og ansvar

Emne	Vurdering
Artikel 5 - dataminimering	Positivlisten og fravær af råfiler understøtter minimering og formålsbegrænsning.
Artikel 25 - databeskyttelse gennem design	Privatlivsfilter, sikre standarder og Manager-godkendelser er indbygget.
Artikel 28 - databehandler	Roller, instrukser, underdatabehandlere og sletning skal aftales.
Artikel 32 - sikkerhed	Hashing, adgangskontrol, TLS, sikkerhedsheadere og test er implementeret; effekten skal vurderes løbende.

Resterende organisatoriske opgaver

Databehandleraftale og underdatabehandlerliste; konkrete frister for ruter, GPS og logs; procedure for registreredes rettigheder; hændelsesberedskab; gendannelsestest; MFA eller stærkere login for privilegerede konti; godkendelse af valgfrie importfelter.

Dokumentet er en teknisk vurdering, ikke juridisk rådgivning eller certificering. Den dataansvarlige skal vurdere hjemmel, oplysningspligt, behov for DPIA og nationale krav.

Kilder og gennemgangsgrundlag

EU GDPR, Regulation (EU) 2016/679, Articles 5, 25, 28 and 32: eur-lex.europa.eu

EDPB Guidelines 4/2019, Data Protection by Design and by Default: edpb.europa.eu

Danish Data Protection Authority, controller obligations and security: datatilsynet.dk

Supabase documentation, verified SSL database connections: supabase.com/docs

Cloudflare Turnstile, mandatory server-side token validation: developers.cloudflare.com

DevDeliver code and live configuration review, commits 954c39d and f89dd0c, verified by 123 automated tests.

SV | Säkerhetsarkitektur och EU GDPR-bedömning

Sammanfattning för ledningen

DevDeliver behandlar som standard endast de operativa data som behövs för att bygga rutter och navigera leveranser. Kundidentitet och produktfält utesluts från standardimporten. Den aktuella versionen stärker autentisering, företagsisolering, webbläsarskydd och verifierad TLS-anslutning till databasen.

Aktuellt läge

De väsentliga tekniska bristerna i den första rapporten har åtgärdats. Systemet innehåller kontroller som stödjer GDPR-förenlig användning, men är ingen juridisk certifiering och ersätter inte den personuppgiftsansvariges avtal, information, lagringsregler eller riskbedömning.

Dataflöde och ändamålsbegränsning

Steg	Behandling	Skydd
1. Import	Ruttkällan behandlas i webbläsaren.	Standardfält: adress, koordinater, rutt, ordning och operativ status.
2. Integritetsfilter	Webbläsare och server tillämpar en tillåten lista.	Råfil samt kund- och produktuppgifter sparas inte som standard.
3. Applikation	API kontrollerar session, roll och företag.	Varje åtkomst begränsas av companyld och tillåten roll.
4. Lagring	Rensat operativt tillstånd sparas i PostgreSQL.	RLS, återkallade publika rättigheter och TLS med CA- och värddnamnskontroll.

Aktiva tekniska kontroller

Område	Införd kontroll
Inloggning	Sexsiffriga PIN-koder hashas med unikt salt och scrypt; jämförelsen är tidskonstant. PIN visas inte efter skapandet.
Sessioner	HttpOnly-, SameSite- och HTTPS Secure-cookies; PIN-återställning ogiltigförklarar befintliga sessioner.
Missbruk	Begränsning av inloggningsförsök per konto, Turnstile vid registrering och blockering av cross-site ändringar.
Webbläsare	CSP, HSTS, frame-blockering, nosniff samt referrer- och behörighetspolicy.
Behörighet	Rollbaserad åtkomst för Account Manager, Manager och Courier med företagsgränser.
Databas	TLS med verifierad Supabase-CA och värddnamn; publika roller saknar tabellåtkomst.

SV | Behandlade data och lagring

Kategori	Standardändamål	Kommentar
Adress och koordinater	Rutt och navigation	Kan vara personuppgift utan namn; ange lagringstid.
Rutt och status	Arbetsflöde och framsteg	Dokumentera operativ lagringstid.
Budkonto	Åtkomst, roll och tilldelning	Kräver avsluts- och avaktiveringsprocess.
Leverans-GPS	Godkänd delad position	Transparens och begränsad lagring är viktig.
Incidentfoto	Valfritt bevis	Bilden raderas efter 48 timmar; metadata kan finnas kvar.
Valfria fält	Endast när Manager aktiverar	Utökat omfång kräver ändamål, rättslig grund och tid.

GDPR-koppling och ansvar

Ämne	Bedömning
Artikel 5 - minimering	Tillåten lista och ingen råfil stödjer minimering och ändamålsbegränsning.
Artikel 25 - inbyggt dataskydd	Integritetsfilter, säkra standarder och Manager-godkännanden är inbyggda.
Artikel 28 - personuppgiftsbiträde	Roller, instruktioner, underbiträden och radering ska regleras i avtal.
Artikel 32 - säkerhet	Hashning, åtkomstkontroll, TLS, säkerhetsrubriker och test är införda; effekten ska granskas.

Kvarvarande organisatoriskt arbete

Personuppgiftsbiträdesavtal och lista över underbiträden; konkreta tider för rutter, GPS och loggar; rutin för registrerades rättigheter; incidenthantering; återställningstest; MFA eller starkare inloggning för privilegierade konton; godkännande av valfria importfält.

Detta är en teknisk bedömning, inte juridisk rådgivning eller certifiering. Den personuppgiftsansvarige måste bedöma rättslig grund, transparens, behov av DPIA och nationella krav.

Källor och granskningsunderlag

EU GDPR, Regulation (EU) 2016/679, Articles 5, 25, 28 and 32: eur-lex.europa.eu

EDPB Guidelines 4/2019, Data Protection by Design and by Default: edpb.europa.eu

Danish Data Protection Authority, controller obligations and security: datatilsynet.dk

Supabase documentation, verified SSL database connections: supabase.com/docs

Cloudflare Turnstile, mandatory server-side token validation: developers.cloudflare.com

DevDeliver code and live configuration review, commits 954c39d and f89dd0c, verified by 123 automated tests.

FR | Architecture de sécurité et évaluation du RGPD de l'UE

Synthèse de direction

Par défaut, DevDeliver ne traite que les données opérationnelles nécessaires à la création des tournées et à la navigation. L'identité du client et les champs produit sont exclus de l'import standard. La version actuelle renforce l'authentification, l'isolation des entreprises, la protection du navigateur et la connexion TLS vérifiée à la base de données.

Situation actuelle

Les principales lacunes techniques du premier rapport ont été corrigées. Le système fournit des contrôles favorisant un usage conforme au RGPD, mais ne constitue ni une certification juridique ni un substitut aux contrats, informations, règles de conservation et analyses de risques du responsable.

Flux de données et limitation des finalités

Étape	Traitement	Protection
1. Import	La source des tournées est traitée dans le navigateur.	Champs par défaut : adresse, coordonnées, tournée, ordre et état opérationnel.
2. Filtre de confidentialité	Navigateur et serveur appliquent une liste autorisée.	Le fichier brut et les données client ou produit ne sont pas conservés par défaut.
3. Application	L'API contrôle session, rôle et entreprise.	Chaque accès est limité par companyId et le rôle autorisé.
4. Stockage	L'état opérationnel nettoyé est écrit dans PostgreSQL.	RLS, droits publics retirés et TLS avec CA et nom d'hôte vérifiés.

Contrôles techniques actifs

Domaine	Contrôle mis en œuvre
Identifiants	Les PIN à six chiffres utilisent un sel unique et un hash scrypt avec comparaison en temps constant. Ils ne sont plus visibles après création.
Sessions	Cookies HttpOnly, SameSite et Secure sous HTTPS ; réinitialiser le PIN invalide les sessions existantes.
Abus	Limitation des essais par compte, Turnstile à l'inscription et blocage des modifications cross-site.
Navigateur	CSP, HSTS, blocage des frames, nosniff, politiques de référent et de permissions.
Autorisation	Accès par rôle pour Account Manager, Manager et Courrier avec limites par entreprise.
Base de données	TLS avec CA Supabase et nom d'hôte vérifiés ; aucun accès aux tables pour les rôles publics.

FR | Données traitées et conservation

Catégorie	Finalité standard	Remarque
Adresse et coordonnées	Itinéraire et navigation	Peut rester une donnée personnelle sans nom ; définir une durée.
Tournée et état	Flux et progression	Documenter une durée opérationnelle.
Compte coursier	Accès, rôle et affectation	Prévoir départ et désactivation.
GPS de livraison	Position partagée approuvée	Transparence et durée limitée sont importantes.
Photo d'incident	Preuve facultative	L'image est supprimée après 48 heures ; des métadonnées peuvent rester.
Champs facultatifs	Uniquement si Manager les active	L'extension exige finalité, base légale et durée.

Correspondance RGPD et responsabilités

Sujet	Évaluation
Article 5 - minimisation	La liste autorisée et l'absence de fichier brut soutiennent minimisation et finalité.
Article 25 - protection dès la conception	Filtres, paramètres sûrs et validations Manager sont intégrés au flux.
Article 28 - sous-traitant	Rôles, instructions, sous-traitants ultérieurs et suppression doivent être contractualisés.
Article 32 - sécurité	Hash, contrôle d'accès, TLS, en-têtes et tests sont mis en œuvre ; leur efficacité doit être revue.

Travail organisationnel restant

DPA et liste des sous-traitants ultérieurs ; durées précises pour tournées, GPS et journaux ; procédure de droits ; réponse aux incidents ; test de restauration ; MFA ou authentification renforcée pour comptes privilégiés ; validation des champs d'import facultatifs.

Ce document est une évaluation technique, non un conseil juridique ou une certification. Le responsable doit évaluer la base légale, la transparence, le besoin d'AIPD et les exigences nationales.

Sources et base de l'examen

EU GDPR, Regulation (EU) 2016/679, Articles 5, 25, 28 and 32: eur-lex.europa.eu

EDPB Guidelines 4/2019, Data Protection by Design and by Default: edpb.europa.eu

Danish Data Protection Authority, controller obligations and security: datatilsynet.dk

Supabase documentation, verified SSL database connections: supabase.com/docs

Cloudflare Turnstile, mandatory server-side token validation: developers.cloudflare.com

DevDeliver code and live configuration review, commits 954c39d and f89dd0c, verified by 123 automated tests.