



Hoe verwerken we uw gegevens?

Leeft het bedrijf de AVG en de informatiebeveiliging na?

- Ja, het bedrijf heeft het Gegevensbeschermingsbeleid goedgekeurd.
- Ja, het bedrijf heeft Informatiebeveiligingsbeleid goedgekeurd.
- Ja, het bedrijf heeft een Functionaris gegevensbescherming aangewezen.
- Ja, het bedrijf past de beste praktijken en conforme beveiligingsmaatregelen toe.
- Ja, het bedrijf organiseert regelmatig scholingen voor werknemers.

Waar bewaren we de gegevens?

- Het bedrijf slaat alle gegevens op geografisch van elkaar gescheiden servers op. De systeemserver van Themidentified bevinden zich in de EU.

Wat zijn de bewaartermijnen voor gegevens?

Soort informatie	Nagestreefde bewaartermijn
Coördinaten	24 maanden
Ontstekingsdetectie	24 maanden
Ritten	24 maanden online toegankelijk; op verzoek nog eens 60 maanden toegankelijk vanuit het archief
Rapporten	6 maanden
Evenementen	24 maanden
Meldingen van evenementen	1 maand
Communicatie	24 maanden
Taken	24 maanden
Gedownloade tachograaf-gegevens	24 maanden
Overtredingen	24 maanden
Bestuurdersactiviteiten	24 maanden
Gegevens over eco-rijden	24 maanden

Hoe beschermen we de gegevens?

- **Wachtwoord/authenticatie:**

Het systeem garandeert dat wachtwoorden complex en geldig zijn en maakt gebruik van de OAuth 2.0-implementatie voor de authenticatie van het systeem.

- **Back-ups:**

Back-ups zijn versleuteld en het bedrijf zorgt voor periodieke hersteltests van de back-ups om er zeker van te zijn dat de integriteit van de gegevens in een noodgeval niet verloren gaat.

- **Project- en wijzigingsbeheer:**

Alle systeemwijzigingen worden in Jira vastgelegd. Alle wijzigingen worden in een afzonderlijke testomgeving met gepersonaliseerde gegevens getest.

- **Incidentmanagement:**

Incidenten worden in Zendesk geregistreerd. Het bedrijf heeft de verantwoordelijkheden voor het oplossen van incidenten toegewezen.

- **Technisch logboek:**

Systeemlogboeken worden verzameld en opgeslagen. De klant heeft het recht om persoonsgegevens die niet meer relevant zijn te laten verwijderen.

- **Toegangscontrole:**

Het bedrijf verleent de klant het recht om beheerder te zijn, de toegang wordt echter uitsluitend verleend tot de eigen gegevens van de klant als verwerkingsverantwoordelijke. Klanten kunnen de toegankelijkheid via object/module beperken. Werknemers met beheerdersrechten kunnen alle gegevens inzien die zij nodig hebben voor het uitvoeren van hun directe taken.

Het supportteam van het bedrijf voert het registratie-, wijzigings- en afmeldingsproces van een gebruiker uit.

- **Leveranciersbeheer:**

Het bedrijf neemt de inzet van leveranciers zeer serieus en sluit met de leveranciers daarom verwerkingsovereenkomsten persoonsgegevens en geheimhoudingsverklaringen af.

- **Scannen op beveiligingsproblemen:**

Voor het scannen op beveiligingsproblemen beschikt het bedrijf over een adequate tool die regelmatig controles uitvoert.

- **Geheimhouding:**

Alle werknemers van het bedrijf hebben de geheimhoudingsverklaring gelezen en ondertekend.

Hoe wordt ermee omgegaan als gegevens onverhoopt verloren gaan of beschadigd raken?

- Het incident wordt direct onderzocht en de toezichthoudende autoriteiten en klanten worden op de hoogte gebracht.
- In gevallen waarin gegevens tijdens een incident worden gewijzigd of verloren gaan, worden de gegevens aan de hand van back-ups hersteld.

Verplichtingen van de gegevensverwerkers

- Als uw gegevensverwerkers helpen we u met het volgende:
 - gegevens corrigeren, verwijderen of exporteren
 - de rechten van de betrokkenen toepassen
 - effectbeoordelingen met betrekking tot gegevensbescherming uitvoeren
 - andere nalevingsvereisten implementeren
 - vragen beantwoorden die gesteld worden



We hechten veel waarde aan de veiligheid van de persoonsgegevens die ons worden toevertrouwd, daarom stellen we alles in het werk om deze veiligheid te waarborgen.

Indien u nog vragen heeft, neem dan gerust contact met ons op: dpo@inqo.io of Perkūnkiemio str. 6, Vilnius, Litouwen.