contractify

DATA SECURITY (version 04/2024)

Wij, DB2 Value Creation BV, Polenstraat 163, 9940 Evergem, België (BTW BE0644714953) hechten veel waarde aan de beveiliging van de gegevens van onze klanten. We beseffen dat het vertrouwen van onze klanten ons waardevolste bezit is en dat de beveiliging van hun gegevens essentieel is om dit vertrouwen te behouden. Daarom nemen we proactieve maatregelen om de gegevens van onze klanten te beschermen en te beveiligen tegen ongeautoriseerde toegang, misbruik en datalekken.

Dit document beschrijft de belangrijkste principes en praktijken die we volgen om de veiligheid en vertrouwelijkheid van de gegevens van onze klanten te garanderen.

1. Data

Eigendom van gegevens

Als klant blijf je altijd eigenaar van alle gegevens die je uploadt in Contractify.

Verder kun je altijd vragen om een algemene export van alle gegevens. Dit is eenmaal per jaar gratis.

Jouw gegevens versus AI-training

De gegevens die je uploadt naar Contractify worden nooit door Contractify gebruikt om AI-modellen te trainen. Jouw gegevens worden niet gebruikt om de modellen van OpenAI te trainen. Bij het genereren van content met behulp van AI slaat OpenAI gegevens tijdelijk op voor een korte periode om misbruik van hun platform te voorkomen, maar verder worden je gegevens niet bewaard of gebruikt. Zie OpenAI's Beveiligingspagina voor meer informatie

Je gegevens worden gebruikt als onderdeel van prompts die naar OpenAI worden gestuurd om content te genereren in AI-functies in de Contractify app. De gegevens van je Contractify account worden uitsluitend gebruikt om content te genereren voor je eigen app, en niet voor andere gebruikers van het Contractify platform.

Escrow

Daarnaast is er ook de mogelijkheid om je in te schrijven op onze Escrow-lijst.

De broncode van Contractify wordt in bewaring gegeven bij een notaris die het in een kluis bewaart. Dit proces vindt jaarlijks plaats. Bij grote software-updates kan dit vaker gebeuren.

Als aan bepaalde voorwaarden wordt voldaan, zoals een faillissement, kunnen de klanten die zich hebben ingeschreven op de Escrow aan de notaris vragen om hen te voorzien van de meest recente broncode. Daarna kunnen ze Contractify live houden voor eigen gebruik (dus niet voor commercialisatie).

Als klant kun je je eenvoudig abonneren op onze Escrow-lijst tegen een registratievergoeding van 5% op je licentiekosten.

2. Back-up Procedure

Wat betreft de back-up van de gegevens en database-informatie in Contractify, is er een onderscheid tussen de databasegegevens en de fysieke bestanden.

Database

Voor de database back-ups passen we de volgende back-up bewaarperioden toe:

- Point-in-time herstel gedurende 7 dagen
- Dagelijkse volledige back-up gedurende 14 dagen
- Wekelijkse volledige back-up gedurende 8 weken (1 back-up per week)
- Maandelijkse volledige back-up gedurende 6 maanden (1 back-up per maand)
- Jaarlijkse volledige back-up gedurende 1 jaar (1 back-up per jaar)

De hoofddatabase bevindt zich in Duitsland (Digital Ocean). De back-ups worden gekopieerd naar een ander datacenter van dezelfde provider in Nederland en naar een andere provider in Ierland.

Bestanden

Bestanden worden opgeslagen bij DigitalOcean Spaces (geüploade bestanden, afbeeldingen...).

Er is een on-the-fly synchronisatie naar een aparte DigitalOcean Space in een fysiek datacenter en ook naar een andere provider (Amazon). Deze synchronisatie is ingesteld in een write-only modus.

3. Data beveiliging

De originele gegevens worden opgeslagen op servers van DigitalOcean in hun datacenter in Frankfurt (Duitsland), back-ups worden gemaakt in Amsterdam (Nederland, Digital Ocean) en Dublin (Ierland, Amazon).

De servers van Digital Ocean hebben de volgende certificaten:

- ISO9001
- ISO27001
- ISO14001
- ISO50001
- SSAE16 Type II

Een kopie van de certificaten voor Digital Ocean kan hier worden verkregen. De certificaten voor Amazon zijn hier te vinden .

Beveiliging van bestanden

Bestanden zijn niet openbaar beschikbaar via een directe link. Wanneer een bestand wordt opgevraagd via de applicatie, genereren we een beveiligde link naar het bestand die geldig is voor een beperkte tijd.

Beveiliging van gegevens

Onze databases worden beveiligd door DigitalOcean en er wordt gebruik gemaakt van een IP whitelist. Dit betekent dat zelfs als er referenties zijn gelekt, er geen verbinding kan worden gemaakt als het IP-adres geen verbinding mag maken. Alle communicatie naar de databases is versleuteld met behulp van industriestandaarden.

4. Hoe beschermen we u gegevens

Gegevensversleuteling

- Alle gegevens worden onderweg versleuteld door middel van HTTPS.
- Gegevens die zijn opgeslagen op servers en objectopslag zijn in rust versleuteld

Toegangscontrole

- Sterke authenticatie (twee-factor) is beschikbaar

- Er kunnen verschillende toegangsniveaus worden gedefinieerd (beheerder / manager / gebruiker / viewer) om te bepalen wat de gebruiker wel of niet kan doen en waartoe hij toegang heeft.

Auditing en registratie

- Interne registratie van alle aanmeldpogingen
- Interne registratie van alle gevoelige acties uitgevoerd door gebruikers
- Interne registratie van het gebruik van onze API
- Registratie van alle verzoeken die worden uitgevoerd op onze webservers

Reactie op incidenten

- Er is een protocol voor datalekken geïmplementeerd en dit wordt aan al onze medewerkers gecommuniceerd

Patches and updates

- Wekelijkse updates van bibliotheken van derden die in onze applicatie worden gebruikt
- Maandelijkse “patch dinsdag” om onze servers en infrastructuur up-to-date te houden

Netwerkbeveiliging

- Op alle servers draait een goed geconfigureerde firewall
- Onze hostingprovider biedt bescherming tegen DDoS-aanvallen
- Geïsoleerde productie-, staging- en ontwikkelomgevingen

Veilige ontwikkelingspraktijken

- Geautomatiseerd scannen op kwetsbaarheden en beveiligingen van onze code (Sonarcloud)
- Statische analyse van onze code
- Uitgebreide geautomatiseerde testsuite

Penetratietesten

- Jaarlijkse penetratietesten
- De resultaten van de penetratietest zijn op verzoek beschikbaar