contractify

DATA SECURITY (version 04/2024)

We, DB2 Value Creation BV, Polenstraat 163, 9940 Evergem, Belgium (VAT BE0644714953) attach great value to safeguarding our customer's data. We recognize that the trust of our customers is our most valuable asset, and keeping their data secure is essential for maintaining this trust. Therefore, we take proactive measures to protect and secure our customers' data against unauthorized access, misuse, and data breaches.

This document outlines the key principles and practices that we follow to ensure the security and confidentiality of our customer's data.

1. Data

Data ownership

As a customer, you always remain the owner of all data uploaded in Contractify.

Furthermore you can always ask for a general export of all data. This is free of charge once a year.

Your data versus AI training

The data you upload to Contractify will never be used by Contractify to train AI models.

Your data is not used to train OpenAI's models. When generating content using AI, OpenAI temporarily stores data for a short period of time for preventing abuse of their platform, though otherwise does not retain nor use your data. See OpenAI's Security page for more information.

Your data will be used as part of prompts sent to OpenAI to generate content in AI-powered features in the Contractify app. The data from your Contractify account is exclusively used to generate content for your own app, and not other users of the Contractify platform.

Escrow

In addition, there is also the possibility to subscribe to our Escrow list.

The source code of Contractify is deposited with a notary who keeps it in a safe. This process is done yearly. In cases of big software updates, this can happen more frequently.

If certain conditions are met, such as bankruptcy, the clients who have subscribed to the Escrow can ask the notary to provide them with the most recent source code. Afterwards, they are able to keep Contractify live for their own use (i.e. not for commercialisation).

As a customer you can easily subscribe to our Escrow list at a registration fee of 5% on your license fee

2. Backup Procedure

In regards to backup of the data and database information in Contractify, there is a distinction between the database data and the physical files.

Database

For the database backups, we apply the following backup retention periods:

- Point-in-time recovery for 7 days
- Daily full backup for 14 days
- Weekly full backup for 8 weeks (1 backup per week)
- Monthly full backup for 6 months (1 backup per month)
- Yearly full backup for 1 year (1 backup per year)

The main database is located in Germany (Digital Ocean). The backups are copied to another datacenter from the same provider in the Netherlands and to another provider in Ireland.

Files

Files are stored with DigitalOcean Spaces (uploaded files, images…).

There is an on-the-fly synchronization to a separate DigitalOcean Space in a physical datacenter and as well to another provider (Amazon). This synchronization is set up in a write-only mode.

3. Data security

The original data is stored on DigitalOcean Servers in their data center in Frankfurt (Germany), backups are made in Amsterdam (the Netherlands, Digital Ocean) and Dublin (Ireland, Amazon).

DigitalOcean servers have the following certificates in place:

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

A copy of the certificates for Digital Ocean can be obtained here. For the Amazon certificates, these can be found here.

Security of files

Files are not publicly available via a direct link. When a file is requested via the application, we generate a secure link to the file which is valid for a limited amount of time..

Data Security

Our databases are secured by DigitalOcean and an IP whitelist is used. This means that even when credentials are leaked, no connection can be made if the IP address is not allowed to connect.

All communication to the databases is encrypted using industry standards.

4. How do we protect your data?

Data-encryption

- All data is encrypted in transit by means of HTTPS.
- Data stored on servers and object storage are encrypted at rest

Access control

- Strong authentication (two-factor) is available
- Different access levels can be defined (administrator / manager / user / viewer) to define what the user is able or unable to do and access.

Auditing and logging

- Internal logging of all login attempts
- Internal logging of all sensitive actions performed by users
- Internal logging of the usage of our public API
- Logging of all requests performed on our web servers

Incident Response

- A data breach protocol has been implemented and is communicated to all our employees.

Patches and updates

- Weekly updates of third-party libraries used in our application
- Monthly “patch Tuesday” to keep our servers and infrastructure up-to-date

Network security

- All servers have a properly configured firewall running
- Our hosting provider provides protection against DDoS attacks
- Isolated production, staging and development environments

Secure Development Practices

- Automated vulnerability and security scanning of our code (Sonarcloud)
- Static analysis of our code
- Extensive automated test suite

Penetration testing

- Yearly penetration test
- The results of the penetration test are available upon request