Data Security

1. Data **3**
Data ownership 3
Escrow 3
2. Backup Procedure **4**
Database 4
Files 4
3. Data security **5**
Security of files 5
Data Security 5
4. How do we protect your data? **6**
Data-encryption 6
Access control 6
Auditing and logging 6
Incident Response 6
Patches and updates 6
Network security 7
Secure Development Practices 7
Penetration testing 7

Polenstraat 163, 9940 Evergem| www.contractify.io | info@contractify.be

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.

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.

Polenstraat 163, 9940 Evergem| www.contractify.io | info@contractify.be

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

Polenstraat 163, 9940 Evergem| www.contractify.io | info@contractify.be

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

Thank you!

Contractify

Polenstraat 163,
9940 Sleidinge
+32 9 234 28 97
info@contractify.be
www.contractify.io