Compination GmbH
Austrasse 40
8045 Zürich
Telefon +41 43 960 99 23
hello@compination.ch

compination

Dokumentname	rDSG Compliance Compination
Projekt / ID	Internal & Customer Information

Document-Version	V1.0B29

Last Save Date	11/03/23 - 15:54:59	Author	Tobias Göller
Validity	Until Obsoleted	Published	20230828
Filename	20231103_rDSG_Compliance_Compination_V1.0B30		
Last Saved by	Tobias Göller, 11/03/2023, 15:54		
Remarks	NONE		

	Draft	Audit	Approved
Document Status	X		

Editor	Tobias Göller (TG)
Auditor/Approval	Marc Müller (MM)
User	
Zur Information	All Members of Compination GmbH & All Customers (Public Document)

Inhaltsverzeichnis

1 Introduction....3

2 Document Versions....3

3 Document References....3

3.1 Document Obsolescence....3

4 CDSO / DDSO Roles....4

5 What we do as a Company....4

6 What kind of Data do we collect....4

6.1 Customer Type Specification....4

6.2 Data possibly colllected about Private Customers....4

6.3 Data possibly collected from Business Customers....5

6.4 Data possibly collected from Hosting Customers....6

7 Handling of Data....7

7.1 Data About Customers (Private- & Business-Customers)....7

7.2 Data FROM customers (Hosting-Data)....7

7.2.1 Backup....7

7.2.2 Initial Passwords....7

7.3 Third-Party-Access to Data....7

8 Data REJECTED by us....8

1 Introduction

This document discloses how we handle customer data. It will be adapted over time.

New Releases will receive a new Major Version number.

Minor changes without alteration of the meaning of the contents will be reflected by the subversioning / build number.

All versions below 1.0 have to be considered a “Draft” Version.

2 Document Versions

Version	Date	Author	Comment
1.0B29	20230828	Tobias Göller	First publicly released version.
1.0B30	20231103	Tobias Göller	Minor Change (Re-Assignment of the CSDO / DDSO Role)

3 Document References

Reference	Reverence Version	Author	Document Title
1	LATEST	Tobias Göller	Data Security Policy Compination

3.1 Document Obsolescence

The valid version of this and all referenced documents is, unless explicitly stated otherwise, always the latest released version.

Newer versions always supersede older versions (and render them invalid in the cause).

4 CDSO / DDSO Roles

The CDSO (Chief Data Security Officer) Role is assigned to: Tobias Göller
The DDSO (Deputy Data Security Office) Role is assigned to: Marc Müller

5 What we do as a Company

Compination GmbH is an IT Services Company. We offer professional Services of many kinds to our customers.

Our activities center around solving customer requests and / or developing solutions for our customers. As such we do have to have access to a multitude of data in order to accomplish our services and fulfill our contracts.

6 What kind of Data do we collect

Compination GmbH collects all kinds of Data which are necessary to interact with customers and fulfill it's contracts.

However, some kind of data will be refused and not collected by us in any form (See: Data REJECTED)

6.1 Customer Type Specification

We differentiate between three types of customers:

- Private Customers
- Business Cusomers
- Hosting Customers

6.2 Data possibly colllected about Private Customers

This data we collect may include:

- First and Last-Names
- Birthdates
- Names of Spouses and other Family Members of the Customer
- Postal Addresses
- E-Mail Addresses
- Telephone Numbers
- E-Mail Account Information including Usernames and Passwords
- Access Data to Web-Portals
- Access Data to customer Server Systems
- Payment Information
- License Information
- Trouble-Tickets issued by the customer to us
- Public Keys
- Data about Alarm-Systems (private Premises)

6.3 Data possibly collected from Business Customers

This data we collect may include:

- First and Last-Names
- Birthdates
- Names of Spouses and other Family Members of the Customer
- Postal Addresses
- E-Mail Addresses
- Telephone Numbers
- E-Mail Account Information including Usernames and Passwords
- Access Data to Web-Portals
- Payment Information
- License Information
- Access Data to business Premises (like Keys- or Badge-Data)
- Access Data to customer Server Systems
- Pin-Codes to access the premises
- Trouble-Tickets issued by the customer to us
- Public Keys
- Data about Alarm-Systems (Data-Centers and/or Office Buildings)

6.4 Data possibly collected from Hosting Customers

This data we collect may include:

- First and Last-Names
- Birthdates
- Names of Spouses and other Family Members of the Customer
- Postal Addresses
- E-Mail Addresses
- Telephone Numbers
- E-Mail Account Information including Usernames and Passwords
- Access Data to Web-Portals
- Payment Information
- License Information
- Trouble-Tickets issued by the customer to us
- Public Keys
- **All Data stored on the Hosting Infrastructure**

7 Handling of Data

7.1 Data About Customers (Private- & Business-Customers)

All data is secured on our own Cloud Server Systems and or business devices adhering to the Standards & Requirements in [1]

All Cloud access to our own infrastructure is secured by:

- 2FA Authentication
- Encryption
- Access Restrictions

There is no public access available to this part of the infrastructure.

7.2 Data FROM customers (Hosting-Data)

Data FROM customers (i.e. stored on our hosting platform) is inline encrypted and secured.

All Cloud-Shares are encrypted without any possibility for us to encrypt any of the data.

We do not have any kind of master-key nor do we have plans to create such keys.

7.2.1 Backup

We only backup the data in it's originating form. Encrypted data will not be decrypted.

7.2.2 Initial Passwords

Initial Passwords from customers are stored in encrypted containers.

If we have to set a new password that container data might be updated as well depending on the situation / customer (and if agreed with).

We do not run any reverse cracking software.

In addition we do not enforce any regular password changes but we do enforce a strict password policy on the data hosted by us.

7.2.2.1 Password Security

We can not be held responsible for passwords lost by the customer in any way.

The customer is solely responsible for keeping his passwords / tokens / keys secure.

7.3 Third-Party-Access to Data

No data is handed over to 3rd Parties ***except*** if agreed with by the concerned person / customer.

Normally this is only the case for projects where 3rd Parties are directly involved by us or by the customers.

8 Data REJECTED by us

We do reject any kind of data that could either endanger the integrity of the customers Data or cause harm to the customer or his reputation in any form. As such, data like:

- Private Keys
- ANY Financial Information not required for the Offering and / or Billing Process
- Any personal medical information (as long it is not explicitly requested by the customer) Such data will be immediately deleted after the time period the data is required ends.
- Any contractual information between a customer and third parties.