

## Security Brochure

*Version: June 2020*

At RebaseData, security is our highest priority. We want you to feel safe when you convert your databases, especially when they contain sensitive data like healthcare data. Therefore we invested a lot of effort in securing our service.

### Compliance

We comply with GDPR and offer a Data Processing Agreement (DPA). We provide a commitment regarding § 203 of the German Criminal Code to process health data. Furthermore, we are compliant with HIPAA Privacy/Security to protect your ePHI. We have a designated Privacy/Security officer and all necessary policies and procedures in place. We are available to sign a Business Associate Agreement (BAA) with you, no matter if you are a Covered Entity or a Business Associate under HIPAA.

### Workforce

Our workforce was educated regarding data privacy and security. They went through a GDPR, HIPAA Awareness and HIPAA Security training. We have numerous policies and procedures in place to guarantee GDPR, and HIPAA compliant data processing. Every single team member signed a confidentiality agreement.

### Data center

Our data center Hetzner Online GmbH is located in Sigmundstraße 135, 90431 Nuremberg, Germany. It is compliant with ISO/IEC 27001:2013. We can provide you the certificate and the statement of applicability that shows the security measures that are in place.

### Servers

Our servers are monitored 24/7. Every server has a firewall with strict packet rules configured. The servers' software is updated at least every month. We are part of a security mailing list so that we receive vulnerability notifications as early as possible. Once we receive a relevant vulnerability notification, we will react immediately by updating our servers. The servers have full disk encryption, for which only we have the key (no external party). On request, we also offer our enterprise customers to have a dedicated server that can only be accessed by a certain IP or using a VPN.

**Application**

Our proprietary application that converts the databases is written in a safe programming language, Java. Furthermore, it was reviewed for security. Every conversion is executed in a secure environment on one of our servers so that each conversion is guaranteed to be strictly separated from other conversions.

**Workstations**

By default, data will only be saved on our secure servers. Only in exceptional cases – for example, when debugging a problem – data will also be stored on our workstations. All our workstations must have encrypted disks (data at rest is encrypted), screen lockers, etc.. On request, we can also flag the client's account, so that data will never be processed on a workstation, but only on our servers.

**Encryption**

Data is always encrypted at rest using strong encryption, no matter if it's saved on our servers or a workstation. Also, the data in motion is always encrypted via SSL/TLS.

**Contingency Plan**

For our enterprise customers, we offer a highly available server setup. In addition, we offer superior SLAs.

**Access controls and audits**

Each user has a unique identification. We are very strict when granting permission to a certain user. Permissions are always kept at a minimum level. We regularly check access lists and we audit server logins.

**Subcontractors**

We have no subcontractors that have access to sensitive data. In case we will have subcontractors in the future, we will guarantee that they comply with our highest privacy and security standards.