

ANLAGE ./A ZU DEN AGB

ALLGEMEINE DATENSICHERHEITSRICHTLINIEN (ADSR) DER LDB LABORDATENBANK GMBH

1. Ansprechpartner für Support und Technik

Für jeden Kunden wird ein primärer Ansprechpartner (First-Level-Support) und ein sekundärer Ansprechpartner definiert der als Vertretung und für den Second-Level-Support zur Verfügung steht, sodass eine optimale Betreuung durchgehend gewährleistet ist.

2. Nutzung der Labordatenbank

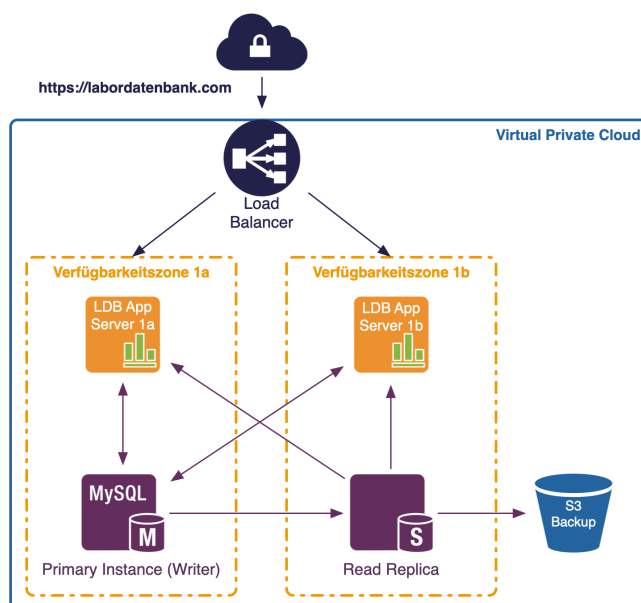
Die Labordatenbank ist unter einer eindeutigen Webadresse mit jedem modernen Web Browser erreichbar. Weitere Information zur Labordatenbank und den unterstützten Web Browsern finden Sie in der Labordatenbank Anleitung unter: <https://labordatenbank.at/manualpages>

3. Verfügbarkeit der Labordatenbank Cloud

Die Labordatenbank Cloud läuft auf mehreren Servern im Amazon Rechenzentrum in Frankfurt – dem größten Anbieter von Rechenzentren weltweit. Dort läuft die Labordatenbank auf zwei unabhängigen Verfügbarkeitszonen. Durch die redundante Serverarchitektur (siehe Abb.) ist eine Verfügbarkeit von mehr als 99,95% sichergestellt.

Die Labordatenbank ist so aufgebaut, dass sie dem Ausfall einer Verfügbarkeitszone standhält und verfügbar bleibt. Jede Verfügbarkeitszone wird auf ihrer eigenen physisch getrennten unabhängigen Infrastruktur ausgeführt und ist auf hohe Zuverlässigkeit ausgelegt. Übliche Fehlerquellen wie Generatoren und Kühlanlagen werden nicht von mehreren Verfügbarkeitszonen geteilt. Die physische Trennung sorgt außerdem dafür, dass sogar bei äußerst seltenen Katastrophen wie Bränden, Stürmen oder Überflutungen nur eine Verfügbarkeitszone betroffen ist.

Nachfolgend ist die Serverarchitektur der Labordatenbank schematisch dargestellt.



Die Labordatenbank wird alle 10 Minuten auf Funktionalität geprüft. Ist die Labordatenbank nicht erreichbar, so wird automatisch Ihr Labordatenbank Ansprechpartner kontaktiert, sodass eine entsprechende Reaktion gestartet werden kann.

4. Updates zur Labordatenbank und Sicherheit

Die Labordatenbank wird laufend gewartet und weiterentwickelt. Während andere Datenbanksysteme keine oder nur spärliche Updates pro Jahr zur Verfügung stellen, gibt es bei der Labordatenbank laufend aktuelle Updates. Die meisten Updates dienen der weiteren Systemverbesserung, Erfüllung normativer Richtlinien und der Entwicklung neuer Funktionen (siehe Versionsverzeichnis: <https://labordatenbank.at/updates>).

Weiters wird die Sicherheit der Labordatenbank von unserer Technik laufend geprüft und verbessert. Mit der Sicherstellung laufender Updates sind auch die Sicherheitseinstellungen immer auf dem aktuellen Stand. Da es sich bei der Labordatenbank außerdem, global gesehen, um kein weit verbreitetes System, sondern um ein geschlossenes System nur für Kunden der LDB Labordatenbank GmbH handelt und der Source Code auch nicht offen liegt, ergibt sich ein zusätzlicher Schutz in Form von „Security by Obscurity“.

5. Schutz vor Zugriff durch Dritte

Die Labordatenbank Cloud verwendet ausschließlich eine HTTPS RSA-Verschlüsselung mit einer Schlüssellänge von 2.048 Bit und erfüllt somit die höchsten Sicherheitsanforderungen.

Die Labordatenbank verwendet eine Benutzerauthentifizierung (Login + Passwort), um den Zugriff auf Ihre Daten auf die von Ihnen freigegebenen Nutzer einzuschränken. Eine Nutzung der Labordatenbank ohne Passwort ist nicht möglich. Für einen zusätzlichen Schutz der Accounts kann darüber hinaus eine 2-Faktor-Authentifizierung nach dem TOTP-Verfahren aktiviert werden.

Jeder Versuch einer Anmeldung wird mit IP-Adresse und Uhrzeit gespeichert. Versucht jemand mehrmals hintereinander sich mit einem falschen Passwort anzumelden, so wird die Anmeldung zur Labordatenbank für einen definierten Zeitraum gesperrt.

6. Datensicherung der Labordatenbank Cloud

Eine vollständige Datensicherung der Labordatenbank erfolgt laufend auf Amazon S3 (<https://aws.amazon.com/de/s3/>). Um unseren Kunden absolute Sicherheit zu gewährleisten, wird bei der Labordatenbank jede Sekunde ein inkrementelles Backup erstellt. Darüber hinaus wird täglich ein vollständiges Backup erstellt.

Alle Tagesbackups werden für eine Woche aufgehoben. Nach einer Woche wird ein vollständiges Backup pro Woche bis auf Widerruf, für zumindest die nächsten 10 Jahre aufbewahrt.

Die Datensicherung ist auf eine Datenbeständigkeit von 99,999999999% über ein Jahr ausgelegt. Diese Zuverlässigkeitsstufe entspricht einem jährlich zu erwartenden Datenverlust von 0,000000001%. Diese Datenbeständigkeit wird erreicht, indem jedes Backup redundant auf drei voneinander unabhängigen Rechenzentren verteilt ist.

Wir können die Labordatenbank jederzeit aus dem letzten Backup wiederherstellen. Ebenso ist auch ein Export der Backups durch den Kunden selbst jederzeit möglich (z.B. zur lokalen Ablage).

7. Erstellung und Unterzeichnung von Berichten

Prüfberichte werden mit der Labordatenbank als PDF erstellt und mit der Labordatenbank unterschrieben.

Das Unterschreiben von Berichten ist nur durch eigens berechnete Nutzer und Passworteingabe möglich. Durch das Unterschreiben des Berichts wird ein digitaler Schlüssel erstellt, der jeden unterschriebenen Bericht vollständig und eindeutig identifiziert. Dieser Schlüssel wird in der Labordatenbank hinterlegt und kann jederzeit zur Validierung von Berichten herangezogen werden.

8. Anforderungen der ISO 17025 und ISO 9001

Die Labordatenbank erfüllt die Anforderungen der ISO 17025 und ISO 9001 und ist für den Einsatz in akkreditierten Laboren geeignet.

9. Datenschutzerklärung Labordatenbank

Die LDB verpflichtet sich, im Rahmen der Zusammenarbeit mit ihren Kunden das Datengeheimnis sowie sämtliche jeweils geltenden nationalen und europäischen Datenschutzbestimmungen einzuhalten, die für die LDB als Auftragsverarbeiter im Sinne der DSGVO und des österreichischen Datenschutzgesetzes (DSG) in der Fassung des Datenschutz-Anpassungsgesetzes 2018 ab 25.5.2018 gelten.