# Recovery Concept After a Physical or Technical Incident

To Supplement the Technical and Organizational Measures
pursuant to Art. 32(1) of the General Data Protection Regulation (GDPR)
for Processors (Art. 30(2)(d))

(Translated version from German, version 1.3 | translation without guarantee | status: 05/2025)

## 1. Introduction

### 1.1. Details of the Data Processor

| | |
|---|---|
| Name | Timebutler GmbH |
| Street | Rathausgasse 1 |
| Postal code | 12529 |
| City | Schönefeld |
| Handelsregister: | Amtsgericht Cottbus, HRB 18094 CB |
| Email address | info@timebutler.de |
| Website | www.timebutler.com |

### 1.2. Terminology

This document uses the terminology and definitions according to the General Data Protection Regulation (hereinafter referred to as "GDPR"). Furthermore, the following terms apply:

- "Contractor" refers to the processor as specified above in this document;
- "Client" refers to the controller pursuant to the GDPR who has entered into a data processing agreement with the processor;
- "Software" refers to the SaaS solution provided by the contractor for use by the client to carry out data processing.

## 2. Recovery Concept

### 2.1. Initial Situation / Hosting System

The software platform provided by the processor is offered to the controller as a Software as a Service (SaaS) solution. The SaaS solution consists of the following software components:

- MySQL database
- Nginx web server
- Load balancer
- Tomcat server

In addition, backup servers are used, on which automated backups of all data are stored.

## 2.2. Failure of the "MySQL Database"

### 2.2.1. Database System Failure

In the event of a failure of the database system, the log files must be analyzed and any errors identified. Based on this analysis, a decision must be made on a case-by-case basis whether the database system should be reinstalled or if the errors can be fixed and/or the database system repaired.

In the case of a reinstallation, the database backup must be restored from the backup server after the reinstallation.

### 2.2.2. Data Loss

If the database system is still available but data has been lost, the database backup must be restored from the backup server to recover the previous data state.

Subsequently, the log files should be reviewed to identify possible causes and to prevent the same error from occurring in the future.

## 2.3. Failure of the "Load Balancer," "Nginx," or "Apache Tomcat"

If the load balancer, Nginx, or Tomcat fails, a system restart should be performed first, which in most cases will restore the availability and functionality of the systems.

Regardless of whether this measure successfully restores functionality, the log files must be reviewed afterward to identify possible errors, in order to prevent such errors in the future or to fix the issue in case of a failed restart.

The database system is not affected, so after the issue with any of the three mentioned components has been resolved, the availability of the software is immediately restored.

## 2.4. Failure of the Operating System or Hardware / Host System

If the operating system or host system fails, for example due to a hardware defect, the following procedure must be followed:

The hosting provider offers failover to another data center. This allows availability to be restored as quickly as possible.

Additionally, the hosting provider initiates an inspection request to investigate the hardware defect or failure, in order to analyze the root cause, assess the likelihood of a similar event occurring again, and to derive and implement possible preventive measures.

### 2.5. Failure of Internet Connectivity

The software is operated on a server in a data center of the hosting service provider. The contractor selects a market-leading hosting provider with many years of experience and a professionally operated data center.

The hosting provider has monitoring systems, redundant connections, 24/7 support, and trained personnel who can restore internet connectivity as soon as it is disrupted. This assurance is part of the hosting service and does not require monitoring or notification by the contractor.