

EXHIBIT 3

Support Services and Service Level

Version 2026-07 · published at tchop.io/resources/security

Table of Contents

1. Availability.....	1
2. Maintenance	2
3. Communication and Support Hours.....	2
4. Incident Management.....	3
4.1 Priority Determination	3
4.2 Response Times	4
5. Capacity Management and Monitoring.....	4
6. Reporting.....	5

1. Availability

For the customer, the availability of the tchop CMS is measured by three relevant functions:

- the availability of the data interface (API) and the resulting ability to retrieve and consume current content in the native apps (critical for all users of the apps),
- the availability of the backend platform, which enables administrators and editors to import, edit and publish content and to exchange messages and content (critical for all administrators and editors of the platform),
- the proper functionality and performance of the native applications (apps) for smartphones and tablets; the supported operating system versions are set out in the platform agreement.

To be deducted from the availability of the first two functions are the periods during which the overall system is unavailable due to disruptions not attributable to tchop, in particular due to:

- force majeure,
- disruptions caused by components outside tchop's area of responsibility,
- misuse of the software by the customer.

Announced scheduled maintenance within the maintenance window (see section “Maintenance”) does not count as downtime. Deduction periods are measured in rounded-down minutes.

Downtime (= DT) means the periods during which the offering is unavailable due to disruptions attributable to tchop, measured in rounded-down minutes.

The maximum monthly availability (= Vmax) is: the number of calendar days of the respective month multiplied by 24 hours, minus the deduction periods.

tchop endeavours to achieve an availability of at least 99.95% for the data interface and the native apps, calculated according to the formula: $(V_{\max} - DT) \times 100 : V_{\max}$. For the backend platform, an availability of at least 99.9% is warranted on the basis of the same formula.

In the past years of operating the platform, actual availability has been significantly above these values, at more than 99.99%.

The native apps that enable users to use the content published and distributed on the platform are made available for download via the app stores of Apple (Apple App Store) and Google (Google Play Store). tchop cannot accept any liability for the availability of downloads in the app stores themselves. However, tchop shall ensure that the apps comply with the terms and requirements of the two software platforms and that the corresponding functionalities are available for use, provided users have a suitable device and a suitable internet connection. For this purpose, tchop provides regular software updates for these applications, which can be obtained via the respective platforms.

Should the availability of the offering be impaired by errors in the native apps, tchop provides so-called “hot fixes”, which are made available as separate updates in the app stores using accelerated release processes (“expedited release”). For the release of these updates, tchop ultimately always remains dependent on the app store review teams.

2. Maintenance

tchop performs scheduled maintenance on hardware, software and network components in the form of updates, preferably between 22:00 and 24:00 (CET/CEST). The availability of content in the native apps is generally not restricted during these periods.

Necessary maintenance outside this window is announced to the customer’s administrators and editors by e-mail in good time, at least three (3) business days in advance.

3. Communication and Support Hours

Within the scope of this agreement, tchop offers the following communication channels:

- for all users: by e-mail to support@tchop.io,
- for administrators and editors with access to the backend platform: by chat via Microsoft Teams or Slack,
- by phone via the hotline +49 30 616 54 883 (see platform agreement).

Business days within the meaning of this exhibit are Monday to Friday, excluding public holidays in Berlin, Germany. All times are stated in CET/CEST.

4. Incident Management

Incidents are registered and processed as follows:

	Step	Description
1	Report	The report by one of the customer's users should, where possible, include comprehensive information, in particular: specification of the incident, time of the incident, application environment and situation, frequency of the problem, error messages, and type and version of the internet browser or smartphone and operating system used.
2	Registration	Incidents are registered centrally and given an identification number. The request is automatically forwarded to the entire support and engineering team; a support employee takes on the request and is responsible for further communication.
3	Determine priority	The priority of the incident is determined jointly; the exact procedure is described under "Priority Determination".
4	Diagnosis	Analysis of the incident and its causes (e.g. by reproducing the incident in different environments).
5	Finding and, where applicable, implementing a solution	A solution for the incident is sought and, where applicable, implemented in the system environment.

4.1 Priority Determination

The priority is determined on the basis of the following procedure:

In a first step, the affected administrator on the customer's side proposes a priority from their point of view. If tchop's support employee agrees, the priority is recorded accordingly. If those responsible cannot agree on the priority in the first step, a managing director of tchop and the customer's lead project manager confer without delay.

If the parties cannot agree on the priority of the incident on the basis of the criteria set out here, the priority defined by the customer applies in case of doubt.

Priority	Description
1 – Critical Incident	This includes all errors that cause a permanent production standstill or simultaneously affect several users to such an extent that they are permanently unable to work with the platform or use content.
2 – Fault to be tolerated	This includes all errors that impair users' work on the platform or the

temporarily	use of content in the apps.
3 – Improvement	This includes all errors that lead neither to significant impairment (error class 2) nor to a permanent production or usage standstill (error class 1).

4.2 Response Times

The response time is the period between receipt of the incident report via one of the communication channels stated above and tchop's first qualified response. It does not include the resolution of the error itself.

Error class/priority 1:

- The response time is a maximum of 1 hour during normal working hours on business days between 9:00 and 18:00, and a maximum of 3 hours outside these times.
- The error is resolved as quickly as possible.

Error class/priority 2:

- The response time is a maximum of 3 hours during normal working hours on business days between 9:00 and 18:00, and a maximum of 6 hours outside these times.
- The error is resolved as promptly as possible.

Error class/priority 3:

- The response time is a maximum of 1 business day (Monday to Friday, excluding public holidays).
- The error is resolved as agreed between the parties.

5. Capacity Management and Monitoring

tchop tracks the available and used capacity of the components deployed. As soon as one or more of the required components reach or threaten to exceed the capacity limit defined for the respective component, capacity is expanded. Among others, the following components are tracked regularly:

- Total requests to the platform ("requests")
- Memory and CPU utilisation ("memory and CPU stats")
- Requests for the various status codes
- Average response time of the platform
- Active, paused and faulty connections ("connections")
- Database activity ("read/write operations")

In addition, tchop continuously monitors the platform with automated monitoring and alerting at the level of individual services and endpoints.

Details on data backups, recovery and the technical and organisational measures (TOM) are set out in the exhibits to the data processing agreement (see [Exhibits 4 to 6]).

6. Reporting

At the end of each calendar year, the customer may request a report containing:

- the service levels achieved and a comparison against the agreed standards,
- documentation of all support requests,
- a qualitative review of support and service.