



Inspectly

CONSTRUCTION · SOFTWARE · QUALITY

Service Level Agreement v. 1.6

Last updated: 18th of January 2023

Inspectly ApS | Lægårdsvej 24 | 8520 Lystrup | +45 7060 6055
contact@inspectly.com | www.inspectly.com | CVR: 3395 4883

Purpose

The purpose of this agreement is to qualify and quantify the service which is delivered by Inspectly during the actual delivery of the Inspectly-software. This is done by breaking down and specifying the individual service elements included in the delivery. This document describes the individual service elements and our service requirements for these.

Introduction

This Service Level Agreement (hereinafter SLA) describes the contractual relationship between the Client and Inspectly (hereinafter the Supplier).

This SLA applies to all products described if the Client has a valid and paid subscription, a signed and approved agreement and that the Client is not in arrears to the Supplier. Also, the following exceptions apply to the SLA:

- Force majeure
- Incidents which are caused by the Client, the Client's employees or others who act on the behalf of the Client
- Inevitable service impairments which is ordered and approved by the Client or which becomes mandatory due to legislation
- Planned maintenance

Unless otherwise defined in the contract between the Client and the Supplier this SLA applies to the Client's service. It can also be stated that the Supplier has an valid information security policy, as well as an established information security committee, who works with constant monitoring of information security in the company.

Definitions	
Downtime	The period of time that a service is unavailable within the agreed opening hours.
Uptime	Describes the percentual relationship between real downtime compared to theoretical maximum uptime (all hours of the day, all days of the week excluding service windows and possible downtime due to backup running.)
Opening hours	Describes the period of time system/service has been available.
Avalability	The percentual relationship between real downtime compared to agreed opening hours.
Response time	The time it takes from an incident/error is created to a solution to be released.
Service window	An agreed recurring time where updates, changes, releases etc. can be implemented with minimal impact on the system.
Normal working hours	Describes when the Client can get in touch with the Supplier. This is all weekdays Monday-Thursday at 8 am – 4 pm and on Fridays at 8 am – 3 pm.
The Supplier	All mentions of the Supplier in this document refers to Inspectly.

The Client

All mentions of the Client in this document refers to the Client(s) who are covered by this service through a signed contract and who have accepted this SLA

Support/help desk

As part of the subscription that you pay to Inspectly, free 1st level support is included. Support is available within normal business hours (see definitions).

1st level support is “help to self-help” and thus NOT the possibility that you can ask us to perform specific tasks for you. If you need direct/specific assistance for specific tasks, Inspectly also sells services at an hourly rate for this purpose.

In addition, it must be pointed out that our support team is trained to answer common software usage questions. Special technical questions such as API-integration, advice on what metrics, controls or similar that the Client should state in Inspectly, are beyond the support tasks/area of support.

Uptime/downtime

Inspectly always works proactively to ensure the Client as much uptime as possible. Planned downtime will be experienced in connection with quarterly updates. In connection with unplanned changes, updates and maintenance on the system, Inspectly has the opportunity to stop the operation during the period from 10 pm to 5 am (CET) on weekdays to inform about the stop with a minimum of 1 days’ notice. However, in the event of critical errors or malfunctions, the operation can be stopped immediately.

All operating information can be viewed at <http://inspectly.com/operatingstatus>

Release of new functionality

Larger system updates are done up to four times a year and coincide with the release of new functionalities. These updates are expected to take place mid-January, mid-April, mid-July and mid-October. Intermediate updates will only concern minor updates or bug fixes and not new, larger features.

In connection with the release of new functionalities you, the customer, will be informed about this in the following time frame:

- At least 30 days prior to the release, an email is sent to you concerning the content of the update
- At least 3 working days prior to the release you will receive an email detailing the content of the update.

The above mentioned content updates are sent to the primary contact person, all administrators and project managers, as well as persons indicated as recipients of product news in the administration system.

The above mentioned content will also be made available in the administration system, through a message in the notification system. Apart from this communication, you are also urged to sign up for the Inspectly newsletters, which will also feature information regarding upcoming products.

Crash/unplanned downtime

In the event of server-crashes, the responsibility to reestablish regular service rests solely on Microsoft. We will inform you, the customer, of the crash, describe the issue, lay out an expected time frame for the solution of the issue, as well as orientate you, at least twice daily, about progress on the issue.

After the solution of the problem, Inspectly will explain why the crash occurred. In addition, Inspectly will elaborate on what initiatives will be taken in the future to avoid similar incidents.

Incident reporting

If you, as a Client, experience an error in the software, we naturally appreciate that you report this so that we can initiate a correction. Reporting must be made to support@inspectly.com.

Response time

In connection with incident reporting we work with following service goals:

	Less critical	Critical	Very critical
Definition	"Cosmetic" error which do not have a disruptive effect.	Errors that mean a given function cannot be used. Meanwhile, there is another way to take the desired action.	Errors that mean a feature is not available on Inspectly. Meanwhile, there is no other way to do the desired action.
Reponse time	30 days	7 days	2 days

Description of technical setup

The purpose of this section is to illustrate the setup of the technical conditions in Inspectly.

Hosting

The Inspectly software is operated from a Microsoft Azure based environment. All data is stored in the "Western European" zone which at the current time means that the data is stored in the Netherlands .

In relation to the uptime on these servers, reference is made to Microsoft's standardized SLA for the Azure platform. Inspectly disclaims all liability on these servers but refers to Microsoft.

Backup

Media backups (images, audio files, etc.) are ongoing and media is mirrored on 2-3 servers as they are uploaded. At the database level, all changes are made via transactions and a copy of each transaction is continuously saved. These backups are saved for 30 days, restores happen to “point in time”. As the backup is stored no more than 30 days, restoration of data beyond the 30 day period is not possible.

This backup secures you as a Client against data loss to the greatest extent possible. The backend is a total backup of our entire production environment and the individual Client is thus a small piece of this total backup. If you, as a Client, need to recover data that has been erased by your own employees by mistake, this is done for a fee.

User management and login

Inspectly is login-protected, so that only the users that you as the Client define, have access to the system. In practice, the Inspectly application checks whether a given user has access to the system at login (by online mode). Thus, you as a Client can at any time shut down users who no longer will have access to the system.

In case a user has indicated that he or she is working offline, it will not be possible to reject the user until he or she goes online again. An offline user cannot access the data stored on the server and as soon as it goes online again, will be logged out of Inspectly.

Data security and management of the devices

At Inspectly we are very committed to stability and security when it comes to registering and storing the data which our clients collect or register through our system. Our app is thus designed so that data is always stored locally on the device’s hard drive. This means that Inspectly works even without internet coverage. As soon as the device is back online, data will automatically be uploaded to our servers. All data – including images – is stored in a local database on the devices.

The app is developed for both iOS and Android and is supported for the three latest versions of the OS. Data saved locally on the Inspectly-app is, at present, unencrypted. At the end of 2020, a new version of the app is to be launched, which will, amongst other things, also contain encryption of locally stored data.

API

All communication between servers and the two apps is via a REST-full API which uses JSON protocols. The API is subject to 128 bit encryption (HTTPS), so traffic between the different parts of the system cannot be intercepted and read.

Read more about our API in our separate document on API specification.

Data security on the servers

Microsoft Azure's servers are secured by the standards of the time, in regards to firewalls and access. Data is stored in individual MS SQL databases where a separate database instance is created per Inspectly-Client. Data in the form of pictures, sound files, drawings etc. are stored in a separate file system besides the database. These data are not encrypted.

A safety report from Microsoft Azure, describing the level of security of the servers, can be requested, if the customer so desires.

Supported devices

Inspectly is developed for iOS and Android respectively. On both devices, the Inspectly app is designed to encrypt data on the devices. Similarly, the data is sent to the servers in an encrypted form.

Changes to this SLA

Inspectly reserves the right to change and update the content of the present SLA and any additions, if the changes do not individually or collectively significantly impair the Client's service and support as described in this SLA.