Service Level Agreement

Version: October 16, 2023

Table of contents

1. General

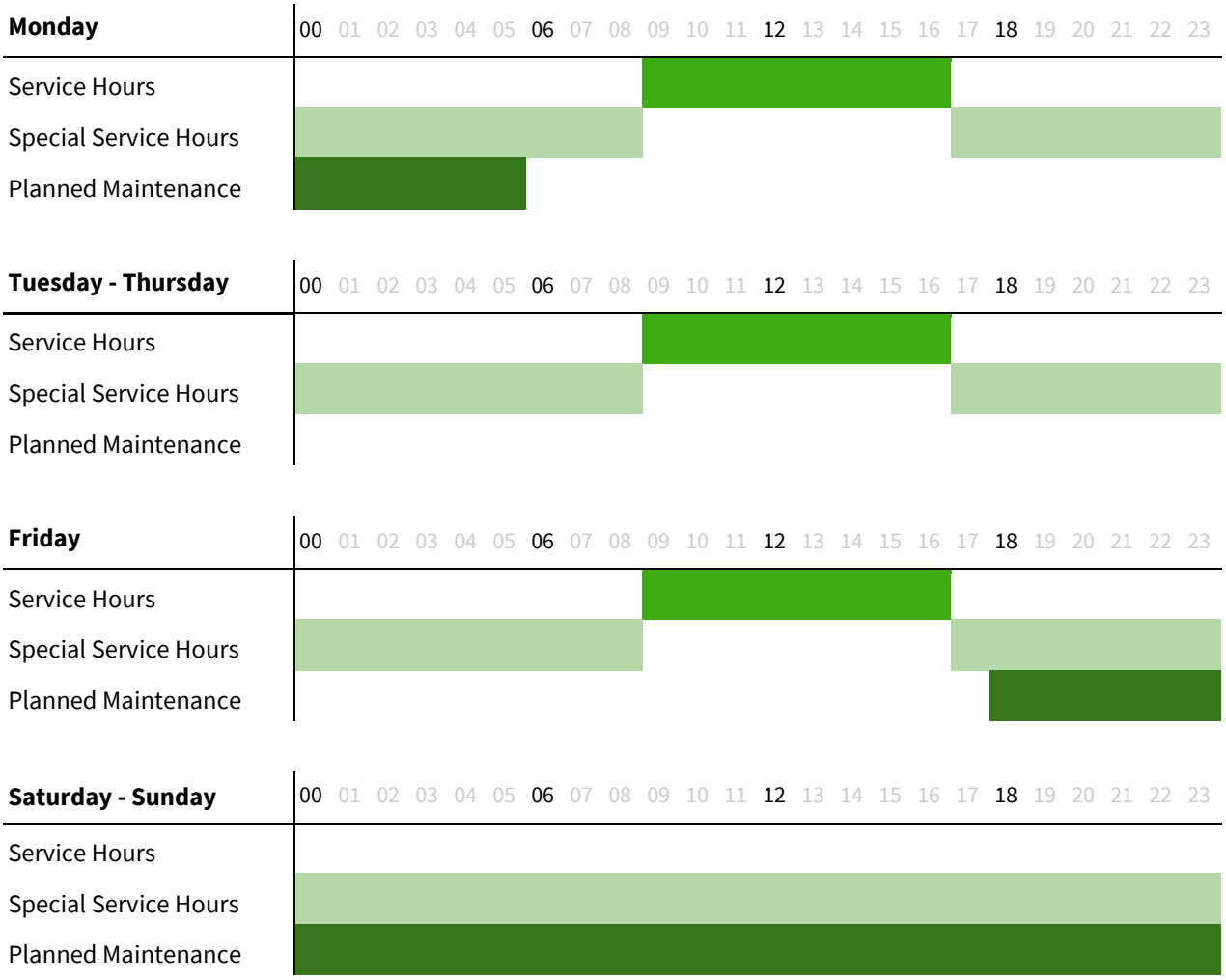
The purpose of this Service Level Agreement (hereafter: SLA) is to specify the performance levels of the services of POM NV (hereafter: POM) for the Customer. This SLA is valid on the date of delivery of the Products and Services and has a term equal to the main agreement.

a. Definitions

Disturbance	A reproducible issue as a result of which the services provided with regards to one of the Software services of POM are not (fully) available to the Customer or available to a lesser extent.
Infrastructure	The hardware, data communication facilities and system software used by POM and under its responsibility.
Necessary extra maintenance	Maintenance during Service Hours of POM for which no postponement is possible (e.g. due to security risks).
Notification	A Notification made by Customer to Support during Service Hours, in accordance with these Terms and Conditions.
Planned maintenance	Possible from Friday 18:00h to Monday 06:00h.
Resolution time	The period of time (including Response Time) within which a detected or reported Disturbance is resolved or repaired (whether or not temporarily by means of a workaround).
Response time	The time that elapses between the reading of a Notification and the time at which POM commences and confirms the Support in a verbal or written communication to the Customer.
Service Hours	POM business hours (9.00 am - 5.00 pm CE(S)T) from Monday to Friday with the exception of National public holidays.
Software service POM	The POM Software Service is defined as the availability of the hosted payment- and landing pages, the DPA system, API and WebApps, as stated in the Agreement.
Special Service Hours	All hours in a day outside of Service Hours.
Support	Assistance by the POM Support Team (hereinafter: Support) during Service Hours with respect to the POM Software Services, including explanation of the standard

user documentation, assistance with the correct functioning of the POM Software Services and verification and analysis by the Customer of the correctness of data entered or processed. Support shall expressly not include, i.a. the provision of implementation services and training at the start of the use of the POM Software Services and the provision of project management.

b. Visualization timeframes



2. Availability and performance

a. Up-/downtime

POM aims, to the best of its ability, to achieve an availability of 99.9% on average per month. Availability is defined as being able to log into the site/portal of POM (to be measured on the server of POM) in the agreed POM Software service(s) and the visibility of the start page of the POM Software service(s).

The achieved availability is calculated as follows: Uptime is the time that the Software service of POM is available. Downtime is the time that the Software service of POM is unavailable. Planned maintenance, necessary additional maintenance and circumstances beyond the control of POM will not be included as Downtime and will not be included when determining the Uptime percentage. The achieved availability is Uptime/ (Uptime + Downtime).

b. Maintenance

POM will do its utmost to ensure that the Customer is informed of any intended activities on the website (portal POM) or via email at least seven (7) business days in advance.

c. Data traffic speed

POM will do its utmost to maintain the speed of the data traffic to and from the Software services at such a level that the Customer can use the service in an acceptable manner during Service Hours. The following measurement is applied as an objective measurement assessment: the requesting or sending of a page in an Environment with an average scope via a computer/smartphone of an average life and averagely maintained with a telephone- or internet connection of average speed, takes place within three (3) seconds in two of the three cases, where the third instance cannot take longer than five (5) seconds. The Customer must assert and substantiate that this is not the case.

d. Monitoring

The availability of the POM Software Service is measured every five minutes from at least three locations worldwide. The most recent availability value is shown on the dashboard in the DPA system. The specified values reflect the minimum availability for the cumulative values of all measurement locations worldwide. Subject to evidence to the contrary, the availability and service level measured by POM shall constitute full proof.

3. Support

Support shall be provided from a location of POM. For support on location of Customer and / or outside Service Hours, separate arrangements can be mutually agreed upon at the then applicable fee for Customer.

a. Submitting a Notification

Notifications can be passed on to Support by e-mail using the contact details below:

- E: services@pom.be
- T: +32 (0)3 747 91 12

Only users with a valid user account can submit Notifications. Users submitting a Notification by e-mail will be authenticated based on the e-mail address and user name in the DPA system. Users submitting a Notification by phone will be authenticated based on a PIN in the DPA system.

b. Required information

A Notification contains at least the following information:

- Customer number;
- Name and contact details of the notifier;
- A detailed description of the notification.

To facilitate processing, the Notification should also contain supporting material, such as screenshots, logs, URLs, IP addresses, information about the operating system, device and browser used and/or a list of activities that led to the Notification.

c. Notification properties

Notification priority

POM uses the following definitions regarding the priority of a Notification.

High	If, due to a Disturbance on the part of POM, its Software Service becomes unavailable or only very limited available to Customer and/or results in a serious application error and jeopardizes the progress of Customer's essential business process. Whether or not through some modification or work around, Customer can still work with a large part of the Software Service with limited disruption.
Medium	Where there is a non-substantive Disturbance in any of POM's Software Services with limited impact on Customer and which does not require an immediate response from POM.
Low	Where there is a non-substantive Disturbance in any of POM's Software Services with no impact on Customer and which does not require an immediate response from POM.

Notification type

POM uses the following definitions regarding the type of a Notification.

Task	Notifications that contain a (standard) task to be performed, for example, a callback request for an employee.
Question	Notifications containing an informational question about the use of the Software, POM, etc.
Request	A request for a change to the Software. This can be a Request for Change (RFC) or a Feature Request (FR).
Vulnerability	A potential weakness that may cause an Incident.
Incident	A Disturbance regarding the 'availability', 'integrity' and/or 'confidentiality' with respect to all types/types of data or processing.

d. Processing a Notification

Notifications are handled during Service Hours; on workdays from Monday through Friday between 09:00 and 17:00 CE(S)T, excluding recognized national holidays.

When the Support Agent opens the Notification, he or she will assess whether the Notification contains sufficient information for further processing. If there is sufficient information, the Support Agent will then determine the type and priority of the Notification based on the notifier's input and his or her own findings. If the information is insufficient, the notifier is asked to supplement it.

The Support Agent then sends an initial response. This could be, for example, a request for more information, a confirmation of the solution or a confirmation that the Report has been dealt with.

For High Priority Notifications, an update is given every two hours during Service Hours. In addition, on request, a report can be made available about the submitted High Priority Notifications.

e. Response- and resolution times

During Service Hours, the following response- and resolution times apply per priority level:

Priority High	8
Priority Medium	16
Priority Low	24

Resolution times cannot be guaranteed and are therefore on a best-effort basis. This is related to dependencies of the notifier, third parties, available time and resources, restore times of (large) backups and other external factors.

4. Information security

POM has implemented an ISO 27001-certified information security management system (ISMS). The sections below describe some of its measures.

a. Vulnerability- and Incident management

Vulnerability management

A weak spot or vulnerability is an error in a digital system, allowing an attacker to gain unauthorized access to systems or information. As a result, the attacker can, for example, access, modify, destroy, install malware and/or take the data hostage, preventing the user from accessing the information.

Employees can report vulnerabilities according to the procedure “Procedure for managing technical vulnerabilities”, using an internal form and customers are able to report the vulnerabilities to Support, as described in chapter 3. Support.

After a vulnerability has been reported, the security risk and possible impact are investigated and assessed. Should the risk and impact turn out to be acceptable, the recovery is allocated to the development team and put on the sprint planning. If the risk cannot be accepted, mitigating measures are taken immediately, implementing temporary workarounds where necessary.

POM will, at its own initiative and expense, have a penetration test performed once per calendar year by ethical hackers at an independent certified Third Party. The report can be viewed by the customer during a physical appointment at POM's office or online using a video conferencing tool.

Additionally, POM provides an opportunity for external parties to report vulnerabilities, through the 'Responsible disclosure' on the POM website.

Incident management

The Notification Type Incident is assigned to the Notification based on the input from Notifier and POM's assessment. Information security incidents are events that have led, or may have led, to:

- Unavailability of information, applications, websites, devices, etc.;
- A breach of confidentiality of information;
- A violation of integrity of information.

Employees and customers must report an incident as soon as possible after detection. Employees can report the incidents through an internal form and customers can report them to Support, as described in chapter 3. Support.

In case of a Customer notification, the incident is assigned the type “Incident” and given an appropriate priority, based on the input from the notifier and the assessment by POM. Subsequently, incidents are handled according to the “Procedure for information security incidents”, where the incident is investigated and appropriate mitigating measures are taken.

For high priority incidents, the reporter is kept informed of the status of the report every two hours. For lower level incidents the reporter is periodically kept up-to-date on the status of the report, however, the reporters are expected to monitor the status of the report themselves as well.

In addition, POM periodically draws up an incident and problem report to assess whether preventive and mitigating measures need to be changed and or supplemented.

If necessary or desired, the Security and Compliance Manager draws up a Corrective Action Plan, hereafter referred to as CAP, for the Customer involved in the incident. The CAP contains a description of the incident, the cause, the correction or containment and the corrective measure.

In the event of a breach of Personally identifiable information (PII), a CAP is always drawn up. Should the breach also be reported as a breach of data, the POM Data Protection Officer will also be informed. POM will support its Customer in reporting the data breach, however, the Customer remains responsible for reporting this to the supervisory authorities, due to its responsibility as a Controller (Art. 4.7 GDPR).

b. Change Management

Changes are defined as changes to the DPA system and are dealt with according to the Change Management procedure. A change may be a new, general functionality or a customer-specific functionality, or may be an extension or improvement of an already existing functionality. Corrections and bug fixes to an existing functionality are not considered, or treated as, changes.

In order to address change management, POM has set up a Change Advisory Board, CAB, where various disciplines meet and discuss the requested changes every fortnight.

POM uses a rolling release method, based on a scrum/agile development methodology. This allows for multiple small releases per day and each user always having the latest version. Larger releases or changes that could potentially impact performance are scheduled and executed outside of Service Hours. These are, as stated in chapter 2 'Planned maintenance', is announced to Customer at least seven working days

before the intended work through a notification on the dashboard in the DPA system and / or via email. POM informs the Customer about implemented changes in the Changelog, the newsletter and/or via the Account Manager.

c. Logical access management

User management is the responsibility of the Customer. Four user roles are applied in the software: Agent, Agent plus, Manager and Manager plus. A user with Manager plus rights can request, modify and block user accounts through User Management in the DPA system. Accounts must meet the following conditions:

- Personal e-mail address
- The domain of the email address corresponds to that of the organization

When a new account is requested, Support automatically receives a Notification. If it is determined that the requested account meets the conditions, the request is accepted and the new user automatically receives an email with an activation link. The activation link is valid for 24 hours and can be used once. All users are responsible for their own password. Within the software, the following password requirements are technically enforced:

- Contains at least 1 lowercase letter, 1 uppercase letter, 1 number, and 1 punctuation mark;
- Contains at least 2 numbers if the password begins or ends with a number;
- Contains at least 10 characters;
- Must not match username;
- Must not match the last 5 passwords.

A password is valid for 180 days. Two weeks before the password expires, the user will receive a notification to change the password. If the password is not changed within the specified time, a change will be forced on the next login attempt.

In addition, mandatory two-factor authentication applies. This can be done using an SMS, Yubikey or authentication app. Optionally, the organization can additionally opt for IP whitelisting, which only allows authorized IP addresses to access the software.

d. File exchange

To exchange files securely, POM recommends using the "Fileshare" in the DPA system. This is an encrypted file location in the DPA system. In it, the following file types are accepted: .txt, .csv, .xml, .xls, .xlsx, .jpeg, .jpg, .png, .doc, .docx, .pdf, .zip and .7z. In addition, files in the Fileshare are deleted after three months.

The Fileshare is accessible to users with Manager or Manager plus privileges through the 'Management' tab in the DPA system.

e. Employees

With respect to employees, POM has established a training and awareness program, which ensures that employees are trained on information security and privacy policies at the start of and during employment. In addition, related procedures and awareness of topics such as phishing, social engineering and other information security topics are updated monthly. Documentation, such as a help center for customers, internal work instructions (operating procedures) and technical documentation, such as the API documentation, supports a uniform way of working and prevents errors.

In addition, a duty of confidentiality applies to every employee during and after employment and a disciplinary procedure is in place if the employee does not comply with this. For employees with access to confidential data and/or exceptional access rights, a Certificate of Good Conduct is also applicable.

Logical access for POM employees is defined in and managed according to a Role Based Access Control authorization matrix. For business critical systems and user accounts with special access rights, e.g. database access, multiple authentication factors and the principle of least-privilege are applied. In addition, the number of accounts with special access rights is limited to a minimum. Login and password management is carried out according to the established procedures.

Company assets used by the employee, such as laptops, contain only approved software, strong passwords, encryption and communication security such as VPN. Employees must also adhere to clean desk and clear screen policies to prevent unintentional access to information. Passwords and other authentication information is kept in a secure environment in a password management system.

f. Continuity

POM has a Contingency Plan which describes various scenarios with the actions to be taken and allowed deviations. In addition, the plan includes a DRP, to ensure effective recovery and progress of the critical business processes. The plan is periodically evaluated and adjusted and updated as necessary. Upon request, the DRP can be shared at specific request with the Customer.

Contingency planning

POM makes use of Managed Hosting. The supplier that POM uses for this is ISO 27001, ISO 20000 and NEN 7510 certified and is responsible for the daily management of the data centers. The data centers use a tier 3 storage and are redundantly designed, as illustrated below in figure 1: Architecture POM, ensuring continuity and availability of services.

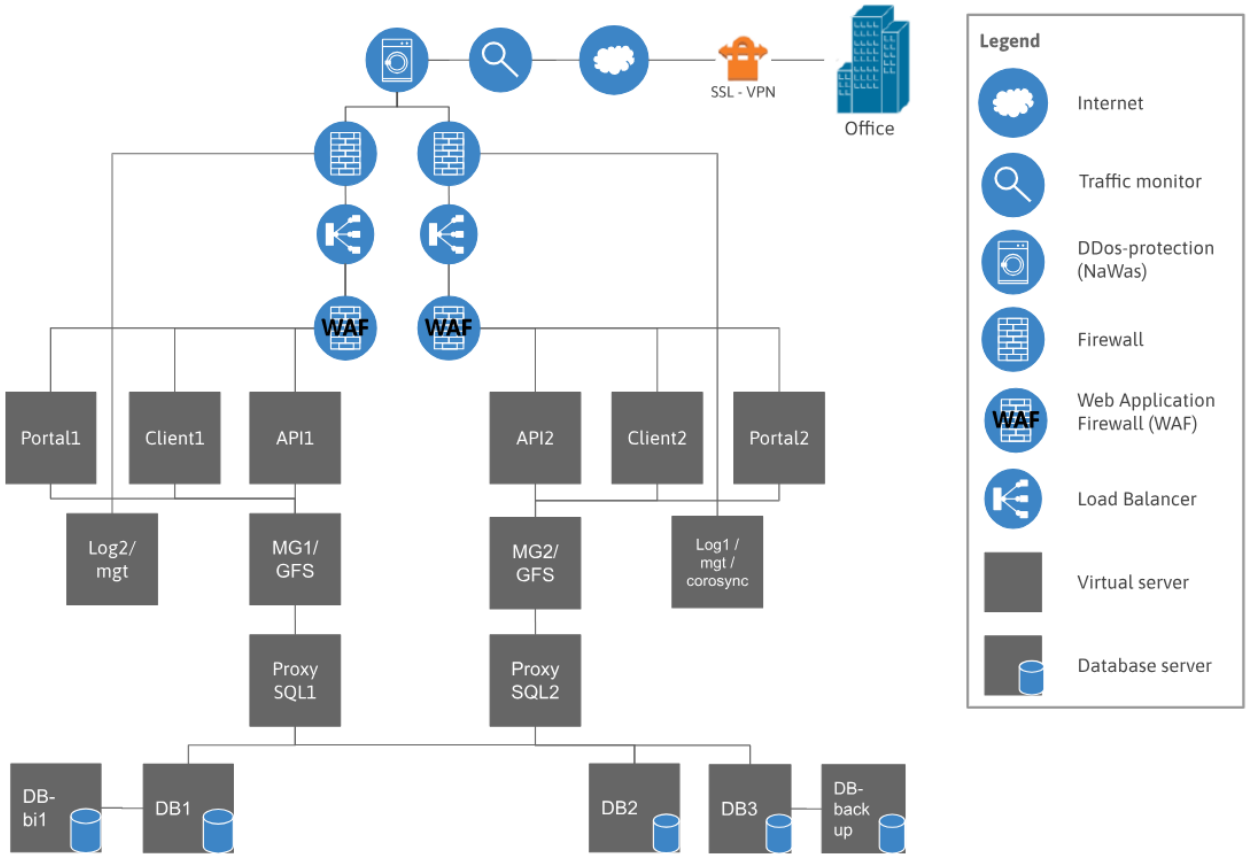


Figure 1: Architecture POM

Recovery Time Objective

In the event of a disruption in the Services, POM is immediately notified by the monitoring software and/or the hosting provider. Immediately upon notification of this disruption, action is taken to resolve it. In the event of a calamity, the DRP procedure is immediately initiated by the crisis team within POM. POM aims, as described in Chapter 2 'Availability and Performance', at an availability of 99.9%. However, it is not possible to determine the exact time needed to reach a solution for each type of incident in advance. Therefore, the maximum interruption time is based on a maximum of four hours in 80% of all cases.

Recovery Point Objective

The Recovery Point Objective, as determined in the DRP is to ensure the progress of critical business processes:

- Being able to do transactions;
- Being able to use and access the DPA system;
- Being able to send and receive API requests; and
- Being able to use the POM (web) apps.

In addition, a backup and restore plan has been implemented. Every two hours a full backup is made and verified automatically. The maximum data loss is therefore set to the processing time between the moment of disruption and the previous backup.

5. Other

The following sections cover system requirements, responsibility and liability, and documentation.

a. System requirements

POM supports the most recent and two previous versions of the following web browsers:

- Google Chrome
- Firefox
- Safari
- Microsoft Edge / Internet Explorer

b. Responsibility and liability

POM shall, without prejudice to the provisions of Section 2 'Availability and Performance', not be responsible and liable for (the consequences of) Disruptions arising from/related to:

- The use of any of POM's Software Services in violation of the applicable terms and conditions or in violation of the instructions contained in the accompanying user documentation or otherwise improper use/error of POM's Software Service, which includes errors in data entry or in the data itself;
- Changes in or errors, defects or imperfections in equipment or software other than the Infrastructure, including incorrect configuration of Customer's equipment and infrastructure as well as Disruption in the telecommunications structure of Customer or third parties or in the power infrastructure of third parties - outside the Infrastructure - for more than 4 hours;
- The non-availability of POM's Software Services (during work) at the request of the Customer;
- If POM, in identifying or isolating the problem or Disruption, requires assistance from Customer which Customer is unable to provide;
- Other causes not attributable to POM.

POM shall not be liable for the incorrect, incomplete, delayed transmission and/or receipt of any Notification sent or made by Customer, whether or not caused by the non-functioning or incomplete functioning of telecom services and equipment of third parties and/or the Customer.

If any provision of this SLA proves to be invalid, void or voidable, the other provisions will continue to have effect. The parties will replace the invalid provision with a valid provision that approaches the purpose and purport of the invalid provision as closely as possible.

c. Documentation

To inform and support users in the use of the Software, POM has made available a help center, changelog and API documentation.

Help center

Each page in the DPA system displays a green button in the lower right corner with a question mark on it. Clicking on this button opens the corresponding help center article in a pop-up window. These articles contain answers to the most frequently asked questions. POM therefore requests users to consult these help center articles first, before contacting Support.

Changelog

POM communicates changes to the Software via the Changelog. This changelog can be viewed by clicking on 'Changelog' in the footer of the DPA system or via this link: https://secure.dpa-cases.io/changelog (login required).

API documentation

POM has a REST web service and supports communication in XML format. This API allows third party systems to communicate with POM's web service.

To be able to use the API, API credentials are required. These can be requested via Support. The documentation can be viewed by clicking on 'API documentation' in the footer of the DPA system or via this link: https://secure.dpa-cases.io/api2-documentation (login required).