SaaS

Cloud Offering & Managed Services

Copyright Notice

Confidentiality Statement

Table of Contents

1. Introduction

This document outlines the scope and key components of our SaaS Cloud Offering & Managed Services, which we provide through a partnership with AWS. It provides a comprehensive overview of the services delivered as part of our cloud-based solution, including hosting services, support plans, and the principles that guide our service delivery. In addition, it details our approach to operational processes such as incident, problem, change, backup, and patch management. The objective is to present a clear understanding of how our managed SaaS solution ensures reliability, security, and operational excellence—while remaining flexible to meet client-specific needs and compliance requirements.

2. Description of services

The following sections provide a detailed overview of our standard Hosting Services and Support Plan as included in our SaaS offering. While these represent our typical service configuration, both areas are fully customizable to accommodate specific client architectures, operational requirements, and compliance considerations.

2.1 Hosting Services:

- Hosts administration and management
- OS updates and patching
    - *Maximum, 2 patch schedules per month. If no patch is needed, then a month might pass without any patching.*
    - *The web and app servers are both split over both patch groups. In case automated patching goes wrong, only 50% of servers will be affected.*
- Security updates and patching is handled automatically by the Cloud provider at Database level due to the usage of AWS RDS managed service. Any other kind of patching at OS level is handled by Profile.
- Vulnerability management via cloud provider managed services(AWS Security Hub, GuardDuty). 24/7 monitoring of cloud resources.
- Backup
    - *Daily 20:00 CET backup of servers on a 14 day retention.*
    - *Daily at 23:23-23:53 UTC a snapshot is made of the database, which is on a 35 day rotation and supports point in time restore.*

- *Daily at 03:00 UTC a snapshot is taken from the shared file server. It is on the default 90 days rotation.*
- *Daily at time to be agreed with the customer, a copy made of the database, retained for 6 months.*

- Profile software updates and patching
    - *Monthly releases*
    - *Production upgrade is done only after Customer's sign-off of the release that is deployed on UAT*
- Profile application management and support

2.2 Support Plan:

The provided Support Plan is the **"Enterprise On Ramp Business Support Plan"** as per the link below. The terms of this support plan apply, whose current version is referenced and copied herein using the following link and will apply as they may be amended from time to time by AWS cloud services.

https://aws.amazon.com/premiumsupport/plans/enterprise-onramp/

3. Principles of provision of services

PROFILE specialises in providing IT services based on public cloud technology. PROFILE focuses on achieving high user satisfaction combined with high operational efficiency in the delivery of Services. In this way, the Customer can meet quality requirements and security and compliance requirements at optimal IT total cost of ownership.

These principles are used in the design and execution of Services:

1. *Customer-oriented, high quality* — In a well-designed and managed public cloud environment, the number of incidents will be significantly *lower* than in a traditional set-up. At the same time, *more* technical knowledge is needed in solving and responding to a relatively *higher* percentage of actions (incidents, changes, requests). This combination makes it possible to improve the design, efficiency and added value of the service and support chain. The quality of this chain is maintained to a high standard by having service delivery staff, administrators and software developers working together as one, focused on fulfilling agreements with Customers and on achieving high user satisfaction. High demands are placed in doing so on the level and up-to-date knowledge of the team; therefore, highly qualified and certified administrators and software developers are employed.

2. *Guaranteed consistency* — Operations are carried out from multiple geographical areas. The internal processes are organised in a uniform and scalable way that is guaranteed through ISO quality philosophy. Management and support processes are also highly automated, making maximum use of the integration and functional capabilities of adequately secure public cloud services.

3. *Operational excellence* — Service management processes are also designed to reduce disruptions to an absolute minimum by following the following principles:

    a. Design and manage structures with as few interdependencies as possible; this reduces the impact of a malfunction and simplifies problem diagnosis;

    b. Make the most of SaaS services and public cloud services with robust SLAs, where security and data privacy issues are addressed;

    c. Intervene as automatically as possible when problems arise;

    d. Apply 'problem management' and ‘knowledge management’ to make Services increasingly robust and efficient.

4. Orchestrating: Service Integration And Management — Service management processes are carried out and monitored with tooling that is suitable for the realisation of Service Integration And Management (SIAM): orchestrating multiple external parties involved in providing a service or achieving a goal, such as Subcontractors, Managed Partners and, if possible and applicable, employees or departments of our Customers.

    In this way, the Customer is supported and relieved of burden. In doing so, PROFILE can also, if desired, support the Customer in drawing up and monitoring SLAs for selected other third party suppliers who, through their contributions, help define the end-to-end quality of certain services.

5. *Efficient and transparent interaction* – Incidents, information and change requests, changes from the Customer and its employees are processed and managed preferably with PROFILE’s service management tool. Employees of the Customer receive their own accounts, with direct access to the system. In accordance with agreements *made* with the Customer, notifications about Services are created directly in this system ('Tickets'). Handling, interaction and status are visible to the employee at all times; performance is transparent and reported periodically.

    Working with Tickets in combination with the direct interaction between transmitter and receiver offer the following important advantages:

    e. *Quality* — Starting with the description of the question or request detector increases the precision with which answer or solution can be worked on;

    f. *Speed* — A Ticket is picked up by the correctly qualified engineer, so that he can also work directly, concentrated on it;

g. *Productivity* — When telephone contact(s) are required, this can be assessed and communicated without waiting times or intermediate links;

h. *Efficiency* — Working with Tickets supports multiple projects which are carried out most efficiently in this way.

The experience of our Customers is that in this way ‘92%’ of Tickets are resolved with a limited PROFILE commitment (15-30 min). Furthermore, this is generally completed the same day. Notifications that require a longer lead time are mainly changes where personal (virtual) contact with the employee is useful. An appropriate time is then chosen in consultation with the requesting person, for example to introduce, discuss or explain the change.

6. *Changes efficiency — Due to the small number of disruptions, many requests concern change requests. In order to maintain quality in providing the Service, it is important to handle these quickly and professionally. In order to execute (standardised) changes with maximum efficiency and minimum lead times, the following design and implementation principles are used:*

   a. Focus on enabling the execution of simple changes faster than the formal SLA agreements;

   b. Automate the execution of as many changes as possible ('workflows') and give the Customer's 'key users' the opportunity to 'carry them out themselves';

   c. Give each requestor access to a service management portal, to make requests themselves and to track status and progress;

   d. If necessary, contact the requestor directly, if desired via a web call to discuss the execution or provide an explanation.

7. *Complex changes — In case of more complex operational changes, PROFILE can also direct or carry out project management in relation to third party suppliers for the realisation of the (project) agreements that the Customer has made with them. The following aspects are taken care of:*

   i. Ensuring that what has been agreed is also delivered in accordance with such agreements;

   j. If necessary, managing and executing escalations;

   k. Ensuring transfer to management after completion of project/change.

4. Incident management

4.1 The primary objective of incident management is to remedy disruptions as soon as possible. Important parts of the process are impact control of the disruption, and the rapid delivery of a solution that allows employees to continue working, if necessary in the form of providing a temporary workaround.

Response and Resolution Times Service Levels are in line with the priority of the disruption:

Priority	Response Time	Resolution Time	Interval Achieved*
Top	30 minutes	4 hours	95% (per month)
High	2 hours	1 working day	95% (per month)
Medium	1 working day	3 working days	95% (per month)
Low	3 working days	2 weeks	95% (per month)

* Within the agreed service windows and with the exception of certain types of incidents as described below ("Exceptions").

4.2 The impact of a disruption determines its priority, and is divided into 4 levels:

	Disturbance level		
Scope affected	Large Scale	Medium Level	Limited
Organisation	Top	High	Medium
Department / team	High	Medium	Low
Employee(s)	Medium	Low	Low

Global definitions of priority characterisation:

a. *Top* — Due to a major disruption, an application or component does not work or is not available to a large group of end users or even to the entire organisation. Furthermore, initially there is no workaround available.

b. *High* — Due to a disruption, an application or component does not work properly or hinders the work process for a large group of end users or even the entire organisation; nonetheless, work can take place (with acceptable limitations and for a certain period) with a workaround.

c. *Medium* — Due to a disruption, an application or component does not work for a limited number of end users (circa 5), or the application or component does not work properly or hinders the work of a larger group of end users.

d. *Low* — A limited number of employees are hindered when using an application or component. With a limited amount of inconvenience, work can be carried out.

4.3 If the Customer considers that an incident has not been properly classified and the classification needs to be adjusted, it will be adjusted. This changes the time record of the ongoing incident, and the response and resolution times start again. In all cases PROFILE may also increase the priority of an incident. The Parties agree to a fair use of this principle.

4.4 Service windows — Service Levels of the incident management process apply during the following service windows:

a. For all levels of priorities: Monday to Friday from 08:00 to 17:00 ('office hours'; CET); excluding Customer public holidays.

b. The Customer has the possibility to extend the service window for 'Top' and for 'High' activities:
(i) during weekday evenings from 17:00 to 24:00; and/or
(ii) during weekends from 09:00 am to 18:00; and/or
(ii) during nights (from 24:00 to 09:00) and during weekends (48 hours);

c. If the Customer opts for one of extensions including weekends, this schedule also applies during public holidays

4.5 Incidents with priority 'Top' and 'High' must be reported by telephone.

4.6 Notification of incidents with a 'Top' or a 'High' priority is limited to Client personnel that are designated by the Client.

4.7 Incidents with priority 'Medium' and 'Low' are preferably logged in PROFILE’s service portal.

4.8 The Client's IT service management system may be linked to PROFILE’s system. As a result of this integration, or when (parts of) processes may otherwise deviate from the above, functional degradation and/or information losses may occur that have an incidental or structural negative impact on the efficiency and/or on Realised Performance. PROFILE will inform the Client about this and, where possible, advise how to prevent or minimise this.

5. Problem management

5.1 A 'problem' is an unknown cause of one or more incidents. In the case of problem management, the cause of incidents is searched in a structured manner in order to arrive at a solution (action) that prevents a recurrence of the disruptions.

5.2 Each Party may propose the initiation of a problem analysis, for example, when incidents occur frequently or when the risk of recurrence of an incident is unknown because its cause is not sufficiently clear.

5.3 For incidents classified as 'Top' or 'High' a problem management process is always carried out, unless the Parties agree otherwise.

Process attributes	Service Level
Start of problem analysis	Within 5 working days, after appointment with the Client.
Lead time of problem analysis and delivery of improvement proposal	Within 10 working days after the start of the problem analysis.
Planning of implementation and validation of the improvement proposal	In consultation with the Client.

5.4 A problem management 'ticket' can be concluded by the Parties working together:

a. As soon as incidents are no longer reported or otherwise no longer cause disruptions, whether or not after implementation of the solution; or

b. Once the problem management process has identified that applying a workaround is the best possible solution to the problem.

6. User questions and requests

6.1 There is deemed to be a ‘user question’ if an employee has a question about the use of an available ICT tool, and there is no disruption.

6.2 There is deemed to be a ‘user request’ if an employee wishes a standardized change to (the use of) an ICT tool made available and there is no disruption.

6.3 User questions and requests are logged into PROFILE’s service management application. The following response and resolution times apply to their processing:

Type of notification	Responsiveness	Resolution time
User questions	1 working day	In consultation
User requests	3 working days	In consultation

Periodically, questions and requests are classified and characterised and, if desired, discussed by the Parties as part of the problem management process.

7. Change management

7.1 Operational changes are additions, deletions or other modifications to components or services that may affect the Services. The process of change management has two important, sometimes conflicting, goals:

a. *Risk management* — changes are the most common cause of disruptions; for this reason, the change management process should evaluate changes in advance and then implement them in a controlled manner.

b. *Speed* — The Customer benefits if the desired changes are carried out efficiently within a short time frame.

7.2 In order to strike the right balance between risk management and speed, changes are divided into 5 categories, each of which takes a different approach:

a. *Standard* — changes made quickly and robustly, often with a high degree of automation ('workflows'). Due to further automation, the share of such workflows increases over the lifetime of the Agreement.

b. *Maintenance* — changes intended to keep the existing infrastructure up to date or to ensure the agreed Service Levels. These include preventive actions to ensure service and security, such as patching infrastructure components.

c. *Non-standard, automatic agreement* — changes made without explicit agreement of the Customer – for the sake of operational efficiency and the avoidance of productivity loss among employees due to queues – and which meet certain agreed criteria.

d. *Non-standard, explicit agreement* — changes that do not fall under any of the categories a., b. or c. Agreement regarding the execution of these changes is explicitly agreed and is approved by the Customer.

e. *Project* — changes that are made as part of a project, or a set of multiple non-standard changes performed on a project-by-project basis.

For each category, the characteristics, and Service Levels are outlined below:

(a) Standard	
Description	Specific defined changes, within the existing environment.
Examples	Off-/onboarding, password resets, (temporarily) disablement of MFA or re-enablement of MFA.
Requestor	Client employees or key users.
Impact analysis	Once; when designing a new type of change procedure.
Risk & Impact	Very low.
Profile Input	< 1 hour per change.
Fee	○ For non-automated changes: on the basis of post-calculation at rates in accordance with the Annex 'Fees'. ○ For building workflows: one-time, post-calculation. For runnign workflows: free of charge. ○ Building workflows take place after approval of the Client.
Procedure	Requests are scheduled and implemented after classification. If via an automated workflow, execution takes place immediately.
Approval required	No.
Service Levels	○ Response time: 1 business day. ○ Completion time: depending on type of change.

(b) Maintenance	
Description	Maintenance of existing functionality and components.
Examples	Patch servers, make periodic backups, 'patch' Appstream and Workspaces images.
Requestor	Not applicable; part of the service arrangements.
Impact analysis	Once, when designing the change procedure, or in the event of modifications to existing change procedures.
Risk & Impact	Very low.
Profile Input	< 1 hour per change.
Fee	Execution is carried out at standard fees per type of activity in accordance with the Annex 'Fees'.
Procedure	As a rule, proactive, repetitive, automatically planned and according to standardised procedures. Corrective maintenance is performed, recorded and evaluated reactively.
Approval required	No.
Service Levels	Not applicable; it concerns planned activities. Exceptions: See Service Levels at Patch Management.

(c) Not automatic by default & (d) explicit agreement & (e) Project	
Description	New functionality or modifications of existing functionalities.
Examples	System upgrades and migrations, introduction of new components, adaptations of existing components.
Requestor	Client
Impact analysis	Is part of the change procedure.
Risk & Impact	Determined as part of the change procedure.
Profile Input	Determined as part of the change procedure.
Fee	Either based on actual time spent against a fixed hourly rate, or has been established as part of the change procedure; including determination of any Recurring Fee.
Procedure	In accordance with the then agreed change procedure.
Approval required	Yes; with the exception of (c) automatic approval: provided that such execution (i) requires less than one (1) hour of work, and (ii) does not lead to a Recurring Fee, and (iii) any purchase of IT resources if applicable remains below €100, and (iv) has negligible risks. If in doubt: submit for approval.
Service Levels	○ Response time: in case of 'automatic agreement' (c): 1 working day; for other changes (d) and (e): 3 working days. ○ Resolution time: depending on the change.

7.3 Registration takes place in PROFILE’s service portal and shall include:

a. A description of the change;

b. The One-Off Fee associated with the change;

c. An impact analysis, which includes insofar applicable:

i. The impact on the Services;

ii. The impact on Recurring Fees;

iii. The acceptance criteria;

iv. Risks of the change and measures to minimise it.

d. The registration of the agreement to proceed and execute by authorised persons.

e. The status of the change.

7.4 If impact and risks allow, the Parties shall use the principle that changes are carried out during working hours and office hours. Changes with a high risk profile or large impact may be planned in consultation, outside office hours or during weekends.

8. Backup management

8.1 Backups are provided according to the following schedule:

KPI	Service level
Backup frequency	○ Daily at 20:00; ○ Deviations can be agreed; ○ For critical systems, a backup schedule can be designed and implemented to take place more often, in consultation.
Backup success	98% of backups (monthly)
(RPO) Recovery Point Objective ○ critical systems ○ standard systems	 ○ In consultation. ○ Less than 24 hours.
(RTO) Recovery Time Objective ○ critical systems ○ standard systems	 ○ Less than 1 hour ○ Less than 24 hours
Backup retention	Standard 14 days, unless more is required by law or requested by the Client.

8.2 Restore — It is important to be able to put data back into the operational system from a successful backup within the set time frames (RPO and RTO). There are periodic checks as to whether backups have been successful. In addition, whether a system can be rebuilt based on the backup data is tested. PROFILE tests the quality of this process by restoring a randomly selected system from the backup at agreed times, in an isolated separate environment, and validates the result. If an unsuccessful backup is used, the restore test is performed with a different (usually 'older') backup.

KPI	frequency	Success
Restore tests	monthly	100%

9. Patch management

9.1 Patches are modifications to the current existing software and infrastructure systems to reduce the risk of security breaches and to ensure proper functioning. Patches are periodically installed on PROFILE’s systems through a controlled, standard procedure.

9.2 Patching is subject to the following service levels:

KPI	Speed	Coverage
Patch compliance	Within 30 days (monthly cycle)	95% (month)

9.3 Systems designated by the Client that are not or are not to be patched in this way are excluded from this; for example, due to the age of the application or the release cycle used. The Parties will make further agreements on the patching of such different systems. These agreements may have negative consequences for the degree of security. These consequences are then automatically accepted by the Client.

10. Lifecycle management

10.1 In addition to patch management, software systems are also maintained by lifecycle management. Whereas patch management involves smaller repairs and release updates that limit and/or improve the existing functionality, in lifecycle management entire systems are modified or replaced. These are, for example, major release upgrades, where an entirely new version of an application or operating system must be installed.

10.2 This type of change is treated as a non-standard change and carried out in consultation and after approval with the Customer in accordance with the appropriate change procedure.

11. Availability management

In availability management, the availability of the services purchased by the Client is examined and taken care of. As a standard, PROFILE will set up the cloud services as 'highly available', so that the risk of failure due to 'single points of failure' is minimised, unless this is not technically feasible or the Client decides otherwise, for example by another cost-risk consideration.

12. Capacity management

Capacity management ensures that the Client has the right capacity and quantities of IT resources. In order to ensure that the Client has the right capacity, monitoring tooling is used to monitor trends, in order to be able to intervene in a timely manner. The Client is informed when the available capacity is in danger of being outside usual or acceptable ranges, and adjustments are needed to prevent this.

If the Parties establish that monitoring trends in this way is (possibly) inadequate, for example due to (the risk of) ad hoc or rapid significant changes, the Parties may decide to conduct Problem Management to assess whether and how this Service should be changed. Such changes shall be treated as project work

13. Configuration management

Maintaining a configuration management database (CMDB) is essential to maintaining the inventory of equipment, software systems, applications, licenses and other IT resources. PROFILE will record, at a sufficient level of detail in this respect, the components and configurations of the Services provided to the Client, insofar as these are also managed or purchased by or through PROFILE.

14. Security and compliance

14.1 PROFILE uses tooling that monitors the environments of the Client and advises on security and compliance. Potential configuration gaps are identified so that they can be fixed. This includes non-security-related compliance aspects. If applicable, proposals are made to improve the security position of the environment; after approval, these are implemented on the basis of actual costs.

14.2 The security of an IT environment in the cloud is a shared responsibility of PROFILE and Client.

PROFILE takes care of the security of (virtual) servers; this includes:

a. monthly patching of the operating system;

b. monthly analysis of log files and alerts that follow from the security management tooling and cloud management tooling.

c. implementing configuration changes to improve security;

d. active monitoring (according to SLA) on the security of servers.