(March, 2025)

Service Level Agreement (SLA)

This document outlines the agreed service levels, responsibilities, and expectations between Qmica and [Company]. Its purpose is to ensure transparency regarding service quality and to define measurable performance standards.

Parties:

1. The private company XXXXXXXX established in xxxx at xxxx xxxxx, at xxxx xx (hereinafter: “Client”), legally represented by xxxx;
2. the private company Qmica B.V., established in the Netherlands at 1742 NE Schagen, at Zijperweg 4N (hereinafter: “Supplier”), legally represented by Mr. J. Kapitein;

Take into account that:

A. The parties have entered into an agreement with regard to the delivery of SaaS services by the Supplier to the Client;
B. In this Service Level Agreement (hereinafter: “SLA”), the parties wish to make further agreements about the level of services provided by the Supplier to the Client and wish to record the agreements made in this Agreement.

Have agreed as follows:

1. Definitions

1.1. Account: the combination of a username and password with which the End User can access the SaaS service.
1.2. Availability: the percentage of the time that the SaaS service is accessible to the End users without interference, measured outside a Maintenance Windows.
1.3. Appendix: an appendix to this Agreement.
1.4. Data Center: the location where the computer system (hardware and software) for the SaaS service is placed.
1.5. End user (s): the employee (s) of the Client, who is / are enabled by the Client and the suppliers of the Client to use the SaaS service.
1.6. Evaluation: discuss the progress of the project and the cooperation
1.7. Export: the possibility to export the converted product data in an Excel format.
1.8. Manual: the (online) manual provided by the Supplier with regard to the use of the SaaS service Qmica.
1.9. Main account: the account within the Client with which complaints / claims can be submitted to the Supplier.

Zijperweg 4 N | 1742 NE Schagen | Tel: +31 (0)72 30 30 364 | www.qmica.io

1.10. Incident: a total or partial interruption or delay in the accessibility or accessibility of the SaaS service.
1.11. IPR: copyrights, design rights, trademark rights, patent rights, database rights and all other intellectual property rights or comparable rights, such as rights to know-how or a domain name, registered or unregistered.
1.12. Office hours: the hours between 9 am and 5 pm on Working Days.
1.13. Supplier: the Party as described above under Parties.
1.14. Maintenance Window: the period of time during which the SaaS service does not have to be available or accessible in connection with Maintenance of the systems.
1.15. Folders: converting Client's product information into market, customer and retail standards included in the SaaS service.
1.16. Mark standard (s): the market standard (s) (such as GS1 and ETIM) included in the SaaS service to which the Client can map, validate and export (product) data.
1.17. Name / logo use: The name and logo of the Client which can be used by the supplier for marketing purposes of the SaaS service Qmica.
1.18. Necessary Maintenance: incidental or unforeseen activities, which in the opinion of the Supplier must be carried out immediately in order to prevent or remedy Incidents.
1.19. Maintenance: Preventive Maintenance or Necessary Maintenance.
1.20. Party: Supplier or Client.
1.21. Preventive Maintenance: performing planned work on the network, hardware or SaaS service to maintain or improve the quality and availability of the SaaS service.
1.22. Product data: product information as available from the Client
1.23. Client: the Party as described above under Parties.
1.24. Agreement: this agreement with Appendices.
1.25. Retail standard (s): the standard (s) included in the SaaS service to which the Client or its suppliers can map, validate and publish (product) data.
1.26. SaaS Service: the full service provided by the Supplier with regard to the use of the SaaS service via a network, including the hosting of servers in a Data Center, the provision of access to the SaaS service via a website, the Maintenance, and the Support.
1.27. SLA: the Service Level Agreement associated with this Agreement.
1.28. Software: the software and functionalities that are made available to the Client and the End User via the internet or an exclusive network ("web based").
1.29. Qmica: the name of the relevant SaaS service, with which mappings between various data models are recorded and maintained.
1.30. Support: the provision of information and advice about the SaaS service by the Supplier by telephone, e-mail, via a website or by means of a helpdesk during office hours, as well as providing remote assistance in detecting and resolving Incidents.

Zijperweg 4 N | 1742 NE Schagen | Tel: +31 (0)72 30 30 364 | www.qmica.io

1.31. Validation: checking and assessing the data after mapping, before export.
1.32. Working days: Monday to Friday, with the exception of official, Dutch, national holidays.

2. General

2.1. This SLA contains the agreements between the Supplier and the Client with regard to the Availability, Service Levels, Support and Incident management of the SaaS service.

3. Availability

3.1. The SaaS service is available 24/7 for the end users who have been admitted to the SaaS service by the Client. The Supplier guarantees an Availability of 99%. An interruption or delay in the availability or availability of the SaaS service as a result of Maintenance or force majeure situations, such as a power failure or a network failure, does not count for the calculation of the Availability.

Zijperweg 4 N | 1742 NE Schagen | Tel: +31 (0)72 30 30 364 | www.qmica.io

4. Data Protection and Security Compliance

4.1. Qmica does not store or process any personal data (as defined under the General Data Protection Regulation – GDPR) in its SaaS solution. Therefore, the GDPR does not apply to the use of the Qmica platform.

4.2. The Qmica SaaS platform is hosted on Amazon Web Services (AWS) infrastructure in Frankfurt, Germany. This hosting environment is fully compliant with relevant international security and privacy standards, including but not limited to:

- ISO 27001, 27017, 27018
- SOC 1, SOC 2, SOC 3
- GDPR compliance for EU data
- CIS Benchmarks and NIST standards

4.3. Security measures implemented include:

- Data encryption in transit and at rest
- Access control based on least privilege using AWS IAM
- Isolated network environments via AWS Virtual Private Cloud (VPC)
- DDoS protection using AWS Shield
- Continuous monitoring and logging using AWS CloudTrail and CloudWatch
- Daily backups and disaster recovery options via AWS S3 and RDS

Qmica continuously evaluates and improves its security protocols in alignment with AWS security developments and industry best practices.

For further information about our security architecture, please refer to the document “Security levels AWS” (available upon request).

Zijperweg 4 N | 1742 NE Schagen | Tel: +31 (0)72 30 30 364 | www.qmica.io

5. Support

5.1. Only the Client's End User (s) listed below are entitled to contact the Supplier's helpdesk:

Name	Telephone	Email
Enduser(s):		
User(s):		

5.2. Support by the Supplier does not include:

A. services with regard to system configurations, hardware and networks of the Client;
B. structural work, such as defining import definitions and links with third party SaaS service;
C. on-site support;
D. expanding the functionality of the SaaS service at the Client's request;
E. converting files and / or importing backup files;
F. services with regard to external databases of producers other than the Supplier;
G. support for operating and other SaaS services from producers other than the Supplier, which also includes the SaaS service from third parties that can be started from the SaaS service or connections to third-party websites;
H. configuration, training, consultancy or other services not expressly described in this Agreement;
I. file fixes where the cause cannot be attributed to the SaaS service;
J. support regarding the network or the internet connection;
K. support for an environment that is not supported according to system requirements.

5.3. If End users make disproportionate use of Support, because they have insufficient knowledge of the systems and the operation of the SaaS service, Supplier can provide Training for these End User (s) in consultation with the Client. The costs of the Training are for the account of the Client.

Zijperweg 4 N | 1742 NE Schagen | Tel: +31 (0)72 30 30 364 | www.qmica.io

6. Maintenance

6.1. In connection with Maintenance, the SaaS service may be temporarily unavailable or inaccessible during the following Maintenance Windows:

- On Business Days between 6:00 PM and 7:00 AM
- On weekends: from Friday 6:00 PM to Monday 7:00 AM

6.2. Necessary Maintenance is also possible outside Maintenance Windows. Necessary Maintenance outside the Maintenance Window is reported at least 1 hour in advance. If possible, a description of the activities, the duration and a realistic estimate of the effects on the accessibility of the SaaS service are given. The resolution of highly critical Incidents, which do not tolerate any delay, will be carried out by the Supplier as soon as possible and without prior notice. A description of the intervention will be sent to the Client as soon as enough information is available.

6.3. The supplier is free to implement innovations, updates or upgrades to the SaaS service. The Supplier will inform the Client in time about innovations, updates or upgrades of the SaaS service, if these innovations, updates or upgrades are relevant for the use of the SaaS service by the Client.

7. Incidents

7.1. An expert from the helpdesk of the Supplier will respond to an Incident reported by the End User (s) of the Client in accordance with the Security Levels as described in article 7, provided that the End User (s) of the Client can describe the Incident sufficiently clearly or reproduce, for example with a screenshot.

7.2. As soon as the Supplier's helpdesk has confirmed that the Incident has been described or reproduced by the Client with sufficient clarity, the Incident will be resolved. This service can be a Temporary Solution or a Permanent Solution. An Incident is resolved if the test by the Supplier shows that the Incident as reported by the Client no longer exists.

Zijperweg 4 N | 1742 NE Schagen | Tel: +31 (0)72 30 30 364 | www.qmica.io

8. Security Levels

Security Level	Definition
1	Security Level 1 will be awarded when the SaaS service is critically disrupted and / or is not available at all to all end users. Neither can the SaaS service be resumed in an alternative manner. Or: The parties agree that the Incident falls under Security Level 1.
2	Security Level 2 will be awarded if a major functionality of the SaaS service is not fully available or missing, or if those functionalities do not function properly, in such a way that normal use of that functionality is impeded by end users, although the SaaS- service is still available to the end users. Or: The parties agree that the Incident falls under Security Level 2.
3	Security Level 3 will be assigned if the reported Incident (i) is not a Security Level 1 or 2, (ii) has little or no impact on the operation or availability of the SaaS service or any functionality. The Incident has only limited consequences for the end users. Or: The parties agree that the incident is a Security 3 Incident.

9. Service Levels

9.1. The Supplier's helpdesk will respond to the call for Support and will contact the Client as soon as possible (response time). The helpdesk will try to resolve all Incidents as quickly as possible (repair time).

9.2. The response times and repair times listed below are target times and not deadlines or deadlines. Exceeding these times or periods cannot directly lead to Supplier's liability, without prejudice to Supplier's responsibility for the quality and availability of the SaaS service. If a response time or repair time is exceeded by the Supplier, the Client can escalate the problem in accordance with the escalation matrix of Chapter 9.

Zijperweg 4 N | 1742 NE Schagen | Tel: +31 (0)72 30 30 364 | www.qmica.io

9.3. Response times

Security Level	Response times
1	Within 4 hours after reporting the Incident, if the incident is reported during Business Hours on Working Days at least 4 hours before the end of the Working Day. Incidents reported outside of Business Hours or Business Days, or less than 4 hours before the end of the Business Day, will have a response time on the next Business Day.
2	Within 1 Business Day after reporting the Incident.
3	Within 5 Business Days after reporting the Incident.

9.4. Fix times

Security Level	Workaround	Permanent Solution
1	As soon as possible, but at the latest within 5 Working Days	In the next update or upgrade
2	Within 10 Working Days	In the next update or upgrade
3	Within a reasonable period of time	At the discretion of Supplier

10. Escalations

10.1. The following persons of the Supplier are responsible for the escalations:

a. Maikel Bollemeijer | Maikel.bollemeijer@qmica.com
b. Jacco Kapitein | j.kapitein@qmica.com

Zijperweg 4 N | 1742 NE Schagen | Tel: +31 (0)72 30 30 364 | www.qmica.io

11. Deviations from Client General Terms and Conditions

In the context of this Agreement and the services provided by Qmica B.V., the following articles from the Client's General Terms and Conditions for the Provision of Services (Version October 2019) are explicitly excluded and do not apply:

- Article 7: Delay
- Article 2.2.1: Personnel replacement rights of the Client
- Article 2.2.2: Restrictions on replacing personnel without prior written consent
- Article 9.1: Full transfer of intellectual property rights to the Client
- Article 9.2: Licensing rights of pre-existing intellectual property

These exclusions are acknowledged and agreed upon by both parties as deviations from the standard terms, and take precedence over the Client's general terms where applicable.

12. Information Security and GDPR Limitations

Qmica does not possess ISO 27001 certification and does not fully comply with all GDPR requirements. As a result, the SaaS solution provided by Qmica is not suitable for processing or storing any personal data.

Accordingly, the following exclusions apply in relation to the Client's Information Security Requirements appendix (Version 2, Rev 2, Approved 2024-08-30):

- Qmica is not certified under ISO/IEC 27001, nor aligned to NIST CSF.
- Qmica is not a GDPR-compliant data processor and does not offer the processing of personal data.
- No personal data may be stored, processed, or transmitted through the Qmica SaaS solution.
- Qmica will not be able to support requirements related to data subject rights, breach notification obligations, or transfer agreements under GDPR.

These exclusions are acknowledged and accepted by the Client, and the use of Qmica's services is limited accordingly. For our Data Protection and Security Compliance, please refer to Article 4 of this SLA.

Zijperweg 4 N | 1742 NE Schagen | Tel: +31 (0)72 30 30 364 | www.qmica.io