Ministry of Economic Affairs and Climate Policy

**Annex 6b_Draft SLA**

This SLA was drawn up between

The State of the Netherlands, which has its seat in The Hague, represented by the Minister of Economic Affairs and Climate Policy,
Legally represented in this matter by,
René van der Burg, Director of Core Processes EU, Netherlands Enterprise Agency (NEA),
hereinafter referred to as the End User

and

**<contractor's full name and legal form>**,
which has its registered office in **<place>**,
legally represented in this matter by
**<signatory's name and position>**
hereinafter referred to as the Contractor,

in relation to the management and maintenance of the application(s) used for QA and red parcel handling, hereinafter referred to as the **QA**, have agreed as follows:

1. **General**
   - This SLA is an integral part of the ARVODI-2018 contract, concerning the 'Quality Assessment and Red Parcel management in the GSA and AMS for 2024-2027' with reference number 202308058.
   - This SLA is subject to the provisions of the ARVODI-2018 contract. With regard these activities, we expect the Contractor to respect the standards for confidentiality and privacy, as also applicable to works undertaken within the contract with the Contractor, on behalf of the NEA.
   - This SLA describes the service level to which the service must comply, according to the quality levels and assessment criteria agreed between the parties.
2. **Term**
   - The term of the SLA for management and maintenance of the QA shall be from 28-03-2024 through to 31-12-2025, defined as the **operational phase of the SLA.** The End User has the option of extending the operational phase, subject to the same conditions, twice within one year.
   - During the operational phase of the SLA, the End User will have access to the full functionality of the web-based viewer, during QA and red parcel handling, with the related guarantees for **Availability and maintenance** as described in Article 3.
   - A certain uptime per edition of the web-based viewer is guaranteed every 24 months. For example, the 2024 to 2026 edition remains available for consultations. Access to the web-based viewer is reserved for RVO.nl, and the parties auditing the QA project (Audit Dienst Rijk). Personal login details will be created for each employee. NEA expects that the number of users for the operational environment will not exceed 20.
   - RVO.nl is not permitted to provide third parties with access to the systems.
   - During the operational phase of the SLA, the End User will not necessarily have access to the full functionality of the archive, but it should be possible to retrieve documents from the archive with the related guarantees for **Availability and maintenance** as described in Article 3.
   - It remains an obligation to keep the QA data accessible, available and consultable. After expiry of the contract, the QA data should be transferred to the End User

- In both the Operational phase and the Archiving phase, NEA is responsible for **user management**: the addition/removal of user accounts:
    - The Contractor is responsible for creating a manager's account for Functional Management, and all necessary functions that permit account management to be carried out.
    - NEA expects that the number of users for the operational environment will not exceed 20.

On request, consultation accounts must be created in the event that audits are conducted. In that case, NEA will pass on the names of officers, the organisation name and the time period.

**3. Availability and maintenance**

- Availability is reproduced in percentages of the total working days during office hours (07.00 - 18.00) per year and amounts to 98%. The availability will be monitored by the Contractor and reported monthly to the End User. This applies in particular to the web-based viewer used by the NEA.
- Since part of the data processing is also carried out outside office hours the above-named percentage of 98% also applies to the environment used for the processing of the source data. In this case, however, the calculation of 98% will be based on 24/7. System failure will result in data loss not exceeding 28 hours.
- The application(s) will have a maximum response time of 10 seconds throughout the term of the SLA.
- In the event of scheduled maintenance, the server and links will not be available. This maintenance will be carried out outside office hours. The Contractor's Service desk will inform the End User at least five working days in advance when maintenance is scheduled. If in exceptional cases an interruption of the facilities is nonetheless necessary, this will be announced, at the latest, two working days in advance.
- Regular maintenance shall include investigation of disruptions and the carrying out of repair work, in the event of disruptions. Repair work may take place both during and outside office hours, depending on the nature and priority of the disruption.
- In accordance with the agreed technical and functional specifications and availability percentages, the application(s) must be functionally available for all users.
- The application(s) is available if:
    - The application/applications functions/function in accordance with the requirements from the tender procedure.
    - No production-disrupting errors are registered.
    - There are minor technical deviations from the agreed specifications, which do not hinder normal use of the application(s), and to which the End User has agreed.

**4. Service Desk**

- The Contractor will provide Service Desk facilities for the 1st, 2nd and 3rd line support. The Service Desk deals with technical problems that hinder the functioning of the application(s) for QA and red parcel handling, for the End User.
- The Service Desk is not intended to support employees of the End User in using the application(s). The End User itself will ensure that its staff are trained in the use of the application(s).
- The Service Desk of the contractor is available by telephone, at the number xxx during office hours from 07.00 to 18.00.
- The Service Desk employs a ticket system for dealing with incoming reports.
- The Service Desk employs a ticket system in the web-based viewer for substantive questions.
- The Service Desk is competent and satisfies the criteria imposed in the tender procedure. The first line of the Service Desk has basic knowledge of the application(s) used for the QA and is able to determine to which aspect the report relates. The Service Desk is responsible

for the administrative processing of the report, the passing on of reports to the 2nd line, the monitoring of progress and feedback to the End User when the incident is solved.

- The 2nd line service will be provided by a support team of the Contractor, that offers sufficient functional and technical knowledge of the application(s) and the hosting environment. The 2nd line may decide to call in the 3rd line for solutions requiring specific knowledge.
- Via a ticket system supplied by the Contractor, the End User will issue at least the following data, with every report:
    - Description of the nature of the observed disruption, including the error message or error code generated by the application(s), or a clearly described question relating to use. A screenshot of the report or finding is not mandatory, but can prove useful in the efficient handling of the report.
    - Name and contact details of the reporting party within the organisation of the End User.
- In the event of error messages, the Service Desk will initiate problem management. Depending on the nature of the error, this may result in a Hotfix for urgent bugs or a regular update for non-urgent errors.
- The Contractor will submit the procedure for change management to the NEA. Following approval of this procedure by the NEA, change management will be managed by the Contractor.
- The standards relating to incident handling, such as response and recovery times, appear in the table below:

| **Standard** | **Description** | **Standard within office hours from 07.00-18.00** |
|---|---|---|
| Answering the telephone | Average Answering Time (AAS) of the 1st line by a speaking person (not an answering machine or voicemail). | In 90% of all cases, the standard answering speed will be within 1 minute. For other cases, a 3-minute limit applies. Feedback to the reporting party will be carried out with Incident no. |
| Report per incident | Reaction from the 1st line to incident reported via the Service Desk. | In all cases, the standard is 100% within 15 minutes following registration (feedback with incident no.) in the event of reporting during office hours. |
| Monitoring of Incidents by 1st line | Check whether 2nd or 3rd line support is active, with the escalated incident. | In all cases, the standard is to check daily on the basis of the registration system. |
| End User informed by the 1st line | Check whether 2nd or 3rd line support solved the incident | In all cases, direct feedback to the End User via the 1st line Service Desk when the Incident is concluded. |
| Mean Time To Repair | The average repair time in the event of a disruption. | < 1 working day (high priority)<br>< 3 working days (low priority) |
| Report of disruption/incident via Ticket system | The average speed with which a reply is issued to tickets + content. | Within 1 day a substantive reaction indicating how the problem will be solved or the solution. |
| Report of RFC via Ticket system | The average speed with which a reply is issued to tickets + content. | Within 7 days a substantive reaction with an action plan and timetable. |

| | | |
|---|---|---|
| Answering substantive questions | The maximum reaction time to the content related tickets, that are raised in the web-based viewer. | In all cases, the maximum reaction time is 48 hours on working days. |

## 5. Security, backup and restore

- **Security**
  - The QA and the underlying infrastructure satisfy the standard requirements for information security, imposed on the basis of the ISO27001 or comparable, held by the Contractor. Maintenance relating to maintaining the security and availability of the environment are part of this SLA.
  - Under all circumstances, data will be considered confidential if designated as such by one of the parties. Confidential data will be dealt with by the Contractor in accordance with the requirements contained in the ISO27001 standard.
  - For security purposes, the necessary Security Patches and Service Packs will be installed within the hosting infrastructure, by the Contractor.

- **Backup and restore**
  - The request to restore can only be submitted by a member of the Management Organisation designated by the End User.
  - The following requirements apply:
    - (a) Data loss is a maximum of 28 hours, so a backup every day.
    - (b) Recovery time in case of incidents is a maximum of 16 working hours (2 days of 8 hours) in 85% of the cases.
  - The backup process provides storage of the backup in one location, where an incident in one location cannot lead to damage in another.
  - The restore procedure is tested at least annually, or after a major change to ensure proper operation, if it has to be carried out in an emergency.

## 6. Communication

- **Regarding the availability of systems and services**
  - For all questions and notifications regarding the availability of the facility and use-related questions, the End User must contact the Service Desk of the Contractor.
  - Communication regarding monitoring of reports and contract management will take place between the members of the Management Organisation appointed by the End User, and a contact person appointed by the Contractor.
- **Regarding management, cooperation and progress**
  - Throughout the control period the contractor will organise weekly progress meetings. Here issues can be presented and discussed. The Contractor will be responsible for carrying out the following activities during these meetings:
    - Keeping track of action items
    - Preparing the agenda
    - Being able to respond to substantive questions
  - Agreements will be established between the NEA and the Contractor regarding scheduled maintenance. These will be included in the maintenance calendar.

- **Regarding reporting on management information, to be issued by the Contractor to the Netherlands Enterprise Agency**
  - Progress and control:
    - Progress-based on planning of processing checks.
    - An indication of whether there is enough footage to draw conclusions.
  - Information Security:
    - (Monthly) reporting on uptime platforms, incidents, leaks etcetera.
    - (Monthly) reporting on response time and content of response from ticketing system (for RFC's, issues etcetera).

        - Annual in control statement on ISO 27001 or comparable.
    - Quality Reports:
        - Annual in control statement on ISO 9001 or about the quality system.
        - Before the season and with each delivery for services and deliveries.
        - Quality and technical delivery notes prior to and during each delivery.
        - At the request of NEA, a statement of assurance to the extent that the Contractor complies with specific laws and regulations.

| **Contacts of the End User, Address P.O. Box 93144 2509 AC The Hague** | | | |
|---|---|---|---|
| **Name** | **Role** | **Telephone** | **Email** |
| | | | |
| Member | Management Organisation Netherlands Enterprise Agency | | |

| **Contacts of the Contractor** | | | |
|---|---|---|---|
| **Name** | **Role** | **Telephone** | **Email** |
| | | | |
| | | | |
| | | | |
| | | | |
| | | | |
| | | | |

## 7. Complaints and escalation procedure

In the event of structural violation of the agreed SLA standards, a complaint can be submitted to the Service Desk of the Contractor, by the End User.

**Complaint procedure level 1:**

- The complaint will be received by the service manager of the Contractor. In joint consultation, the End User and the service manager of the Contractor will take steps to at least return the services to be provided to the level outlined in the SLA. A record will be kept of all activities carried out by the Contractor, to rectify the complaint. When the complaint is dealt with, a cc will be sent to the service manager.
- If the complaint cannot be solved in this manner, the End User can initiate complaint procedure level 2.

**Complaint procedure level 2:**

- The complaint will be received by the account manager. In joint consultation, the End User and the service manager of the Contractor will take steps to at least return the services to be provided to the level outlined in the SLA. A record will be kept of all activities carried out by the Contractor, to rectify the complaint. When settled/When the complaint is dealt with, a cc will be sent to the management (of the Contractor).
- If the complaint cannot be solved in this manner, the End User can initiate the escalation procedure.

**Escalation procedure:**

- Escalation means that the highest level of the contract organisation is activated, to solve the complaint. The complaint will be submitted to the management of the Contractor, in writing. When the complaint is dealt with, a cc will be sent to the quality management of the Contractor.

## 8. Definitions

**QA** Quality Assessment
**ASP Application Service Provider**
The application(s) provided by the Supplier, connected to the Internet by one or more IP addresses, and the TCP/IP protocol.
**Availability**
The availability of the web-based viewer on the Internet.
**Error**
Relating to the application(s) software and website: non-compliance with the agreed functional and technical specifications.
**Duration of use**
Duration agreed with the End User, during which the server must be available for use.
**Repair time**
The time during office hours, within which a disruption to the connection and the Contractor's network must be rectified.
**Hotfix**
Solution to a production-disrupting error, with a high priority that is immediately available.
**Incident**
A reported and registered disruption error, wish or user request.
**Incident management**
A process managed by a service desk, relating to the way in which reports and notifications are dealt with.
**Office hours**
Working days between 7:00 and 18:00 hours.
**Report**
The report of a user request, disruption or error submitted to the Contractor's Service Desk.
**Web-based viewer**
IT environment equipped by the Contractor, on which the QA operates (runs), and that is used by the staff of the End User.
**SLA**
Service Level Agreement.
**Validation**
Confirmation of availability and correct operation of the QA web-based viewer by the End User.
**SIEM/SOC**
A SIEM (Security Information and Event Management) is a specific kind of technology, providing network visibility in a security context (by indicating suspicious/illegitimate activity, through set-up rules and correlation intelligence), and enabling security analysts to act on suspected threats.
A SOC (Security Operations Centre) encompasses the People, Processes, as well as Technology involved in protectively monitoring a network, responding to incidents, and researching/actively searching for known/unknown threats.

**Annex detail requirements for backup**

**Operational requirements**

- Which backups must be made and when, is kept in a file by the IT service provider. This file is verified at least annually, by the process owner of the customer, in accordance with (any) further agreements made in the security agreement (BVO).
- The correct execution of backups is checked at least daily. These checks are logged/documented. Failure to perform the backup successfully will be treated as a security incident, in accordance with the incident management process and policy.
- Accurate and complete records of backup copies and documented recovery procedures must be available. An (offline) administration is kept of backup and recovery activities, and the whereabouts of the media.
- Procedures/work instructions are drawn up by the ICT service provider, for all backup and restore activities.

**Assurance of backup confidentiality**

- Depending on the classification and business impact analysis, the following measures are taken to prevent violation of the confidentiality of data in the backup:
    - Backup of data with confidentiality classification 'Confidential' and 'Departmental Confidential' must be stored encrypted, with approved algorithms (AES256), so that they cannot be read by persons who have access to the storage media.
    - The key management must meet the requirements of the ISO 27002, and of supplier crypto policy.
    - Access to backup should be limited to need-to-process as a minimum. For the backup, the IT service provider draws up an authorisation matrix, and applies the logical and physical access policy.
    - Access to backup is logged and analysed periodically, ideally as part of SIEM/SOC.

**Assurance of backup integrity/protection against ransomware**

- To ensure that backups are not damaged, modified, deleted or encrypted by malicious actors, operator errors, physical damage or technical failures, the following measures are taken, depending on the classification and business impact:
    - Backups or copies thereof, must at least be kept at a location other than the production location, in order to restore the data, in the event of physical damage to the production and/or backup storage at the production location.
    - An offline copy must be made of every backup. This offline copy can be physically offline or realised virtually, for example, by:
        - Completely separating the access of backups from that of the production environment (separating AD without trusts, separating accounts and separating two-factor authentication for access); and
        - By only allowing read access between the backup and production environment.
    - Immediately after making a backup, a hash value is calculated and stored in the backup administration. This hash value can be used to verify the integrity of the backup.
    - It must be avoided that one account has access to both the production and the backup environment.

**Testing backups**

- The backup restore procedure should be tested annually, to ensure that the backup is reliable, if needed, in an emergency, and a test plan should be in place.

**Backup retention**

- All (daily) backups are kept for at least two weeks.
- One backup per week, made on a fixed day of the week, is kept for at least one month
- One backup per month, made on a fixed day in the month, or the first fixed weekday in the month, is stored for a maximum of one year.
- Backups are deleted after one year at the latest.