SERVICE LEVEL AGREEMENT (SLA)

1. General
This Service Level Agreement (SLA) relates to the use of Services based on a User Agreement between the Supplier and the Customer. The SLA must be understood in conjunction with the User Agreement and General Terms and Conditions of Delivery. In the SLA, the mutual obligations and efforts are laid down with regard to the Service.

2. Definitions
Supplier: Informer Online Nederland BV, registered with the Chamber of Commerce no. 63388928.
Customer: The user of services provided by the Supplier based on a User Agreement.
Service: Software as a Service (SaaS), through which the Customer is provided by the Supplier with an online system consisting of multiple software applications.
Service Window: Period of time during which the Service is available: 24 hours a day, with the exception of essential maintenance.
Session: Registration with the Service, whereupon the Service can be used. A session ends when the user logs out or happens automatically one hour after the last interaction with the Service.
Secure Socket Layer (SSL): Generally used Internet protocol that provides secure connections.
Server: A computer that stores and processes data within a network on behalf of multiple client computers.
Firewall System: Protection of computers and networks of computers by controlling incoming and outgoing (data) traffic.
Maintenance and Preventive Maintenance: The performance of corrective work on hardware and software to guarantee the continuity of the Service.
Incident: A possible problem in the Service reported by the Customer that requires a solution.
Response Time: The time between notification of an incident and the first response from the Supplier.

3. Obligations
The obligations set out below apply without prejudice to the obligations set out in the General Terms of Delivery.
3.1 The Customer is responsible for the following: hardware and software in the workplace; infrastructure and security within their own organisation; connection to the Internet; data input; protection of means of access; duty of care in respect to the use of the Service.
3.2 The Supplier is responsible for: providing access; providing codes and instructions; availability of the Service; security of the Service; support for the Customer.
3.3 At the Customer's request, the Supplier can advise the Customer on the design and security of workstations and infrastructure. In appropriate cases, the Supplier and the Customer will enter this into an additional agreement.

4. Availability and maintenance
4.1 Continuous availability of the Service is the starting point. The Supplier will make the Service available to the Customer in any event during the Service Window. The Supplier strives for an availability of 99.7% during the Service.
4.2 In order to ensure the availability of the Service, the Supplier's systems are equipped with a double emergency power supply, which is used to absorb power failures from the public electricity grid.
4.3 The Service requires (preventive) maintenance. The Supplier shall announce maintenance in advance. The Supplier shall carry out (preventive) maintenance outside the time span stated in clause 4.1 where possible.
4.4 The time the Service is unavailable as a result of (preventive) maintenance does not count against the availability referred to in clause 4.1.
4.5 During the time the Service is not available, the Customer can contact the company via the HelpDesk or social media. The HelpDesk will inform the Customer about the cause and expected duration of the interruption. Upon request, the Customer can receive a message as soon as the Service is resumed.

5. Security
5.1 The Service runs on systems owned by the Supplier. These systems are placed in a permanently secured environment at several levels. Only authorised people have access to this environment.
5.2 The environment is equipped with fire- and burglary-resistant devices.
5.3 The Supplier shall take drastic measures to prevent the Service from being influenced by viruses and the like, as well as unauthorised access and use.
5.4 The Supplier reserves the right to block the access of one or more Customers with regard to the security of the Service. In such cases, the Supplier shall inform the Customer concerned as soon as possible.
5.5 Non-compliance with the obligations mentioned in article 3.1 can be a reason to block access.

6. Access security, integrity and reliability
6.1 The Supplier provides every Customer with a unique user ID and password.
6.2 At any time, the Customer may use this user ID at one workstation, with only one login permitted at a time.
6.3 If the Customer has logged in to more than one session at the same time, the Customer takes on the risk and the cost of recovery of lost or incorrect processing of data.
6.4 Only the Customer and the authorised system administrators can change the password.
6.5 The user's data is only accessible to the Customer from outside the Supplier's system. The Customer can make their user data accessible to other users or advisors. The Customer is then responsible for the integrity of the data and for informing the User about the access and use of the Service. For reasons of security and privacy, the Supplier cannot inform anyone other than the Customer.
6.6 The link between the Customer and the Service can only be made by means of a Secure Socket Layer (SSL). The Supplier will inform the Customer about the SSL.
6.7 Access to the central system is controlled by a Firewall System. Only access and activities allowed by the Firewall System can be performed.
6.8 The Supplier shall treat the Customer's personal or business data as strictly confidential. The Supplier will only make the data available to third parties if it is obliged to do so pursuant to the law or a court ruling.
6.9 When processing data, the Supplier will, where possible, check and validate the results in order to maximise the reliability of the output.

7. Backup and Audit File
7.1 The Supplier shall make a daily backup of the data on its systems. Backups are intended solely to prevent loss of data as a result of Service disruptions.
7.2 Only files that have changed since the last backup will be backed up (incremental backup).
7.3 A maximum of seven versions of one data file will be stored. If a data file is modified while seven versions are already stored, the latest incremental backup will be added to the series and the oldest version will be permanently deleted.
7.4 When a user deletes a datafile, the two most recent versions are retained for 21 days. After 21 days, the versions are permanently deleted.
7.5 Backups do not serve to repair the input errors of individual Customers. As often as desired, the Customer can request an audit file from the application in order to save it themself.

8. Support

8.1 The HelpDesk is available to the Customer free of charge for support of the application and system software used in connection with the Service.
8.2 The Customer's chat service HelpDesk is available on working days from 9.00 a.m. to 4.30 p.m. and can be accessed by using the help button or by sending an e-mail to helpdesk@informer.nl.
8.3 The HelpDesk is closed on national holidays and at the weekend. The HelpDesk can always be reached by e-mail: helpdesk@informer.nl. E-mails are, in principle, only answered within the period stated in article 8.2.
8.4 Only incidents reported by Customers by e-mail shall automatically be assigned an incident number, based on which a correspondence shall be conducted, along with the progress of handling the Incident.
8.5 The Response Time to Incidents is one hour. Time outside of the period mentioned in article 8.2 does not count as Response Time.
8.6 The resolution time for Incidents is basically four hours. Time outside of the period mentioned in article 8.2 does not count as resolution time.
8.7 If the resolution time is expected to be longer than four hours, or the report does not appear to concern an Incident, the Supplier shall inform the Customer as soon as possible.

9. Various

9.1 The Supplier shall strive for continuity of the application and system software. The basic principle is the use of the most up-to-date versions of the application and system software; however, the Supplier particularly aims at the optimum combination of software components, whereby it is possible that a less up-to-date version, free of teething troubles, will be used because it produces a better result.
9.2 The Supplier uses the legal storage terms for storing data in its systems. The Customer is obliged to take care of the applicable storage terms in their own administration.

10. Amendments and location of the Service Level Agreement

10.1 The Service Level Agreement may be amended at any time. The Customer will be notified of any amendments.
10.2 The most recent version of the Service Level Agreement can, at all times, be found online at the URL: http://www.informer.eu/downloads/sla-en.pdf.
10.3 The most recent Service Level Agreement applies to all agreements with the Customer. The URL to the Service Level Agreement will always be stated in all agreements.
10.4 Upon the Customer's written request, the applicable Service Level Agreement can be sent to the Customer.