DATA PROCESSING AGREEMENT

Effective as of July 1, 2023

This Data Processing Agreement (“**DPA**”), including its corresponding schedules, is an addendum to the "**Service Agreement**" between **XLReporting Software BV**, registered number 75064383, located at Winthontlaan 200, 3526KV Utrecht, the Netherlands ("**Processor**") and you, the customer ("**Controller**"). We will hereinafter be referred to collectively as "**Parties**", or each individually as "**Party**".

This DPA reflects the agreement of Parties with respect to Processing of Personal Data by Processor on behalf of Controller, is supplemental to, and forms an integral part of, the Service Agreement, and its duration shall be in accordance with the Service Agreement.

Parties declare to have agreed as follows:

Article 1. Definitions

Except to the extent expressly provided otherwise, in this Agreement the following terms will have the following meaning:

- "**GDPR**": Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data and repealing Directive 95/46/EC (General Data Protection Regulation);
- "**Data Subject**": the living, natural person to whom Personal Data relates;
- "**Data breach**": any situation where, due to a security incident, Personal Data is lost, destroyed, modified, unlawfully processed or unintentionally accessed by an unauthorised person;
- "**Service Agreement**": the Service Agreement dated July 1, 2023 which describes how Processor shall provide the agreed services;
- "**Agreement**": this processing agreement including schedules;
- "**Written/In Writing**": notice by post or email;
- "**Personal Data**": any information about an identified or identifiable natural person, which Processor processes or is required to process under the Service Agreement, the types of personal data and categories of Data Subjects of which are further specified in Schedule 1;
- "**Third Party/Parties**": natural or legal persons who are not contracting parties to this Agreement;
- "**Privacy Legislation**": all applicable laws and regulations relating to the Processing and Protection of Personal Data, including but not limited to the GDPR and the GDPR Implementation Act;
- "**Processing/Processes**": an operation or set of operations involving personal data or a set of Personal Data, whether or not carried out by automated means, such as the collection, recording, organisation, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, blocking, erasure or destruction of Personal Data;

Article 2. Scope of the Agreement

1. Unless the Parties have agreed otherwise In Writing, the provisions of this Agreement shall apply to any Processing by Processor under the Service Agreement that takes place from the time this Agreement is in effect.
2. Processor Processes Personal Data on behalf of Controller, under its responsibility and in the manner set out in the Service Agreement.
3. Processor Processes Personal Data only on behalf of Controller, with the exception of differing legal obligations.

Article 3. General obligations of Processor

1. Processor has no control over the purposes and means of the Processing of Personal Data and does not make any independent decisions regarding the use of the Personal Data, the possible disclosure of Personal Data to Third Parties and the duration of the storage of Personal Data.
2. Processor shall immediately notify Controller In Writing if, in Processor's reasonable opinion, an instruction violates applicable Privacy Laws.
3. Upon the Controller's first request, Processor shall make available all information necessary to demonstrate compliance with the obligations laid down in this Agreement. Any costs involved in this shall be at the Controller's expense and risk.
4. Processor shall ensure compliance with the conditions imposed on the Processing of Personal Data under the applicable Privacy Legislation.
5. Processor only provides access to Personal Data to its employees to the extent necessary to perform the services under the Service Agreement.

Article 4. Division of responsibility

1. Processor is only responsible for the Processing of Personal Data under this Agreement, in accordance with the Controller's Written instructions and under the Controller's express (ultimate) responsibility. For other Processing, including in any case, but not limited to the collection of Personal Data by the Controller, Processing for purposes not reported to the Processor by the Controller, Processing of Personal Data of types of Data Subjects not reported to the Processor by the Controller and Processing by Third Parties, the Processor is explicitly not responsible.
2. Controller agrees and warrants that the content, use and commissioning of the Personal Data Processing referred to in this Agreement is in accordance with applicable privacy laws, is not unlawful and does not infringe any right of Third Parties. For example, Controller has ensured that the Processing of Personal Data of Data Subjects is based on a valid ground for Processing.

Article 5. Provision of Personal Data to Third Parties

1. Processor will not provide or make Personal Data available to a Third Party unless:
   (a) this is explicitly permitted in the Service Agreement;
   (b) this is pursuant to an express Written instruction from Controller; or
   (c) this by order of a judicial or administrative authority, is on condition that in such case Processor notifies Controller within 24 (twenty-four) hours of receiving such an order in order to enable Controller thereby to exercise a remedy available.
2. If Processor is of the opinion that it needs to make Personal Data available to a competent authority pursuant to a legal obligation, it will not do so until after consultation with and approval by the Controller. Processor shall notify the Controller in Writing of the legal obligation as soon as possible, providing all relevant information that the Controller reasonably requires to take the necessary measures to determine whether disclosure can take place and, if so, under what conditions.

Article 6. Processing outside the EEA

1. Controller declares to have given express consent for Processor to Process Personal Data outside the European Economic Area, provided the legal conditions for this are met. Controller may attach certain conditions to this Processing. The Processing of Personal Data occurring outside the European Economic Area is set out in Schedule 1.
2. Processor shall inform the Controller as soon as possible about changes in its intended Processing outside the EEA. The Controller has the right to object to such Processing outside the EEA, In Writing and with reasons, within 14 (fourteen) calendar days after the announcement of its intended Processing outside the EEA. If the Controller objects, the Parties shall consult with each other to reach a solution. If Controller does not object within the aforementioned period, Controller shall be deemed to have agreed to the Processing in question.
3. In the event that the Parties cannot reach an agreement after mutual consultations and without this intended Processing outside the EEA it is no longer possible to perform the services as agreed in the Service Agreement, then Processor has the right to terminate this Agreement, as well as the Service Agreement with immediate effect without owing any compensation to Controller.

Article 7. Requests from Data Subjects

1. Processor shall notify Controller of any requests received directly from Data Subjects regarding Data Subjects' rights under applicable Privacy Laws, including but not limited to requests for inspection, rectification, deletion, restriction of Processing or transfer of Personal Data. Processor shall only comply with such request if Controller has instructed Processor In Writing to do so. Upon its first request, Processor shall provide Controller with all cooperation in fulfilling its duty to respond to requests to exercise the established rights of Data Subjects.
2. Processor shall deal promptly and properly with all requests for information from Controller regarding the Processing of Personal Data. Upon the Controller's first request, Processor shall make available all information necessary to demonstrate the fulfilment of the Controller's obligations set out in this Agreement and Article 28 GDPR.

3. Upon Controller's request, Processor shall cooperate in conducting a data protection impact assessment (DPA) and any prior consultation under applicable Privacy Laws.

Article 8. Engaging Third Parties by Processor in performance of Contract

1. Controller hereby authorises Processor to use Third Parties (Subprocessors) in the Processing of personal data under this Agreement, subject to the applicable Privacy Laws. If a Third Party is engaged to perform specific Processing Activities on behalf of the Controller (as a Subprocessor), the Processor shall ensure that this Third Party also Processes in accordance with the applicable Privacy Legislation. The Third Parties engaged by Processor are listed in Schedule 1 of this Agreement.
2. Processor shall inform the Controller as soon as possible of any intended changes in the Third Parties to be engaged. The Controller has the right to object to any Third Parties to be newly engaged or changed by the Processor, In Writing and with reasons, within 14 (fourteen) calendar days after the announcement of the Third Parties to be engaged. Where the Controller objects, the Parties shall consult with each other to reach a solution.

Article 9. Audit

1. The Controller may, upon request and at its own expense, arrange for an audit to verify compliance with this Agreement.
2. The audit referred to in 9.1 shall take place no more than once every 12 (twelve) months.
3. If Controller wishes to carry out this audit, then Processor shall provide all reasonable cooperation in this regard by, inter alia, granting access to the database and making all relevant information available.
4. Controller shall pay all costs, fees and expenses related to the audit, including reasonable internal costs incurred by Processor. Reasonable internal costs incurred by Processor will be calculated on a post-calculation basis using the rates applicable at Processor, excluding external costs.
5. If the audit results in recommendations for Processor, then Processor shall implement these recommendations to the extent that Processor can reasonably be expected to do so. If these changes result from changed insights or legislation, the costs involved will be at the Controller's expense and risk.
6. If the changes result from the failure to comply with the agreed security requirements, these costs shall be at the expense and risk of the Processor.
7. If the Data Protection Authority or another competent authority wishes to conduct an investigation, Processor shall provide all reasonable cooperation to that end and Processor shall notify the Controller accordingly.

Article 10. Confidentiality

1. Processor shall keep the Personal Data and other information obtained from Controller strictly confidential, exercising at least the same degree of care as it exercises with respect to the protection of its own information of a highly confidential nature. The results of the audit as described in Article 9 are subject to an obligation of confidentiality for the Controller towards Third Parties. The duty of confidentiality referred to in this article does not apply in any of the cases mentioned in Article 5(1).

2. Processor shall not disclose, distribute, provide or otherwise disclose the Personal Data or other confidential information obtained from Controller to persons other than its employees, who need to know the Personal Data or other confidential information obtained from Controller in order to perform their work. Processor shall only give these employees access to the Personal Data and confidential information after they have been informed of the confidential nature of the Personal Data and/or information. Processor shall impose the duty of confidentiality stipulated in this Agreement on its employees as well.

Article 11. Duty to report data breaches

1. Processor shall notify Controller immediately, and in any event no later than 48 (forty-eight) hours after Processor becomes aware of it, of any breach or serious suspicion of such breach (of whatever nature) that (partly) relates or may relate to the Processing of Personal Data.
2. In any case, Processor should provide Controller with information on the following:
   (a) the nature of the breach, where possible indicating the categories of Data Subjects concerned and, approximately, the number of Data Subjects concerned;
   (b) the Personal Data (potentially) affected and, approximately, the number of Personal Data affected;
   (c) the identified and expected consequences of the breach for the Processing of Personal Data and the individuals affected; and
   (d) the measures that Processor has taken and will take to address the breach, including, where applicable, the measures to mitigate any negative consequences of the breach.
3. The notification referred to in Article 11.1 shall be sent by Processor to the Controller's designated contact person. The Controller shall indemnify Processor against any damages arising as a result of the failure to notify (on time) or incorrect notification of this contact person. The notification will be made both by telephone and email. Upon receipt of the notification, the Controller shall inform Processor of the manner in which the Controller shall, if necessary, report any data breach to the Data Protection Authority.
4. Processor acknowledges that Controller is under circumstances legally obliged to report to Data Subjects and/or authorities a security breach (of whatever nature) that (partly) relates or may relate to the Personal Data Processed by Processor. Such a notification by Controller shall never be considered a breach of this Service Agreement or otherwise an unlawful act. Processor shall take all measures necessary to limit the (possible) damage of a security breach and shall support Controller in notifications to Data Subjects and/or authorities.
5. Processor shall ensure that (possible) evidence relating to the breach referred to in Article 11.1, including but not limited to log files, analyses of network traffic and access control data, is preserved as much as possible and made available to Controller upon request.
6. Controller shall pay all costs, fees and expenses related to the notification referred to in Article 11.1, including reasonable internal costs incurred by Processor. Reasonable internal costs incurred by Processor will be calculated on a post-calculation basis using the rates applicable at Processor, excluding external costs.

Article 12. Retention period of Personal data

1. Processor shall not Process the Personal Data for longer than for the duration of the Service Agreement and 2 (two) months thereafter unless the Controller has expressly instructed Processor to do so In Writing with reasons and Processor has accepted such instruction or this results from a legal obligation. In the event that Controller controls Processor's access to the Personal Data, then Processor shall not process the Personal Data for longer than until Controller denies Processor such access.
2. If, in the opinion of Controller, certain Personal Data should not or need not be retained any longer, then upon the Controller's Written request, Processor shall promptly destroy the relevant Personal Data specified by Controller.

Article 13. Security measures and inspection

1. Processor shall take all appropriate technical and organisational measures to secure Personal Data against loss or any form of unlawful Processing in accordance with Article 32 GDPR. These measures, provide an appropriate level of security considering the state of the art, the implementation costs, as well as considering the nature, scope, context and Processing purposes and the risks, varying in terms of probability and severity, that Processing the Personal Data Processed by the Processor entails for the rights and freedoms of Data Subjects.
2. Processor does not guarantee that the security is effective under all circumstances. If there is no expressly defined security in the Contract, Processor shall make every effort to ensure that the security meets a level that is not unreasonable, given the state of the art, the sensitivity of the personal data and the costs associated with implementing the security.
3. Processor has taken the organisational and technical measures listed in Schedule 1.
4. Processor shall provide specific restrictions and/or additional safeguards if the Processing concerns 'special' personal data as referred to in Article 9 of the GDPR.
5. Processor should inform Controller if any of the security measures change.
6. Processor shall allow Controller to inspect Processor's compliance with the security measures or, at the request of Controller, to have Processor's data processing facilities inspected by an investigative body to be appointed by Controller in connection with the Processing Activities covered by this Agreement ('the Inspection'). The Inspection shall be conducted by an investigative body, which shall be neutral and competent in the reasonable opinion of Controller. Controller shall ensure that the investigating authority is obliged to keep its findings confidential from Third Parties.
7. The Inspection referred to in 13.6 shall take place at most once (once) every 12 (twelve) months.
8. Controller shall pay all costs, fees and expenses related to the Inspection, including reasonable internal costs incurred by Processor. Reasonable internal costs incurred by Processor will be calculated on a post-calculation basis using the rates applicable at Processor, excluding external costs.
9. Controller will provide Processor with a copy of the Inspection report.

Article 14. Obligations of Controller

1. Controller is, in respect of the Processing of Personal Data pursuant to this Agreement, the "Controller" as defined in Article 4(7) GDPR.
2. Controller shall keep a Processing Register of all Personal Data it Processes. In this register, it shall at least record its own name and contact details, the categories of Personal Data to be Processed, the Processing Purposes and the categories of Data Subjects.
3. The categories of Personal Data to be Processed, the Processing Purposes, and the categories of Data Subjects that Controller believes will be Processed pursuant to the Service Agreement shall be submitted to Processor within 14 (fourteen) business days of the signing of this Agreement and shall be attached to this Agreement as an attachment. Processor warrants the accuracy of this information.
4. Controller agrees and warrants that the Processing of Personal Data pursuant to this Agreement complies with applicable Privacy Laws.

Article 15. Liability

1. Processor shall only be liable for damages arising from or related to non-performance of this Agreement or acting in violation of applicable Privacy Laws. The liability of Processor to Controller under this Agreement in respect of any compensation for damages shall not exceed the total amount paid and payable by the Customer to the Processor under the Service Agreement in the 6-month period preceding the commencement of the event or events. In no event will the total compensation exceed the amount to be paid out by the Processor’s liability insurance.
2. Controller shall indemnify Processor against any damage arising from or related to acting in breach of the applicable Privacy Laws, in cases where this was done on the instructions of or with the consent of Controller.
3. Any claim for damages by Controller against Processor that is not specified and explicitly reported shall expire by the mere lapse of twelve (12) months after the claim arises.

Article 16. Duration and termination

1. The Agreement is entered into for an indefinite period of time and ends at the time the Service Agreement ends. Provisions of this Agreement that purport to retain their validity after the termination of the Agreement shall remain in full force and effect after the termination of the Agreement.
2. Notwithstanding a Written instruction to the contrary from Controller, in case of termination of the Agreement, Processor shall destroy and/or return to Controller all Personal Data made available to it as soon as possible, but in accordance with the retention period as mentioned in this Agreement.
3. If in Processor's reasonable opinion an independent legal obligation of Processor prohibits or restricts the total or partial destruction of the Personal Data by Processor, it shall notify Controller in Writing of the legal obligation as soon as possible, providing all relevant information that Controller reasonably needs to determine whether destruction can take place and, if so, under what conditions. If, in the Controller's reasonable opinion, the legal obligation permits (partial) destruction of the Personal Data by

Processor, then Processor shall promptly do so at the Controller's request. If the Controller considers that destruction may not take place, it shall notify the Processor thereof In Writing. In such a case, Processor shall guarantee the confidentiality of the Personal Data to Controller and shall not Process the Personal Data except in fulfilment of its aforementioned legal obligation or after being instructed In Writing by Controller.

Article 17. Transfer of rights and obligations

1. The rights and obligations under this Agreement may not be assigned by Controller to Third Parties without the prior Written consent of Processor. This provision counts as a clause with effect under property law as referred to in Article 3:83 paragraph 2 of the Dutch Civil Code.

Article 18. Divisibility and final provisions

1. If one or more provisions of this Agreement are null and void or annulled, this shall not affect the validity of the entire Agreement. The parties shall consult in order to agree on a new provision to replace the void or nullified provision, taking into account as much as possible the purpose and meaning of the void or nullified provision.
2. In case of conflict between the Service Agreement pursuant to which the Service is provided and this Agreement, the provisions of this Agreement shall prevail as far as it concerns provisions on the Processing of Personal Data. In the event of other conflicting provisions, those of the Service Agreement shall prevail.
3. The schedules form an integral part of this Agreement.

Article 19. Applicable law and disputes

1. This Agreement shall be exclusively governed by and construed in accordance with Dutch law.
2. Any disputes relating to this Agreement shall be subject to the exclusive jurisdiction of the courts of The Netherlands.

Schedule 1

1. Description of Processing operations and purposes

Data Subjects concerned	Users of XLReporting, typically staff members of Controller.
Processed Personal Data	Personal Data of “Users": • User details (email address, password, name); • Logging of activity data (IP address, browser type).
Purpose	Processor Processes Personal Data for the following purposes: • Performing the Service Agreement between Processor and Controller.

2. Overview of engaged Subprocessors

Name Subprocessor	Enabled for purpose	Transfer outside the European Economic Area
Digital Ocean	Data centers and hosting	No (EU region) Yes (AP+US region)
Microsoft 365	Email, Teams, Documents	No
Stripe	Invoices and Payment processing	No
Site24x7	Server monitoring and logging	No

3. Security instructions and measures

Subject	Instructions from Processor	Measures taken
Access management	Processor shall apply the principles of least privilege and need-to-know to its staff and permitted Subprocessors. Processor shall revoke or change user access in a timely manner upon any change in the status of its staff, suppliers, customers, business partners or third parties. Processor shall use current and generally considered secure forms of encryption and encryption for the purposes of identification, authentication and authorisation.	Processor has arranged for staff to have access only to the data currently required for his/her job. This has been done through the following: • There are multiple roles/ levels within the systems being worked in. • There is an "In-service" protocol that is followed, which determines entitlements. • There is an "Out of Service" protocol that is followed, in which dues are revoked.
Staff	Processor informs its employees about their responsibilities regarding information security and ensures that employees fulfil their obligations.	Processor has included responsibility over information security in the employment contract.
Contract management Subprocessors	Processor shall enter into a Subprocessor Agreement with each permitted Subprocessor, which contractually obliges the Subprocessor to fulfil the same obligations in connection with the Processing as those to which Processor is bound under this Agreement. Processor shall closely monitor Subprocessors' compliance with their obligations.	Processor shall enter into a Subprocessor agreement with permitted Subprocessors.
Security incident & response	Processor has a documented security incident response plan suitable for detecting, resolving and reporting Data Breaches, in accordance with the obligations in Article 10.	Processor has included a security incident response plan in its "Data Protection Plan". In addition, the Processor continuously monitors the service for security incidents.
Vulnerability/ patch management	Processor periodically searches for vulnerabilities within the applications, systems and networks used. Processor installs and implements security patches immediately or without delay after their appearance.	Processor periodically monitors and searches for vulnerabilities within the service at the application level: server state, file changes, malware scan, content safety and vulnerabilities.

Network and system security	Processor has measures in place to deter and detect misuse and malware of Processor's network and systems (such as firewalls and antivirus software from trusted vendors).	Processor has several firewalls running to prevent unauthorised access. Processor periodically monitors and searches for vulnerabilities within the service at the application level: server state, file changes, malware scan, content safety and vulnerabilities.
Physical access security	Processor shall take appropriate measures (such as locks and lockers) to secure the hardware on which the (Personal) Data may be Processed against unauthorised access.	Processor has lockers to secure the hardware thereby against unauthorised access.
Business continuity & disaster recovery	Processor has implemented policies, procedures and processes to ensure that the services or products provided and the Processed (Personal) Data remain available in case of unforeseen circumstances and disasters, or are fully restored as soon as possible.	Processor has included a business continuity & disaster recovery plan in its "Data Protection Plan".
Independent audit	Processor shall allow an external party to perform audits, vulnerability scans and periodic penetration tests on its applications and networks on behalf of Processor, in consultation with Controller.	In consultation, Processor will allow an external party to conduct audits.