IT SUPPORT ACCESS AGREEMENT

By and between

etster Company Name
Address
Address
VAT

- Customer -

and

Complianz BV
Kalmarweg 14-5 9723
JG Groningen, The Netherlands
VAT: NL858847000B01
UK VAT: 371 7310 10

- Provider –

Together referred as the "parties".

Preamble
This agreement (the "Agreement") is concluded between the parties as a supplementary regulation for compliance with Art. 28 GDPR, when the Provider provides support to the Customer upon the Customer's specific request.

Definitions
a. "**Data Subject(s)**" refers to the data subjects, whose personal data is processed or may be processed by the Provider upon request and on behalf of the Customer.
b. "**Personal Data**" means any information relating to an identified or identifiable natural person; an identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person.

1. General information
The Provider provides services that are implemented in the Customer's IT systems on a subscription basis. The Customer has explicitly requested exceptional support in the implementation of such services, which does not fall within the scope of the support services provided by the Provider. While it is understood that the Provider does not generally offer such assistance, the parties convene that the Provider will execute the requested exceptional support assistance as regulated herein as a one-off service, as per Customer's request at no cost. In this context, it cannot be ruled out that the Provider's personnel process personal data to carry out the exceptional support service requested by the Customer.

2. Duration and termination of the order

This Agreement shall commence upon signature by both parties and shall apply for the duration of the intervention by the Provider's personnel.

3. Application and data processing

Under exceptional circumstances and as explicitly requested by the Customer, the Provider shall provide the following additional services:

- Remote support of Complianz's services implementation, pursuant to which the Provider's personnel shall access the Customer's IT system to provide the requested assistance in relation to the Complianz services implemented by the Customer.

It may also include the processing of the following types of personal data:

- Name and contact details of users of the Customer;
- any other Personal Data of Data Subjects that could be stored or accessed while working on the support request.

Group of Data Subjects affected by the data processing:

- Employees of the Customer;
- Customers of the Customer, if applicable;
- Third parties, if applicable.

The Customer hereby confirms and warrants that prior to the Provider's access to their IT systems, which may lead to the processing of Personal Data of the mentioned Data Subjects by the Provider or the Provider's personnel, the Customer has sought authorization from any Data Subjects that might be affected by such processing or secured any other suitable legal basis to allow for such processing.

4. Remote maintenance

In the event that the Customer is subject to a statutory professional secrecy obligation according to applicable law or to any contractual non-disclosure obligations, the Customer must ensure that unauthorized disclosure does not occur through remote maintenance. In this respect, the Provider is obliged to give the Customer the option of ceasing the remote maintenance work at any time, upon the Customer's request.

5. Confidentiality

The Provider undertakes to observe a strict confidentiality obligation in relation to Personal Data and relevant processing activities carried out in performance of the Agreement. The Customer shall inform the Provider of any specific and additional confidentiality obligations that might apply. The Provider represents that it is aware of applicable data protection regulations and familiar with their provisions and requirements. The Provider further represents that all employees involved in the activities subject matter of the Agreement have been trained and instructed on applicable data protection legislation and are equally subject to a duty of confidentiality in relation to Personal Data.

6. Data integrity and safeguarding the rights of data subjects

The Customer acknowledges, accepts and guarantees that any and all data and information stored on the IT systems accessed by the Provider within the scope of this Agreement have been secured, backed-up and safely stored prior to the Provider's access to the IT system. The Provider shall not bear any liability for loss or alteration of such data and information.

It is solely the Customer's responsibility to safeguardthe rights of the Data Subjects.

7. Technical and organizational measures for data security, subprocessing

The Provider undertakes vis-à-vis the Customer to comply with the technical and organizational measures required under Art. 32 GDPR. The Provider must comply with the technical and organizational measures for the protection of personal data as specified in this contract.

The Provider may utilize specialized third-party services, such as cloud infrastructure or security solutions, to support the implementation of these measures. The Provider guarantees that such third-party services – if any – shall only perform their services from within the European Union or the EEA, thereby preventing any transfer of personal data outside the EU/EEA. To the extent any of such third-party services should process personal data, the Provider shall impose on them obligations at least equivalent to those under this contract and in any case in line with Art. 28 GDPR. Details on the technical and organizational measures implemented and subprocessing are mentioned in the Annex to this agreement.

8. Waiver

Neither the Provider nor any of its personnel shall be liable for any loss or expenses suffered or incurred by the Customer or the Customer's data subjects due to any acts or omissions by the Provider or its personnel, while carrying out this additional one-off service at the explicit request of the Customer. In accordance with this clause 8, the Customer agrees to hold the Provider harmless against all losses, actions, claims, expenses whether legal or otherwise, interest and demands and further waives any form of liability which may be incurred by the Provider in the execution of this additional one-off service which is expressly demanded by the Customer.
The exemption of liability shall not apply if willful misconduct or gross negligence by the Provider or its personnel has been established by a final judgement of a court of competent jurisdiction as defined in clause 10. Clause 8 supersedes the termination of this agreement.

9. Term

This agreement will automatically expire upon completion of the support services by the Provider's personnel, without the need for a formal termination.

10. Final provisions

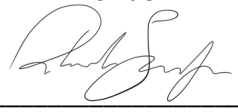
The Agreement and all the disputes arising in connection to its execution, interpretation and validity shall be subject to the Dutch law. The exclusive venue of jurisdiction shall be Groningen. Should any parts of this agreement be invalid, this shall not affect the validity of the remaining provisions of the contract.

Groningen, _____

- Customer -

_____

- Provider -



_____

ANNEX

The Provider shall implement and maintain technical and organizational measures (ToMs) as required by Article 32 GDPR. These measures are designed to ensure a level of security appropriate to the risk, protecting personal data against unauthorized or unlawful processing, accidental loss, destruction, or damage. In determining these measures, the Provider considers the state of the art, implementation costs, the nature, scope, context, and purposes of processing, as well as risks to the rights and freedoms of data subjects.
Our ToMs include, but are not limited to, the following key components:

1. **Risk-Based security approach**
    - We implement a dynamic risk management framework that continuously assesses and mitigates potential security threats. This ensures that our security protocols are proportionate to the identified risks and are adaptable to the evolving cybersecurity landscape.
2. **Data Protection by design and by default**
    - We integrate data protection principles into the core of our systems and processes from the outset. This includes utilizing advanced encryption standards, pseudonymization techniques, and strict data minimization policies to enhance the confidentiality, integrity, and availability of personal data.
3. **Access control and monitoring**
    - Robust access management policies are in place to enforce role-based access restrictions. We employ authentication mechanisms such as multi-factor authentication to ensure that only authorized personnel can access personal data. Regular monitoring and logging of access activities enable prompt detection and response to any unauthorized access attempts.
4. **Operational resilience and recovery**
    - To ensure business continuity and data integrity, we have developed comprehensive disaster recovery plans and incident response procedures. Secure and regular backups are performed to facilitate quick recovery in the event of data loss or system failure.
5. **Regular testing and evaluation**
    - Routine security audits and vulnerability assessments are conducted to evaluate the effectiveness of our ToMs. This proactive approach allows us to identify and address potential security weaknesses before they can be exploited.
6. **Qualifying and monitoring procedure for subprocessors**
    - We carefully select and monitor our service providers to ensure they adhere to our stringent data protection standards. All third-party processors, including iubenda s.r.l., via S. Raffaele 1, Milan (I), are required to implement appropriate security measures and comply fully with GDPR requirements.
7. **Employee training and awareness**
    - We provide continuous training to our staff on data protection regulations and best practices. By fostering a culture of security awareness, we ensure that all employees understand their responsibilities in safeguarding personal data.
8. **Data Breach notification procedures**
    - In the unlikely event of a data breach, we have established protocols to ensure timely notification to relevant supervisory authorities and affected data subjects, in accordance with GDPR Articles 33 and 34.
9. **Continuous improvement**
    - We are committed to the ongoing enhancement of our security measures. This includes staying informed about emerging threats and advancements in technology to continually strengthen our data protection strategies.