Appendix 4:

Data Processing Agreement

1. Purpose and Definitions

When fulfilment of the SLA will involve processing of Personal Data (as defined in the SLA-Agreement, and will be limited to the processing of Personal Data in relations to the Application, as specified in the SLA-Agreement, section 1, and herein) it will be subject to statutory provisions and obligations under relevant data protection legislation.

Service Provider, hereafter the “Processor”, and The Client, hereafter the “Controller”, have entered into this Data Processing Agreement to govern the Processor’s rights and obligations, with regard to all Processing of Personal Data on behalf of the Controller under the SLA and under this agreement, in order to ensure that all Processing of Personal Data is conducted in compliance with applicable data protection legislation.

In addition to Processing Personal Data as part of the SLA, the Parties acknowledges that the Processor may also Process Personal Data as a Controller for the purpose of, or in connection with: (i) applicable legal or regulatory requirements; (ii) request and communications from competent authorities; and (iii) administrative, financial accounting, risk analysis, and Client relationship purposes.

For the purposes of this Data Processing Agreement, The Client will be considered the controller ("Controller") who determines the purposes and means of the processing in accordance with applicable data protection legislation, and Service Provider will be considered the processor ("Processor"), meaning the legal entity Processing Personal Data on behalf of the Controller.

This Agreement shall ensure that the Controller’s data is processed in accordance with:

- The EU-Regulation 2016/679 (the "**General Data Protection Regulation**" or “**GDPR**”) as amended from time to time and all relevant national legislation including national implementations of the Regulation.

This Data Processing Agreement is intended to fulfil the requirements set down in the Data Protection Regulation. The parties agree to amend this Data Processing Agreement to the extent necessary due to any mandatory new requirements according to the Norwegian implementation of the Regulation.

"**Personal Data**" shall mean any information relating to an identified or identifiable natural person, as further defined in article 4 (1) in GDPR.

"**Processing of Personal Data**" shall mean any operation or set of operations which is performed upon personal data, whether or not by automatic means, such as collection, transfer, storage, alteration, disclosure as further defined in article 4 (2) in GDPR.

“Sub-processor” shall mean any other processor or third parties Processing Personal Data which the Processor engages, intentionally or unintentionally, for carrying out specific Processing activities on behalf of the Controller, including software-entities and affiliates.

“**Third Countries”** shall mean countries outside of the EU/EEA.

This Agreement shall also include:

- Appendix 2a: Type of personal data and data subjects to be processed by Processor and it’s Sub-processors
- Appendix 2b: Scope of processing activities
- Appendix 2c: List of approved Sub-Processors
- Appendix 2d: Security measures in place for the Processing of Personal Data

2. The Controller’s obligations

The Controller confirms that Controller:

- Has sufficient legal basis for the Processing of Personal Data
- Has responsibility for the correctness, integrity, content, reliability and legality of the Personal Data,
- Complies with applicable law on notification to and authorizations from relevant authorities
- Has informed the Data subject in accordance with applicable law

The Controller shall implement sufficient technical and organizational measures to ensure and demonstrate compliance with the Regulation.

The Controller shall notify any personal data breaches to the relevant authorities and if necessary, the data subjects without undue delay in accordance with applicable law.

3. The Processor’s obligations

The Processor shall only Process Personal Data to the extent necessary to fulfill its obligations towards The Controller (The Client) under the SLA and for the purposes mentioned in section 1 above. Furthermore, The Processor may Process Personal Data on instructions from the Controller and strictly in accordance with such instructions, unless such instructions violates any provision in the Regulation and/or national applicable data protection legislation.

4. Use of Sub-Processor’s

The Processor shall not sub-contract any of the Processing assigned to him by the Controller to any other entity or third party without the express, written agreement or written consent from the Controller. However, by executing this Data Processing Agreement, the Controller acknowledges and accepts the Processor's use of Sub-Processors as set out in Appendix 2c to this Data Processing Agreement. The Processor shall, by written agreement,

with any Sub-Processor's ascertain that any Processing of Personal Data by Sub-Processor's shall be subject to the same obligations and limitations imposed on the Sub-Processors as those imposed on the Processor pursuant to this Data Processing Agreement.

If the Processor plans to replace or use a new Sub-Processor, the Processor shall notify the Controller in writing 14 days before the new Sub-Processor begins Processing Personal Data, and the Controller may within two weeks after such notice oppose or accept the change. If the Controller opposes the change, both Parties may terminate the agreement with 1 days' notice. Notification of termination must be given within 7 days after the Controller opposed the change. If the Data Controller does not oppose the change or terminate the agreement within the deadlines specified above, the new Sub-Processor will be deemed as accepted by the Controller.

5. Discrepancies

Any use of the information systems and the personal data that contravenes established routines, instructions from the Controller or applicable data protection legislation, as well as any security breaches, shall be treated as a discrepancy.

The Processor shall have in place routines and systematic processes to follow up discrepancies which shall include re-establishing the normal state of affairs, eliminating the cause of the discrepancy and preventing its recurrence.

In case of a discrepancy, the Processor shall immediately notify the Controller if a discrepancy results in accidental, unlawful or unauthorized access to, use or disclosure of personal data, or that the data has been compromised. The Processor shall provide the Controller with all information necessary to enable the Controller to comply with applicable data protection legislation and enabling the Controller to answer any inquiries from the data protection authorities. It is for the Controller to notify the applicable data protection authority of discrepancies in accordance with applicable law.

6. Security audits and control

The Processor will implement sufficient technical and organizational measures to ensure a security level which is in compliance with the risk of processing the data. A detailed description of the data security measures put in place shall be set out in Appendix 2d to this Data Processing Agreement.

The Controller, or a competent authority, has the right to demand regular security audits or revisions in accordance with at any time applicable legislation, performed by an independent third party. The third party will deliver a report that will be delivered to Controller upon request. The purpose of such audits shall be for the Controller to verify that the Processor complies with the requirements of this Data Processing Agreement and applicable legislation. Such audits shall not be made more than once annually. Each Party will cover its own costs in connection with the audit and/or inspection.

7. Confidentiality

The Processor (including the Processor's representatives and employees) shall keep confidential all personal data and other confidential information, that the Processor accesses in accordance with this Agreement and the SLA.

The Controller (including the Controller's representatives and employees) shall keep confidential all information the Controller receives from the Processor or from The Processor's Sub-Processors including, but not limited to, information regarding security, customers and business. The Controller shall under no circumstances unjustly exploit, share or redistribute the aforementioned information.

Both parties shall take all necessary precautions to prevent unauthorised persons from gaining access to, or knowledge of, confidential information. The duty of confidentiality shall also apply after termination of this Data Processing Agreement.

8. Transfer of personal data to Third Countries

The processing of Personal Data shall predominantly take place in a member state of the European Economic area, such as in Norway or other European countries. The Processor may only transfer Personal Data to Third Countries or to third parties based in Third Countries based on European Commission adequacy decision or if agreed upon (e.g by consent) in writing by the Controller or if the Processor has a lawful basis for the transfer of personal data to a Third Country under Article 44-49 of the GDPR.

In the above cases the Processor shall, when deemed relevant, enter into a data transfer agreements based on the EU Standard Contractual Clauses for the transfer of Personal Data to Processors established in Third Countries in accordance with the Decision 2010/87/EU, or any replacement or alternative clauses approved by the European Commission.

9. Liability and Breach

<u>The Controller</u>

The Controller ensures that any Personal Data provided to the Processor by, or on behalf of, the Controller has been collected lawfully, fairly, and in a transparent manner so as to enable Personal Data to be Processed by The Processor and Sub-Processors.

The Controller acknowledges that it has primary responsibility for the Processing of Personal Data as part of the SLA and shall notify Processor of any assistance it requires pursuant to GDPR Article 28 (3) letter e and f.

Controller shall indemnify the Processor against all costs, expenses (including legal expenses), damages, losses (including loss of business or loss of profits), liabilities, demands, claims, actions, or proceedings, which Processor may incur arising out of:

i. Processor compliance with any instruction given by the Controller to the Processor in relation to the Processing of Personal Data (including wrongful instructions in connection with requests from individuals exercising their rights under Data Protection Legislation and any instructions to retain, disclose, amend, or otherwise Process Personal Data);
ii. Any breach by the Controller of the Data Protection Legislation; or
iii. Personal Data Breach inflicted by or under responsibility of the Controller.

The Processor

The Processor is liable for any action, proceeding, liability, loss, damage, cost, claim, fine, expense and/or demand ("claim") incurred by the Controller and which arise from the Processor's breach of obligations under this Data Processing Agreement. The Processor is in the same way responsible and liable for all acts and omissions by the Processor's Sub-Processors, exempt from liability under GDPR article 82 paragraph 2 and 3, if Processor proves that it is not in any way responsible for the event giving rise to the damage. .

Processor shall at any rate not be liable for indirect, special or consequential damages.

In the event of simple negligence on the part of the Processor or the Processor's Sub-Processor, the Processor's total liability under this agreement, including any attachments thereto, will be limited to a maximum amount corresponding to 50% of the compensation and fees paid under the contract during the last 6 months.
The limitation of liability lapses in the event that the Processor has shown gross negligence in breach of this agreement.

10. Term

This Agreement shall be effective from the date it is signed by both parties and will not expire as long as the Processor is processing or has access to the Controllers personal data in accordance with this Agreement and the SLA.

11. Obligations in coherence with termination

The parties agree that upon termination of the SLA, this Agreement will be deemed as terminated as well. And in accordance with section 3.3 Termination in the Service Agreement, each party may terminate the Agreement with immediate effect.

Upon the expiry of the termination period mentioned above and in section 3.8.1 in the SLA, the Processor (and its permitted Sub-Processors) shall cease to Process the Client's Data. The Processor shall in such an event return and subsequently delete all Personal Data and copies of Data provided to, or further Processed by the Processor for the purposes of the

SLA or this Agreement, save to the extent that the Processor is prevented by mandatory law from deleting the personal data.

For the avoidance of doubt, nothing in this clause shall require Processor to delete copies of Personal Data that it holds on its own behalf as a controller.

12. Other duties and rights

Other duties and rights are stipulated in the SLA.

13. Dispute and Jurisdiction

This Agreement shall be governed by and construed in its entirety in accordance with Norwegian law, save for mandatory provisions in applicable data protection legislation.

Disputes shall be subject to the jurisdiction of Oslo City court, if no other mandatory jurisdiction applies in applicable data protection legislation.

Appendix 2a: Data subjects and type of personal data

Data subjects:

The Personal Data which will be Processed is of data subjects such as:

- Employees: If customer performs self-validation themselves, information will be shared such as username* and mail addresses*.
- Customer- and contact information, such as email addresses, phone numbers and names.
- Customer`s supplier information, such as email address and other invoice information decided by the customer.
- Other users If the customer is in need of support, information such as phone numbers* and mail addresses* might be shared to get in contact with the correct person after support is provided.

*PII – Personal Identifiable Information

Type of personal data:

The categories of Personal Data may include:

Product name	Product Line	Type of data	Description of relevance	Classified as personal data	Location data storage
ECIT Portal	Office support	Invoices/ orders Access and User information	ECIT Digital Portal provides secure storage and sharing of documents in the cloud.	No	Google Cloud EU

Appendix 2b: Scope of processing activities

The Processor will access Personal Data from the Controller for Processing purposes in connection with the SLA. This includes collection, structuring, storage, adaptation or alteration, retrieval, use, alignment or combination of personal data related to:

i. External hosting, management, support, and maintenance of Service Provider platform, and related services, and appurtenant deliveries by Processor to Controller;

ii. Consulting, software engineering and operational- and technical services in connection with platform use;

iii. Provide relevant assistance, such as remotely accessing the Controllers Personal Data on the request of the Controller and in relation to support and other maintenance;

Processors purpose for the collection, Processing and use of Personal Data from Controller is to provide the Services stated above and in the SLA. Processor will not store Personal Data in a greater extent than necessary in order to provide the agreed Services.

Appendix 2c: List of approved Sub-Processors

In the below table is a summary of the categories of data, storage locations, data flows and legal basis for the respective Approved Subcontractor's processing activities.

Approved Subcontractor [Fill in company name, registration no., address, contact details]	**Scope and purpose of processing**	**Categories of Data**	**Processing (and storage) locations (e.g. country/state)**	**Legal basis for transfer of Personal Data (if applicable) (e.g. standard contractual clauses, BCR etc.)**
Google Ireland Ltd. Gordon House Barrow Street Dublin 4, D04E5W5 Ireland	Service Analytics, DataCenter and Infrastructure Services (Google Cloud Platform)	Data on invoices received. -Amount, duedate, invoicedate, payment, VAT number, suppliername, product information	All processing conducted within EU/EEA	N/A
Elasticsearch B.V. Keizersgracht 281 1016 ED Amsterdam The Netherlands	Storage of log data, and OCR data.	Data on invoices received. -Amount, duedate, invoicedate, payment, VAT number, suppliername, product information, Username (email) of users that approves invoices in the system	All processing conducted within EU/EEA	N/A
Attest.nu i Sverige AB Midgårdsgatan 2 831 45 Östersund	Scanning and storage of paper documents	Paper documents and files after scanning of documents	Midgårdsgatan 2 831 45 Östersund Sweden	N/A
ColliCare AB Tysjövägen 8 83152 Östersund	Storage of paper documents	Storage of paper invoices	Sälgatan 1 Tysjövägen 883152 Östersund	N/A
RaceIT Digital SRL Bulevardul Mihai Viteazu, nr. 18, sc. C, et. 2, ap. 77, Sibiu, Romania	Validation of document data	Data on invoices received. -Amount, duedate, invoicedate, payment ID, accountnumber, VAT number, suppliername, product information.	Bulevardul Mihai Viteazu, nr. 18, sc. C, et. 2, ap. 77, Sibiu, Romania	N/A

No data transferred outside the EU.

See: https://cloud.google.com/terms/eu-model-contract-clause
https://cloud.google.com/security/compliance/soc-2