Version: JUL 2022

Data Processing Agreement

Standard Contractual Clauses

For the purposes of Article 28(3) of Regulation 2016/679 (the GDPR)

between

[NAME]
CVR [CVR-NO]
[ADDRESS]
[POSTCODE AND CITY]
[COUNTRY]

(the data controller)

and

TARGIT A/S
CVR: 11562639
Gasværksvej 24, 2. Sal
9000 Aalborg
Denmark

(the data processor)

each a 'party'; together 'the parties'

HAVE AGREED on the following Contractual Clauses (the Clauses) in order to meet the requirements of the GDPR and to ensure the protection of the rights of the data subject.

1. Table of Contents

2. Preamble

1. These Contractual Clauses (the Clauses) set out the rights and obligations of the data controller and the data processor, when processing personal data on behalf of the data controller.

2. The Clauses have been designed to ensure the parties' compliance with Article 28(3) of Regulation 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).

3. In the context of the provision of TARGIT Cloud, BI solution, the data processor will process personal data on behalf of the data controller in accordance with the Clauses.

4. The Clauses shall take priority over any similar provisions contained in other agreements between the parties.

5. Four appendices are attached to the Clauses and form an integral part of the Clauses.

6. Appendix A contains details about the processing of personal data, including the purpose and nature of the processing, type of personal data, categories of data subject and duration of the processing.

7. Appendix B contains the data controller's conditions for the data processor's use of sub-processors and a list of sub-processors authorised by the data controller.

8. Appendix C contains the data controller's instructions with regards to the processing of personal data, the minimum security measures to be implemented by the data processor and how audits of the data processor and any sub-processors are to be performed.

9. Appendix D contains provisions for other activities which are not covered by the Clauses.

10. The Clauses along with appendices shall be retained in writing, including electronically, by both parties.

11. The Clauses shall not exempt the data processor from obligations to which the data processor is subject pursuant to the General Data Protection Regulation (the GDPR) or other legislation.

3. The rights and obligations of the data controller

1. The data controller is responsible for ensuring that the processing of personal data takes place in compliance with the GDPR (see Article 24 GDPR), the applicable EU or Member State[1] data protection provisions and the Clauses.

2. The data controller has the right and obligation to make decisions about the purposes and means of the processing of personal data.

[1] References to "Member States" made throughout the Clauses shall be understood as references to "EEA Member States".

3. The data controller shall be responsible, among other, for ensuring that the processing of personal data, which the data processor is instructed to perform, has a legal basis.

4. The data processor acts according to instructions

1. The data processor shall process personal data only on documented instructions from the data controller, unless required to do so by Union or Member State law to which the processor is subject. Such instructions shall be specified in appendices A and C. Subsequent instructions can also be given by the data controller throughout the duration of the processing of personal data, but such instructions shall always be documented and kept in writing, including electronically, in connection with the Clauses.

2. The data processor shall immediately inform the data controller if instructions given by the data controller, in the opinion of the data processor, contravene the GDPR or the applicable EU or Member State data protection provisions.

5. Confidentiality

1. The data processor shall only grant access to the personal data being processed on behalf of the data controller to persons under the data processor's authority who have committed themselves to confidentiality or are under an appropriate statutory obligation of confidentiality and only on a need to know basis. The list of persons to whom access has been granted shall be kept under periodic review. On the basis of this review, such access to personal data can be withdrawn, if access is no longer necessary, and personal data shall consequently not be accessible anymore to those persons.

2. The data processor shall at the request of the data controller demonstrate that the concerned persons under the data processor's authority are subject to the abovementioned confidentiality.

6. Security of processing

1. Article 32 GDPR stipulates that, taking into account the state of the art, the costs of implementation and the nature, scope, context and purposes of processing as well as the risk of varying likelihood and severity for the rights and freedoms of natural persons, the data controller and data processor shall implement appropriate technical and organisational measures to ensure a level of security appropriate to the risk.

   The data controller shall evaluate the risks to the rights and freedoms of natural persons inherent in the processing and implement measures to mitigate those risks. Depending on their relevance, the measures may include the following:

   a. Pseudonymisation and encryption of personal data;

   b. the ability to ensure ongoing confidentiality, integrity, availability and resilience of processing systems and services;

   c. the ability to restore the availability and access to personal data in a timely manner in the event of a physical or technical incident;

d. a process for regularly testing, assessing and evaluating the effectiveness of technical and organisational measures for ensuring the security of the processing.

2. According to Article 32 GDPR, the data processor shall also – independently from the data controller – evaluate the risks to the rights and freedoms of natural persons inherent in the processing and implement measures to mitigate those risks. To this effect, the data controller shall provide the data processor with all information necessary to identify and evaluate such risks.

3. Furthermore, the data processor shall assist the data controller in ensuring compliance with the data controller's obligations pursuant to Articles 32 GDPR, by *inter alia* providing the data controller with information concerning the technical and organisational measures already implemented by the data processor pursuant to Article 32 GDPR along with all other information necessary for the data controller to comply with the data controller's obligation under Article 32 GDPR.

   If subsequently – in the assessment of the data controller – mitigation of the identified risks require further measures to be implemented by the data processor, than those already implemented by the data processor pursuant to Article 32 GDPR, the data controller shall specify these additional measures to be implemented in Appendix C.

7. Use of sub-processors

1. The data processor shall meet the requirements specified in Article 28(2) and (4) GDPR in order to engage another processor (a sub-processor).

2. The data processor shall therefore not engage another processor (sub-processor) for the fulfilment of the Clauses without the prior general written authorisation of the data controller.

3. The data processor has the data controller's general authorisation for the engagement of sub-processors. The data processor shall inform in writing the data controller of any intended changes concerning the addition or replacement of sub-processors at least 30 days in advance, thereby giving the data controller the opportunity to object to such changes prior to the engagement of the concerned sub-processor(s). Longer time periods of prior notice for specific sub-processing services can be provided in Appendix B. The list of sub-processors already authorised by the data controller can be found in Appendix B.

4. Where the data processor engages a sub-processor for carrying out specific processing activities on behalf of the data controller, the same data protection obligations as set out in the Clauses shall be imposed on that sub-processor by way of a contract or other legal act under EU or Member State law, in particular providing sufficient guarantees to implement appropriate technical and organisational measures in such a manner that the processing will meet the requirements of the Clauses and the GDPR.

   The data processor shall therefore be responsible for requiring that the sub-processor at least complies with the obligations to which the data processor is subject pursuant to the Clauses and the GDPR.

5. A copy of such a sub-processor agreement and subsequent amendments shall – at the data controller's request – be submitted to the data controller, thereby giving the data controller the opportunity to ensure that the same data protection obligations as set out in the Clauses are imposed on the sub-processor. Clauses on business related issues that do not affect the legal data protection content of the sub-processor agreement, shall not require submission to the data controller.

6. The data processor shall agree a third-party beneficiary clause with the sub-processor where – in the event of bankruptcy of the data processor – the data controller shall be a third-party beneficiary to the sub-processor agreement and shall have the right to enforce the agreement against the sub-processor engaged by the data processor, e.g. enabling the data controller to instruct the sub-processor to delete or return the personal data.

7. If the sub-processor does not fulfil his data protection obligations, the data processor shall remain fully liable to the data controller as regards the fulfilment of the obligations of the sub-processor. This does not affect the rights of the data subjects under the GDPR – in particular those foreseen in Articles 79 and 82 GDPR – against the data controller and the data processor, including the sub-processor.

8. Transfer of data to third countries or international organisations

1. Any transfer of personal data to third countries or international organisations by the data processor shall only occur on the basis of documented instructions from the data controller and shall always take place in compliance with Chapter V GDPR.

2. In case transfers to third countries or international organisations, which the data processor has not been instructed to perform by the data controller, is required under EU or Member State law to which the data processor is subject, the data processor shall inform the data controller of that legal requirement prior to processing unless that law prohibits such information on important grounds of public interest.

3. Without documented instructions from the data controller, the data processor therefore cannot within the framework of the Clauses:

    a. transfer personal data to a data controller or a data processor in a third country or in an international organization

    b. transfer the processing of personal data to a sub-processor in a third country

    c. have the personal data processed in by the data processor in a third country

4. The data controller's instructions regarding the transfer of personal data to a third country including, if applicable, the transfer tool under Chapter V GDPR on which they are based, shall be set out in Appendix C.6.

5. The Clauses shall not be confused with standard data protection clauses within the meaning of Article 46(2)(c) and (d) GDPR, and the Clauses cannot be relied upon by the parties as a transfer tool under Chapter V GDPR.

9. Assistance to the data controller

1. Taking into account the nature of the processing, the data processor shall assist the data controller by appropriate technical and organisational measures, insofar as this is possible, in the fulfilment of the data controller's obligations to respond to requests for exercising the data subject's rights laid down in Chapter III GDPR.

   This entails that the data processor shall, insofar as this is possible, assist the data controller in the data controller's compliance with:

   a. the right to be informed when collecting personal data from the data subject
   b. the right to be informed when personal data have not been obtained from the data subject
   c. the right of access by the data subject
   d. the right to rectification
   e. the right to erasure ('the right to be forgotten')
   f. the right to restriction of processing
   g. notification obligation regarding rectification or erasure of personal data or restriction of processing
   h. the right to data portability
   i. the right to object
   j. the right not to be subject to a decision based solely on automated processing, including profiling

2. In addition to the data processor's obligation to assist the data controller pursuant to Clause 6.3., the data processor shall furthermore, taking into account the nature of the processing and the information available to the data processor, assist the data controller in ensuring compliance with:

   a. The data controller's obligation to without undue delay and, where feasible, not later than 72 hours after having become aware of it, notify the personal data breach to the competent supervisory authority, The Danish Data Protection Authority, unless the personal data breach is unlikely to result in a risk to the rights and freedoms of natural persons;

   b. the data controller's obligation to without undue delay communicate the personal data breach to the data subject, when the personal data breach is likely to result in a high risk to the rights and freedoms of natural persons;

   c. the data controller's obligation to carry out an assessment of the impact of the envisaged processing operations on the protection of personal data (a data protection impact assessment);

   d. the data controller's obligation to consult the competent supervisory authority, The Danish Data Protection Authority, prior to processing where a data protection impact assessment indicates that the processing would result in a high risk in the absence of measures taken by the data controller to mitigate the risk.

3. The parties shall define in Appendix C the appropriate technical and organisational measures by which the data processor is required to assist the data controller as well as the scope and the extent of the assistance required. This applies to the obligations foreseen in Clause 9.1. and 9.2.

10. Notification of personal data breach

1. In case of any personal data breach, the data processor shall, without undue delay after having become aware of it, notify the data controller of the personal data breach.

2. The data processor's notification to the data controller shall, if possible, take place within 36 hours after the data processor has become aware of the personal data breach to enable the data controller to comply with the data controller's obligation to notify the personal data breach to the competent supervisory authority, cf. Article 33 GDPR.

3. In accordance with Clause 9(2)(a), the data processor shall assist the data controller in notifying the personal data breach to the competent supervisory authority, meaning that the data processor is required to assist in obtaining the information listed below which, pursuant to Article 33(3)GDPR, shall be stated in the data controller's notification to the competent supervisory authority:

    a. The nature of the personal data including where possible, the categories and approximate number of data subjects concerned and the categories and approximate number of personal data records concerned;

    b. the likely consequences of the personal data breach;

    c. the measures taken or proposed to be taken by the controller to address the personal data breach, including, where appropriate, measures to mitigate its possible adverse effects.

4. The parties shall define in Appendix C all the elements to be provided by the data processor when assisting the data controller in the notification of a personal data breach to the competent supervisory authority.

11. Erasure and return of data

1. On termination of the provision of personal data processing services, the data processor shall be under obligation to delete all personal data processed on behalf of the data controller and certify to the data controller that it has done so unless Union or Member State law requires storage of the personal data.

12. Audit and inspection

1. The data processor shall make available to the data controller all information necessary to demonstrate compliance with the obligations laid down in Article 28 and the Clauses and allow for and contribute to audits, including inspections, conducted by the data controller or another auditor mandated by the data controller.

2. Procedures applicable to the data controller's audits, including inspections, of the data processor and sub-processors are specified in appendices C.7. and C.8.

3. The data processor shall be required to provide the supervisory authorities, which pursuant to applicable legislation have access to the data controller's and data processor's facilities, or representatives acting on behalf of such supervisory authorities, with access to the data processor's physical facilities on presentation of appropriate identification.

13. The parties' agreement on other terms

1. The parties may agree other clauses concerning the provision of the personal data processing service specifying e.g. liability, as long as they do not contradict directly or indirectly the Clauses or prejudice the fundamental rights or freedoms of the data subject and the protection afforded by the GDPR.

14. Commencement and termination

1. The Clauses shall become effective on the date of both parties' signature.

2. Both parties shall be entitled to require the Clauses renegotiated if changes to the law or inexpediency of the Clauses should give rise to such renegotiation.

3. The Clauses shall apply for the duration of the provision of personal data processing services. For the duration of the provision of personal data processing services, the Clauses cannot be terminated unless other Clauses governing the provision of personal data processing services have been agreed between the parties.

4. If the provision of personal data processing services is terminated, and the personal data is deleted or returned to the data controller pursuant to Clause 11.1. and Appendix C.4., the Clauses may be terminated by written notice by either party.

5. Signature

   On behalf of the data controller

Name	[NAME]
Position	[POSITION]
Date	[DATE]
Signature	[SIGNATURE]

   On behalf of the data processor

Name	[NAME]
Position	[POSITION]
Date	[DATE]
Signature	[SIGNATURE]

15. Data controller and data processor contacts/contact points

1. The parties may contact each other using the following contacts/contact points:

2. The parties shall be under obligation continuously to inform each other of changes to contacts/contact points.

Name	[NAME]
Position	[POSITION]
Telephone	[TELEPHONE]
E-mail	[E-MAIL]

Name	[NAME]
Position	[POSITION]
Telephone	[TELEPHONE]
E-mail	[E-MAIL]

Appendix A Information about the processing

A.1. The purpose of the data processor's processing of personal data on behalf of the data controller is:

The data processor provides a BI solution that consists of three base parts. TARGIT Control, TARGIT Server TARGIT Anywhere and TARGIT Data Discovery.

A.2. The data processor's processing of personal data on behalf of the data controller shall mainly pertain to (the nature of the processing):

The data processor will host all information which the data controller provides and stores on the cloud-based service.

A.3. The processing includes the following types of personal data about data subjects:

Special categories of personal data (tick the boxes):	
☐ Racial or ethnic origin	☐ Health data
☐ Political opinions	☐ Sex life or sexual orientation
☐ Religious beliefs	☐ Genetic or biometric data for the purpose of identification
☐ Philosophical beliefs	
☐ Trade union membership	☐ Criminal convictions and offenses
☒ Non-sensitive categories of personal data: Name, e-mail, phone number, address, employment information e.g. place of employment, title and department	

A.4. Processing includes the following categories of data subject:

Since the data processor will host the data stores by the data controller on the cloud-based solution, the data processor's processing may include any categories of data subjects that the data controller is providing and storing on the cloud-based solution.

A.5. The data processor's processing of personal data on behalf of the data controller may be performed when the Clauses commence. Processing has the following duration:

The data processor and data controller has entered into an agreement regarding a cloud-based BI solution, period of duration is determined in the General agreement. For the duration of this agreement, the data processor may host data containing personal information on behalf of the data controller.

Appendix B Authorised sub-processors

B.1. Approved sub-processors

On commencement of the Clauses, the data controller authorises the engagement of the following sub-processors:

NAME	CVR	ADDRESS	DESCRIPTION OF PROCESSING
Microsoft Azure		Nyverheidspln 21a, 3771 Barneveld, Nederlands	Hosting of data and programable and software infrastructure.

The data controller shall on the commencement of the Clauses authorise the use of the abovementioned sub-processors for the processing described for that party. The data processor shall not be entitled – without the data controller's explicit written authorisation – to engage a sub-processor for a 'different' processing than the one which has been agreed upon or have another sub-processor perform the described processing.

B.2. Prior notice for the authorisation of sub-processors

The data processor shall inform in writing the data controller of any intended changes concerning the addition or replacement of sub-processors at least 30 days in advance, thereby giving the data controller the opportunity to object to such changes prior to the engagement of the concerned sub-processor(s).

Appendix C Instruction pertaining to the use of personal data

C.1. The subject of/instruction for the processing

The data processor's processing of personal data on behalf of the data controller shall be carried out by the data processor performing the following:

- The processor's processing of personal data on behalf of the data controller is done by the processor providing software as a service (SAAS) BI solution. It consists of four base parts. TARGIT Cloud control panel, TARGIT Server stage, TARGIT Anywhere workers, TARGIT Data Discovery and TARGIT Datawarehouse. The processor is responsible for the operation, hosting, further development, and maintenance of the BI solution.
- The processor is instructed only to provide designated persons at the data controller access to the Cloud solution.

C.2. Security of processing

The level of security shall consider:

That the processing takes places as part of the BI solution provided and that confidential personal data can thus be processed, including potentially special categories of personal data.

The data processor is the entitled and obliged to make decisions about what technical and organizational security measures must be implemented to establish the necessary (and agreed) level of security.
However, the data processor must - in any case and as a minimum - implement the following measures, which have been agreed with the data controller:

Data flow and security

TARGIT Cloud is a software as a service (SAAS) BI solution. It consists of four base parts. TARGIT Cloud control panel, TARGIT Server stage, TARGIT Anywhere workers, TARGIT Data Discovery and TARGIT Datawarehouse.

<u>TARGIT Cloud control panel</u>

- TARGIT Cloud control panel is the TARGIT Server stage management web site.
- Users can create their own TARGIT Server stages and grant access by using an e-mail address.
- TARGIT Cloud control panel stores the following data in Cosmos DB:
    - Tenant name, which is normally company name
    - The customers TARGIT Cloud license for the TARGIT Server stage.
    - GUID for each user with access to the TARGIT Cloud tenant. It does not contain username or email.
- Data in Cosmos DB is only accessible by TARGIT Cloud Azure AD tenant admin users.
- Security is managed by Azure Active Directory B2C.
    - Users are only registered with an e-mail address and password.
    - Password cannot be read by TARGIT employees.

<u>TARGIT Server</u>

- The TARGIT Server stage stores server configuration data, all managed by the customer.
    - User logins and rights.

    - Passwords are not stored. Only a hash number is stored which makes the password unable to be restored.
    - Connection information for accessing the customers own hosted data.
    - Analysis and reports created by the customer. Analysis and reports do not contain data, but they can contain criteria (filters) added when creating the reports.
- All configuration files are stored on an Azure file share. Only TARGIT employees with TARGIT Cloud tenant admin rights have access to the fileshare.
- When requesting an analysis or report from the server, data is fetched from the customers data warehouse, then processed in memory and discarded after the analysis or report is sent to the customer.
- All communication between the client and TARGIT Server is SSL encrypted.
- The customer can grant specific TARGIT employees access to manage the TARGIT Server stage. This is typically done when a customer has requested the TARGIT consultants assistance to setup and configure their solution.

TARGIT Anywhere

- Data is not stored on the TARGIT Anywhere

TARGIT Data Discovery

- Data Discovery is a software as a service data processing tool, provided at subscription bases by the data processor.
- The data controller manages the data added to TARGIT Data Discovery.
- TARGIT employees will have audited access to data, specifically granted by the data controller.
- The data processor does not have any control over the data uploaded by the data controller, except the data processor can remove the subscription and any data uploaded.
- Data can be removed by the data controller at any given time.
- Any stored data will be deleted when the data controller cancel the subscription.
- Data communication between the data controller and TARGIT Data Discovery is encrypted.
- Data communication between TARGIT Data Discovery and TARGIT Server is encrypted.

TARGIT Datawarehouse

- The TARGIT Datawarehouse is a hosting option of the dw and population options for this DW (ETL tool)
- The data controller manages the data added to TARGIT Data Warehouse.
- TARGIT employees' will have audited access to data, specifically granted by the data controller.
- The data processor does not have any control over the data uploaded by the data controller, except the data processor can remove the subscription and any data uploaded.
- Data can be removed by the data controller at any given time.
- Any stored data will be deleted when the data controller cancel the subscription.
- Data communication between the data controller and TARGIT Data Warehouse is encrypted.
- Data communication between TARGIT Data Warehouse and TARGIT Server is encrypted.

Risk assessment

The data processor must carry out a risk assessment on an ongoing basis, and then implement appropriate technical and organizational measures to address identified risks.

Information security policy
The data processor must ensure that there is a management-approved information security policy.

Organization of information security
The data processor must ensure that there is a focus on information security in one's own organization with a defined division of roles and responsibilities.

In addition, the data processor's access to the data controller's data must be secured through contracts, declarations of confidentiality and ensuring functional separation to minimize errors and misuse of data.

Employee safety
The data processor must have established a process so that any person who performs work for the data processor and who has access to personal data covered by these Regulations knows their responsibility in relation to information security.

The Data Processor shall perform awareness training of any natural person who performs work for the Data Processor and who has access to personal data covered by these Provisions regarding their obligations and this training shall be maintained throughout the employment relationship.

The Data Processor shall ensure that any natural person performing work for the Data Processor and who has access to personal data covered by these Regulations only processes this personal data in accordance with the data controller's documented instructions unless other processing is required by EU or national law.

Access control
The data processor must have a documented access management process and ensure that access is granted solely based on a work-related need.
The data processor must have established procedures for the establishment, closure and ongoing review of allocated rights based on the principle of a work-related need as well as the decision on segregation of duties.
The data processor must have secure log-on procedures to minimize the potential for unauthorized access to systems and applications.

Cryptography
The data processor must ensure encryption with up-to-date encryption level when communicating over open networks and between systems and ensure that key management takes place after a documented process.

The data processor must, at the request of the data controller, provide a decrypted copy of all the stored data (which, however, do not include customer and user sensitive information). Upon disclosure, the storage of such data is considered to be the responsibility of the data controller.

Physical protection and environmental protection
The data processor must organize and establish physical protection of the data processor's physical locations, including against natural disasters, malicious attacks, or accidents.

The data processor must also ensure protection against unauthorized access to the data processor's physical locations via access control procedures.

Reliability

The data processor must ensure that operating procedures are documented and maintained. As a minimum, the following procedures must be included:

- Malware protection

C.3. Assistance to the data controller

The data processor shall insofar as this is possible – within the scope and the extent of the assistance specified below – assist the data controller in accordance with Clause 9.1. and 9.2. by implementing the following technical and organisational measures:

The data processor will

- keep personal data secure by implementing the security measures listed below;
- notify personal data breaches to the supervisory authority;
- notify personal data breaches to data subjects;
- carry out data protection impact assessments (DPIAs) when required;
- and consult the supervisory authority where a DPIA indicates there is a high risk that cannot be mitigated.

The data processor will implement and follow the following security measures:

- Workstations can only be accessed with individual username and password.
- There exist requirements for passwords and passwords must be changed on a regular basis. The user will be notified when the password must be changed.
- Remote access requires either VPN or Teamviewer.
- Processing activities are carried out in accordance with internal guidelines establishing the specific security requirements, including rules for authorisation, access administration and access control and logging of login attempts.

C.4. Storage period/erasure procedures

When the TARGIT server license expires, the customer will no longer have access to logon to the TARGIT Server with any clients. The server will enter a maintenance mode state where the customer can still manage the server e.g., delete users and connections.

The customer can at any given time request that any data stored in TARGIT Cloud is deleted.

C.5. Processing location

Data is only processed at the Microsoft Azure hosting center which at this moment is in the West Europe hosting center, which is physically located in the Netherlands. Regardless of which subcontractor Microsoft – or Targit - is utilizing, data is not stored outside Europe. Targit refers to Microsoft's terms of condition which state that Microsoft EU only store personal data within the EU.

When accessing Microsoft Customer support, it is the data processors responsibility to assure that customer data cannot be accessed or viewed outside EU.

C.6. Instruction on the transfer of personal data to third countries

The data controller hereby instructs the data processor in using Microsoft Cloud, which can include transfer of personal data to third countries via Microsoft's use of support functions in third countries.

If the data controller does not in the Clauses or subsequently provide documented instructions pertaining to the transfer of personal data to a third country, the data processor shall not be entitled within the framework of the Clauses to perform such transfer.

C.7. Procedures for the data controller's audits, including inspections, of the processing of personal data being performed by the data processor

Once a year, the data controller or the data controller's representative may request the data processor to answer specific control questions to ascertain the data processor's compliance with the GDPR, the applicable EU or Member State data protection provisions and the Clauses. Both the Data Controller's and the Data Processor's expenses in relation to the Data Controller's audit/supervision shall be solely borne by the Data Controller.

In addition the data controller may – once a year or when it is deemed required by the data controller - perform a physical inspection of the places, where the processing of personal data is carried out by the data processor, including physical facilities as well as systems used for and related to the processing to ascertain the data processor's compliance with the GDPR, the applicable EU or Member State data protection provisions and the Clauses.

The data controller's and the Data Processor's costs, if applicable, relating to physical inspection shall be defrayed by the data controller. The data processor shall, however, be under obligation to set aside the resources (mainly time) required for the data controller to be able to perform the inspection.

The Data Controller may, at the data controller's cost, require an auditors' statement from an independent third party, regarding the Data Processor's compliance with this Data Processing Agreement.

C.8. Procedures for audits, including inspections, of the processing of personal data being performed by sub-processors

The data controller may – if required – elect to initiate and participate in a physical inspection of the sub-processor. This may apply if the data controller deems that the data processor's supervision of the sub-processor has not provided the data controller with sufficient documentation to determine that the processing by the sub-processor is being performed according to the Clauses.

The data controller's participation in an inspection of the sub-processor shall not alter the fact that the data processor hereafter continues to bear the full responsibility for the sub-processor's compliance with the GDPR, the applicable EU or Member State data protection provisions and the Clauses.

The data processor's and the sub-processor's costs related to physical supervision/inspection at the sub-processor's facilities shall not concern the data controller – irrespective of whether the data controller has initiated and participated in such inspection.

Appendix D The parties' terms of agreement on other subjects

D.1. Liability

- The Data Processor and the Data Controller is responsible for its own acts and omissions that may cause or result in a financial loss or fine as a consequence of its insufficient compliance with its obligations under this DPA and the GDPR. The Data Processor are not liable for any incompliance or unlawful act by it if such act derives from instructions given by the Data Controller, or any act or omission of the Data Controller, provided that the Data Processor has fulfilled its obligations under Article 28 (3) of the GDPR.
- The regulation of breach, responsibility, and limitation on liability in the Parties General Agreement will apply to this DPA subsequently and as if this DPA was an integral part thereof. The Parties liability for all cumulated claims and damages that may arise under the duration of this DPA, is limited to the amount paid by the Data Controller over a three (3) month period to the Data Processor, based on the latest invoice issued to the Data Controller.