Version: DEC 2024_2

DATA PROCESSING AGREEMENT

This Data Processing Agreement, including its appendices, ("**DPA**") is made by the parties for the purposes of Article 28(3) of Regulation 2016/679 ("**the GDPR**"), and is applicable between TARGIT A/S, with company registration number 11562639, located at Gasværksvej 24, 2., 9000 Aalborg, Denmark as the **data processor**, and the TARGIT customer ("**Customer**"), as the **data controller.**

This DPA forms part of the agreement regarding the "Services" referred to in Section 1 below and applies per default for all personal data specified in Appendix A.

Customer is responsible for ensuring the adequacy of this DPA considering the personal data being processed through the Services and shall notify TARGIT in writing and take the necessary steps to agree to an addendum of this DPA with TARGIT, if the type or scope of the personal data being processed is not or is no longer adequately reflected herein.

1. DEFINITIONS

In addition to terms elsewhere defined in this DPA, the following terms shall be defined as set out below:

TERM	DEFINITIONS
Support Services	data processor's support services to data controller
Consultancy Services	data processor's consultancy services to data controller
TARGIT SaaS Solution	data processor's cloud-based software-as-a-service as subscribed to by data controller, if applicable.
TARGIT Software Solution	data processor's software licensed by data controller, if applicable.
TARGIT SaaS Add-on(s)	data processor's cloud-based software-as-a-service add-on to the TARGIT Software Solution, including TARGIT Insight (cf. Appendix A)
TARGIT Cloud Services	TARGIT SaaS Solution and TARGIT SaaS Add-on(s), collectively.
TARGIT Solution	TARGIT Software Solution and TARGIT Cloud Services, as applicable.
Services	Consultancy Services, Support Services, and TARGIT Cloud Services.

2. CONTEXT

1. For data controller's receipt or utilization of the Services, data controller has agreed to be subject to data processor's applicable terms and conditions for such Services (the **"Main Agreement"**), and to this DPA, which is incorporated into the Main Agreement by reference.

2. The terms and conditions of this DPA shall take priority over any similar provisions contained in any other terms and conditions applicable between the Parties in respect of the processing of personal data as part of the Services.

3. However, the DPA shall not otherwise extend data controller's rights to use and access the Services, nor data processor's obligations to provide the Services by any other means than as set out pursuant to the terms and conditions of the Main Agreement.

3. 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 the Services, 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.

4. 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.

5. 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.

6. 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.

7. 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.

8. 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.

9. 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.

10. 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.

11. 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.

12. 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.

13. 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.

14. 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.

15. 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.

APPENDIX A

INFORMATION ABOUT THE PROCESSING

A.1. Purpose
Data controller's utilization of the TARGIT Cloud Services and/or to enable data controller to receive and data processor to provide Support and/or Consultancy Services in relation to the applicable TARGIT Cloud Services or the TARGIT Software Solution.

A.2. Nature of processing
TARGIT Cloud Services
Data processor's processing of personal data on behalf of data controller shall mainly pertain to the hosting, storing, organisation, structuring of, and/or illustration of patterns in, Customer Data and the User Login Data.

TARGIT Cloud Services may include data processor's product TARGIT Insight, if opted for by data controller, and in such event, the TARGIT Cloud Services will process TARGIT Insight Data as well.

Support and/or Consultancy Services
For data processor to provide Support and/or Consultancy Services, data processor will gain access to all data, including personal data, stored on or through the applicable TARGIT Solution.

Support and/or Consultancy Services may be required by data controller for incident and problem management and for optimally utilizing the TARGIT Solution, including for structuring, organizing and/or generate data based on Customer Data and/or User Login Data stored in the TARGIT Solution and/or personal data stored in data controller's other systems to which the TARGIT Solution integrates.

A.3. Types of personal data
The following types of personal data will be processed by the data processor:

"User Login Data" meaning the data about a user registered by TARGIT for granting access/logging in to the TARGIT Solution, and comprising:
- Full name
- E-mail
- Phone number
- Address
- Employment information e.g. specific place and legal entity of employment, title, and department

"Customer Data" meaning the business relevant data stored on the TARGIT SaaS Solution or TARGIT Software Solution, and comprising:
- No personal data will be processed as part of Customer Data, unless otherwise agreed with TARGIT in an amendment or addendum hereto.

"TARGIT Insight Data" meaning data on the actual use of the TARGIT Solution, as applicable, by the data controller's registered users, and comprising:
- User Login Data on the registered users, if data controller uses the TARGIT Software Solution, and
- data on the actual use and patterns of use of the TARGIT Solution, as applicable, by a registered user.

A.4. Categories of data subjects

The data subjects will comprise:

- Employees, third-party consultants, owners, advisors, or other stakeholders of data controller.

A.5. Duration

see Section C.4 of Appendix C.

APPENDIX B

AUTHORISED SUB-PROCESSORS

B.1. Approved sub-processors
On the effective date of these Clauses, data controller authorises the engagement of the following sub-processors:

For the Services

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

For Support and Consultancy Services

NAME	CVR	ADDRESS	DESCRIPTION OF PROCESSING
Optimitas		Ivane Brlić Mažuranić 80D 10090 Zagreb Kroatien	Consultancy and support assistance
Yanchware	42380490	YanchWare Aps Mågevej 11 9640, Farsø Denmark YanchWare Italia Via A. M. Mazzei 21 95030, Nicolosi (CT)	Monitoring of Cloud Infrastructure (Cloud Operations)

As of the effective date of the Main Agreement the data controller authorises the use of the abovementioned sub-processors for the processing described for that party.

B.2. Prior notice for the authorisation of sub-processors
Cf. clause 8 of the DPA.

APPENDIX C

INSTRUCTION PERTAINING TO THE USE OF PERSONAL DATA

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

TARGIT Cloud Services

The data processor shall process the personal data as part of providing the TARGIT Cloud Services in accordance with the Main Agreement (cf. Clause 1), and subject to change from time-to-time.

Data processor is responsible for the operation, hosting, further development, maintenance, and performance, as applicable, of the TARGIT Cloud Services, and any processing of personal data in connection therewith.

Only designated persons of data controller, i.e. the registered users, shall have access thereto.

The designation of such persons shall be based on the instructions by data controller to data processor of the identity of such persons, from time to time.

Support and Consultancy Services

The data processor will be able to access any personal data stored in the TARGIT Solution, , when providing Support and/or Consultancy Services.

Unless necessary for performing the Support and/or Consultancy Services, the data processor will not download any data from the TARGIT Solution, and data processor shall not use the data other than for the purposes of performing its obligations under the Main Agreement and/or as instructed by the data controller from time to time.

C.2. Security of processing

TARGIT's technical and organizational measures in terms of security for protecting personal data processed under this DPA are specified in the TARGIT Security Specifications as available on https://www.targit.com/legal.

C.3. Assistance to the data controller

The data processor shall to the extent possible – and within the scope and the extent of the assistance specified below – assist the data controller in accordance with Clause 10.1 and 10.2 by implementing the following technical and organisational measures necessary to:

- respond to verified access requests by a data subject;
- 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.

C.4. Storage period/erasure procedures

Personal data will be subject to the following storage periods/erasure procedures:

For TARGIT Cloud Services

User Login Data

From the actual date of the User Login Data being registered in the TARGIT Cloud Services, through the duration of the Main Agreement and up to

- 30 days from the removal of a registered user's access to the TARGIT Cloud Services,
- 30 days from the termination or expiry of the Main Agreement

TARGIT Insight Data

If data controller has opted for TARGIT Insight

- 6 months from the registration of the data.
- Upon TARGIT Insight being disabled, the TARGIT Insight Data will become inaccessible and be automatically deleted after 6 months from the date of its storage, except in relation to User Login Data for the data controller using the TARGIT SaaS Solution, for which the storage period/erasure procedures set out above for User Login Data will apply.

Customer Data

From the actual date of the TARGIT Cloud Services being given access to the Customer Data, through the duration of the Main Agreement and up to up to 30 days after the termination or expiry thereof.

For Support and/or Consultancy Services

If for the performance of Support and/or Consultancy Services data processor downloads Customer Data, User Login Data or TARGIT Insight Data from

(a) the TARGIT SaaS Solution, such data will be deleted from data processor's systems as deemed necessary.
(b) the TARGIT Software Solution, such data will be deleted as soon as the relevant solution is implemented therein and approved by the data controller. Such data will be stored by data processor on a temporary virtual server.

Data controller shall explicitly notify TARGIT, if any such data is considered sensitive and/or otherwise requires urgent deletion. Upon data controller's request, data processor shall delete such data without undue delay. Data processor's execution of such deletion may be subject to additional charges.

C.5. Processing location

Processing of the personal data under these Clauses may be performed at the location of data processor at its address and the addresses of its sub-processors, and via remote access by data processor's or its sub-processors' employees.

Data processed by or through the TARGIT Cloud Services, including for avoidance of doubt TARGIT Insight, shall be processed at the Microsoft Azure hosting center which at this moment is in the West Europe hosting center physically located at the location set out in Appendix B. Regardless of which subcontractor Microsoft – or data processor – is utilizing, data is not stored outside Europe. Data processor refers to Microsoft's terms of condition which state that Microsoft EU only store personal data within the EU.

C.6. Instruction on the transfer of personal data to third countries
The data controller hereby instructs data processor in using the cloud computing and storage through Microsoft Azure and acknowledges and agrees that irrespective of the above this can entail the transfer of personal data to third countries via Microsoft's use of support functions in such third countries.

Except as stipulated immediately above or elsewhere in the Clauses, if data controller does not in the Clauses or subsequently give documented instructions on the transfer of personal data to a third country, data processor shall not be entitled 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
No more than once in a period of 12 (twelve) months may data controller 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.

Additionally, data controller may once a year or when it is deemed required by the data controller perform a physical inspection and audit of the places, where the processing of personal data is carried out by the data processor itself, 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 physical inspections and audits shall be carried out by IT auditors from reputed audit firms and subject to strict confidentiality in relation to all information which in data processor's opinion is business sensitive.

Data controller shall notify data processor in writing 45 (forty-five) days in advance of any inspection and/or audit and shall disclose the identity of the audit firm which will be used, and data processor may within 10 days of receipt of the notification object to the date and/or audit firm, such objection not to be unreasonable.

In the event of an objection by data processor, data controller shall find an alternative audit firm and/or date, as applicable, and notify data processor thereof.

Data processor shall make the resources available for data controller's auditors to be able to perform the inspection.

Data controller shall disclose the full report of its auditors with data processor, except for any information which is unrelated to data processor's processing of data under these Clauses.

Both the data controller's and the data processor's expenses and time used by data processor in connection with the data controller's audit/supervision shall be borne solely by the data controller at the data processor' standard hourly or daily rates.

C.8. Procedures for audits, including inspections, of the processing of personal data being performed by sub-processors
If data controller deems that data processor's supervision of the sub-processor has not provided data controller with sufficient documentation to determine that the processing by the sub-processor is being performed according to this DPA, data controller may, upon written notification to data processor, initiate and together with the data processor participate in a physical inspection

of the sub-processor, subject, however, to the same restrictions which data processor is subject to as per its agreement with the sub-processor, e.g. Microsoft's restrictions or instructions for auditing if the audit concerns facilities or resources controlled by Microsoft Azure. Data controller will not be permitted to perform an audit of the sub-processor without data processor being involved.

Any costs related to such physical supervision/inspection at the sub-processor's facilities shall be at the data controller's expense, including for the time used by data processor, by sub-processor and their agents or subcontractors, at the applicable hourly rates.

APPENDIX D

THE PARTIES' TERMS OF AGREEMENT ON OTHER SUBJECTS

D.1. Liability and Indemnity

Each of the data processor and the data controller are responsible for their 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 is 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.

This Appendix D supplements the provisions on liability and indemnification in the TARGIT Cloud GTC.

In the event that liability to pay any amounts to data subjects such as damages, compensation, indemnification, tort, etc., or to other relevant data subjects or third parties, has been imposed on the data processor due to violations of data protection legislation, the Clauses, privacy notices, instructions, etc., to the data processor, and the data controller is fully or partly responsible for such violation, the data controller shall indemnify the data processor with a proportionate share of the amount (including any related costs or fees) corresponding to the proportionate share of liability that is incumbent on the data controller.

If the data processor has been imposed to pay an administrative fine, fines, etc. to public authorities, the state treasury, labour court, etc. due to violation of data protection legislation, the Clauses, privacy notices, instructions to the data processor, etc., and the data controller is fully or partly responsible for such violation, the data controller shall indemnify the data processor with a proportionate share of the amount (and any related costs and fees) corresponding to the proportionate share of liability that is incumbent on the data controller.

The data controller shall take all steps necessary to defend any claim of infringement or alleged infringement of applicable data protection legislation.

D.2. Commercial Terms

Data processor's compliance with the requirements under these Clauses shall be at data processor's own cost, except that all obligations by data processor which are to be performed on data controller's request or the request by data subjects to data controller or to data processor shall be performed on a time and material basis, at data processor's standard hourly or daily rates, including as set out in a professional services agreement between the parties, if any.

In connection with an inspection and/or audit request by data controller, data processor shall on data controller's request provide an offer for data processor making available the relevant resources. Data processor's offer shall be based on (i) a reasonable estimate of time required by data processor, at its standard hourly or daily rates and (ii) data processor's documented costs with an addition of an overhead of 10%.

Data processor shall invoice its fees to data controller monthly in arrears with a payment term of 30 days.