Data Processor Agreement

Qarma Services

Version 2.2

between

Customer
[Stated in the Agreement between Customer and Qarma on the provision of Qarma service to Customer (hereinafter the "Agreement")]

(The Customer is hereinafter referred to as the "Controller")

and

Qarma ApS
Hermodsvej 5B, 3.
8230 Åbyhøj
Denmark

(Qarma ApS is hereinafter referred to as the "Processor")

Each of the Controller or Qarma can be referred to as a "Party", and together the "Parties".

Have agreed on the following clauses (hereinafter referred to as 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

1. Table of Contents 2
2. Preamble 3
3. The rights and obligations of the Controller 3
4. The Processor acts according to instructions 3
5. Confidentiality 4
6. Security of processing 4
7. Use of sub-processors 5
8. Transfer of data to third countries or international organisations 5
9. Assistance to the Controller 6
10. Notification of personal data breach 6
11. Erasure and return of data 7
12. Audit and inspection 7
13. The parties' agreement on other terms 7
14. Commencement and termination 7
15. Data controller and Processor contacts/contact points 8

Appendix A Information about the processing 9
Appendix B Authorised sub-processors 11
Appendix C Instruction pertaining to the use of personal data 13
Appendix D The parties' terms of agreement on other subjects 18
Appendix E Standard Contractual Clauses 19

2. PREAMBLE

1. These Clauses set out the rights and obligations of the Controller and the Processor, when processing personal data on behalf of the 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 Qarma services (which services are relevant, follow from the Agreement), the Processor will process personal data on behalf of the Controller in accordance with the Clauses.

4. The Clauses shall take priority over any similar provisions contained in other agreements between the Parties, except for the Standard Contractual Clauses in appendix E and thereto attached annexes.

5. Four appendices (A-D) are attached to the Clauses and form an integral part of the Clauses. As appendix E is attached the Standard Contractual Clauses for transfer of personal data to third countries.

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

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

8. Appendix C contains the Controller's instructions with regards to the processing of personal data, the minimum security measures to be implemented by the Processor and how audits of the 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. Appendix E contains Standard Contractual Clauses for the transfer of personal data to third countries regarding transfer of personal data to Qarma entities in China and Vietnam.

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

12. The Clauses shall not exempt the Processor from obligations to which the Processor is subject pursuant to the GDPR or other legislation.

3. THE RIGHTS AND OBLIGATIONS OF THE CONTROLLER

1. The 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 data protection provisions and the Clauses.

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

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

4. THE PROCESSOR ACTS ACCORDING TO INSTRUCTIONS

1. The Processor shall process personal data only on documented instructions from the 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 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 Processor shall immediately inform the Controller if instructions given by the Controller, in the opinion of the Processor, contravene the GDPR or the applicable EU or Member State data protection provisions.

3. If any subsequent instructions given by the Controller, obstructs or complicates the processing af personal data necessary for the Processor to perform its services to the Controller, either a) the Controller shall recall such instruction, b) the Controller shall cover any extra costs necessary, as determined by the Processor, for the Processor to provide its services and comply with such instruction, in such time as deemed necessary by the Processor, or c) the Processor shall be entitled to terminate the Agreement with the Controller regarding provision of its services to the Controller.

5. CONFIDENTIALITY

1. The Processor shall only grant access to the personal data being processed on behalf of the Controller to persons under the 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 such personal data shall consequently not be accessible anymore to those persons.

2. The Processor shall at the request of the Controller demonstrate that the concerned persons under the 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 Controller and Processor shall implement appropriate technical and organisational measures to ensure a level of security appropriate to the risk.

   The 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:

   - pseudonymisation and encryption of personal data;
   - the ability to ensure ongoing confidentiality, integrity, availability and resilience of processing systems and services;
   - the ability to restore the availability and access to personal data in a timely manner in the event of a physical or technical incident;
   - 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 Processor shall also – independently from the 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 Controller shall provide the Processor with all information necessary to identify and evaluate such risks.

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

   If subsequently – in the assessment of the Controller – mitigation of the identified risks require further measures to be implemented by the Processor, than those already implemented by the Processor

pursuant to Article 32 GDPR, the Controller shall specify these additional measures to be implemented in Appendix C.

7. USE OF SUB-PROCESSORS

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

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

3. The Processor has the Controller's general authorisation for the engagement of sub-processors. The Processor shall inform in writing the Controller of any intended changes concerning the addition or replacement of sub-processors at least 60 days in advance, thereby giving the Controller the opportunity to object to such changes prior to the engagement of the concerned sub-processor(s). See details on changes regarding sub-processors in Appendix B. The list of sub-processors already authorised by the Controller can be found in Appendix B.

4. Where the Processor engages a sub-processor for carrying out specific processing activities on behalf of the Controller, the same or similar 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 Processor shall therefore be responsible for requiring that the sub-processor at least complies with the obligations to which the 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 Controller's request – be submitted to the Controller, thereby giving the 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 Controller.

6. If the sub-processor does not fulfil his data protection obligations, the Processor shall remain fully liable to the 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 Controller and the 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 Processor shall only occur on the basis of documented instructions from the Controller and shall always take place in compliance with Chapter V GDPR.

2. In case transfers to third countries or international organisations, which the Processor has not been instructed to perform by the Controller, is required under EU or Member State law to which the Processor is subject, the Processor shall inform the 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 Controller, the Processor therefore cannot within the framework of the Clauses:

    a. transfer personal data to a Controller or a 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 by the Processor in a third country

4. The 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. For that reason, Standard Contractual Clauses for the transfer of personal data to third countries, are included in appendix E.

9. ASSISTANCE TO THE CONTROLLER

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

   This entails that the Processor shall, insofar as this is possible, assist the Controller in the 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 Processor's obligation to assist the Controller pursuant to Clause 6.3., the Processor shall furthermore, taking into account the nature of the processing and the information available to the Processor, assist the Controller in ensuring compliance with:

   a. The 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, unless the personal data breach is unlikely to result in a risk to the rights and freedoms of natural persons;
   b. the 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 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 Controller's obligation to consult the competent supervisory 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 Controller to mitigate the risk.

3. The parties shall define in Appendix C the appropriate technical and organisational measures by which the Processor is required to assist the 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 Processor shall, without undue delay after having become aware of it, notify the Controller of the personal data breach.

2. The Processor's notification to the Controller shall, take place within reasonable time after the Processor has become aware of the personal data breach to enable the Controller to comply with the

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 Processor shall assist the Controller in notifying the personal data breach to the competent supervisory authority, meaning that the Processor is required to assist in obtaining the information listed below which, pursuant to Article 33(3) GDPR, shall be stated in the 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 Processor when assisting the 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 Processor shall be under obligation to delete all personal data processed on behalf of the Controller and certify to the Controller that it has done so, or at the request of the Controller prior to the termination date, to return all the personal data to the Controller and delete existing copies unless Union or Member State law requires storage of the personal data. See also appendix C.4.

12. AUDIT AND INSPECTION

1. The Processor shall make available to the 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 Controller or another auditor mandated by the Controller.

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

3. The Processor shall be required to provide the supervisory authorities, which pursuant to applicable legislation have access to the Controller's and Processor's facilities, or representatives acting on behalf of such supervisory authorities, with access to the 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 of the Agreement between the parties to regarding the provision of Qarma services to the Controller, to which the Clauses are an integral part.

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 Controller pursuant to Clause 11.1. and Appendix C.4., the Clauses may be terminated by written notice by either Party.

15. DATA CONTROLLER AND PROCESSOR CONTACTS/CONTACT POINTS

1. The parties may contact each other using the contacts/contact points stated in the Agreement on the provision of Qarma Services to the Controller.

APPENDIX A INFORMATION ABOUT THE PROCESSING

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

For the Processor to provide its Qarma services to the Controller, cf. the Agreement between the Parties. The purpose being, depending on the services in the Agreement, to provide software solutions that supports the Controller in:

- Quality control and quality assurance of products
- Product compliance
- Supplier compliance

When using the Qarma services, the user records activities, information and documentation regarding products, the production of these and suppliers. Furthermore, data may be collected through integration to the it-systems of the Controller. Such recordings, information and documentation is then inspected, verified and approved by other of the Controller's employees, statistics may be calculated and reports may be made through the Qarma services.

Collected information on activities, information and documentation as well as reports are stored with Qarma services and made accessible to and shareable by the Controller.

The overall purpose of the processing of personal data within Qarma services is for the Controller to assign work to specific users, to follow up on such assignments and for the Controller to document which users have performed which collection of information and documentation.

Any use of the Qarma services is logged at the user-level.

Further, processing of personal data may be taking place, when Processor assist the Controller with setting up data integrations between the Qarma services and Controller's other systems and when providing support, training an maintenance services to the Controller in relation to the Qarma services.

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

The Controller's named and identified users, collecting information and documentation on the production, quality control, production or supplier compliance, through the Qarma services, which is web- and app-based. This collected information includes descriptions, documents, photo- and video-documentation, which may on occoasion show employees or other persons at the production facility, and which photos and videos may also include location information. The collected information may be used for statistical calculations and is integrated into reports made available to the Controller and stored with the Processor for the Controller to access such information and share the information within or outside its organisation.

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

- Name,
- Job-title,
- Contact information, including e-mail address,
- Place of employment,
- Documents (which may contain personal data)
- Photos (of work situations, which may on occasion show persons),
- Video (of work situations, which may on occasion show persons),
- Location data (if included in photos or video).

Generally no sensitive data is processed. In rare situations processed data may include sentive information as part of photo- or video documentation. It is however never intented to include such information in the documentation.

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

- Employees of Controller,
- Employees of Controller's subsidiaries,
- Employees of Controller's cooperation partners / suppliers.

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

The processing of personal data on behalf of the Controller shall continue for as long, as the Processor provides Qarma services to the Controller, as set out int the Agreement between the Parties.

APPENDIX B AUTHORISED SUB-PROCESSORS

B.1. Approved sub-processors

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

Amazon Web Services, EMEA Sarl One Burlington Rd, Dublin 4, D04 HH21, Ireland	Provides hosting services for Qarma Services, within the EU.
Qarma Việt Nam 94 Xuan Thuy, Thao Dien Ward Thu Duc City Ho Chi Minh City Vietnam	Provides development, setup of and maintenance of data integrations between Qarma services and Controller's systems and support, training and maintenance services to Controller, at request. Transfer of personal data is based on Standard Contractual Clauses, cf. appendix E.
Qarma (Shanghai) Co. ltd. 7th Floor, Tower 1, West Tianmu Road 128, Jing'an District, Shanghai China	Provides development, setup of and maintenance of data integrations between Qarma services and Controller's systems and support, training and maintenance services to Controller, at request. Transfer of personal data is based on Standard Contractual Clauses, cf. appendix E.
Tradeshift Belgium SA 6, Rue Louis de Geer BE-1348 Louvain-la-Neuve Belgium	Provides data integration services between Controller's systems and Qarma services. Data is processed in the EU, and transferred between Qarma services in the EU and the place of Controller's systems
Sumo Logic Inc. 855 Main Street Suite 100 Redwood City, CA 94063 USA	Provides logging services. Data is stored and processed in the EU.
Snowflake Inc. 106 E. Babcock Street, Suite 3A, Bozeman, MT 59715 USA	Provides data warehouse services. Data is stored and processed in the EU.
Omni Analytics Inc. 375 Alabama Street, Ste 350 San Francisco California 94110, USA	Provides data visualization services. Data is stored and processed in the EU.

The Controller shall on the commencement of the Clauses authorise the use of the abovementioned sub-processors for the processing described for that party. The Processor shall not be entitled – without the Controller's explicit written authorisation – to engage a sub-processor for other 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

If the Processor wish to engage further sub-processors, or change one or more of the listed sub-processors, the Processor shall provide the Controller, with a notice of this at least 60 days in advance. Any objection from the Controller to such new sub-processors, shall be in writing and shall be clearly motivated and shall be received by the Processor no later than 14 days after the date of the notification of change from the Processor. If the Processor cannot accept an objection received, the Processor shall be entitled to terminate the Agreement between the Parties, upon a 1 month notice, rendering the Data Processor Agreement terminated as well. The Processer shall be without any liability towards the Controller, in such situations, if the Processor chooses to terminate the Agreement with the Controller.

APPENDIX C INSTRUCTION PERTAINING TO THE USE OF PERSONAL DATA

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

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

Providing Qarma services to the Controller in accordance with the Agreement entered into between the Parties. This includes the following processing operations:

- Collecting data, including personal data, when entered into the Qarma service by the Controller or anyone given access by the Controller to the Qarma provided user interfaces.
- Assigning tasks to specific users, and reminding them thereof.
- Calculations based on the data collected by the Controller, for statistical and reporting purposes
- Reporting based on the the data, including personal data, collected by the Controller etc.
- Storing of collected data and reports
- Access to and sharing of the stored data, including personal data, to anyone give such access by the Controller

- Transferring data, including personal data, to any location, where anyone, who is granted access by the Controller to the Qarma services, resides.
- Transferring data, including personal data, to Qarma entities in Vietnam and China, if Controller or anyone who is granted access by the Controller to the Qarma services requests support or training, as well as when maintenance of the Qarma services is required.

C.2. Security of processing

The level of security shall take into account that the processing may involve a high number of non-sensitive/non-special category personal data. In rare instances the personal data being processed, may be of a sensitive nature.

The Processor shall be entitled to and under obligation to make decisions about the technical and organisational security measures that are to be applied to create the necessary level of personal data security. And is always entitled to make changes to the adopted security measures, provided the necessary level of data security is always complied with.

The Processor is, and shall continue to be, ISO 27001 certified. All organisational and technical controls from ISO 27001 are in place to protect personal data, including:

- Privileged access rights
- Protection against malware
- Management of technical vulnerabilities
- Data leakage prevention

The Processor shall further, as a minimum, implement the following measures which have been agreed with the Controller:

Login

- When Controller's users are logging in, username and password is always required. The Controller may choose to have MFA enabled in addition to username and password.
- Passwords shall consist of at least 8 characters, which is enforced by the Qarma system.
- Passwords can only be restored, through e-mail sent to the user's e-mail address. Qarma supports users having trouble resetting their password or have trouble accessing the service.
- Login by Processor requires use of username and password when login is performed from the Processors domains.
- Only relevant staff members of Processor have access to personal data, and proper training is ensured for all staff members having such access.

Encryption

- Any transfer of personal data, shall be encrypted
- Data at rest must be encrypted, with the exception of photos, videos, and documents.

Firewall

- All computers and servers in use by the Processor are behind updated firewalls or similar.

Logging and monitoring

- Any access to data, including personal data, by Controller's users and the Processor's employees, in the Qarma services is logged.
- Access logs are stored by the Processor for a period of 120 days from the access in question.
- Monitoring and incident reporting is carried out out by Processor. This includes detailed action plans created to rectify any issues and their root cause.

Backup and Disaster Recovery

- Processor has defined Recovery Time Objective and Recovery Point Objectives.
- All personal data processed is backed up. Point-in-time backups are on-site, and off-site backups are made daily and stored for 30 days.
- Restoring of backup and disaster recovery plans, including restore of backups, are maintained and tested on a regular basis.

Security policies

- Processor has security policies in place. These are continiously reviewed an controlled to protect data in Qarma's services.

C.3. Assistance to the Controller

The Processor shall insofar as this is possible – within the scope and the extent of the assistance specified below – assist the Controller in accordance with Clause 9.1. and 9.2. by providing the following:

The Processor shall assist the Controller with meeting its obligations in the Chapter III GDPR, in accordance with Clause 9.1. and 9.2., at the Controller's request, by providing the personnel resources necessary for such assistance in due and reasonable time, to the extent reasonably possible.

Taking into account the nature of the processing, the at the request of the Controller, Processor shall assist the Controller, insofar as this is possible, in the fulfilment of the Controller's obligations to respond to requests for exercising the data subject's rights laid down in Chapter III GDPR.

This entails that the Processor shall, insofar as this is possible, assist the Controller in the 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

If the Processor is contacted by a data subject intending to invoke one or more of its rights (a-j), the Processor shall, prior to providing the data subject with an answer, inform the Controller of the contact, and await instructions from the Controller on how to react to being contacted.

In addition to the Processor's obligation to assist the Controller pursuant to Clause 6.3., the Processor shall furthermore, taking into account the nature of the processing and the information available to the Processor, and at the Controller's request, assist the Controller in ensuring compliance with:

a. The 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, unless the personal data breach is unlikely to result in a risk to the rights and freedoms of natural persons;
b. the 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 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 Controller's obligation to consult the competent supervisory 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 Controller to mitigate the risk.

The Processor is entitled to invoice the Controller for any such assistance requested by the Controller, including for time spent, at the Processor's at any time standard hourly rate for such work, and costs.

C.4. Storage period/erasure procedures

Personal data being processed on behalf of the Controller, is stored for as lang as the Controller has an active Agreement regarding the provision of Qarma services. When the Agreement is terminated, for whatever reason, the stored data, including personal data is erased 30 days after such termination has come into effect, unless the Controller, prior to erasure of the data, in writing requests the Processor for a prolongated period of storage. The Processor may require a fee for such prolongation.

The Controller may at any time, up to and until such time where the stored data, including stored personal data is erased, delete its own data within Qarma services.

Further, the Controller may at any time, up to and until such time where the stored data, including stored personal data is erased, request the Processor to transfer all of the Controller's data to an internet resource provided by the Controller. The Processor may require a fee for such transfer of data.

Any logged use of the Qarma services, is stored by the Processor for a period of 120 days after the logged action having taken place. When the Agreement regarding the provision of Qarma services to the Controller is terminated, the last logged entry regarding the Controller's use of Qarma services, will be erased 120 days after the termination coming into effect. Such period may be prolonged, if the Controller request a prolongation of the storage period.

C.5. Processing location

Processing of the personal data under the Clauses cannot be performed at other locations than the following without the Controller's prior written authorisation:

Qarma ApS	Denmark
Qarma Việt Nam	Vietnam
Qarma (Shanghai) Co. ltd.	China
Amazon Web Services	EU
Tradeshift Belgium SA	EU
Sumo Logic Inc.	EU

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

If the Controller, as part of or based on the Agreement, obtains services from the Processer regarding setup, maintenance, support or training from the Processor, the Controller instructs the Processor to transfer personal data to Qarma (Shanghai) Co. ltd. and/or Qarma Việt Nam, by way of remote online access to the Controller's personal data stored with the Processor in the EU. Transfers of personal data, are in such instances based on Standard Contractual Clauses, cf. appendix E.

If the Controller makes use of the Qarma services from locations outside the EU/EEA, the Processor shall transfer relevant personal data being processed on behalf of the Controller to such location. Any such use by the Controller, shall be considered an instruction to the Processor for performing such transfer. The Controller is fully responsible for having ensured the legal basis for such transfers, if necessary.

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

If the Processor have had a general third-party audit made, the Controller shall at request be entitled to receive a copy of the conclusions of such report made by the third-party auditor. The Controller shall consider the copy of the report as confidential, and the Processer shall prior to providing the Controller with such copy, be entitled to strike out information in the report, which the Processor considers highly confidential and/or of no relevance for the Controller.

At the Controller's request, the Processor shall, no more than once a year, at the Controller's expense obtain an audit report from an independent third party auditor concerning the Processor's compliance with the GDPR, the applicable EU or Member State data protection provisions and the Clauses. The Parties have agreed that the audit report, in such cases, shall be of the type ISAE 3000 type 2. The Parties may agree on the scope and/or methodology of the report, within such boundaries. The audit report shall be submitted to the Controller, without undue delay, after having been performed within reasonable time after the Processor having received the request from the Controller.

Further, at the Controller's request and expense, the Controller or a fully independent representative, which shall be reasonably acceptable by the Processer, shall have access to inspect, including physically inspect, the place, where the Processor conducts processing of personal data on behalf of the Controller. Such inspection shall be performed no more than annually, on no less than 30 days written notice, and the Controller shall defray all costs related to the inspection, including the reasonable costs for the Processor's time spent.

Any audit or inspection related to sub-processors of the Processor, shall be conducted as described in C.8.

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

The Processor shall, whenever relevant, obtain copies of audit report, regarding the processing performed at it's sub-processors, if such reports are made available by the sub-processor. To the extent allowed, the Processor shall forward a copy of such report to the Controller, at the Controller's request.

The Processor shall, no more than once a year, at the Controllers request and expense assist the Controller, with obtaining an audit report made by an independent third party auditor, chosen by the Controller, regarding a sub-processor's compliance with the GDPR, the applicable EU or Member State data protection provisions and the Clauses. The Parties shall agree on the scope and/or methodology of the report, taking into consideration the opinion, requests and terms of the sub-processor. The audit shall be performed as soon as possible, after the Parties having agreed on the scope and/or methodology.

Further, at the Controller's request and expense, the Processor shall assist the Controller or a fully independent representative appointed by the Controller, which shall be reasonably acceptable by the Processer and the sub-processor, with obtaining access to inspect, including physically inspect, the place, where a sub-processor conducts processing of personal data on behalf of the Controller. Such inspection shall be performed no more

than annually, on no less than 60 days written notice, and the Controller shall defray all costs related to the inspection, including the reasonable costs for the Processor's and the sub-processor's time spent. The inspection shall take place taking the reasonable demands or terms of the sub-processor into consideration.

APPENDIX D THE PARTIES' TERMS OF AGREEMENT ON OTHER SUBJECTS

D.1. Liability

The Parties agree that the limitations of liability agreed between the Parties in the Agreement between the Parties shall also apply to any possible liability of the Processor/Data Exporter towards the Controller following from these Clauses or following from the Standard Contractual Clauses, cf. appendix E. The Parties further agree, that any liability of the two Data Importers; Qarma Việt Nam and Qarma (Shanghai) Co. ltd., following from the Standard Contractual Clauses, cf. appendix E, towards the Controller shall also be limited to the same extent.

APPENDIX E STANDARD CONTRACTUAL CLAUSES

Transfer processor to processor

Entered into between Qarma ApS (as Processor/Data Exporter) and Qarma (Shanghai) Co. ltd. and Qarma Việt Nam (as sub-processors/Data Importers)

Annex to the Commission implementing decision on Standard Contractual Clauses for the transfer of personal data to third countries pursuant to Regulation (EU) 2016/679 of the European Parliament and of the Council (GDPR).

Clause 1

Purpose and scope

(a) The purpose of these Standard Contractual Clauses is to ensure compliance with the requirements of Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data (General Data Protection Regulation) for the transfer of personal data to a third country.

(b) The Parties:

(i) the natural or legal person(s), public authority/ies, agency/ies or other body/ies (hereinafter "entity/ies") transferring the personal data, as listed in Annex I.A. (hereinafter each "Data Exporter"), and

(ii) the entity/ies in a third country receiving the personal data from the Data Exporter, directly or indirectly via another entity also Party to this SCC, as listed in Annex I.A. (hereinafter each "Data Importer")

have agreed to these Standard Contractual Clauses (hereinafter: "SCC").

(c) This SCC apply with respect to the transfer of personal data as specified in Annex I.B.

(d) The Appendix to this SCC containing the Annexes referred to therein forms an integral part of this SCC.

Clause 2

Effect and invariability of the SCC

(a) This SCC set out appropriate safeguards, including enforceable data subject rights and effective legal remedies, pursuant to Article 46(1) and Article 46 (2)(c) of Regulation (EU) 2016/679 and, with respect to data transfers from controllers to processors and/or processors to processors, Standard Contractual Clauses pursuant to Article 28(7) of Regulation (EU) 2016/679, provided they are not modified, except to select the appropriate Module(s) or to add or update information in the Appendix. This does not prevent the Parties from including the Standard Contractual Clauses laid down in this SCC in a wider contract and/or to add other clauses or additional safeguards, provided that they do not contradict, directly or indirectly, this SCC or prejudice the fundamental rights or freedoms of data subjects.

(b) This SCC are without prejudice to obligations to which the Data Exporter is subject by virtue of Regulation (EU) 2016/679.

Clause 3

Third-party beneficiaries

(a) Data subjects may invoke and enforce this SCC, as third-party beneficiaries, against the Data Exporter and/or Data Importer, with the following exceptions:

(i) Clause 1, Clause 2, Clause 3, Clause 6, Clause 7;

(ii) Clause 8 - Module One: Clause 8.5 (e) and Clause 8.9(b); Module Two: Clause 8.1(b), 8.9(a), (c), (d) and (e); Module Three: Clause 8.1(a), (c) and (d) and Clause 8.9(a), (c), (d), (e), (f) and (g); Module Four: Clause 8.1 (b) and Clause 8.3(b);

(iii) Clause 9 - Module Two: Clause 9(a), (c), (d) and (e); Module Three: Clause 9(a), (c), (d) and (e);

(iv) Clause 12 - Module One: Clause 12(a) and (d); Modules Two and Three: Clause 12(a), (d) and (f);

(v) Clause 13;

(vi) Clause 15.1(c), (d) and (e);

(vii) Clause 16(e);

(viii) Clause 18 - Modules One, Two and Three: Clause 18(a) and (b); Module Four: Clause 18.

(b) Paragraph (a) is without prejudice to rights of data subjects under Regulation (EU) 2016/679.

Clause 4

Interpretation

(a) Where this SCC use terms that are defined in Regulation (EU) 2016/679, those terms shall have the same meaning as in that Regulation.

(b) This SCC shall be read and interpreted in the light of the provisions of Regulation (EU) 2016/679.

(c) This SCC shall not be interpreted in a way that conflicts with rights and obligations provided for in Regulation (EU) 2016/679.

Clause 5

Hierarchy

In the event of a contradiction between this SCC and the provisions of related agreements between the Parties, existing at the time this SCC are agreed or entered into thereafter, this SCC shall prevail.

Clause 6

Description of the transfer(s)

The details of the transfer(s), and in particular the categories of personal data that are transferred and the purpose(s) for which they are transferred, are specified in Annex I.B.

Clause 7

Docking clause

(a) An entity that is not a Party to this SCC may, with the agreement of the Parties, accede to this SCC at any time, either as a Data Exporter or as a Data Importer, by completing the Appendix and signing Annex I.A.

(b) Once it has completed the Appendix and signed Annex I.A, the acceding entity shall become a Party to this SCC and have the rights and obligations of a Data Exporter or Data Importer in accordance with its designation in Annex I.A.

(c) The acceding entity shall have no rights or obligations arising under this SCC from the period prior to becoming a Party.

Clause 8

Data protection safeguards

The Data Exporter warrants that it has used reasonable efforts to determine that the Data Importer is able, through the implementation of appropriate technical and organisational measures, to satisfy its obligations under this SCC.

8.1 Instructions

(a) The Data Exporter has informed the Data Importer that it acts as processor under the instructions of its controller(s), which the Data Exporter shall make available to the Data Importer prior to processing.

(b) The Data Importer shall process the personal data only on documented instructions from the Controller, as communicated to the Data Importer by the Data Exporter, and any additional documented instructions from the Data Exporter. Such additional instructions shall not conflict with the instructions from the Controller. The controller or Data Exporter may give further documented instructions regarding the data processing throughout the duration of the contract.

(c) The Data Importer shall immediately inform the Data Exporter if it is unable to follow those instructions. Where the Data Importer is unable to follow the instructions from the Controller, the Data Exporter shall immediately notify the Controller.

(d) The Data Exporter warrants that it has imposed the same data protection obligations on the Data Importer as set out in the contract or other legal act under Union or Member State law between the Controller and the Data Exporter.

8.2 Purpose limitation

The Data Importer shall process the personal data only for the specific purpose(s) of the transfer, as set out in Annex I.B., unless on further instructions from the Controller, as communicated to the Data Importer by the Data Exporter, or from the Data Exporter.

8.3 Transparency

On request, the Data Exporter shall make a copy of this SCC, including the Appendix as completed by the Parties, available to the data subject free of charge. To the extent necessary to protect business secrets or other confidential information, including personal data, the Data Exporter may redact part of the text of the Appendix prior to sharing a copy, but shall provide a meaningful summary where the data subject would otherwise not be able to understand its content or exercise his/her rights. On request, the Parties shall provide the data subject with the reasons for the redactions, to the extent possible without revealing the redacted information.

8.4 Accuracy

If the Data Importer becomes aware that the personal data it has received is inaccurate, or has become outdated, it shall inform the Data Exporter without undue delay. In this case, the Data Importer shall cooperate with the Data Exporter to rectify or erase the data.

8.5 Duration of processing and erasure or return of data

Processing by the Data Importer shall only take place for the duration specified in Annex I.B. After the end of the provision of the processing services, the Data Importer shall, at the choice of the Data Exporter, delete all personal data processed on behalf of the Controller and certify to the Data Exporter that it has done so, or return to the Data Exporter all personal data processed on its behalf and delete existing copies. Until the data is deleted or returned, the Data Importer shall continue to ensure compliance with this SCC. In case of local laws applicable to the Data Importer that prohibit return or deletion of the personal data, the Data Importer warrants that it will continue to ensure compliance with this SCC and will only process it to the extent and for as long as required under that local law. This is without prejudice to Clause 14, in particular the requirement for the Data Importer under Clause 14(e) to notify the Data Exporter throughout the duration of the contract if it has reason to believe that it is or has become subject to laws or practices not in line with the requirements under Clause 14(a).

8.6 Security of processing

(a) The Data Importer and, during transmission, also the Data Exporter shall implement appropriate technical and organisational measures to ensure the security of the data, including protection against a breach of security leading to accidental or unlawful destruction, loss, alteration, unauthorised disclosure or access to that data (hereinafter "personal data breach"). In assessing the appropriate level of security, they shall take due account of the state of the art, the costs of implementation, the nature, scope, context and purpose(s) of processing and the risks involved in the processing for the data subject. The Parties shall in particular consider having recourse to encryption or pseudonymisation, including during transmission, where the purpose of processing can be fulfilled in that manner. In case of pseudonymisation, the additional information for attributing the personal data to a specific data subject shall, where possible, remain under the exclusive control of the Data Exporter or the Controller. In complying with its obligations under this paragraph, the Data Importer shall at least implement the technical and organisational measures specified in Annex II. The Data Importer shall carry out regular checks to ensure that these measures continue to provide an appropriate level of security.

(b) The Data Importer shall grant access to the data to members of its personnel only to the extent strictly necessary for the implementation, management and monitoring of the contract. It shall ensure that persons authorised to process the personal data have committed themselves to confidentiality or are under an appropriate statutory obligation of confidentiality.

(c) In the event of a personal data breach concerning personal data processed by the Data Importer under this SCC, the Data Importer shall take appropriate measures to address the breach, including measures to mitigate its adverse effects. The Data Importer shall also notify, without undue delay, the Data Exporter and, where appropriate and feasible, the Controller after having become aware of the breach. Such notification shall contain the details of a contact point where more information can be obtained, a description of the nature of the breach (including, where possible, categories and approximate number of data subjects and personal data records concerned), its likely consequences and the measures taken or proposed to address the data breach, including measures to mitigate its possible adverse effects. Where, and in so far as, it is not possible to provide all information at the same time, the initial notification shall contain the information then available and further information shall, as it becomes available, subsequently be provided without undue delay.

(d) The Data Importer shall cooperate with and assist the Data Exporter to enable the Data Exporter to comply with its obligations under Regulation (EU) 2016/679, in particular to notify its controller so that the latter may in turn notify the competent supervisory authority and the affected data subjects, taking into account the nature of processing and the information available to the Data Importer.

8.7 Sensitive data

Where the transfer involves personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade union membership, genetic data, or biometric data for the purpose of uniquely identifying a natural person, data concerning health or a person's sex life or sexual orientation, or data relating to criminal convictions and offences (hereinafter "sensitive data"), the Data Importer shall apply the specific restrictions and/or additional safeguards set out in Annex I.B.

8.8 Onward transfers

The Data Importer shall only disclose the personal data to a third party on documented instructions from the Controller, as communicated to the Data Importer by the Data Exporter. In addition, the data may only be disclosed to a third party located outside the European Union (in the same country as the Data Importer or in another third country, hereinafter "onward transfer") if the third party is or agrees to be bound by this SCC, under the appropriate Module, or if:

(i) the onward transfer is to a country benefitting from an adequacy decision pursuant to Article 45 of Regulation (EU) 2016/679 that covers the onward transfer;

(ii) the third party otherwise ensures appropriate safeguards pursuant to Articles 46 or 47 of Regulation (EU) 2016/679;

(iii) the onward transfer is necessary for the establishment, exercise or defence of legal claims in the context of specific administrative, regulatory or judicial proceedings; or

(iv) the onward transfer is necessary in order to protect the vital interests of the data subject or of another natural person.

Any onward transfer is subject to compliance by the Data Importer with all the other safeguards under these Clauses, in particular purpose limitation.

8.9 Documentation and compliance

(a) The Data Importer shall promptly and adequately deal with enquiries from the Data Exporter or the Controller that relate to the processing under this SCC.

(b) The Parties shall be able to demonstrate compliance with this SCC. In particular, the Data Importer shall keep appropriate documentation on the processing activities carried out on behalf of the Controller.

(c) The Data Importer shall make all information necessary to demonstrate compliance with the obligations set out in this SCC available to the Data Exporter, which shall provide it to the Controller.

(d) The Data Importer shall allow for and contribute to audits by the Data Exporter of the processing activities covered by this SCC, at reasonable intervals or if there are indications of non-compliance. The same shall apply where the Data Exporter requests an audit on instructions of the Controller. In deciding on an audit, the Data Exporter may take into account relevant certifications held by the Data Importer.

(e) Where the audit is carried out on the instructions of the Controller, the Data Exporter shall make the results available to the Controller.

(f) The Data Exporter may choose to conduct the audit by itself or mandate an independent auditor. Audits may include inspections at the premises or physical facilities of the Data Importer and shall, where appropriate, be carried out with reasonable notice.

(g) The Parties shall make the information referred to in paragraphs (b) and (c), including the results of any audits, available to the competent supervisory authority on request.

Clause 9

Use of sub-processors

(a) The Data Importer has the Controller's general authorisation for the engagement of sub-processor(s) from an agreed list. The Data Importer shall specifically inform the Controller in writing of any intended changes to that list through the addition or replacement of sub-processors at least 4 weeks in advance, thereby giving the Controller sufficient time to be able to object to such changes prior to the engagement of the sub-processor(s). The Data Importer shall provide the Controller with the information necessary to enable the Controller to exercise its right to object. The Data Importer shall inform the Data Exporter of the engagement of the sub-processor(s).

(b) Where the Data Importer engages a sub-processor to carry out specific processing activities (on behalf of the Controller), it shall do so by way of a written contract that provides for, in substance, the same data protection obligations as those binding the Data Importer under this SCC, including in terms of third-party beneficiary rights for data subjects. The Parties agree that, by complying with this Clause, the Data Importer fulfils its obligations under Clause 8.8. The Data Importer shall ensure that the sub-processor complies with the obligations to which the Data Importer is subject pursuant to this SCC.

(c) The Data Importer shall provide, at the Data Exporter's or controller's request, a copy of such a sub-processor agreement and any subsequent amendments. To the extent necessary to protect business secrets or other confidential information, including personal data, the Data Importer may redact the text of the agreement prior to sharing a copy.

(d) The Data Importer shall remain fully responsible to the Data Exporter for the performance of the sub-processor's obligations under its contract with the Data Importer. The Data Importer shall notify the Data Exporter of any failure by the sub-processor to fulfil its obligations under that contract.

(e) The Data Importer shall agree a third-party beneficiary clause with the sub-processor whereby - in the event the Data Importer has factually disappeared, ceased to exist in law or has become insolvent - the Data Exporter shall have the right to terminate the sub-processor contract and to instruct the sub-processor to erase or return the personal data.

Clause 10

Data subject rights

(a) The Data Importer shall promptly notify the Data Exporter and, where appropriate, the Controller of any request it has received from a data subject, without responding to that request unless it has been authorised to do so by the Controller.

(b) The Data Importer shall assist, where appropriate in cooperation with the Data Exporter, the Controller in fulfilling its obligations to respond to data subjects' requests for the exercise of their rights under Regulation (EU) 2016/679 or Regulation (EU) 2018/1725, as applicable. In this regard, the Parties shall set out in Annex II the appropriate technical and organisational measures, taking into account the nature of the processing, by which the assistance shall be provided, as well as the scope and the extent of the assistance required.

(c) In fulfilling its obligations under paragraphs (a) and (b), the Data Importer shall comply with the instructions from the Controller, as communicated by the Data Exporter.

Clause 11

Redress

(a) The Data Importer shall inform data subjects in a transparent and easily accessible format, through individual notice or on its website, of a contact point authorised to handle complaints. It shall deal promptly with any complaints it receives from a data subject.

(b) In case of a dispute between a data subject and one of the Parties as regards compliance with this SCC, that Party shall use its best efforts to resolve the issue amicably in a timely fashion. The Parties shall keep each other informed about such disputes and, where appropriate, cooperate in resolving them.

(c) Where the data subject invokes a third-party beneficiary right pursuant to Clause 3, the Data Importer shall accept the decision of the data subject to:

  (i) lodge a complaint with the supervisory authority in the Member State of his/her habitual residence or place of work, or the competent supervisory authority pursuant to Clause 13;

  (ii) refer the dispute to the competent courts within the meaning of Clause 18.

(d) The Parties accept that the data subject may be represented by a not-for-profit body, organisation or association under the conditions set out in Article 80(1) of Regulation (EU) 2016/679.

(e) The Data Importer shall abide by a decision that is binding under the applicable EU or Member State law.

(f) The Data Importer agrees that the choice made by the data subject will not prejudice his/her substantive and procedural rights to seek remedies in accordance with applicable laws.

Clause 12

Liability

(a) Each Party shall be liable to the other Party/ies for any damages it causes the other Party/ies by any breach of this SCC.

(b) The Data Importer shall be liable to the data subject, and the data subject shall be entitled to receive compensation, for any material or non-material damages the Data Importer or its sub-processor causes the data subject by breaching the third-party beneficiary rights under this SCC.

(c) Notwithstanding paragraph (b), the Data Exporter shall be liable to the data subject, and the data subject shall be entitled to receive compensation, for any material or non-material damages the Data Exporter or the Data Importer (or its sub-processor) causes the data subject by breaching the third-party beneficiary rights under this SCC. This is without prejudice to the liability of the Data Exporter and, where the Data Exporter is a processor acting on behalf of a controller, to the liability of the Controller under Regulation (EU) 2016/679 or Regulation (EU) 2018/1725, as applicable.

(d) The Parties agree that if the Data Exporter is held liable under paragraph (c) for damages caused by the Data Importer (or its sub-processor), it shall be entitled to claim back from the Data Importer that part of the compensation corresponding to the Data Importer's responsibility for the damage.

(e) Where more than one Party is responsible for any damage caused to the data subject as a result of a breach of this SCC, all responsible Parties shall be jointly and severally liable and the data subject is entitled to bring an action in court against any of these Parties.

(f) The Parties agree that if one Party is held liable under paragraph (e), it shall be entitled to claim back from the other Party/ies that part of the compensation corresponding to its / their responsibility for the damage.

(g) The Data Importer may not invoke the conduct of a sub-processor to avoid its own liability.

Clause 13

Supervision

(a) The supervisory authority with responsibility for ensuring compliance by the Data Exporter with Regulation (EU) 2016/679 as regards the data transfer, as indicated in Annex I.C, shall act as competent supervisory authority.

(b) The Data Importer agrees to submit itself to the jurisdiction of and cooperate with the competent supervisory authority in any procedures aimed at ensuring compliance with this SCC. In particular, the Data Importer agrees to respond to enquiries, submit to audits and comply with the measures adopted by the supervisory authority, including remedial and compensatory measures. It shall provide the supervisory authority with written confirmation that the necessary actions have been taken.

Clause 14

Local laws and practices affecting compliance with the SCC

(a) The Parties warrant that they have no reason to believe that the laws and practices in the third country of destination applicable to the processing of the personal data by the Data Importer, including any requirements to disclose personal data or measures authorising access by public authorities, prevent the Data Importer from fulfilling its obligations under this SCC. This is based on the understanding that laws and practices that respect the essence of the fundamental rights and freedoms and do not exceed what is necessary and proportionate in a democratic society to safeguard one of the objectives listed in Article 23(1) of Regulation (EU) 2016/679, are not in contradiction with this SCC.

(b) The Parties declare that in providing the warranty in paragraph (a), they have taken due account in particular of the following elements:

(i) the specific circumstances of the transfer, including the length of the processing chain, the number of actors involved and the transmission channels used; intended onward transfers; the type of recipient; the purpose of processing; the categories and format of the transferred personal data; the economic sector in which the transfer occurs; the storage location of the data transferred;

(ii) the laws and practices of the third country of destination– including those requiring the disclosure of data to public authorities or authorising access by such authorities – relevant in light of the specific circumstances of the transfer, and the applicable limitations and safeguards;

(iii) any relevant contractual, technical or organisational safeguards put in place to supplement the safeguards under this SCC, including measures applied during transmission and to the processing of the personal data in the country of destination.

(c) The Data Importer warrants that, in carrying out the assessment under paragraph (b), it has made its best efforts to provide the Data Exporter with relevant information and agrees that it will continue to cooperate with the Data Exporter in ensuring compliance with this SCC.

(d) The Parties agree to document the assessment under paragraph (b) and make it available to the competent supervisory authority on request.

(e) The Data Importer agrees to notify the Data Exporter promptly if, after having agreed to this SCC and for the duration of the contract, it has reason to believe that it is or has become subject to laws or practices not in line with the requirements under paragraph (a), including following a change in the laws of the third country or a measure (such as a disclosure request) indicating an application of such laws in practice that is not in line with the requirements in paragraph (a). The Data Exporter shall forward the notification to the Controller.

(f) Following a notification pursuant to paragraph (e), or if the Data Exporter otherwise has reason to believe that the Data Importer can no longer fulfil its obligations under this SCC, the Data Exporter shall promptly identify appropriate measures (e.g. technical or organisational measures to ensure security and confidentiality) to be adopted by the Data Exporter and/or Data Importer to address the situation, if appropriate in consultation with the Controller. The Data Exporter shall suspend the data transfer if it considers that no appropriate safeguards for such transfer can be ensured, or if instructed by the Controller or the competent supervisory authority to do so. In this case, the Data Exporter shall be entitled to terminate the contract, insofar as it concerns the processing of personal data under this SCC. If the contract involves more than two Parties, the Data Exporter may exercise this right to termination only with respect to the relevant Party, unless the Parties have agreed otherwise. Where the contract is terminated pursuant to this Clause, Clause 16(d) and (e) shall apply.

Clause 15

Obligations of the Data Importer in case of access by public authorities

15.1 Notification

(a) The Data Importer agrees to notify the Data Exporter and, where possible, the data subject promptly (if necessary with the help of the Data Exporter) if it:

(i) receives a legally binding request from a public authority, including judicial authorities, under the laws of the country of destination for the disclosure of personal data transferred pursuant to this SCC; such notification shall include information about the personal data requested, the requesting authority, the legal basis for the request and the response provided; or

(ii) becomes aware of any direct access by public authorities to personal data transferred pursuant to this SCC in accordance with the laws of the country of destination; such notification shall include all information available to the importer.

The Data Exporter shall forward the notification to the Controller.

(b) If the Data Importer is prohibited from notifying the Data Exporter and/or the data subject under the laws of the country of destination, the Data Importer agrees to use its best efforts to obtain a waiver of the prohibition, with a view to communicating as much information as possible, as soon as possible. The Data Importer agrees to document its best efforts in order to be able to demonstrate them on request of the Data Exporter.

(c) Where permissible under the laws of the country of destination, the Data Importer agrees to provide the Data Exporter, at regular intervals for the duration of the contract, with as much relevant information as possible on the requests received (in particular, number of requests, type of data requested, requesting authority/ies, whether requests have been challenged and the outcome of such challenges, etc.). The Data Exporter shall forward the information to the Controller.

(d) The Data Importer agrees to preserve the information pursuant to paragraphs (a) to (c) for the duration of the contract and make it available to the competent supervisory authority on request.

(e) Paragraphs (a) to (c) are without prejudice to the obligation of the Data Importer pursuant to Clause 14(e) and Clause 16 to inform the Data Exporter promptly where it is unable to comply with this SCC.

15.2 Review of legality and data minimisation

(a) The Data Importer agrees to review the legality of the request for disclosure, in particular whether it remains within the powers granted to the requesting public authority, and to challenge the request if, after careful assessment, it concludes that there are reasonable grounds to consider that the request is unlawful under the laws of the country of destination, applicable obligations under international law and principles of international comity. The Data Importer shall, under the same conditions, pursue possibilities of appeal. When challenging a request, the Data Importer shall seek interim measures with a view to suspending the effects of the request until the competent judicial authority has decided on its merits. It shall not disclose the personal data requested until required to do so under the applicable procedural rules. These requirements are without prejudice to the obligations of the Data Importer under Clause 14(e).

(b) The Data Importer agrees to document its legal assessment and any challenge to the request for disclosure and, to the extent permissible under the laws of the country of destination, make the documentation available to the Data Exporter. It shall also make it available to the competent supervisory authority on request. The Data Exporter shall make the assessment available to the Controller.

(c) The Data Importer agrees to provide the minimum amount of information permissible when responding to a request for disclosure, based on a reasonable interpretation of the request.

Clause 16

Non-compliance with the SCC and termination

(a) The Data Importer shall promptly inform the Data Exporter if it is unable to comply with this SCC, for whatever reason.

(b) In the event that the Data Importer is in breach of this SCC or unable to comply with this SCC, the Data Exporter shall suspend the transfer of personal data to the Data Importer until compliance is again ensured or the contract is terminated. This is without prejudice to Clause 14(f).

(c) The Data Exporter shall be entitled to terminate the contract, insofar as it concerns the processing of personal data under this SCC, where:

(i) the Data Exporter has suspended the transfer of personal data to the Data Importer pursuant to paragraph (b) and compliance with this SCC is not restored within a reasonable time and in any event within one month of suspension;

(ii) the Data Importer is in substantial or persistent breach of this SCC; or

(iii) the Data Importer fails to comply with a binding decision of a competent court or supervisory authority regarding its obligations under this SCC.

In these cases, it shall inform the competent supervisory authority [for Module Three: and the Controller] of such non-compliance. Where the contract involves more than two Parties, the Data Exporter may exercise this right to termination only with respect to the relevant Party, unless the Parties have agreed otherwise.

(d) Personal data that has been transferred prior to the termination of the contract pursuant to paragraph (c) shall at the choice of the Data Exporter immediately be returned to the Data Exporter or deleted in its entirety. The same shall apply to any copies of the data.] The Data Importer shall certify the deletion of the data to the Data Exporter. Until the data is deleted or returned, the Data Importer shall continue to ensure compliance with this SCC. In case of local laws applicable to the Data Importer that prohibit the return or deletion of the transferred personal data, the Data Importer warrants that it will continue to ensure compliance with this SCC and will only process the data to the extent and for as long as required under that local law.

(e) Either Party may revoke its agreement to be bound by this SCC where (i) the European Commission adopts a decision pursuant to Article 45(3) of Regulation (EU) 2016/679 that covers the transfer of

personal data to which this SCC apply; or (ii) Regulation (EU) 2016/679 becomes part of the legal framework of the country to which the personal data is transferred. This is without prejudice to other obligations applying to the processing in question under Regulation (EU) 2016/679.

Clause 17

Governing law

This SCC shall be governed by the laws of Denmark.

Clause 18

Choice of forum and jurisdiction

(a) Any dispute arising from this SCC shall be resolved by the courts of an EU Member State.

(b) The Parties agree that those shall be the courts of Denmark.

(c) A data subject may also bring legal proceedings against the Data Exporter and/or Data Importer before the courts of the Member State in which he/she has his/her habitual residence.

(d) The Parties agree to submit themselves to the jurisdiction of such courts.

ANNEXES

ANNEX I

A. LIST OF PARTIES

Data Exporter:

Qarma ApS

Hermodsvej 5B, 3.
8230 Åbyhøj
Denmark

Contact person: Søren Mønsted, smo@qarmainspect.com

Role: Data processor on behalf of Qarma customers.

Activities relevant to the data transferred under this SCC: Processing data of the Controller as part of providing the Qarma services.

Signature and date:

_____

Søren Riis Mønsted, Qarma ApS

6 April - 2023

Data importer(s):

1: Qarma Việt Nam

94 Xuan Thuy, Thao Dien Ward
Thu Duc City
Ho Chi Minh City
Vietnam

Contact person: Søren Mønsted, smo@qarmainspect.com

Role: Sub-processor of Qarma ApS.

Activities relevant to the data transferred under this SCC:

Qarma Việt Nam is providing:

- Development, setup of and maintenance of data integrations between Qarma services and Controller's systems,
- Support, training and maintenance services to Controller in relation to Qarma services provided to Controller

Qarma Việt Nam may gain online access to personal data within the Qarma services stored within the EU, when Data Exporter as a processor is to provide such services to Controller, at Controllers request.

Signature and date:

_____

Søren Mønsted, Qarma Việt Nam

6. april 2024

2: Qarma (Shanghai) Co. ltd.

Room 520, 5th floor
555 Wuding Road
Jing an District
Shanghai 2000041
China

Contact person: Søren Mønsted, smo@qarmainspect.com

Role: Sub-processor of Qarma ApS.

Activities relevant to the data transferred under this SCC:

Qarma (Shanghai) Co. ltd. is providing:

- Development, setup of and maintenance of data integrations between Qarma services and Controller's systems,
- Support, training and maintenance services to Controller in relation to Qarma services provided to Controller

Qarma (Shanghai) Co. ltd. may gain online access to personal data within the Qarma services stored within the EU, when Data Exporter as a processor is to provide such services to Controller, at Controllers request.

Signature and date:

_____

Søren Riis Mønsted, Qarma (Shanghai) Co. ltd.

6 April 2024

B. DESCRIPTION OF TRANSFER

Categories of data subjects whose personal data is transferred

Employees of Controller,
Employees of Controller's subsidiaries,
Employees of Controller's cooperation partners / suppliers,

Categories of personal data transferred

Name,
Job-title,
Contact information, including e-mail address,
Place of employment,
Documents (which may contain personal data),
Photos (of work situations, which may on occasion show persons),
Video (of work situations, which may on occasion show persons),
Location data (if included in photos or video).

Generally no sensitive data is tranferred. In rare situations transferred data may include sentive information as part of photo- or video documentation. It is however never intented to include such information in the documentation.

The frequency of the transfer (e.g. whether the data is transferred on a one-off or continuous basis).

Personal data is transferred continously – by way of online remote access to hosting facilities in the EU - when Qarma Việt Nam or Qarma (Shanghai) Co. ltd. is providing setup, support, training or maintenance services to the Controller (customer of Qarma ApS), where personal data, may be viewed or processed on a remote basis.

Nature of the processing

Personal data, stored with Qarma ApS' hosting provider in the EU, may be acceessed, viewed and edited – by way of online remote access - by employees of Qarma Việt Nam or Qarma (Shanghai) Co. ltd., when providing setup, support, training or maintenance services to Controller (customer of Qarma ApS).

Purpose(s) of the data transfer and further processing

The purposes of Qarma Việt Nam or Qarma (Shanghai) Co. ltd. accessing, viewing or editing of personal data is for such entities to provide setup, support, training and maintenance services in relation to the Qarma services, provided to the customer by Qarma ApS.

The period for which the personal data will be retained, or, if that is not possible, the criteria used to determine that period

Personal data is available to employees of Qarma Việt Nam Qarma (Shanghai) Co. ltd., only during such time, where the employees have online remote access to the the personal data, stored in the EU.

The personal data accessed by the employees of Qarma Việt Nam or Qarma (Shanghai) Co. ltd. is not to be copied, printed or saved locally in their respective countries.

Refer to Appendix C.4. for information as to when data, including personal data, being processed by the Processor/Data Exporter is erased.

C. COMPETENT SUPERVISORY AUTHORITY

The competent supervisory authority is (in accordance with Clause 13 of this SCC):

Datatilsynet (the Danish Data Protection Agency)

Carl Jacobsens Vej 35
DK-2500 Valby

Phone: 33 19 32 00
e-mail: dt@datatilsynet.dk

ANNEX II

TECHNICAL AND ORGANISATIONAL MEASURES INCLUDING TECHNICAL AND ORGANISATIONAL MEASURES TO ENSURE THE SECURITY OF THE DATA

See Appendix C.2. in the Data Processor Agreement between the Controller and Qarma ApS for a list of minimum security measures.

ANNEX III – LIST OF SUB-PROCESSORS

The Controller has authorised the use of the following sub-processors:

See Appendix B.1. in the Data Processor Agreement between the Controller and Qarma ApS.

The Data Importers do not use specific sub-processors, except for the sub-processors of the Processor/Data Exporter regarding the processing of the data of the Controller.