Gulagervej 3
4173 Fjenneslev, Denmark
Office: +45 8213 0060
info@global-tunnelling-experts.com
www.global-tunnelling-experts.com

Joint data controller agreement

Between

GTE NL
Global Tunnelling Experts B.V.
Registration no.24419447
P.O. Box 419
2900 AK Capelle aan den Ijssel
The Netherlands

and

GTE DK
Global Tunnelling Experts Danmark ApS
CVR no. 33356005
Gulagervej 3
DK-4173 Fjenneslev
Denmark

and

GTE UK
Global Tunnelling Experts UK Ltd.
Registration no. 06353379
Unit 2 Gordano Court
Serbert Close
Bristol – BS20 7FS
United Kingdom

and

GTE TR
Global Tunnelling Experts Turkey
Registration no. 67458-5
Maslak Mahallesi
Soğut Sokak Ağaoğlu 1453 Sitesi
A4 Blok Kat 12 Daire 86
Sarıyer / İstanbul
Turkey

and

GTE Q
Global Tunnelling Experts Qatar
Registration no. 69622
Global Tunnelling Experts Doha Contracting
LLC P.O box 16095 Mohajl House
29 Ali Bin Abi Talib Street
Doha Qatar

In the following jointly referred to as "**the Data Controllers**".

April 2019

1. Joint data controllers

1.1. This agreement lays down the distribution of responsibilities among the Data Controllers in connection with:

The parties being joint data controllers for all personal data in the shared CV and employee database BrowSen.

1.2. In addition to the Data Controllers' head offices, the Data Controllers have the following offices:

- GTE DK has one representative in Singapore and one in Spain
- GTE NL has an office in Germany situated at Im Heidenwinkel 5, D-77963 Schwanau.

The Data Controllers are at all times obliged to inform each other about the establishment of new offices, subsidiaries, etc., which means that personal data are transferred to new third countries under this agreement.

1.3. Article 26 of the General Data Protection Regulation (GDPR) states that where two or more data controllers jointly determine the purposes and means of processing, they are joint data controllers.

In the event of joint data controllers, the joint data controllers must in a transparent manner determine their respective responsibilities for compliance with the obligations under the GDPR, in particular as regards the exercising of the rights of the data subject and their respective duties to provide the information referred to in Articles 13 and 14, by means of an arrangement between them unless, and in so far as, the respective responsibilities of the data controllers are determined by Union or Member State law to which the data controllers are subject.

Pursuant to Article 26(2), the arrangement must duly reflect the respective roles and relationships of the joint data controllers *vis-à-vis* the data subjects. The essence of the arrangement must be made available to the data subjects.

Irrespective of the terms of the arrangement, the data subject may exercise his or her rights under the GDPR in respect of and against each of the data controllers.

The "internal" distribution of responsibilities in the joint data controller agreement does not prevent the supervisory authority from exercising its powers *vis-à-vis* each of the Data Controllers.

1.4. The Data Controllers agree that in connection with the shared use of the CV and employee database, they are joint data controllers. The assessment has taken into account that:

All relevant employees of the Data Controllers have access to and use the CV and employee database in connection with the delivery of the Data Controllers' services in the form of supply of staff to tunnel projects.

In connection with the Data Controllers' access to the CV and employee database, they have access to the data of all registered persons.

There are joint guidelines for the Data Controllers' use of the CV and employee database, including in the form of access restrictions for certain types of personal data.

1.5. This agreement has been drawn up to ensure that the Data Controllers can comply with the requirements relating to joint data controllers as laid down in Article 26 of the GDPR. The agreement determines the Data Controllers' respective responsibilities for compliance with the obligations under the GDPR, in particular as regards the exercising of the rights of the data subject and their respective duties to provide the information referred to in Articles 13 and 14.

2. General distribution of responsibilities

2.1. GTE DK has been designated as contact point for data subjects, always provided that data subjects can exercise their rights under the GDPR *vis-à-vis* each individual data controller.

2.2. The Data Controllers are each responsible for the data subjects with whom the individual Data Controller enters into an employment contract, including the responsibility

- to inform the data subject of the processing of personal data and the rights of the data subject;
- to ensure that the necessary authority exists for the processing of the registered data, including the obtaining of consent; and
- that data are erased when they are no longer necessary.

2.3. The Data Controller who obtains specific data from sources other than the data subject is responsible for informing the data subject accordingly.

3. Principles and authority to process data

3.1. The Data Controller who obtains specific data is responsible for ensuring that there is a valid legal ground for processing and for documenting this to both supervisory authorities and the data subject.

3.2. Each Data Controller is responsible for compliance with the principles for the processing of personal data, insofar as the rules apply to the individual Data Controller's areas of responsibilities according to this agreement.

4. Rights of the data subjects

4.1. Each Data Controller is responsible for ensuring the rights of the data subjects in accordance with the below provisions of the GDPR:

- duty of disclosure when collecting personal data from the data subject;
- duty of disclosure if personal data are not collected from the data subject;
- right of access by the data subject;
- right to rectification;
- right to erasure (the right to be forgotten);

- right to restriction of processing;
- notification obligation regarding rectification or erasure of personal data or restriction of processing;
- right to data portability (but not for public authorities); and
- right to object to processing.

4.2. If one of the Data Controllers receives a request or inquiry from a data subject regarding matters covered by another Data Controller's responsibilities, see above, the request is forwarded to such Data Controller without undue delay.

4.3. The parties are responsible for assisting each other to the extent this is relevant and necessary in order for both parties to comply with their obligations to the data subjects.

5. Security of processing and proof of compliance with the GDPR

5.1. Taking into account the nature, scope, context and purposes of processing as well as the risks of varying likelihood and severity for the rights and freedoms of natural persons, each Data Controller must implement appropriate technical and organisational measures to ensure and to be able to demonstrate that processing is performed in accordance with the GDPR. Those measures must be reviewed and updated where necessary (Article 24 of the GDPR). Common procedures will be prepared for the handling of security breaches, requests for access and compliance with the duty of disclosure.

5.2. Appropriate joint data protection policies are prepared, which each Data Controllers is responsible for implementing in its own company.

5.3. The Data Controllers are jointly responsible for compliance with the provision on data protection by design and by default in Article 25 of the GDPR.

5.4. Each Data Controller is responsible for compliance with the requirement for security of processing in Article 32 of the GDPR. This involves 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 Controllers must implement appropriate technical and organisational measures to ensure a level of security appropriate to the risk.

Consequently, each Data Controller must make (and be able to document) a risk assessment, and subsequently implement measures to mitigate the risks identified.

6. Use of data processors and sub-processors

6.1. The Data Controllers are entitled to use other data processors and/or sub-processors in connection with the joint processing.

6.2. If any data processors and/or sub-processors are used, each Data Controller is responsible for compliance with the requirements of Article 28 of the GDPR. The Data Controller is obliged, *inter alia*, to:

- use only data processors providing sufficient guarantees to implement appropriate technical and organisational measures in such a manner that processing will meet the requirements of the GDPR and ensure the protection of the rights of the data subject;
- ensure that a valid data processing agreement has been made between the Data Controllers and the data processor; and
- ensure that a valid sub-processing agreement has been made between the data processor and any sub-processor.

6.3. If a Data Controller uses data processors and/or sub-processors in connection with the joint processing other than BrowSen and Microsoft Office 365, the Data Controller in question must inform the other Data Controllers.

7. Standard Contractual Clauses

7.1. GTE TR and GTE Q are unsecure third countries. Therefore The Global Tunnelling Experts group shall conclude Standard Contractual Clauses adopted by the European Commission as a supplement to this agreement to ensure sufficiently protection of personal data shared with GTE TR and GTE Q.

7.2. If the United Kingdom leaves the EU, and if the United Kingdom has not been declared as adequate by the European Commission through an Adequate Decision, The Global Tunnelling Experts group shall as well conclude Standard Contractual Clauses adopted by the European Commission with the United Kingdom as a supplement to this agreement to ensure sufficiently protection of personal data shared with GTE UK.

8. Records

8.1. Each Data Controller is responsible for compliance with the requirement for records of processing activities in Article 30 of the GDPR. Each Data Controller prepares records of the processing activities, for which the parties are joint data controllers.

8.2. The Data Controllers inform each other about the contents of the above records.

8.3. On the basis of the contents of each other's records, the Data Controllers prepare their own records of the processing activities covered by the agreement.

9. Notification of a personal data breach to the supervisory authority

9.1. Each Data Controller is responsible for compliance with Article 33 of the GDPR on notification of a personal data breach to the supervisory authority.

9.2. The Data Controller with whom a personal data breach was committed or from whom the reason for the breach originates is responsible for notifying the personal data breach to the supervisory authority.

9.3. Immediately after having become aware of a personal data breach, the Data Controller must inform the other Data Controllers of the breach. The other Data Controllers must be kept informed of the process after the discovery of the personal data breach and will receive a copy of the notification to the supervisory authority.

9.4. If the reason for the breach is not immediately attributable to one of the Data Controllers, GTE DK is responsible for notifying the personal data breach to the supervisory authority.

10. Communication of a personal data breach to the data subject

10.1. Each Data Controller is responsible for compliance with Article 34 of the GDPR on communication of a personal data breach to the data subject.

10.2. If a personal data breach is likely to result in a high risk to the rights and freedoms of natural persons, the Data Controller with whom the personal data breach was committed, or from whom the reason for the breach originates is responsible for communicating the personal data breach to the data subjects affected.

10.3. If the reason for a personal data breach is not directly attributable to one of the Data Controllers, and the breach is likely to result in a high risk to the rights and freedoms of natural persons, GTE DK is responsible for communicating the personal data breach to data subjects affected.

11. Data protection impact assessment and prior consultation

11.1. Each Data Controller is responsible for compliance with the requirement in Article 35 of the GDPR on data protection impact assessment. Where a type of processing in particular using new technologies, and taking into account the nature, scope, context and purposes of the processing, is likely to result in a high risk to the rights and freedoms of natural persons, the Data Controllers must, prior to the processing, carry out an assessment of the impact of the envisaged processing operations on the protection of personal data.

11.2. Likewise, the Data Controllers are obliged to comply with the requirement in Article 36 of the GDPR on prior consultation of the supervisory authority when this is relevant.

12. Transfers of personal data to third countries or international organisations

12.1. The Data Controllers may decide that personal data can be transferred to third countries or international organisations.

12.2. The Data Controllers are responsible for compliance with the requirements in Chapter V of the GDPR if personal data are transferred to third countries or international organisations.

12.3. Each Data Controller is responsible for its own personal data transfers to third countries, including for ensuring that a legal basis for transfer exists and that Chapter V of the GDPR has been observed.

13. Complaints

13.1. Each Data Controller is responsible for the handling of any complaints from data subjects if the complaints relate to the infringement of provisions in the GDPR, for which the Data Controller is responsible according to this agreement.

13.2. If one of the Data Controllers receives a complaint which should rightfully be handled by one of the other Data Controllers, the complaint is forwarded to such Data Controller without undue delay.

13.3. If one of the Data Controllers receives a complaint, part of which should rightfully be handled by one or more of the other Data Controllers, such part is forwarded for reply by the Data Controller(s) without undue delay.

13.4. In connection with the forwarding of a complaint or part of a complaint to the other Data Controllers, the data subject must be notified about the essence of this agreement.

13.5. Generally, the Data Controllers inform each other about all complaints received.

14. Information of the other parties

14.1. The Data Controllers inform each other about matters of the essence to the joint processing and this agreement.

15. Commencement and termination

15.1. This agreement enters into force at the time of the parties' signing hereof.

15.2. The agreement is in force as long as the data concerned are processed, or until the agreement is replaced by a new agreement determining the distribution of responsibilities in connection with processing.

15.3. Signatures

On behalf of GTE NL

Date:

MD Claus Nielsen

Date:

MD Kevin Browning

On behalf of GTE DK

Date:

MD Claus Nielsen

On behalf of GTE UK

Date:

MD Kevin Browning

On behalf of GTE TR

Date:

MD Kevin Browning

On behalf of GTE Q

Date:

MD Kevin Browning