PTV GROUP
the mind of movement

AGREEMENT ON DATA PROCESSING PTV XSERVER INTERNET

Karlsruhe, 25/05/2018

Agreement on Data Processing

between

Company
Contact person
Address
E-mail
Telephone
Fax

- hereinafter referred to as the "Client" or “Controller”–

and

PTV Planung Transport Verkehr AG, Haid-und-Neu-Str. 15, 76131 Karlsruhe, Germany

- hereinafter referred to as "PTV", the "Contractor” or the “Processor" -

Contents

1 Basis of the contract

(1) The contracting parties have entered into a contract on the use of the service PTV xServer internet (the "***Service***") in compliance with PTV's Terms of Use (the "***License Agreement***"). Using the Service, the Client also has the option of collecting, processing and using the personal data of third parties. Pursuant to the Terms of Use of the Service, the Client is only entitled to do so with the consent of the affected third parties or if a statutory authorization exists.

(2) Notwithstanding the above, the collection, processing and/or use of personal data through the use of the Service is also permitted if the Client awards PTV a contract that complies with the legal requirements for data processing in accordance with Art.28 GDPR. The contract award becomes effective only if the Client fills out this document completely, signs and returns it to PTV, and PTV confirms this in writing.

(3) With the written confirmation of the contract at hand, the Client authorises PTV to process the personal data specified below to the extent regulated herein.

(4) At the same time, the Customer is permitted to use the Service in such a way as to import and manage personal data in compliance with the rules of the Terms of Use.

2 Definitions of Terms

(1) Under Article 4 (7) GDPR, the Controller is the role which, alone or jointly with other controllers, determines the purpose of processing personal data and the means used to do so.

(2) Under Article 4 (8) GDPR, the Processor is a natural or legal person, public authority, agency or other body which processes personal data on behalf of the Controller.

(3) Under Article 4 (1) GDPR, personal data is any information relating to an identified or identifiable natural person (referred to hereinafter as the "Data Subject"); an identifiable natural person is one who can be identified directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person.

(4) Personal data requiring particular protection is personal data under Article 9 GDPR, regarding the Data Subject's racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade union membership; personal data under Article 10 GDPR regarding criminal convictions and offences or related security measures, and genetic data under Article 4 (13) GDPR, biometric data under Article 4 (14) GDPR, data concerning health under Article 4 (15) GDPR and data on the sex life or sexual orientation of a natural person.

(5) Under Article 4 (2) GDPR, processing is any operation or set of operations which is performed on personal data or on sets of personal data, whether or not by automated means, such as collection, recording, organisation, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or

otherwise making available, alignment or combination, restriction, erasure or destruction.

3 Subject of the contract

(1) The subject of the contract is the provision of the Service. PTV thereby provides the Client with the technical ability to collect personal data with the help of the service, to store the data on the server infrastructure of the Service and to use the data. PTV does not take note of any of the data content of the Client, with the exception of circumstances set forth in the Data Privacy Statement (http://xserver.ptvgroup.com/index.php?id=966&L=0) of the Service. As the responsible person for the data, the Client is solely responsible for the legality of the data processing and for compliance with the applicable privacy laws.

(2) The duration of the contract corresponds to the term of the License Agreement.

(3) Scope, manner and purpose of the collection, processing and use of data

(4) Type of the client's affected personal data

(5) Affected persons

(6) This agreement does not apply to data in the sense of ss.2 and 3 of the Data Privacy Statement (http://xserver.ptvgroup.com/index.php?id=966&L=0), which PTV requires to provide or charge for the service. Only the provisions of the Data Privacy

Statement and the License Agreement and the relevant statutory provisions apply to such data.

(7) The data processing agreed through the contract shall be performed solely in a European Union member state or in another state which is party to the agreement on the European Economic Area.
Any storage in a third-party country requires prior permission from the Client and may only occur if the particular requirements under Article 44 et seq. of the GDPR are met.

4 Rights, obligations and instructions on the part of the Client

(1) The client is solely responsible for judging the lawfulness of the collection, processing and use of data as well as for upholding the rights of those affected.

(2) Any changes to the subject matter processed and any procedural changes must all be agreed upon and defined in writing.

(3) PTV is permitted to process the personal data of the Client only for the purpose of providing the Services stipulated in the License Agreement. The Client reserves a comprehensive right of direction for the type, scope and processing procedure of this personal data.

(4) Client instructions

a) Client instructions must be provided in writing. All instructions are to be kept together with this agreement by both the Client and PTV so that all relevant provisions are available at all times. PTV is entitled to postpone carrying out an instruction provided verbally until it is confirmed in writing by the Client.

b) People authorised to provide instructions on behalf of the Client:

_____

(Name, organisational unit, function, e-mail, telephone)

_____

(Name, organisational unit, function, e-mail, telephone)

Instruction recipients at PTV are:
Head of service support, IT, head of service support,
support.inter@xserver.ptvgroup.com

_____

(Name, organisational unit, function, e-mail)

c) If the contact person changes or is unavailable for an extended period of time, the contracting partner must be informed of the successor or substitute in writing immediately. If any instructions change, annul or amend the definitions set forth in s.2 of this agreement, the instructions are permitted only if a new definition is agreed accordingly.

(5) The Client is obliged to treat all knowledge of PTV's business secrets and data protection measures obtained within the scope of this contractual relationship as strictly confidential throughout the term of the License Agreement and beyond.

5 Obligations on the part of PTV

(1) PTV processes personal data exclusively within the scope of the agreements that have been reached and in accordance with the Client instructions. PTV must correct, delete or block personal data if the Client requests this in an instruction pursuant to s.4.4.

(2) PTV shall not use the data provided for data processing for any other purposes; in particular, PTV shall not use the data for its own purposes.

(3) PTV shall carry out the following controls with regard to technical and organisational measures in accordance with s.6 and compliance with the statutory provisions on data protection and with this contract.

(4) PTV will inform the Client immediately if an instruction provided by the Client, according to PTV, violates statutory provisions. PTV is entitled to postpone carrying out the relevant instruction until it has been changed by the Client's responsible person so that it complies with the statutory provisions.

(5) The client is entitled, after prior agreement and within the normal business hours, to check the compliance with the provisions on data protection, this agreement and the technical and organisational measures (see s.6; together, the ***"Data Privacy Provisions"***) to the extent necessary, or to have the compliance checked by a third party who is sworn to a professional duty of confidentiality (for example, lawyers or tax advisers), in particular by requesting information and accessing the stored data and data processing programs as well as carrying out other on-site tests. PTV shall – if necessary – cooperate appropriately in these tests.

(6) The Client will inform PTV immediately if the Client notices errors or irregularities in the course of such tests or through any other means.

(7) PTV shall delete at the end of the contract all documents, processing and usage results that have been created and databases containing the client's personal data that are in PTV's possession, or earlier on a respective request by the Client. If the Client requests such a deletion before the end of the contract, and if PTV is prevented, either in whole or in part, from continuing to fulfil the License Agreement due to the deletion, then PTV is released to this extent from its service obligations under the License Agreement. This shall not affect PTV's entitlement to the agreed remuneration.

6 Technical organisational protective measures put in place by the Contractor

(1) Before starting processing, the Contractor must document the implementation of the requisite technical and organisational measures laid out before the order was issued, particularly with regard to specific performance of the order, and hand this over to the Client for review. When they are accepted by the Client, the documented measures form the basis of the order. If the Client's review/audit results in a need for amendments, these should be implemented by mutual agreement.

(2) The Contractor should provide security as per Article 28 (3) (c), 32 GDPR, particularly in connection with Article 5 (1) and (2) GDPR. Overall, the measures to be agreed should cover data security measures and measures to ensure a level of protection appropriate to the risk, with regard to confidentiality, integrity, availability and system robustness. In doing so, 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, as per Article 32 (1) GDPR, should be taken into account [details in appendix 1].

(3) The technical and organisational measures are subject to technical progress and development. To this extent, the Contractor is permitted to implement adequate alternative measures. These must not fall below the level of security provided by the specified measures. Significant changes must be documented.

7 Quality assurance and other obligations of the Contractor

In addition to adherence to the regulations related to this order, the Contractor has legal obligations under Articles 28 to 33 GDPR; to this extent, it guarantees adherence to the following provisions in particular:

a) Written appointment of a data protection officer who performs their role in accordance with Articles 38 and 39 GDPR.
The Contractor's data protection officer is
Mr Thomas Heimhalt, DATENSCHUTZ *perfect* GbR,
Wilhelm-Kolb-Strasse 1a; D-76187 Karlsruhe, Germany
datenschutz@ptvgroup.com
.
The Client should be notified immediately if the data protection officer changes.

b) Ensuring confidentiality under Articles 28 (3) (2) (b), 29, 32 (4) GDPR. To perform the work, the Contractor shall only use employees who have an obligation of confidentiality and have been made aware of the data protection provisions relevant to them in advance. The Contractor and every person who works for the Contractor and has access to personal data may only process these data in accordance with the Client's instructions, including the permissions granted in this contract, unless they are legally obliged to carry out processing.

c) Implementation of and adherence to all technical and organisational measures required for this order, under Articles 28 (3) (2) (c), 32 GDPR [details in appendix 1].

d) The Client and the Contractor shall cooperate with the supervisory authority upon request, to assist in the fulfilment of its tasks.

e) Prompt notification to the Client about audits and measures conducted by the supervisory authority, insofar as these relate to this order. This shall also apply if a responsible authority carries out an investigation as part of administrative or criminal proceedings relating to the processing of personal data during order processing by the Contractor.

f) If the Client is subject to an audit by the supervisory authority, administrative or criminal proceedings, a liability claim from a data subject or a third party, or another claim in connection with order processing by the Contractor, the Contractor must make every effort to support the Client.

g) The Contractor shall regularly monitor its internal processes and the technical and organisational measures to guarantee that processing in its area of responsibility is consistent with the requirements of current data protection law and that the protection of the rights of the data subject is guaranteed.

h) Ability to provide evidence to the Client of the technical and organisational measures in place as part of its powers of inspection under item 9 of this agreement.

8 Use of subcontractors

(1) Subcontractor relationships within the meaning of this regulation should be understood to include services which directly relate to provision of the main service. They do not include ancillary services which the Contractor commissions e.g. as telecommunications services, post/transport services, maintenance and user services or the disposal of hardware and other measures to guarantee the confidentiality, availability, integrity and resilience of the hardware and software in data processing equipment. However, to guarantee data protection and the security of the Client's data, the Contractor is also obliged to put in place adequate and legally compliant contractual agreements and monitoring measures for outsourced ancillary services.

(2) The service is operated via the Azure platform. This platform is provided by Microsoft Ireland Operations Ltd., Carmenhall Road, Sandyford, Dublin 18, Ireland ("***Microsoft Ireland***"). PTV and Microsoft Ireland have reached an agreement on order data processing.

(3) The following rules apply to the commissioning of other subcontractors:

a) PTV (i) notifies the Client of the name and address of the subcontractor, (ii) carefully chooses the subcontractor, particularly based on the suitability of the technical and organisational measures taken by the contractor, and (iii) ensures through suitable contractual agreements that the provisions agreed

upon between the Client and PTV in this agreement also apply to the subcontractor.

b) The checks that PTV has to carry out must be agreed to in writing before data is forwarded to the subcontractor. Each check result must be documented.

c) In the contract with the subcontractor, the technical and organisational measures to be taken by the subcontractor and the obligations under this agreement must be defined in such a precise manner that the responsibilities of PTV and the subcontractor are clearly distinguishable from each other.

d) If several subcontractors are used, then this also applies to the responsibilities between these subcontractors.

9 Control rights of the Client

(1) The Client has the right to conduct checks in its interaction with the Contractor, or to have these performed by auditors (to be nominated) in individual cases. It has the right to satisfy itself that the Contractor is adhering to this agreement in its business activities through random checks, which should generally be pre-announced in good time.

(2) The Contractor ensures that the Client can satisfy itself that the Contractor is meeting its obligations under Article 28 GDPR. The Contractor undertakes to provide the Client with the necessary information on request and, in particular, to demonstrate the implementation of the technical and organisational measures.

(3) Such measures, which do not relate to the specific order, may be demonstrated using current testimonies, reports or excerpts from reports by independent authorities (e.g. auditors, inspectors, data protection officers, the IT security department, data protection auditors, quality auditors).

(4) The Contractor may claim remuneration for enabling audits to be carried out by the Client.

10 Notification in case of Contractor breaches

(1) The Contractor shall support the Client in adhering to the obligations in GDPR Articles 32 to 36 regarding the security of personal data, the obligation to report data breaches, data protection impact assessments and prior consultations. Among other things, this includes

a) guaranteeing an adequate level of protection through technical and organisational measures which consider the circumstances and purpose of the processing and the forecast likelihood and severity of any potential legal breach due to gaps in security and enable immediate identification of relevant breaches

b) the obligation to report breaches relating to personal data to the Client immediately

c) the obligation to keep a record of all categories of processing activity carried out on the Client's behalf, containing all information required under Article 30 (2) GDPR. The record should be made available to the Client on request

d) the obligation to support the Client in its obligation to notify the data subject and to promptly provide the Client with all relevant material in this connection

e) support to the Client in relation to its activity record and data protection impact assessment

f) support to the client in the context of prior consultations with the supervisory authority

(2) If the Client's data held by the Contractor is put at risk through seizure or confiscation, insolvency proceedings or similar, or other events or measures connected to third parties, the Contractor must inform the Client of this immediately, unless forbidden to do so by a court order or administrative order. In this connection, the Contractor shall immediately inform all competent authorities that the power to take decisions relating to the data lies solely with the Client as the "Controller" within the meaning of the GDPR.

(3) The Contractor can claim remuneration for support services which are not included in the Service Level Agreement or which are not due to misconduct on the part of the Contractor.

11 Queries and rights of data subjects

(1) The Contractor shall support the Client where possible in fulfilling its obligations under Articles 12 - 22 and 32 and 36 GDPR with appropriate technical and organisational measures.

(2) If a data subject approaches the Contractor directly to exercise their right to access, correct or delete his or her data, the Contractor shall not act independently, but shall instead immediately refer the data subject to the Client and await its instructions.

12 Deletion and restoration of personal data

(1) Copies or duplicates of the data shall not be created without the Client's knowledge. The exceptions to this are backup copies, if required to ensure correct data processing, and data which are required for adherence to statutory retention requirements.

(2) Once the contractually agreed work is complete, or earlier at the Client's request – when the Service Level Agreement has terminated, at the latest – the Contractor must hand over to the Client all documents which have entered its possession, the results of processing and use generated and databases connected to the order, or, with prior permission, destroy these in accordance with data protection legislation. The same

applies to test and scrap material. The record of deletion should be submitted on request.

(3) In accordance with relevant retention periods, the Contractor should retain documentation proving that the data was processed in compliance with the order and correctly after the agreement ends. If it is easier, the Contractor may hand this over to the Client when the agreement ends.

13 Liability

(1) The Client and Contractor are liable towards data subjects in accordance with the regulation in Article 82 GDPR.

(2) The parties exempt one another from liability if one party can prove that it is in no way responsible for the circumstance which caused damage to the data subject.

14 Impact on PTV's services

(1) If a service that PTV is contractually obliged to perform is made impossible or significantly more difficult due to an instruction from the Client, or if the Client requests the deletion of data before the end of the contract, and if PTV is partially or fully prevented from continuing to fulfil the service due to the deletion, then PTV is released to this extent from its service obligations under the License Agreement. This shall not affect PTV's entitlement to the agreed remuneration.

(2) If the effort required from PTV to fulfil the service increases due to an instruction from the Client, PTV can demand a corresponding adjustment of the agreed remuneration.

15 Final Provisions

(1) The parties agree that the objection of the rights of retention by the Contractor within the meaning of §273 of the German Civil Code in relation to the data to be processed and the associated storage media is excluded.

(2) Amendments and additions to this Agreement shall require the written form. This provision shall also apply to any waiver of this formal requirement. This shall not affect the priority of individual contractual agreements.

(3) Should any of the provisions of this agreement be or become fully or partly legally invalid or unfeasible, this shall not affect the validity of the remaining provisions.

(4) This agreement shall be governed by German law The exclusive place of jurisdiction shall be Karlsruhe.

Appendices:

Appendix 1 – the Contractor's technical and organisational measures

.

Karlsruhe, _____ (date)	Place, _____ (date)
PTV Planung Transport Verkehr AG	Company Client
_____	_____
First name, surname (in block capitals) Role	First name, surname Role
_____	_____
Signature PTV	Signature Client

Appendix 1 - General technical and organisational measures

To ensure adherence to the requirements for data processing security, technical and organisational measures are adopted as per Article 32 GDPR.

The measures taken should be appropriate for the type of personal data or data categories to be protected.

1 Confidentiality (Article 32 (1) (b) EU-GDPR)

Physical access control

No unauthorised access to data processing systems

Extract from the measures taken at PTV Planung Transport Verkehr AG:

- Guard service with direct link to the police
- Video monitoring of non-public areas (outside) and partially inside
- Building access with chip key
- Reception staffed during opening hours
- Locking system for sensitive work areas/rooms
- Access to server rooms only for authorised persons, special locking system

System access control

No unauthorised system use

Extract from the measures taken at PTV Planung Transport Verkehr AG:

- User ID query with password
- Password convention in use, drafted according to latest recommendations
- Password valid for a limited time
- Password generations
- Encryption of laptop hard drives

Data access control

No unauthorised reading, copying, changing or removal

Extract from the measures taken at PTV Planung Transport Verkehr AG:

- Authorisation and administration scheme in use
- User roles / group concept
- Access verification by protocol
- Requirement to lock workstations during breaks (screen saver)
- Password-protected screen savers, time-controlled activation

Separation control:

Separate processing of data serving different purposes

Extract from the measures taken at PTV Planung Transport Verkehr AG:

- Company data processed separately from the respective customer data

2 Integrity (Article 32 (1) (b) EU-GDPR)

Disclosure control

No unauthorised reading, copying, changing or removal during electronic transfer or transportation

Extract from the measures taken at PTV Planung Transport Verkehr AG:

- Use of VPNs
- Encryption of laptop hard drives

Input control

Identification of whether personal data have been entered in systems, changed or removed and if so, by whom

Extract from the measures taken at PTV Planung Transport Verkehr AG:

- Logging of all input in the central CRM and the other relevant programmes

3 Availability and resilience (Article 32 (1) (b) and (c) EU-GDPR)

Availability monitoring, fast recoverability

Protection against accidental or deliberate destruction or loss

Extract from the measures taken at PTV Planung Transport Verkehr AG:

- Daily to annual backup, additional backups and tested backups
- RAID hard disk storage
- Tested emergency plan
- Virus scanners and multistage firewalls
- Server room air conditioning, UPS, CO2 fire extinguishers, fire detectors
- Regular software updates
- Backups kept in purpose-made data safes.

4 Process for regular checking, assessment and evaluation (Article 32 (1) (d) EU-GDPR; Article 25 (1) EU-GDPR)

Job control

Measures which ensure that personal data processed on behalf of others are only processed strictly in compliance with the Client's instructions:

- Our employees are obliged to adhere to data protection legislation.

Data protection management

Jointly with the external data protection officer, a data protection management system (DPMS) is operated, showing all measures, processes, actions etc. The DPMS contains the main provisions of data protection legislation and a comprehensive structure to depict the data protection measures. The DPMS is maintained and updated on an ongoing basis.

Incident response management

An organisational and technical process to manage security incidents has been defined and implemented. This ensures both a standardised response and a process for handling identified and suspected security incidents/disruptions. This also includes standardised follow-up and monitoring as part of a continuous process of improvement.

Default settings which promote data protection (Article 25 (2) EU-GDPR)

Fundamentally, only data which are appropriate and necessary for business purposes are collected and processed. Automated data capture and processing procedures are designed such that only the required data are collected.