LOGISTIK IM FLUSS.

Contract processing agreement
(in accordance with Article 28 of the General Data Protection Regulation)

between

the **User** (as defined in the Main Agreement)

(hereinafter the **Client**)

and

TB Digital Services GmbH, Oskar-Schlemmer-Str. 19 - 21, 80807 Munich

(hereinafter the **Contractor**)
(the Client and the Contractor may hereinafter be individually referred to as a "**Party**" and collectively as the "**Parties**").

Preamble

(A) This contract processing agreement (the **Agreement**) applies to all activities in which the Contractor encounters personal data (as defined in paragraph 1.5 below) belonging to the Client, third-party providers or other data subjects in connection with the activities described in para. 2 deriving from the General Framework Conditions on Platform Use and any individual contracts for other services (the "**Main Agreement**").

(B) Under this Agreement, the Client acts as the data controller and the Contractor acts as the contract processor, under a contract processing agreement in accordance with Article 28 of the General Data Protection Regulation (as defined below).

The Parties therefore agree the following:

1 Definitions and interpretation

1.1 **"European law"** is the applicable law of the European Union, the applicable laws of the current Member States of the European Union and the applicable laws of any individual country that subsequently becomes a member of the European Union.

1.2 **"European Data Protection Law"** is the law of the European Union applicable to the processing of personal data (in particular, the General Data Protection Regulation), the applicable laws of the current Member States of the European Union concerning the processing of personal data (including the current version of the German Data Privacy Act), and the applicable laws of any country that subsequently becomes a Member State of the European Union, concerning the processing of personal information.

1.3 "**General Data Protection Regulation**" is DIRECTIVE 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).

1.4 "**German Data Privacy Act**" is the Data Protection Act of Germany.

1.5 "**Personal Data**" has the meaning defined in the German Data Privacy Act/in the General Data Protection Regulation.

2 Object of data processing / Client's obligations

2.1 This Agreement governs the Parties' obligations in connection with the processing of the Client's Personal Data by the Contractor within the scope of the Main Agreement in Annex 1.

2.2 The object and duration of the processing, the type and purpose of the processing, the type of Personal Data, the categories of the data subjects concerned and the obligations and rights of the data controller are stated in Annex 1 to this Agreement, and in the description of services in the Main Agreement.

2.3 The Client will remain the data controller as defined by the General Data Protection Regulation and guarantee that it will be permissible to process the Personal Data of the relevant parties (driver and other persons if necessary). In this respect, the Client will in particular fulfil the full scope of its information obligations and ensure that there is a basis in data protection law for processing the Personal Data (in order to conclude a works agreement, for example, with the processing restricted to the purposes of the employment relationship).

3 Contractor's obligations

3.1 The Contractor will process the Client's Personal Data exclusively for the purposes stipulated in Annex 1 and in the context of the Main Agreement and on behalf of the Client and according to the documented instructions in Annex 1 given by the Client; the Contractor will not process the Personal Data in this Agreement for any other purposes. This will not affect the processing outside of this Agreement for its own purposes, in accordance with paragraph 8.3.4 of the Main Agreement. No copies or duplicates of the Personal Data will be made without the knowledge of the Client. This excludes backup copies, if they are required to guarantee the proper processing of the data, and files that are necessary in order to comply with statutory retention obligations.

3.2 Upon completion of the contractual services, the Contractor will return all the Client's Personal Data and/or, at the discretion of the Client, will dispose of the data in accordance with the data protection laws, provided that this is not prevented by the statutory retention periods, and provided that the Contractor does not process the data for its own purposes unrelated to this Agreement under paragraph

8.3.4 of the Main Agreement. The same will apply to test and waste material. At the request of the Client, the complete deletion or return of the data is to be confirmed in writing, with the date of destruction or return also to be confirmed.

3.3 If required by the scope of services, the Contractor will assist the Client in satisfying data subjects' rights (of access, rectification, objection and erasure) as instructed by the Client.

3.4 The Contractor confirms that, in so far as required by law, it has appointed a company data protection officer (see Section 38 of the German Data Privacy Act, Article 37 of the General Data Protection Regulation).

3.5 The Contractor will immediately inform the Client of the results of any audits by the data protection authorities, to the extent that such audits relate to the processing of the Client's data. The Contractor will resolve any complaints within an appropriate period and will inform the Client.

3.6 The processing of data by the Contractor, and by a subcontractor approved by the Client, will only take place within the area of the Federal Republic of Germany, in a Member State of the European Union, or in another signatory state to the European Economic Area treaty. Any transfer of data to any other country ("**Third Country**") requires the Client's express prior consent and will only take place if the special conditions for the exporting of data to Third Countries have been met (see Article 40 ff. of the General Data Protection Regulation). The details stipulated in Annex 1, and any other contractual documents, are required in this regard.

3.7 The Contractor is required to inform the employees involved in carrying out the processing of the relevant data protection conditions, and require them to maintain data secrecy (see Article 28(3)(b) of the General Data Protection Regulation). Additionally, the Contractor is required to take appropriate steps to ensure that the employees in question only process Personal Data if instructed to do so by the Client.

3.8 The Contractor will monitor compliance with the data protection provisions of this Agreement, and with the Client's documented instructions, at regular intervals throughout the entire term of the Agreement. The results of these checks will be submitted to the Client on request, where such results are relevant for processing of the Client's data. The monitoring measures will be set out in a data protection policy, to be provided to the Client on request.

3.9 Considering the nature of the data processing, and where possible with appropriate technical and organisational measures, the Contractor will support the Client in fulfilling its duty to respond to queries about the exercise of rights of the data subjects as indicated in Chapter III of the General Data Protection Regulation. The Client will bear any costs incurred by the Contractor in this regard.

3.10 In consideration of the type of the data processing and the information made available to it, the Contractor will assist the Client in complying with the duties stipulated in Articles 32-36 of the General Data Protection Regulation.

4 Technical and organisational data security measures

4.1 The Contractor will take the appropriate technical and organisational measures to protect the data (see Article 32 of the General Data Protection Regulation). In particular, the Contractor is obligated to implement the contractually agreed technical and organisational measures as contained in Annex 2 to this Agreement. These measures are to be adapted by the Contractor during the contractual term, without impairing the level of protection. Any significant changes are to be agreed in writing.

4.2 The Contractor will prove to the Client, on request, that the technical and organisational measures have been carried out.

4.3 The Contractor is obligated to provide appropriate data processing records, on the basis of which the Client can prove that the data has been duly processed. The proof can also take the form of an approved certification procedure in accordance with Article 42 of the General Data Protection Regulation.

5 Subcontractors

5.1 The Contractor is hereby authorised to engage the subcontractor named in Annex 1.

5.2 The commissioning of additional subcontractors in general is hereby approved. However, the Contractor will inform the Client of any planned changes to the involvement or use of subcontractors; the Client may object to the planned changes. Any services that the Contractor obtains from third parties as ancillary contractual services are not to be construed as subcontracting arrangements for the purposes of this provision. This includes, for example, telecommunications services, cleaning, auditing and the destruction of data carriers. However, with regard even to such ancillary services provided by third parties, the Contractor will guarantee the protection and security of the Client's data by entering into appropriate, legally compliant contractual arrangements and by implementing control measures.

5.3 If the Contractor uses a subcontractor, the Contractor will ensure that the subcontractor is bound by the same data protection obligations as those that bind the Contractor under this Agreement, by means of either (i) a contract between the subcontractor and the Contractor or (ii) another legal instrument that is valid under European Data Protection Law. In this regard, the Contractor will ensure, in particular, that the subcontractor offers sufficient guarantees that the appropriate technical and organisational measures have been implemented in such a way that the Personal Data is processed in accordance with the requirements of the General Data Protection Regulation. At the written request of the Client, the Contractor will provide the Client with information about the significant contents of the Agreement, and

the implementation of obligations relevant to data protection within the subcontracting agreement, by giving the Client access to the relevant contractual documents if required. The commercial terms and conditions may be redacted by the Contractor. The Client is obligated to keep this information secret.

6 Right of audit

6.1 The Client has the right to audit or arrange for the auditing of compliance with the contractual obligations (including any instructions given), either itself or through an appropriate designated third party.

6.2 The Contractor will provide the Client with appropriate assistance during such audits. In particular, the Contractor will allow access to the data protection documents and will provide the necessary information.

6.3 If an audit shows that the Contractor and/or the data processing does not conform to the requirements of this Agreement and/or to European Data Protection Law, the Contractor will take all the necessary corrective measures to ensure compliance with the provisions of this Agreement and/or with European Data Protection Law.

6.4 Any costs incurred by the Client in carrying out an audit will be borne by the Client itself. The costs incurred by the Contractor as a result of the Client carrying out an audit may be reclaimed from the Client, if the Client carries out or allows the carrying out of more than one audit per calendar year.

6.5 Audits of the Contractor are to be announced in good time and must not cause excessive disturbance to the Contractor's business operations.

7 Duty to inform

The Contractor will report to the Client immediately if, in the Contractor's opinion, an instruction given by the Client breaches European Data Protection Law. Any instruction queried with good reason does not need to be followed, unless it is changed or expressly confirmed by the Client. The Contractor is not obligated to carry out a check as to the legal substance of the instructions.

If the Contractor detects any errors or irregularities in the data processing, or if there is a suspicion of a data protection breach (an "**Incident**"), the Contractor is required to inform the Client as appropriate, without delay. The Contractor is required to document the Incident, including all details of the circumstances and effects of the Incident and all measures required to remedy the situation; at the request of the Client, this documented information is to be submitted to the Client immediately, in writing or electronically.

8 Liability and indemnity

8.1 The Contractor will be liable for any loss or damage that is attributable to intentional acts and/or gross negligence on the part of the Contractor or its vicarious agents. The Contractor will only be liable for loss or damage resulting from ordinary negligence by the Contractor or its vicarious agents if a cardinal obligation has been breached. Cardinal obligations are essential contractual obligations that ensure due implementation of the contract and the observance of which the Client has relied upon and was entitled to do so. In the event of a breach of these cardinal obligations caused by ordinary negligence, the Contractor's liability will be limited to typically foreseeable loss or damage.

8.2 The Client will indemnify the Contractor in respect of any claims by third parties (including data subjects and/or data protection authorities), losses or expenses that may be based on the Client's breach of the provisions of this Agreement and/or of European Data Protection Law; this will not apply if the Client did not cause the breach or if the Contractor contributed to it.

9 Term

The term of this Agreement corresponds to the term of the Main Agreement. This Agreement will end automatically upon termination of the Main Agreement for whatever reason. This will not affect the possibility of terminating the Agreement for good cause.

10 Miscellaneous

10.1 The Contractor's services under this Agreement are fully remunerated by the consideration stipulated in the Main Agreement.

10.2 If the Client's Personal Data is put at risk by the Contractor because of measures by a third party (including seizure or confiscation), or because of insolvency or composition proceedings or other similar events, the Contractor will inform the Client immediately.

10.3 If individual provisions of this Agreement are or become ineffective, the effectiveness of the remaining provisions will not be affected. In the event that a clause is ineffective, the Parties agree to replace it with a clause whose technical and financial content reflects the original purpose of the Agreement.

10.4 In the event that the United Kingdom leaves the European Union, the Contractor hereby agrees to enter into any agreements and undertake any actions that may be necessary in order to render the contractual data processing in the United Kingdom compliant with the data protection laws at the time of the exit. If no positive adequacy decision has been made by the European Commission at the point at which the United Kingdom leaves the European Union, from today's perspective this will in particular be the standard data protection clauses according to Article 46(2)(c) for the transmission of personal data to contract processors based in Third Countries in which no adequate level of protection is guaranteed.

If the Contractor does not fulfil its obligations, the Client is entitled, with effect from the date of the United Kingdom's exit from the European Union, to require of the Contractor that the services be carried out by an affiliated company or company division permanently based within the European Union area, without any additional expense or cost being incurred by the Client in that regard.

10.5 This contract processing agreement is available in 18 language versions. The original German version will have priority in the event of any discrepancies.

10.6 This Agreement is subject to the law of the Federal Republic of Germany to the exclusion of the UN Convention on Contracts for the International Sale of Goods. The exclusive place of jurisdiction is Munich, Germany.

10.7 The following Annexes form an integral part of this Agreement:

Annex 1 – Description of contract processing
Annex 2 – Technical and organisational measures

ANNEX 1 – Description of contract processing

1 Main Agreement

The Main Agreement as defined in paragraph 2.1 of this Agreement is the "General Framework Conditions on Platform Use".

Title / Parties: **TB Digital Services GmbH**, Oskar-Schlemmer-Str. 19-21, 80807 Munich / **User**

2 Object and duration

The object of the Agreement is stated in paragraph 1 (*Object*) and paragraph 8 (*User's Data and Data Protection*) of the Main Agreement; the duration of the Agreement is stated in paragraph 7 (*Formation of contract, contract term and termination rights*) of the Main Agreement.

3 Scope, type and purpose of data processing/data processing measures

The scope, type and purpose of the processing of the Personal Data is described in paragraph 8 of the Main Agreement.

Detailed description of the object of the Agreement with regard to the scope, type and purpose:

In order for the services offered by the Contractor (as defined in the Main Agreement) to be fulfilled, the Contractor must obtain the Client's Personal Data via connected vehicles or mobile devices (and if necessary Personal Data transferred from a third-party provider with whom the User has agreed third-party services), to the extent required for the fulfilment of the services, transfer that information to the Contractor's platform and store it there. The Contractor will process the data stored on the platform, to the extent necessary to fulfil the services (for instance, in order to analyse and evaluate handling or the use of the connected vehicle or mobile device, based on the Personal Data, and to propose customised offers to the Client based on that information, such as driver training, equipment specifications or recommendations on efficiency improvements). More precise information about the scope, type and purpose can be obtained from the additional individual contracts to be concluded.

4 Data subjects (categories of data subject)

The data processing affects the following categories of data subject:

- **Drivers and other employees** (employees of the Client's company) e.g. staff, trainees, applicants and former employees;
- **Drivers** who are not employees;
- **Contacts** from loading/unloading agents or other business partners of the Client; and
- **Group employees** (employees of other companies in the Client's group).

5 Type of Personal Data

The data processing includes the following types of Personal Data:

- Driver's name and driver ID number;
- Vehicle identification number;
- Location data;
- Driving time and rest time data;
- Handling data;
- Connected vehicle status data;
- Trailer status data;
- Data on the status of structures, assemblies, aggregates and other vehicle components;
- Data on the status of any other connected IOT devices
- Mobile device status data;
- Load data;
- Job data; and
- Contact details for loading/unloading agents or other business partners of the Client.

6 Documented instructions

The Client hereby informs the Contractor that the Personal Data will be processed in accordance with paragraph 8 of the Main Agreement. This includes, in particular, the following data processing:

- The Personal Data will be transferred via the connected vehicle or mobile device to the Contractor's cloud-based platform, where it will be stored.
- The Personal Data will only be processed under this Agreement to the extent necessary to fulfil the Main Agreement; this will not affect paragraph 8.3.4 of the Main Agreement.
- The Contractor will transfer the Personal Data to a third-party provider (as defined in the Main Agreement) to the extent that this is necessary in order for the third-party service (as defined in the Main Agreement) to be provided to the Client.
- The Contractor will analyse and evaluate the handling and the use of the connected vehicles based on the Personal Data, and will propose customised offers to the Client based on that information, such as driver training, equipment specifications or recommendations on efficiency improvements.

7 Place of processing

- Germany.
- United Kingdom; if data is processed for IT hosting and/or IT support purposes within the European Union, the corresponding contract processing agreements will be entered into.

- If the Contractor uses subcontractors for IT hosting and/or IT support purposes from outside the European Union (see paragraph 8 of this Annex 1), the Personal Data will be forwarded on the basis of standard contractual terms/data protection clauses concluded between the Contractor and the subcontractor for the purpose of transferring Personal Data to contract processors in Third Countries in accordance with Article 46(2)(c) of the General Data Protection Regulation.

8 Subcontractors

The Contractor will use the following subcontractors (who may use further subcontractors if necessary):

No.	Subcontractor (company name, address, contact person)	Categories of processed data	Processing stages/Purpose of the subcontracted data processing
1	Salesforce.com EMEA Limited Salesforce.com Privacy, The Landmark @ One Market Street, Suite 300, San Francisco, CA 94105, USA	All Personal Data on the platform that has to do with the sales area (i.e. where a customer can register on the platform and place orders)	Platform Hosting
2	Salesforce.com, Inc., Privacy, The Landmark @ One Market Street, Suite 300, San Francisco, CA 94105, USA	All Personal Data on the platform that has to do with the sales area (i.e. where a customer can register on the platform and place orders)	IT Support regarding the Platform
3	Amazon Web Services, Inc., Amazon Web Services, Inc. 410 Terry Avenue North Seattle WA 98109 USA https://aws.amazon.com/de/compliance/contact/	All other Personal User Data transmitted to the Contractor via the vehicle	Platform Hosting / IT Support regarding Platform Hosting
4	If necessary, in the future instead of no. 3: Amazon Web Services (EU) Amazon Web Services, Inc. P.O. Box 81226 Seattle, WA 98108-1226 USA https://aws.amazon.com/de/compliance/contact/	All other Personal User Data transmitted to the Contractor via the vehicle	Platform Hosting
5	MAN Service und Support GmbH Dachauer Strasse 667	All Personal Data required for the processing of customer queries (1st	1st Level Support

	80995 Munich Germany	and 2nd level support)	
6	Zuora Inc. 3050 S. Delaware Street, Suite 301 San Mateo, CA 94403 USA	All Personal Data required for the processing of invoices/order processing	Platform Hosting (EU Tenant – Hosted by Amazon Web Services (EU) – see para. 4
7	MAN Truck & Bus AG Dachauer Str. 667 80995 Munich Germany	All other Personal User Data transmitted to the Contractor via the connected vehicle and/or mobile device	Platform Hosting
8	T-Systems International GmbH Hahnstraße 43 d 60528 Frankfurt am Main Germany	All other Personal User Data transmitted via the TBM1/2 vehicle to the Contractor	Platform Hosting
9	Scania AB Vagnmakarvägen 1 15187 Södertälje Sweden	All other Personal User Data transmitted to the Contractor via the vehicle	Platform Hosting
10	Volkswagen Nutzfahrzeuge Mecklenheidestr. 74 30419 Hannover Germany	All other Personal User Data transmitted to the Contractor via the vehicle	Platform Hosting

ANNEX 2 – Technical and organisational measures

The technical and organisational measures to be taken by the Contractor in order to guarantee an appropriate level of risk protection are described in the data protection concept on the RIO platform. They include, in particular:

1. Pseudonymisation

If the Personal Data is used for evaluation purposes which can also be fulfilled with pseudonymised data, then pseudonymisation techniques will be used. For each data field, it will be pre-defined whether pseudonymisation needs to be used or not, in order to avoid it being traced back to a particular person. The pseudonymisation key will be stored in a data safe, in order to restrict access as far as possible.

2. Encryption

The communication between the mobile devices and the terminal is encrypted, by means of individual device certification. The data is transmitted within the RIO platform using ubiquitous encryption/encryption everywhere.

3. Obligation of non-disclosure

All employees are advised of their obligation of non-disclosure and are required to give a written undertaking to keep the data secret.

The IT infrastructure will be provided via Amazon Web Services (AWS) within a cloud (IaaS & PaaS). Access control is provided by the AWS data centre operator: the highly secure AWS data centres use state-of-the-art electronic supervision and multi-level access control systems. The data centres are staffed round the clock by trained security personnel. Access is strictly controlled, according to the principle of least privilege, and is exclusively for the purposes of system administration.

Access to the hardware components (clients) at TB Digital Services GmbH takes place according to the appropriate standard measures in each case. These measures include, for example, restricted access via single-access entry control systems (turnstiles), video surveillance systems, alarms and/or guards, electronically or mechanically locked doors, intruder-proof buildings, documented access (for visitors and external contractors) or designated security areas.

The access controls include hardware protection, network security and application protection measures.

The hardware protection measures used on board the vehicle include: The mobile devices are installed in the vehicle and have secure boot, i.e. there is no possibility of uploading or using a foreign operating system. The communication between the mobile devices and the terminal is encrypted, by means of individual device certification. The data are transmitted within the RIO platform using ubiquitous encryption/encryption everywhere. The terminals are kept up to date by means of regular security updates (patch management).

The network security measures include various standard measures: State-of-the-art password defaults are implemented (password length, complexity, validity periods etc.). If the user ID/password combination is repeatedly entered incorrectly, this will result in the (temporary) blocking of the user credentials. The corporate network is isolated from unsafe public networks by a firewall. An OTA process is in place to secure the regular supply of security updates to mobile devices. Appropriate technologies (such as intrusion detection systems) are used to uncover and prevent attacks to the Intranet. Employees are regularly informed of the risks and dangers.

Various standard application protection measures are used:

The relevant applications are secured against unauthorised access by means of appropriate authentication/authorisation mechanisms. State-of-the-art password defaults are implemented (password length, complexity, validity periods etc.). For applications with particular protection requirements, strong authentication mechanisms such as tokens and PKIs are used. If the user ID/password combination is repeatedly entered incorrectly, this will result in the (temporary) blocking of the user credentials. The data used in key processes is encrypted on a mobile data carrier. All accesses and attempted accesses to the applications are recorded. The created log file is kept for an appropriate period of time (at least 90 days) and checked on a random basis.

User authorisations (for access and sharing) are secured by means of various measures; in principle the authorisations are allocated to a specific person. Authorisations are allocated by the Platform Manager and are regularly checked. Access authorisations are only issued after a defined, documented process. Access authorisations are changed according to the dual-control principle and are documented in a version-numbered log file.

Various access control/monitoring measures are used: Access rights are defined and documented in a role/authorisation policy and are allocated in accordance with the job-specific requirements of each role. There are specific roles and authorisations for technical administrators (who do not allow any access to Personal Data in so far as technically possible). There are specific roles/authorisations for technical support (which do not include technical administration rights).

The definition and allocation of roles/authorisations is not carried out, in so far as technically and organisationally possible, by the same people. It is time-limited as part of a tamper-proof approval process. Direct database access that bypasses the roles/authorities policy is only possible through the authorised database administrators. There is a regulation on the use of private data carriers or the use of private data carriers is prohibited. There are binding regulations regarding data access by external/remote maintenance workers and teleworkers. Documents and data carriers are destroyed or disposed of in accordance with the data protection laws (e.g. using shredders/data protection bins) by licensed disposal firms.

The roles/authorisations policy is regularly adapted to changes in the work organisation (e.g. new roles) and the allocated roles/authorisations are checked regularly (e.g. by the supervisors) and adapted or removed as necessary. Regular central controls are carried out on the assigned standard profiles. Modifying accesses

(editing, deleting) are recorded. The log files are kept for an appropriate period of time (at least 90 days) and are checked on a random basis.

Various standard confidentiality protection measures are used:

The people responsible for forwarding the information are familiarised with the applicable security measures in advance. The recipient group is determined in advance so that a corresponding check (authentication) is possible. The overall data transfer process is determined and documented and the actual data disclosure is recorded or documented (e.g. confirmation of receipt, acknowledgement). The people responsible for disclosing the information first carry out a plausibility, completeness and accuracy assessment.

The recipient's address (e.g. email address) is checked before the data is actually transferred. The transmission of data via the Internet is encrypted (e.g. file encryption). Where technically possible, the integrity of transmitted data is guaranteed through digital signature processes. Electronic confirmations of receipt are archived in an appropriate form. Undesirable Internet data transfers are prevented by means of appropriate technologies such as proxies and firewalls.

Various standard measures are also used to implement the separation rule:

There are binding regulations regarding the designated purpose of processing, in order to comply with the separation rule. Data acquired for specific purposes is stored separately from data acquired for other purposes. The IT systems allow the separate storage of data (by means of multiclient capability or access policies). There is data separation within the test and production systems. With pseudonymised data, the key bridge, which enables re-identification, is stored or kept separately. For contract processing or function transfer, the Contractor processes the data from different clients separately. The configuration of the existing roles/authorisations policy enables the logical separation of processed data.

4. Guarantee of integrity

Various standard input recording measures are used:

Changes to access rights, and all administrative activities, are recorded. Editing accesses (input, changes, deletions) and changes to data fields are recorded (e.g. content of the new or changed datasets). Transmissions such as downloads are recorded, and there is also a record of logins.

The records are documented and archived so that the input can be reproduced. The records include the date, time, user, type of activity, application and dataset reference number. The logging settings are documented.

The log files can only be accessed using read-only access. Only a very limited group of people are allowed access to the log files (e.g. the administrator, authorised data processors, the auditor). The log files are kept for a fixed period (e.g. 1 year) and are then disposed of in accordance with data protection laws. The log files are automatically evaluated on a regular basis. If possible, the log files are analysed in pseudonymised form.

5. Guarantee of availability

The architecture is secured against data loss by means of an internal replication mechanism on the AWS platform. The following standard AWS object protection measures are also used:

Fire prevention measures are used (e.g. fire doors, smoke alarms, fire barriers, smoking bans). The computer systems are protected against flooding (e.g. the computer room is on the first floor, water detectors). Anti-vibration measures are in place (e.g. the computer room is not close to major roads, railways or machine rooms). The computer rooms are secured against electromagnetic fields (e.g. steel plates in the external walls). Measures are taken against vandalism and theft (see access controls). The computer systems are located in air-conditioned rooms (temperature and moisture levels are regulated through the air-conditioning system). The computer systems have surge protection devices. Measures are in place to secure minimum disruption and continuity of power supply (e.g. UPS systems, emergency generators).

The data stock is regularly secured by backup copies on the AWS platform. The backup concept is documented and is regularly checked and updated. Backup media are protected against unauthorised access. The backup programs meet the latest quality standards, and are regularly updated to those standards. A backup data centre (remote from the processing site) has been set up and can continue the data processing operations in the event of a catastrophe. The various measures used to control access are documented by AWS in an emergency management plan.

Before an order for data processing is given, there will be a thorough checking of the Contractor, according to predetermined criteria (technical and organisational measures). This requires a detailed representation of the technical/organisational data protection measures put in place by the Contractor (responses to questionnaire, or data protection concept), which will be checked. Depending on the quantity and sensitivity of the processed data, this check will also be carried out at the premises of the Contractor, if necessary. Appropriate certifications (e.g. ISO 27001) will be taken into account when selecting the Contractor. The Contractor's adequacy will be documented in an appropriate, demonstrable form.

A contract processing agreement will be concluded between the Client and the Contractor, to be used as a basis for the contractual relationship. This will set out, in detail and in writing, the responsibilities, duties and obligations of both Parties. If a service provider is based outside the EU or the EEA, the EU standard contractual terms will apply. The contract will stipulate that the data processing can only be carried out by the Contractor on the basis of the Client's instructions. The Contractor is obligated to report to the Client immediately if, in the Contractor's opinion, an instruction given by the Client breaches the data protection laws. In order to respect the rights of the data subject, the contract processing agreement will stipulate that the Contractor must provide the Client with appropriate support if necessary; for example, in the provision of information to the data subject.

During the course of the contract processing, the Client will check the form and content of the Contractor's work. Compliance with the technical and organisational measures put in place by the Contractor will be checked regularly. This will primarily involve submitting the current certificates or attestations, and providing evidence

of completed IT security or data protection audits. If subcontractors are used, it will be stipulated in the contract that they must undergo the corresponding audits.

6. System capacity guarantee

The AWS cloud infrastructure has been designed to be one of the most flexible and most secure cloud computing environments. It has been conceived to guarantee optimum availability with full customer separation. It offers a highly scalable platform with high operating security that enables the customer to distribute applications and content quickly and securely as required, worldwide. The services provided by AWS are content-independent in so far as they offer all customers the same high level of security, regardless of the type of content or the geographical region in which the content is stored.

The highly secure, world class AWS data centres use state-of-the-art electronic supervision with multi-level access control systems. The data centres are staffed round the clock by trained security personnel. Access is strictly controlled, according to the principle of least privilege, and is exclusively for the purposes of system administration.

7. Procedure for recovering Personal Data after a physical or technical incident

The AWS data centres are configured in clusters, in different regions of the world. All data centres are online and serve clients; no data centre is disconnected. In the event of an incident, automated processes will move the customer data traffic away from the affected areas. The core applications are deployed in an N+1 configuration, so that in the event that a data centre becomes breaks down or otherwise becomes unavailable, there is sufficient capacity to distribute the data traffic among the remaining sites.

AWS offers the flexibility of placing requests and storing data within multiple geographical regions, or among multiple availability zones within the individual regions. Each availability zone has been developed as an independent breakdown zone. This means that availability zones within a typical city region are physically dispersed and are located, for example, in areas with a lower flooding risk (there are different flooding zone categories, depending on the region). In addition to an independent uninterruptible power supply and emergency generators on site, all availability zones are powered by different power networks from independent power suppliers, in order to minimise individual points of failure. All availability zones are redundant, with multiple Tier 1 transit providers.

The Amazon incident management team uses industry-standard diagnostics procedures in order to eliminate business-critical incidents. Operators offer a continual round-the-clock service, 7 days a week, 365 days a year, in order to identify incidents and manage and eliminate their effects.

8. Procedure for the regular checking, assessment and evaluation of the effectiveness of technical and organisational measures

The information security guidelines and instructions and standards implemented by the company are also applied with regard to the implementation and operation of the RIO platform. The company has data protection and information security roles (data protection officer and information security officer). Employees are bound by data secrecy and kept informed of data security or IT security measures by means of leaflets, flyers and Intranet announcements.

The internal processes are checked for compliance with the technical and organisational data security measures by means of audits, information security and data protection.

The processing operations and data security measures are documented in a processing inventory. There is a regular internal and external audit on the effectiveness of the measures.