Porsche Digital

Data Processing Agreement
concerning commissioned processing
according to art. 28 of the General Data Protection Regulation (GDPR)

between the respective supplier ("**Processor**") and
the respective Porsche Digital company ("**Controller**"),
both as defined in the corresponding contract/order,
each as "Party" and jointly as "Parties":

Section 1 Subject matter and duration of the assignment, type and purpose of the processing, type of personal data, categories of data subjects

The subject matter and duration of the assignment, type and purpose of the processing, type of personal data as well as the categories of data subjects of the assignment are specified in **Annex 1**.

Section 2 Processing subject to instructions and remonstration obligation

The Controller shall be responsible for the compliance with the applicable data protection regulations with regard to admissibility. The processing of data shall take place exclusively within the framework of the concluded contract and in accordance with the instructions of the Controller. Within the framework of the description of the assignment set out in this contract, the Controller reserves a comprehensive right of instruction concerning type, scope and method of the processing which can be defined in detail by individual instructions. Instructions of the Controller must be documented.

To the extent that, in deviation from this provision, the Processor is obliged to carry out processing due to the laws of the Union or the member states to which the Processor is subject, the Processor shall inform the Controller about these legal requirements before processing, unless that law prohibits such information due to important grounds of public interest.

In general, the Controller shall issue instructions in text form (e.g. by e-mail). If an instruction is issued orally by way of exception, it shall be confirmed by the Processor in text form (e.g. by e-mail).

If the Controller at the same time acts as a Processor for a third party, the Processor's obligations under this contract shall also apply directly in the relationship between the third party and the Processor. This shall apply to all services provided by the Processor to the third party on behalf of the Controller. In particular, the third party shall be entitled to the control and information rights from Section 10 directly against the Processor.

The Processor shall immediately inform the Controller if the Processor is of the opinion that compliance with an instruction issued by the Controller infringes the GDPR or another data protection provision (remonstration obligation).

Section 3 Confidentiality obligation / obligation to secrecy

For the execution of the contract, the Processor shall only engage persons who have been obligated by the Processor to maintain confidentiality or who are subject to an appropriate statutory obligation of confidentiality.

Section 4 Processing security / technical and organisational measures according to article 32 GDPR

The Processor shall take all necessary technical and organisational measures according to Article 32 GDPR. These are specified in **Annex 2**.

Notwithstanding these measures, the Processor (or the sub-processor, as applicable) shall maintain an IEC/ISO 27001 certification and shall adhere to the standards as required by the IEC/ISO 27001 certification for the term of this contract. On request of the Controller, the Processor is obliged to have a TISAX assessment (www.tisax.de) carried out with the TISAX assessment scope specified by the Controller within a reasonable period of time and to make the results available to the Controller.

Technical and organisational measures are subject to technological progress and development. For the duration of this assignment, the Processor shall continuously adjust them according to the requirements of the assignment and further develop them in accordance with the technological progress. The level of protection must not fall below the technical and organisational measures determined herein and in **Annex 2**. This data security concept shall be submitted on a regular basis.

The Processor undertakes to document changes to the technical and organisational measures that have a significant impact on the guaranteed level of protection in writing as addition to **Annex 2** and to notify the Controller thereof; such documentation can also be made in electronic form.

Section 5 Engagement of other processors

The other processors (sub-processors) engaged at the time of the conclusion of the contract are listed in **Annex 3** to this contract (if any). The Processor is granted approval for the engagement of the processors listed in **Annex 3**.

The Processor shall not engage any other processor (sub-processor) without the separate written consent of the Controller; such consent can also be granted in electronic form.

If the Processor engages another Processor (sub-processor) for carrying out specific processing activities on behalf of the Controller, the same data protection obligations as set out in this contract shall be imposed on that sub-processor by way of a written contract, which can also be in electronic form, or by way of another legal instrument according to the laws of the Union or the respective member state. In particular, sufficient guarantees shall be provided that the appropriate technical and organisational measures are implemented in such a manner that the processing complies with the requirements of the GDPR. If the sub-processor fails to fulfil their data protection obligations, the initial Processor shall be liable to the Controller for the performance of that sub-processor's obligations.

Section 6 Place of processing and EU standard contractual clauses

The processing of data by the Processor and the sub-processors approved by the Controller shall, as a matter of principle, take place exclusively in Member States of the European Union, Contracting States to the Agreement on the European Economic Area and/or countries for which and to the extent there is a valid adequacy decision of the Commission applicable to the processing within the meaning of Article 45 (3) of the GDPR. Any processing in any other country ("Unsafe Third Country") requires the prior written consent of the Controller and may also only take place if the legal requirements for data transfers to Unsafe Third Countries under the applicable data protection laws are met. The Parties shall document all necessary information and measures taken in this regard.

If the (respective) processing of the Data is carried out directly by the Processor (also) in an Unsafe Third Country, the EU Standard Contractual Clauses applying the module(s) applicable to the roles of the Parties relating to such Processing shall be annexed to this Agreement.

If sub-processors process data in an Unsafe Third Country, the Processor shall ensure, prior to the commencement of the processing by such sub-processors, that EU standard contractual clauses within the meaning of Article 46 (2) (c) of the GDPR have been concluded for the Processing of the data by the relevant sub-processors or that binding internal data protection rules pursuant to Article 47 of the GDPR ("BCR") apply.

In these cases, the Processor shall be obliged to determine whether the sub-processors are prevented from complying with their obligations under the EU standard contractual clauses or BCRs by the laws and practices in the Unsafe Third Countries applicable to their processing of the data, including requirements to disclose personal data or measures. The Processor confirms that it has obtained, assessed and documented from the sub-processors, inter alia, (i) relevant information regarding relevant laws and practices in the relevant Unsafe Third Countries and (ii) information regarding the applicability or practical exercise of such laws and practices in relation to the sub-processors (collectively, a "Transfer Impact Assessment"). A transfer may only take place if the Transfer Impact Assessment has shown that it is permissible. The documentation of this Transfer Impact Assessment shall be made available to the Controller at any time upon request.

The Processor shall provide the Controller with evidence of the conclusion of the EU standard contractual clauses with the sub-processors or the applicability of the BCRs upon request.

Section 7 Duty to cooperate / duty to provide assistance

Taking into account the nature of the processing, the Processor shall assist the Controller by appropriate technical and organisational measures in the fulfilment of the Controller's obligation to respond to requests for exercising the data subject's rights laid down in Chapter III of the GDPR. These rights shall in particular include the consideration of the data subject’s rights with regard to transparency, the right of access by the data subject, the right to rectification, the right of erasure and the right ‘to be forgotten’, the right to restriction of processing, the right of notification in case of rectification and erasure as well as restriction of processing, the right to data portability, the right to object as well as the rights in case of automated individual decision-making.

Section 8 Support in fulfilling the Controller´s obligations

The Processor shall assist the Controller in ensuring compliance with the obligations according to articles 32 to 36 GDPR, taking into account the nature of processing and the information available to the Processor. These obligations shall in particular include ensuring the security of processing, the notification of personal data breaches to the supervisory authorities, the communication of a personal data breach to the data subject, data protection impact assessment as well as the prior consultation with one of the competent supervisory authorities.

Section 9 Deletion and return of personal data

If no legal or other retention obligations apply, the Processor shall return the used personal data to the Controller in a readable and editable form after completion of the assignment, unless the Controller requests the Processor to delete the personal data. If the Processor returns the data, any copies which might be in their area of responsibility shall be deleted immediately after the Controller has confirmed proper receipt of the data.

Furthermore, the Processor shall take all appropriate measures in order to exclude the continuous, unauthorized access to the Controller's data.

Upon termination of the contract, the Processor shall retain documents providing evidence concerning the fulfilment of this provision for a reasonable period of time after the end of the contract and provide them, if required.

Section 10 Proof of obligations and support during audits

Upon request, the Processor shall provide the Controller with reports on compliance with the obligations under this contract.

The Processor shall make available to the Controller all information necessary to demonstrate compliance with the obligations laid down in art. 28 GDPR. The Processor shall allow for and assist during audits - including inspections - conducted by the Controller or another auditor engaged by the Controller.

Section 11 Other obligations

The Processor ensures that they have designated a data protection officer, if required by law.

The Controller shall be informed immediately about any suspicion of an infringement of data protection regulations or other disorders in the processing of personal data of the Controller and about inspections and measures of the competent supervisory authority at the premises of the Processor. If a data subject directly contacts the Processor for the purpose of answering requests for exercising the data subject's rights according to Chapter III of the GDPR, the Processor shall forward this request to the Controller and wait for the Controller’s instruction in this regard.

The Processor shall in particular ensure, with the reasonable care, that their employees comply with the statutory data protection regulations and that the information received from the Controller is not disclosed to a third party or used in any other way. Upon the Controller’s

request, the Processor shall provide evidence concerning the data protection training and the obligation with regard to data protection law.

Section 12 Other provisions

If the proper fulfilment of the purpose of the assignment as set out in section 1 of this contract is jeopardized on the part of Processor as a result of attachment or seizure, as a result of insolvency or settlement proceedings or as a result of other events or measures instituted by third parties, the Processor shall inform the Controller immediately. The Processor shall immediately inform any and all involved parties that the Controller has the exclusive right to dispose of the data.

In the event of possible contradictions between this contract and a main contract, the provisions of this contract shall have precedence over the provisions of the main contract.

If individual parts of this contract should be invalid, this shall not affect the validity of the remaining parts of the contract.

Any amendment to this contract, including its termination and this clause, requires the written form; this shall also include the electronic form.

Porsche Digital

Annexes

Annex 1 **Determinations on the contract**

Annex 2 **Technical and organisational measures**

Annex 3 **Other processors (sub-processors)**

Porsche Digital

Schedule: Data Processing Agreement concerning commissioned processing according to art. 28 of the General Data Protection Regulation (GDPR)

between the respective supplier ("**Processor**") and
the respective Porsche Digital company ("**Controller**"),
both as defined in the corresponding contract/order,
each as "Party" and jointly as "Parties":

Preamble

This data protection contract is concluded in relation to the service contract / order which the parties have entered into hereby (hereafter "**Main Contract**").

Annexes

Annex 1

General information regarding the contract

1. Subject matter of the assignment

The subject matter of the assignment is described through the Main Contract.

2. Duration of the assignment

The duration of the assignment follows the duration of the Main Contract.

3. Nature and purpose of the data processing

The processing activity of the Processor, including nature and purposes, follow the contractual services agreed upon in the Main Contract.

4. Categories of data subjects

The categories of data subjects which are subject matter of this assignment concern:

- **(Former) employees and similar persons**, such as applicants, apprentices / interns, employees' relatives;
- **Customers, users and similar persons** such as clients, interested parties, subscribers, indirectly involved persons / persons in the environment / occupants, visitors, event participants, communication participants;
- **Business contact persons**, such as shareholders / bodies, business partners, suppliers and service providers, consultants, contact persons for business matters, sales representatives;
- **Press representatives**

in each case depending on and as relevant for the services specified in the Main Contract. If and to the extent the Main Contract sets out the categories of data subjects concerned, such description prevails.

5. Types of personal data (type of personal data)

The types of personal data which are subject matter of this assignment concern:

a. **With regard to former employees and similar persons**
- **General data / contact details,** such as names, private address data and (personal) profiles;
- **Master data and qualified HR data,** such as master data, job function, contractual details, national ID, nationality, date of birth, gender, information on education and work experience, Qualifications and skills, CV, employment status, type of contract, working time data and professional profiles;
- **Payroll data**, such as banking data, compensation information, statutory and other deductions, information on leaves, allowances, bonuses, stock purchase plans and expenses data;
- **Training information**, such as participation in training-sessions, qualifications;
- **special categories of personal data**, such as health data, data on religious affiliation, trade or union memberships, criminal history (where absolutely necessary and to the extent permitted / required by law)

in each case depending on and as relevant for the services specified in the Main Contract. If and to the extent the Main Contract sets out the types of personal data concerned, such description prevails.

b. **With regard to other data subject categories**
- **General data / contact details,** such as names, work address data, work telephone number, work fax number, work email address, work mobile phone number, job title;
- **Contract data,** such as contract/usage histories (e.g. payment information, provided services);
- **Vehicle, location and context data,** such as vehicle identification data, vehicle condition data;
- **Service and IT (usage) data,** such as device identifiers and access data;
- **Creditworthiness data,** such as payment behavior, scores, asset information;
- **special categories of personal data**, such as racial origin, political opinions, religious beliefs, trade union membership, biometric data, health data, data concerning sexual orientation (where absolutely necessary and to the extent permitted / required by law),

in each case depending on and as relevant for the services specified in the Main Contract. If and to the extent the Main Contract sets out the types of personal data concerned, such description prevails.

6. Regular submission of the data security concept

An updated version of the technical and organisational measures as well as the data security concept, if required, and/or certificates concerning data security shall be submitted to the Controller upon request.

Annex 2

Technical and organisational measures

Taking into account

- the state of the art,
- the costs of implementation and
- the nature, scope, context and
- the purpose of processing as well as
- the different probability of occurrence and the risk of varying likelihood and severity for the rights and freedoms of natural persons,

the processor shall implement appropriate technical and organisational measures to ensure a level of security appropriate to the risk.

In assessing the appropriate level of security account shall be taken in particular of the risks that are presented by processing, in particular from accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to personal data transmitted, stored or otherwise processed.

If the Processor has no possibility to access the data of the Controller and the commissioned processing is completely carried out by one or more other processors (sub-processors), these sub-processors' security concepts according to art. 32 GDPR shall be described in **Annex 2**.

The Processor as well as the sub-processor(s) listed in Annex 3 shall take the following measures:

1. Pseudonymisation

Personal data of the Controller can be processed in such a manner that the personal data can no longer be attributed to a specific data subject without the use of additional information, provided that such additional information is kept separately and is subject to technical and organisational measures which exclude the unauthorized identification of the data subject.

Nevertheless, data pseudonymized in this way remain personal data according to the GDPR. Pseudonymisation is a technical and organisational measure and can be implemented by the Processor as follows:

- Separate storage of additional information for identification
- Use of (personnel, customer or user) IDs instead of names
- Encryption of additional information for identification
- Management and documentation of differentiated authorizations concerning additional information for identification
- Authorization process or approval routines for authorizations to process additional information for identification
- Copy protection with regard to additional information for identification
- Four-eyes principle for identification

2. Measures for encryption

- Encryption of mobile devices such as laptops, tablets, smartphones
- Encryption of mobile storage media (CD/DVD- ROM, USB sticks, external hard drives)
- Encryption of files

- Encryption of systems/devices
- Encrypted storage of passwords
- Encryption of e-mails and e-mail attachments
- Secured data sharing (e.g. SSL, FTPS, TLS)
- Secured WLAN

3. Measures to ensure confidentiality

3.1. Measures which ensure that unauthorized persons do not gain access:

- Access control system, document reader (magnetic / chip card)
- Door protections (electric door opener, number lock, etc.)
- Safety doors / windows
- Grates in front of windows / doors
- Fence systems
- Key management / documentation of key assignment
- Protection of facilities, guards
- Alarm system
- Video surveillance
- Special protective measures for the server room
- Special protective measures for storage of back-ups and/or other data carriers
- Irreversible destruction of data carriers
- Employee and authorization documents
- Prohibited areas
- Visitor rules (e.g. pick-up at reception, documentation of visiting hours, visitor pass, accompanying visitors to exit after visit)

3.2. Measures which prevent unauthorized persons from using the processing systems:

- Personal and individual user log-in for registration in the systems or company network
- Authorization process for access authorizations
- Limitation of authorized users
- Single sign-on
- Two-factor authentication
- BIOS passwords
- Password procedures (indication of password parameters with regard to complexity and update interval)
- Electronic documentation of passwords and protection of this documentation against unauthorized access
- Personalized chip cards, token, PIN/TAN, etc.
- Logging of access
- Additional system log-in for certain applications
- Automatic locking of the clients after expiry of a certain period without user activity (also password-protected screensaver or automatic stand-by)
- Firewall

3.3. Measures which ensure that only authorized persons have access to the processing systems and that personal data cannot be read, copied, modified or removed without authorization:

- Management and documentation of differentiated authorizations
- Evaluations/logging of data processing
- Authorization process for authorizations
- Approval routines

- Profiles / roles
- Encryption of CD/DVD-ROM, external hard drives and/or laptops (e.g. via operating system, Safe Guard Easy, PGP)
- Measures to prevent unauthorized transfer of data onto data carriers which can be used externally (e.g. copy protection, locking of USB ports, “Data Loss Prevention (DLP) system”)
- „Mobile Device Management” system
- Four-eyes principle
- Segregation of functions “segregation of duties”
- Expert destruction of records and data carriers in accordance with DIN 66399
- Irreversible deletion from data carriers
- Privacy foil for mobile data processing systems

3.4. Measures which ensure that data collected for different purposes can be processed separately:

- Storage of the data sets in physically separated databases
- Separate systems
- Access authorizations by functional responsibility
- Separate data processing by differentiating access rules
- Multi-client capability of IT systems
- Use of test data
- Separation of development and production environments

4. Measures to ensure integrity

- Access rights
- System-side logging
- Document management system (DMS) with change history
- Security / logging software
- Functional responsibilities, organisationally specified responsibilities
- “Multiple-eyes principle”
- Tunnelled remote data connections (VPN = virtual private network)
- “Data Loss Prevention (DLP) system”
- Electronic signature
- Logging of data transfer or data transport
- Logging of read accesses
- Logging of the copying, modification or removal of data

5. Measures to ensure and restore availability

- Security concept for software and IT applications
- Back-up procedures
- Storage process for back-ups (fire-protected safe, separate fire sections, etc.)
- Ensuring data storage in a secured network
- Need-based installation of security updates
- Mirroring of hard drives
- Set-up of an uninterrupted power supply
- Suitable archiving facilities for paper documents
- Fire and/or extinguishing water protection for the server room
- Fire and/or extinguishing water protection for the archiving facilities
- Air-conditioned server room
- Virus protection

- Firewall
- Emergency plan
- Successful emergency exercises
- Redundant, locally separated data storage (off-site storage)

6. Measures to ensure resilience

- Emergency plan in case of machine breakdown
- Redundant power supply
- Sufficient capacity of IT systems and equipment
- Logistically controlled process to avoid power peaks
- Redundant systems / equipment
- Resilience and error management

7. Procedure for regular review, assessment and evaluation of the effectiveness of the technical and organisational measures

- Procedures for regular inspections/audits
- Concept for regular review, assessment and evaluation
- Reporting system
- Penetration tests
- Emergency tests
- Certification, if available

8. “Control of instructions / assignment control”

- Contract for commissioned data processing according to art. 28, para. 3 GDPR with provisions concerning the rights and obligations of the Processor and the Controller
- Process of issuing and/or following instructions
- Designation of contact persons and/or responsible employees
- Control / examination that the assignment is executed in accordance with instructions
- Training / instruction of all Processor’s access-authorized employees
- Independent auditing of adherence to instructions
- Obligation of employees to maintain confidentiality
- Agreement on penalties for infringements of instructions
- Appointment of a data protection officer according to art. 37 et seq. GDPR
- Data protection manager / coordinator
- Keeping records of processing activities in accordance with art. 30, para. 2 GDPR
- Documentation and escalation process for personal data breaches
- Guidelines / instructions which guarantee technical-organisational measures for the security of the processing
- Process for forwarding queries of data subjects

Annex 3

Other processors (sub-processors)

The subcontractors engaged under and in compliance with the Main Contract and this data processing agreement to provide subcontracted services are the authorized sub-processors hereunder with the subject matter and duration following the subcontracted services (further details may be specified in the following).

Name and address of the sub-processor	Subject matter of the subcontracting	Date of the contract concerning subcontracting