VOLKSWAGEN

KONZERNLOGISTIK

EU Standard Contractual Clauses pursuant to the Commission Implementing Decision (EU) 2021/914

(MODULE ONE: controller to controller transfers)

with regard to

Communication within our entire logistic process chain, logistic projects and logistic campaigns

Volkswagen Konzernlogistik GmbH & Co. OHG

Heßlinger Straße 12

38436 Wolfsburg, Germany

hereafter referred to as “data exporter”

and

Company Name

Address (street)

Address (City, Country)

hereafter referred to as “data importer”

each a “party”, jointly “the parties”.

Version 1.0 from 01.05.2024

If the Parties have already concluded EU standard contractual clauses on the basis of Commission Decision 2001/497/EC (Set I) or the Commission Decision 2004/915/EC amending Decision 2001/497/EC as regards the introduction of an alternative set of standard contractual clauses for the transfer of personal data to third countries (Set II) prior to the conclusion of the following EU standard contractual clauses for their data protection relationship as controllers with regard to the addressed processing activities, the following EU standard contractual clauses shall replace these already concluded EU standard contractual clauses.

SECTION I

Clause 1

Purpose and scope

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

b) The Parties:

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

ii) the entity/ies in a third country receiving the personal data from the data exporter, directly or indirectly via another entity also Party to these Clauses, as listed in Annex I.A. (hereinafter each “data importer”)

have agreed to these standard contractual clauses (hereinafter: “Clauses”).

c) These Clauses apply with respect to the transfer of personal data as specified in Annex I.B.

d) The Appendix to these Clauses containing the Annexes referred to therein forms an integral part of these Clauses.

Clause 2

Effect and invariability of the Clauses

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

b) These Clauses are without prejudice to obligations to which the data exporter is subject by virtue of Regulation (EU) 2016/679.

Clause 3

Third-party beneficiaries

a) Data subjects may invoke and enforce these Clauses, as third-party beneficiaries, against the data exporter and/or data importer, with the following exceptions:

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

ii) Clause 8.5 (e) and Clause 8.9 (b);

iii) [not applicable to MODULE ONE]

iv) Clause 12(a) and (d);

v) Clause 13;

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

vii) Clause 16 (e);

viii) Clause 18(a) and (b).

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

Clause 4

Interpretation

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

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

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

Clause 5

Hierarchy

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

Clause 6

Description of the transfer(s)

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

Clause 7

Docking clause

a) An entity that is not a Party to these Clauses may, with the agreement of the Parties, accede to these Clauses at any time, either as a data exporter or as a data importer, by completing the Appendix and signing Annex I.A.

b) Once it has completed the Appendix and signed Annex I.A, the acceding entity shall become a Party to these Clauses and have the rights and obligations of a data exporter or data importer in accordance with its designation in Annex I.A.

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

SECTION II - OBLIGATIONS OF THE PARTIES

Clause 8

Data protection safeguards

The data exporter warrants that it has used reasonable efforts to determine that the data importer is able, through the implementation of appropriate technical and organisational measures, to satisfy its obligations under these Clauses.

8.1 Purpose limitation

The data importer shall process the personal data only for the specific purpose(s) of the transfer, as set out in Annex I.B. It may only process the personal data for another purpose:

i) where it has obtained the data subject’s prior consent;

ii) where necessary for the establishment, exercise or defence of legal claims in the context of specific administrative, regulatory or judicial proceedings; or

iii) where necessary in order to protect the vital interests of the data subject or of another natural person.

8.2 Transparency

a) In order to enable data subjects to effectively exercise their rights pursuant to Clause 10, the data importer shall inform them, either directly or through the data exporter:

i) of its identity and contact details;

ii) of the categories of personal data processed;

iii) of the right to obtain a copy of these Clauses;

iv) where it intends to onward transfer the personal data to any third party/ies, of the recipient or categories of recipients (as appropriate with a view to providing meaningful information), the purpose of such onward transfer and the ground therefore pursuant to Clause 8.7.

b) Paragraph (a) shall not apply where the data subject already has the information, including when such information has already been provided by the data exporter, or providing the information proves impossible or would involve a disproportionate effort for the data importer. In the latter case, the data importer shall, to the extent possible, make the information publicly available.

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

d) Paragraphs (a) to (c) are without prejudice to the obligations of the data exporter under Articles 13 and 14 of Regulation (EU) 2016/679.

8.3 Accuracy and data minimisation

a) Each Party shall ensure that the personal data is accurate and, where necessary, kept up to date. The data importer shall take every reasonable step to ensure that personal data that is inaccurate, having regard to the purpose(s) of processing, is erased or rectified without delay.

b) If one of the Parties becomes aware that the personal data it has transferred or received is inaccurate, or has become outdated, it shall inform the other Party without undue delay.

c) The data importer shall ensure that the personal data is adequate, relevant and limited to what is necessary in relation to the purpose(s) of processing.

8.4 Storage limitation

The data importer shall retain the personal data for no longer than necessary for the purpose(s) for which it is processed. It shall put in place appropriate technical or organisational measures to ensure compliance with this obligation, including erasure or anonymisation[1] of the data and all back-ups at the end of the retention period.

8.5 Security of processing

a) The data importer and, during transmission, also the data exporter shall implement appropriate technical and organisational measures to ensure the security of the personal data, including protection against a breach of security leading to accidental or unlawful destruction, loss, alteration, unauthorised disclosure or access (hereinafter “personal data breach”). In assessing the appropriate level of security, they shall take due account of the state of the art, the costs of implementation, the nature, scope, context and purpose(s) of processing and the risks involved in the processing for the data subject. The Parties shall in particular consider having recourse to encryption or pseudonymisation, including during transmission, where the purpose of processing can be fulfilled in that manner.

b) The Parties have agreed on the technical and organisational measures set out in Annex II. The data importer shall carry out regular checks to ensure that these measures continue to provide an appropriate level of security.

[1] This requires rendering the data anonymous in such a way that the individual is no longer identifiable by anyone, in line with recital 26 of Regulation (EU) 2016/679, and that this process is irreversible.

c) The data importer shall ensure that persons authorised to process the personal data have committed themselves to confidentiality or are under an appropriate statutory obligation of confidentiality.

d) In the event of a personal data breach concerning personal data processed by the data importer under these Clauses, the data importer shall take appropriate measures to address the personal data breach, including measures to mitigate its possible adverse effects.

e) In case of a personal data breach that is likely to result in a risk to the rights and freedoms of natural persons, the data importer shall without undue delay notify both the data exporter and the competent supervisory authority pursuant to Clause 13. Such notification shall contain i) a description of the nature of the breach (including, where possible, categories and approximate number of data subjects and personal data records concerned), ii) its likely consequences, iii) the measures taken or proposed to address the breach, and iv) the details of a contact point from whom more information can be obtained. To the extent it is not possible for the data importer to provide all the information at the same time, it may do so in phases without undue further delay.

f) In case of a personal data breach that is likely to result in a high risk to the rights and freedoms of natural persons, the data importer shall also notify without undue delay the data subjects concerned of the personal data breach and its nature, if necessary in cooperation with the data exporter, together with the information referred to in paragraph (e), points ii) to iv), unless the data importer has implemented measures to significantly reduce the risk to the rights or freedoms of natural persons, or notification would involve disproportionate efforts. In the latter case, the data importer shall instead issue a public communication or take a similar measure to inform the public of the personal data breach.

g) The data importer shall document all relevant facts relating to the personal data breach, including its effects and any remedial action taken, and keep a record thereof.

8.6 Sensitive data

Where the transfer involves personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade union membership, genetic data, or biometric data for the purpose of uniquely identifying a natural person, data concerning health or a person’s sex life or sexual orientation, or data relating to criminal convictions or offences (hereinafter “sensitive data”), the data importer shall apply specific restrictions and/or additional safeguards adapted to the specific nature of the data and the risks involved. This may include restricting the personnel permitted to access the personal data, additional security measures (such as pseudonymisation) and/or additional restrictions with respect to further disclosure.

8.7 Onward transfers

The data importer shall not disclose the personal data to a third party located outside the European Union[2] (in the same country as the data importer or in another third country, hereinafter “onward transfer”) unless the third party is or agrees to be bound by these Clauses, under the appropriate Module. Otherwise, an onward transfer by the data importer may only take place if:

[2] The Agreement on the European Economic Area (EEA Agreement) provides for the extension of the European Union’s internal market to the three EEA States Iceland, Liechtenstein and Norway. The Union data protection legislation, including Regulation (EU) 2016/679, is covered by the EEA Agreement and has been incorporated into Annex XI thereto. Therefore, any disclosure by the data importer to a third party located in the EEA does not qualify as an onward transfer for the purpose of these Clauses.

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

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

iii) the third party enters into a binding instrument with the data importer ensuring the same level of data protection as under these Clauses, and the data importer provides a copy of these safeguards to the data exporter;

iv) it is necessary for the establishment, exercise or defence of legal claims in the context of specific administrative, regulatory or judicial proceedings;

v) it is necessary in order to protect the vital interests of the data subject or of another natural person; or

vi) where none of the other conditions apply, the data importer has obtained the explicit consent of the data subject for an onward transfer in a specific situation, after having informed him/her of its purpose(s), the identity of the recipient and the possible risks of such transfer to him/her due to the lack of appropriate data protection safeguards. In this case, the data importer shall inform the data exporter and, at the request of the latter, shall transmit to it a copy of the information provided to the data subject.

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

8.8 Processing under the authority of the data importer

The data importer shall ensure that any person acting under its authority, including a processor, processes the data only on its instructions.

8.9 Documentation and compliance

a) Each Party shall be able to demonstrate compliance with its obligations under these Clauses. In particular, the data importer shall keep appropriate documentation of the processing activities carried out under its responsibility.

b) The data importer shall make such documentation available to the competent supervisory authority on request.

Clause 9

[not applicable to MODULE ONE]

Clause 10

Data subject rights

a) The data importer, where relevant with the assistance of the data exporter, shall deal with any enquiries and requests it receives from a data subject relating to the processing of his/her personal data and the exercise of his/her rights under these Clauses without undue delay and at the latest within one month of the receipt of the enquiry or request.[3] The data importer shall take appropriate measures to facilitate such enquiries, requests and the exercise of data subject rights. Any information provided to the data subject shall be in an intelligible and easily accessible form, using clear and plain language.

b) In particular, upon request by the data subject the data importer shall, free of charge:

i) provide confirmation to the data subject as to whether personal data concerning him/her is being processed and, where this is the case, a copy of the data relating to him/her and the information in Annex I; if personal data has been or will be onward transferred, provide information on recipients or categories of recipients (as appropriate with a view to providing meaningful information) to which the personal data has been or will be onward transferred, the purpose of such onward transfers and their ground pursuant to Clause 8.7; and provide information on the right to lodge a complaint with a supervisory authority in accordance with Clause 12(c)(i);

ii) rectify inaccurate or incomplete data concerning the data subject;

iii) erase personal data concerning the data subject if such data is being or has been processed in violation of any of these Clauses ensuring third-party beneficiary rights, or if the data subject withdraws the consent on which the processing is based.

c) Where the data importer processes the personal data for direct marketing purposes, it shall cease processing for such purposes if the data subject objects to it.

d) The data importer shall not make a decision based solely on the automated processing of the personal data transferred (hereinafter “automated decision”), which would produce legal effects concerning the data subject or similarly significantly affect him / her, unless with the explicit consent of the data subject or if authorised to do so under the laws of the country of destination, provided that such laws lays down suitable measures to safeguard the data subject’s rights and legitimate interests. In this case, the data importer shall, where necessary in cooperation with the data exporter:

i) inform the data subject about the envisaged automated decision, the envisaged consequences and the logic involved; and

ii) implement suitable safeguards, at least by enabling the data subject to contest the decision, express his/her point of view and obtain review by a human being.

e) Where requests from a data subject are excessive, in particular because of their repetitive character, the data importer may either charge a reasonable fee taking into account the administrative costs of granting the request or refuse to act on the request.

f) The data importer may refuse a data subject’s request if such refusal is allowed under the laws of the country of destination and is necessary and proportionate in a democratic society to protect one of the objectives listed in Article 23(1) of Regulation (EU) 2016/679.

g) If the data importer intends to refuse a data subject’s request, it shall inform the data subject of the reasons for the refusal and the possibility of lodging a complaint with the competent supervisory authority and/or seeking judicial redress.

[3] That period may be extended by a maximum of two more months, to the extent necessary taking into account the complexity and number of requests. The data importer shall duly and promptly inform the data subject of any such extension.

Clause 11

Redress

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

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

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

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

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

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

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

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

Clause 12

Liability

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

b) Each Party shall be liable to the data subject, and the data subject shall be entitled to receive compensation, for any material or non-material damages that the Party causes the data subject by breaching the third-party beneficiary rights under these Clauses. This is without prejudice to the liability of the data exporter under Regulation (EU) 2016/679.

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

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

e) The data importer may not invoke the conduct of a processor or sub-processor to avoid its own liability.

Clause 13

Supervision

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

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

SECTION III - LOCAL LAWS AND OBLIGATIONS IN CASE OF ACCESS BY PUBLIC

Clause 14

Local laws and practices affecting compliance with the Clauses

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

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

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

  ii) the laws and practices of the third country of destination- including those requiring the disclosure of data to public authorities or authorising access by such authorities - relevant in light of the specific circumstances of the transfer, and the applicable limitations and safeguards[4];

[4] As regards the impact of such laws and practices on compliance with these Clauses, different elements may be considered as part of an overall assessment. Such elements may include relevant and documented practical experience with prior instances of requests for disclosure from public authorities, or the absence of such requests, covering a sufficiently representative time-frame. This refers in particular to internal records or other documentation, drawn up on a continuous basis in accordance with due diligence and certified at senior management level, provided that this information can be lawfully shared with third parties. Where this practical experience is relied upon to conclude that the data importer will not be prevented from complying with these Clauses, it needs to be supported by other relevant, objective elements, and it is for the Parties to consider carefully whether these elements together carry sufficient weight, in terms of their reliability and representativeness, to support this conclusion. In particular, the Parties have to take into account whether their practical experience is corroborated and not contradicted by publicly available or

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

c) The data importer warrants that, in carrying out the assessment under paragraph (b), it has made its best efforts to provide the data exporter with relevant information and agrees that it will continue to cooperate with the data exporter in ensuring compliance with these Clauses.

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

e) The data importer agrees to notify the data exporter promptly if, after having agreed to these Clauses and for the duration of the contract, it has reason to believe that it is or has become subject to laws or practices not in line with the requirements under paragraph (a), including following a change in the laws of the third country or a measure (such as a disclosure request) indicating an application of such laws in practice that is not in line with the requirements in paragraph (a).

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

Clause 15

Obligations of the data importer in case of access by public authorities

15.1 Notification

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

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

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

otherwise accessible, reliable information on the existence or absence of requests within the same sector and/or the application of the law in practice, such as case law and reports by independent oversight bodies.

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

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

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

e) Paragraphs (a) to (c) are without prejudice to the obligation of the data importer pursuant to Clause 14(e) and Clause 16 to inform the data exporter promptly where it is unable to comply with these Clauses.

15.2 Review of legality and data minimisation

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

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

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

SECTION IV - FINAL PROVISIONS

Clause 16

Non-compliance with the Clauses and termination

a) The data importer shall promptly inform the data exporter if it is unable to comply with these Clauses, for whatever reason.

b) In the event that the data importer is in breach of these Clauses or unable to comply with these Clauses, the data exporter shall suspend the transfer of personal data to the data importer until compliance is again ensured or the contract is terminated. This is without prejudice to Clause 14(f).

c) The data exporter shall be entitled to terminate the contract, insofar as it concerns the processing of personal data under these Clauses, where:

i) the data exporter has suspended the transfer of personal data to the data importer pursuant to paragraph (b) and compliance with these Clauses is not restored within a reasonable time and in any event within one month of suspension;

ii) the data importer is in substantial or persistent breach of these Clauses; or

iii) the data importer fails to comply with a binding decision of a competent court or supervisory authority regarding its obligations under these Clauses.

In these cases, it shall inform the competent supervisory authority of such non-compliance. Where the contract involves more than two Parties, the data exporter may exercise this right to termination only with respect to the relevant Party, unless the Parties have agreed otherwise.

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

e) Either Party may revoke its agreement to be bound by these Clauses where (i) the European Commission adopts a decision pursuant to Article 45(3) of Regulation (EU) 2016/679 that covers the transfer of personal data to which these Clauses apply; or (ii) Regulation (EU) 2016/679 becomes part of the legal framework of the country to which the personal data is transferred. This is without prejudice to other obligations applying to the processing in question under Regulation (EU) 2016/679.

Clause 17

Governing law

These Clauses shall be governed by the law of one of the EU Member States, provided such law allows for third-party beneficiary rights. The Parties agree that this shall be the law of the Federal Republic of Germany.

Clause 18

Choice of forum and jurisdiction

a) Any dispute arising from these Clauses shall be resolved by the courts of an EU Member State.

b) The Parties agree that those shall be the courts of the Federal Republic of Germany.

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

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

Appendix

to the EU Standard Contractual Clauses

Annex I

A. List of parties

Data exporter(s):

1.

Name:	Volkswagen Konzernlogistik GmbH & Co. OHG
Address:	Heßlinger Straße 12, 38436 Wolfsburg, Germany
Contact person's name, position and contact details (data protection officer where applicable):	Data Protection Management Organisation: task-force-dsgvo-produktion@volkswagen.de
Activities relevant to the data transferred under these Clauses:	Communication within our entire logistic process chain, logistic projects and logistic campaigns
Role:	Controller

2. […]

Data importer(s):

1.

Name:	Company name
Address:	Company address
Contact person's name, position and contact details:	Contact
Activities relevant to the data transferred under these Clauses:	Communication within our entire logistic process chain, logistic projects and logistic campaigns
Role:	Controller

2. […]

B. Description of transfer

Categories of data subjects whose personal data is transferred:

(Multiple selections possible)

	Group of data subjects	Description	Examples
☒	Employees	Employee of the own Group Company (within the meaning of employee of the Controller)	employee, trainee, applicant, former employees
☒	Group employees	Employees of another Volkswagen Group Company (within the meaning of employee of a company of the Volkswagen Group with said company not being the Controller)	For example, from the perspective of Volkswagen AG: Employees of AUDI, FSAG, PORSCHE, etc.
☒	Employees of partner companies	Employees of a supplier, service provider, joint venture, temporary employment agency of the Principal	employees of IT service providers or suppliers, employees of joint ventures, temporary employees
☒	Customers	Any person who has a (customer) business relationship (with the respective Controller)	Vehicle buyers, bank customers, policyholders, renters
☒	Other business partners	Any natural person or legal entity that has a business relationship (with the respective Controller), except for customers	Suppliers, importers or service partners themselves; intermediaries, shareholders, freelancers, etc.
☐	Outsiders	Any person that has no business relationship with the respective Group Company (Controller)	visitors, guests, interested parties
☐	Children	Persons under 16 years of age	

Categories of personal data transferred:

(Multiple selections possible)

	Data Category	Examples of data
☒	Job-related contact and (work) organisation data	Surname, given name, sex, address, email address, phone number, mobile phone number, (Group) company, area, department, cost centre, personnel number, responsibilities, functions, presence (yes/no), etc.
☒	IT usage data	UserID, roles, permissions, log-in times, computer name, IP address, GID, Legic no., etc.
☐	Special category: Photo of the employee	Portrait photo voluntarily published by the employee (intranet telephone directory, internal social media platform, etc.)
☐	Private contact and identification data	Surname, given name, sex, address, email address, phone number, mobile phone number, date/place of birth, identification numbers, nationality, etc.
☐	Contract data	Purchased products, (financial) services, date of purchase agreement, purchase price, extras, warranties, etc.
☒	Vehicle usage data with VIN/number plate *Guarantee, warranty, product liability, safe vehicle operation*	Data generated during vehicle use which is linked to the VIN/number plate and which is of importance in connection with workshop repairs, guarantees, warranties, product liability or the availability of what is required for the safe operation of the vehicle.
☐	Vehicle usage data with VIN/number plate *Comfort settings, multimedia, navigation*	Data generated during vehicle use that are linked to the VIN/number plate and that relate to comfort settings, such as seat adjustment, preferred radio stations, climate settings, navigation data, email / SMS contact information, etc.
☐	Vehicle usage data with VIN/number plate *Assistance systems, driving behaviour etc.*	Data generated during vehicle use that are linked to the VIN/number plate and that relate to the driving behaviour or the use of assistance systems and their specific operational data, etc.
☐	Position data	GPS, wireless positioning/tracking, movement profile, WLAN hotspot tracking/positioning, etc.
☐	Data regarding personal / professional circumstances and characteristics	Data concerning spouse or children, marital status, portrait photo, volunteer work, job title, career, length of service, tasks, activities, log-file analyses, joining and leaving dates, qualifications, assessments/evaluations, etc.
☐	Payment and time management data	Pay scale group, payroll accounting, special payments, garnishment, daily attendance times, reasons for absence, etc.
☐	Creditworthiness and other financial data, bank details	Payment behaviour, balance sheets, credit bureau data, credit score values, financial circumstances, bank account details, credit card number, etc.

□	Special categories of personal data	Article 9(1) GDPR: racial and ethnic origin, political opinions, religious or philosophical beliefs, trade union membership, genetic data, biometric data for the purpose of uniquely identifying a natural person, data concerning health or data concerning a natural person's sex life or sexual orientation
□	Criminal offences / regulatory offences	Data relating to (suspected) criminal acts and other special requirements under Article 10 GDPR

Sensitive data transferred (if applicable) and applied restrictions or safeguards that fully take into consideration the nature of the data and the risks involved, such as for instance strict purpose limitation, access restrictions (including access only for staff having followed specialised training), keeping a record of access to the data, restrictions for onward transfers or additional security measures:

n/a

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

Regularly during the term of the Framework Agreement

Nature of the processing:

Manual or automatic processing depending on the concrete service performed under the (Framework) Agreement

Purpose(s) of the data transfer and further processing:

The data importer is the data exporter's service provider in the logistics sector. The Data Transfer is carried for the coordination of the business relationship and the fulfillment of the concluded contract(s). In particular, data will be transferred for the following purposes (not conclusive):

- Procurement and sourcing processes
- Filing and administration of documents
- Contract maintenance of supplier/service provider contracts
- Recording of the participation of employees in projects and plans
- Creation of organizational overviews
- Identification/documentation/contacting
- Transmission of tasks and messages
- Documentation and processing of complaints
- Planning and execution of audits
- Administration of taxes and duties
- Fulfilment of legal obligations

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

The data will be retained according the terms of the (Framework) Agreement

C. Competent supervisory authority

Identify the competent supervisory authority/ies in accordance with Clause 13: Data protection authority of the state of Lower Saxony (Germany)

Annex II

Technical and organisational measures including technical and organisational measures to ensure the security of the data

Measure	Detailing
Organisational control	The internal organisation shall be designed in such a way that it ensures compliance with the requirements of data protection. The Data Importer shall appoint a data protection officer if this is legally required under the laws it is subject to. The Data Importer shall take appropriate organisational measures to ensure the lawful processing of Data, such as the internal appointment of a contact person for data protection, the implementation of processes to ensure the cooperation of the data protection officer and the establishment of clear internal rules on data protection. The Data Importer shall continuously train and sensitise its employees with regard to the requirements of data protection and the implementation of technical and organisational measures.
Access control	Buildings and rooms in which data processing takes place shall be secured against unauthorised access. Measures such as the installation of systems and terminals in secured rooms, that are only accessible to authorised persons, or measures of object security are taken into account. In principle, IT systems are protected against access by unauthorised persons.
Access control	The actual use of data processing equipment by unauthorised persons shall be prevented. This is ensured by user administration and ensuring an adequate password security. User administration requires the establishment of a central point for user administration and the associated identity and access authorisation, as well as regular checking of the validity of user access. Adequate password security requires at least the presence of a basic password strength and securing passwords via login storage systems with hashing functions. In addition, the underlying processing activity may require extended password strength through cross-system password policies up to multi-factor authentication(e.g. magnetic card and PIN) and cryptographic procedures (e.g. AES-128, AES-256) or asymmetric encryption procedures. Hardware components and physical data storage devices will be protected against misuse, e.g. through data carrier encryption, instructions to lock away notebooks and careful handling of mobile devices and confidential paper documents. The data importer will record the measures in a data security concept and oblige its employees to comply with the data security concept.
Access control	Access to data processing systems shall be restricted to authorised users. The authorised users shall only have access to the Data that is necessary for the specific fulfilment of their tasks. This is implemented through a mandatory authorisation concept (differentiation between types of users) by setting time limits and logging unauthorised activities.

Transmission control	Integrity and confidentiality in the transmission of Data shall be guaranteed. Data shall be secured against inspection or modification by unauthorised persons both during its transmission and its transport. To ensure the integrity and confidentiality of Data, the Data Importer shall take into account, inter alia: • Central issuance, management and locking of data carriers; • Documentation of the transmission of Data; • Classification of data according to the degree of confidentiality; • Introduction of technical measures to restrict the unauthorised loss of Data; • Use of encrypted ways of transport; • Encryption of transmitted Data using a high-quality cryptographic procedure.
Input control	The Data Importer shall take appropriate measures, depending on the processing, to be able to review details such as the time and duration of an access to Data. The Data Importer shall ensure, on the one hand, that Data are processed for the intended purpose and, on the other hand, that complete and accurate Data are always available. The Data Importer shall take into account measures such as logging login and logout operations as well as input, modification and deletion access.
Deletion control	The Data Importer has implemented all necessary measures to enable deletion / restriction of Data. This is ensured by: • Work instructions on deletion / restriction / storage limitation; • Implementation of technical and automated deletion concepts • Ensuring the appropriate disposal of data carriers or documents, e.g. by commissioning specialised disposal companies.
Availability control	The Data Importer has taken technical and organisational measures to ensure the availability of Data and systems as quickly as possible, even in the event of damage. This includes measures such as a backup and recovery plan and the creation of backup copies. Synchronous and / or asynchronous physical mirroring of hard disks at separate data centre locations as well as certification of a major incident process (ISO9k) are generally expected. The protection of data carriers against elementary influences such as fire, water and electromagnetic radiation must be ensured. This includes measures such as the installation of smoke detectors and sprinkler systems, fire doors and an independent power supply. Protective measures are used to combat malware. To ensure the correct functioning and integrity of IT systems, protection against malware (malware, viruses, etc.) is a mandatory requirement. To ensure regulated and correct access to the entire system environment and the integrity of the IT systems, the Data Importer will continuously implement the following technical facilities and ensure their operation: • Use of a firewall for effective protection against unauthorised access; and • Use of a proxy server for access to resources outside the Volkswagen network.

Separation control	The purpose-related processing of the Data shall be ensured. The Data Importer shall take the following methods into account: • Use of multi-client capable systems; • access concepts; • Work instructions for purpose limitation; • Encryption of data records; • Logging of events
Pseudonymisation	The Data Importer shall pseudonymise Data as early as possible if purpose of the processing can be fulfilled. Only authorised persons may be able to resolve pseudonymised Data in justified cases. This is ensured by the mandatory authorisation concept.
Transmission control	The parties involved in a communication agree on the use of trusted infrastructures and certification authorities.
Access control	During transmission, Data is encrypted end-to-end using a high-quality cryptographic process. During storage, Data shall be encrypted using a high-quality cryptographic process. The Data Importer shall use automated processing procedures, that make it unnecessary to review the processed Data, to the extent that the purpose of the processing can be fulfilled.