Agreement for order processing between

Karl Wörwag Lack- und Farbenfabrik GmbH & Co. KG

Strohgäustraße 28, 70435 Stuttgart

and

SUPPLIER

Preamble

The contractual parties have entered into an order data processing relationship by a service agreement or the data processing mentioned in the service agreement is performed on behalf of the controller (the so-called order processing) according to Art. 28 of the EU GDPR. The contractual parties have concluded the following agreement to specify the rights and obligations under the order processing relationship according to the legal requirement.

1 Scope of application

The agreement shall apply to all activities which form the subject matter of the service agreement and whose performance makes the employees of the processor or third parties authorised by the processor according to this agreement come into contact with personal data which the controller is responsible for (Art. 4 (7) of the GDPR).

2 Definition

2.1 This agreement refers to the processing of personal data according to the instructions given by the controller.

2.2 Processing means each procedure performed with or without an automatic operation or each of those sets of operations related to the personal data, such as collecting, recording, organising, sorting, saving, adjusting or changing, separating, searching, using, disclosing by transfer, processing or any other form of making data available, matching or linking, reducing, deleting or destroying.

2.3 Personal data are all information which refer to an identified or identifiable natural person (hereinafter the “data subject”); an identifiable person is considered to be a natural person who can be directly or indirectly identified, in particular, by allocation of the identifier such as a name, identification number, location data, online identification or one or several special features which show the physiological, genetical, psychological, economic, cultural or social identity of this natural person.

2.4 The processor is a natural person or corporate entity, authority, institution or another centre which processes personal data on behalf of the controller.

2.5 An instruction is an indication of the controller for a specific handling of data by the processor according to data protection measures (e.g., anonymisation, blocking, deleting, disclosing) which involves personal data. Existing instructions (e.g., by supplements to this agreement) can be later amended, supplemented or replaced by the controller with individual instructions (individual instruction).

3 Specification of the order content

3.1 The subject matter and duration of the order data processing, the scope and purpose of the above-mentioned processing of data shall be stated in the service agreement.

3.2 The type of personal data used has been described in detail in Annex 2 (“Specification of data categories”).

3.3 The group of data subjects whose data are involved has been described in detail in Annex 3 (“Approved subcontractors”).

4 Responsibility and authorisation to instruct

4.1 The controller shall be responsible for observing the legal data protection regulations, in particular for the lawfulness of data transfer to the processor and for the lawfulness of data processing (Art. 4 (7) of the GDPR). The controller can demand disclosing, correcting, deleting and destroying of data at any time (Art. 28 (3)(g) of the GDPR) as long as there is no legal obligation of saving personal data. If the data subjects directly request the processor to delete or correct their data, the processor shall immediately forward this request to the controller and support the latter in fulfilling the request with the data available to the processor (Art. 28 (3)(f) of the GDPR).

4.2 The processor can process the data only within the framework of the documented instructions of the controller, unless the processor is obligated to do so by the laws of the EU or member states which the processor is subject to. In such a case, the processor shall immediately notify the controller about these legal requirements before processing. An instruction is a written indication of the controller for a specific handling of data by the processor according to data protection measures which involves personal data. The instructions are initially defined by the service agreement and can later be amended, supplemented or replaced by the controller in writing by an individual instruction (Art. 28 (3)(a) of the GDPR).

4.3 The processor must immediately notify the controller according to Art. 28 (3) of the GDPR, if the processor is of the opinion that the instruction might breach the legal data protection regulations. The processor shall be entitled to suspend the performance of the respective instruction until it is confirmed or amended by the controller.

4.4 Amendments to the subject matter of processing by changing the procedures shall be agreed and documented mutually. Information to third parties or data subjects can only be given by the processor with a previous written consent of the controller. The processor shall not use the data for any other purposes and in particular, the processor shall not be entitled to transfer the data to third parties. Copies and duplicates shall not be made without the knowledge of the controller. This shall only applyif there is a contrary provision in the agreement or in the cases mentioned in Clause 4.2 of this agreement.

4.5 The controller shall maintain records of processing activities according to Art. 30 (1) of the GDPR. Upon request, the processor shall provide the controller with the information to be included in the records of activities.

4.6 The processing and use of the data on behalf of the person responsible takes place exclusively within the territory of the European Union or the European Economic Area Federal Republic of Germany. A transfer to a state outside the territory of the Federal Republic of Germany requires the prior consent of the responsible person. This does not apply to companies affiliated with the processor pursuant to § 15 of the German Stock Corporation Act, provided that binding corporate rules or EU standard contractual clauses have been agreed with these companies. The special requirements of Art. 44 to 49 GDPR remain unaffected for other cases.

4.7 Processing personal data in private flats of the processor's employees (remote workplace, work from home) shall only be permitted subject to the following requirements: it concerns the hardware of the processor which has been transferred to the employees for work purposes and is operated under the protection of firewall software and secured with VPN client certificate. Access by own hardware of the employee shall not be permitted.

5 Observance of obligatory legal regulations of the controller by the processor

5.1 Apart from the contractual provisions of this agreement and the service agreement, the processor undertakes the following legal obligations according to Art 28 (3), Art. 30 of the GDPR.

5.2 The processor ensures that the employees involved in processing data of the controller have undertaken the obligation according to Art. 5 (I)(c) of the GDPR and have been introduced to the protection provisions of the data protection law. This also includes a notification of the instruction- and purpose-related commitments existing under this order data processing relationship.

5.3 The processor has appointed an internal data protection officer according to Art. 37 of the GDPR who performs his/her activities according to Art. 38 and Art 39 of the GDPR. The contact data of the data protection officer must be provided to the controller for the purpose of direct contact.

5.4 The processor shall immediately notify the controller about the controls and measures of the supervisory authorities according to Art. 58 of the GDPR or if a supervisory authority investigates the processor according to Art. 83 of the GDPR. Moreover, the processor shall immediately notify the controller if the processor is sued for compensation due to a breach of the GDPR, and thereafter, the processor shall inform the controller about the ongoing proceedings at regular intervals.

5.5 When the GDPR comes into force, the processor undertakes to maintain records of processing activities which include all categories of processing activities performed on behalf of the controller (Art. 30 (2) of the GDPR). The records shall include at least

(a) the name and contact data of the processor and each employee of the controller on whose behalf the processor is acting, and, if applicable, of the controller's or processor's representative and any data protection officer;

(b) the categories of processing which is performed on behalf of the controller;

(c) if applicable, transfers of personal data to a third country or international organisation, including the description of the respective third country or international organisation, and in the case of data transfers mentioned in Article 49 (1)(2), the documentation of the suitable guarantee;

(d) if possible, a general description of the technical and organisational measures according to Article 32 (1) of the GDPR.

The processor guarantees a review by the controller of the information in the records related to this processing within 14 days after a written request.

6 Security of processing and its control

6.1 The contractual parties agree on the specific technical and organisational protection measures mentioned in Annex 1 “Technical and organisational measures” to this agreement according to Art. 28 (3)(c) of the GDPR in conjunction with Art. 32 (1) of the GDPR or Art 22 of the BDSG 2018 to guarantee the security of processing performed on behalf of the controller. The Annex constitutes the subject matter of this agreement.

6.2 Technical and organisational measures take into consideration the state of technology at the time of concluding this agreement and are subject to the relevant technical progress. Insofar, the processor is permitted to implement alternative adequate measures. Thereby, the security level determined in the Annex “Technical and organisational measures” cannot be lowered. Important amendments must be documented.

6.3 The processor undertakes to check and evaluate the specific technical and organisational measures with respect to their effectiveness regarding the security of processing at regular intervals and to document this risk evaluation.

6.4 Upon request, the processor shall provide the controller with required information about the fulfilment of its obligation to control the order and make the relevant evidence available. Due to the controller’s obligation to control according to Art. 28 (1)(3) of the GDPR from the beginning of data processing and during the term of the order, the processor ensures that it can convince the controller about the compliance with the agreed technical and organisational measures. For this purpose, the processor shall provide evidence to the controller upon request about the implementation of technical and organisational measures according to Art. 32 (1) and performance of regular risk evaluation according to Clause 6.3. Thereby, evidence for implementation of such measures which do not only concern the specific order can also be provided by submitting valid certificates or reports of independent entities (e.g., certified auditors, auditors committee, data protection officer, IT security department, data protection auditors) or a suitable certification by IT security or data protection audit (e.g. according to BSI basic protection, ISO 27001).

6.5 For checking purposes, the controller can inspect the adequacy of measures regarding the compliance with technical and organisational requirements of the data protection laws applicable to the order data processing at the business premises of the processor during the regular working hours without a disruption of the operating procedures (Art. 28 (3)(h) of the GDPR).

7 Notification of breach by the processor

7.1 The processor shall immediately notify the controller after serious disruptions to its operating procedures are detected, if a breach of contractual or legal data protection provisions is suspected, or other irregularities in the processing of the controller’s data (Art. 28 (3)(3), Art. 33, Art 34 of the GDPR). Thereby, the notification must include at least the following

(a) a description of the type of the personal data protection breach, if possible, including the categories and approximate number of the data subjects, affected categories and approximate number of affected personal data records;

(b) a description of probable consequences of the personal data protection breach;

(c) a description of already taken or proposed measures to remove the personal data protection breach and, if applicable, measures to reduce its possible adverse effects.

If it is not possible to provide all information mentioned in Clause 7.1 (a–c) at the time of notification, such information must be immediately provided when it is known or, if applicable, provided gradually.

7.2 The processor must take adequate measures to secure the data and reduce possible adverse effects for the data subjects in consultation with the controller.

8 Deleting and returning data

8.1 Transferred data carriers and data records shall remain the property of the controller.

8.2 Upon request of the controller, however not later than the statute of limitations for the claims resulting from the underlying service agreement, the processor must return to the controller all documents, generated processing and use results and records (and also copies and reproductions thereof) which remain in his possession and are related to the contractual relationship or destroy them in compliance with data protection law and after prior consent of the controller (Art. 28 (3)(g) of the GDPR). The same shall apply to test and raw materials. A documentation of ensuring proper destruction and a destruction report must be submitted to the controller upon request.

8.3 The processor can store the documentation used as evidence for proper data processing in compliance with the order after the agreement ends, according to the respective statute of limitations or storage periods. Alternatively, the processor can hand over the documentation to the controller in its defence at the end of the agreement.

9 Subcontractors

9.1 The processor shall not commission any other processors without a prior separate written approval of the controller and undertakes to engage subcontractors only according to the following requirements:

(a) The processor shall carefully select subcontractors and prove before commissioning them that they can respect what has been agreed between the controller and processor. In particular, the processor must check before and during the term of agreement on a regular basis that the subcontractor complies with the suitable technical and organisational measures for protection of personal data according to Art. (32)(1) of the GDPR. The results of checks must be documented by the processor. The processor must have the subcontractor confirm that the latter, to the extent required by law, has appointed an internal data protection officer according to Art. 37 of the GDPR.

(b) The processor shall draft the contractual agreements with a subcontractor (subcontractors), so that they would comply with data protection provisions in the contractual relationship between the controller and processor.

9.2 According to this provision, the services rendered to the processor by third parties as ancillary services to support the performance of order are not considered subcontracting. These include, for example, telecommunications services, maintenance and user service, cleaning services, auditors and disposal of data carriers. However, the processor must also conclude proper and lawful contractual agreements and take control measures to guarantee the protection and security of the controller's data, also in the case of third party ancillary services.

9.3 At the time of signing this agreement, the commissioned subcontracters are documented in Annex 3 (“Approved subcontractors”), including the processing locations and type of service. The subcontractors mentioned on this list shall be considered lawfully commissioned from the start according to Clause 9.1, if the implementation of the requirements mentioned therein is guaranteed by the processor.

9.4 The subcontractor may only access data, if the subcontractor also fulfils the obligations of the processor under this agreement or has ensured this to the processor and the processor regularly checks the compliance of the subcontractor with these obligations.

10 Ancillary services

Clauses 1 through 8 shall apply accordingly, if inspection or maintenance of automatic procedures or data processing facilities is performed by other entities on behalf of the processor and thereby, access to personal data cannot be excluded.

11 Confidentiality and data protection control

11.1The controller and the processor undertake to preserve the confidentiality of all company or business secrets which they learn of within the framework of this contractual relationship. This shall apply for the period stipulated in the service agreement and also after the end of individual orders or business relationship.

11.2The processor undertakes to guarantee the access for the internal data protection officers of the controller at any time during regular business hours for the purpose of performing their respective legal tasks in relation to this order.

12 Final provisions

12.1Amendments and supplements to this annex and all its integral parts, including any assurances of the processor require a written agreement and clear indication that they are amendments or supplements to these terms. This shall also apply to waiving the written form requirement. The written form requirement shall not apply if it is cancelled between the contractual parties based on a clear and individual agreement.

12.2The following annexes form integral parts of this agreement:

Annex 1 “Technical and organisational measures”

Annex 2 “Specification of data types/data categories”

Annex 3 “Approved subcontractors”

Annex 1 to Agreement of order processing

A. Technical-organisational measures according to Art. 32 (1)(a-d) of the EU GDPR

1. Pseudonymisation (Art. 32 (1)(a) of the EU GDPR)
The data that must be analysed for statistical purposes are pseudonymised and saved without personal reference. The data which subcontractors must forward are pseudonymised, if possible and then, do not constitute personal data for the subcontractor according to the judgement of the EU Court dated 19th October 2016 (C 582/2014).

2. Encryption (Art. 32 (1)(a) of the EU GDPR)
Personal data are saved on mobile data carriers and mobile devices only as encrypted data. Access to the data saved at the data centre is possible only through encrypted connections. Data are transferred only when strongly encrypted according to the BSI Guideline TR-2102.

3. Guarantee of confidentiality (Art. 32 (1)(b) of the EU GDPR)
Unauthorised persons must be prevented from penetrating the data processing systems. The authorisations are managed according to a role-based concept of rights. Each employee has access to the data processing system which is secured by a password protection. The password must include a mix of numbers, letters and special symbols and consist of a minimum of eight characters. Individual data processing systems are blocked during break times. It is possible to unblock the systems only with a password. Authorisations are regularly checked for validity. Numerous measures ensure that personal data collected for different purposes can be processed separately (eg through multi-client capability and authorization concept). Access to rooms where data processing takes place is controlled and denied to unauthorized persons. The offices are secured by a locking system, visitors must register with attendance times in a list. The rooms of the data center are secured by an electronic access system with documented permissions, a stay of unauthorized persons in the data center is only permitted for cases of maintenance and only in the company of an authorized person. Attendance times in the data center are logged electronically. Processors are only commissioned with the processing of personal data if equivalent technical and organizational measures are guaranteed. Personal data are, as far as it is not a processor, only passed on the instructions of the person responsible or on a legal basis.

4. Guarantee of integrity (Art. 32 (1)(b) of the EU GDPR)
Only limited write authorisations are granted for data. There are regular integrity tests. There are regular security tests such as penetration tests.

5. Guarantee of availability (Art. 32 (1)(b) of the EU GDPR)
The data must be protected against incidental destruction or loss. In principle, all data are stored redundantly (at least on fail-safe RAID systems level 5 or 6). Full multiple redundant data security and/or replication is created and stored outside the building with the original data. Uninterruptable power supply, firewall and anti-virus software are used to secure the availability of data.

6. Guarantee of system capacity (Art. 32 (1)(b) of the EU GDPR)
The capacity of communication connections and computing capacity are ensured by an on-going supervision of the equipment.

7. Procedures for restoring the availability of personal data after a physical or technical incident (Art. 32 (1)(c) of the EU GDPR)
Regular restoring of back-up data takes place. We strive to reduce the number of incidents by redundant storage at different locations.

8. Performance of regular supervision, analysis and evaluation of the effectiveness of technical and organisational measures (Art. 32 (1)(d) of the EU GDPR
An IT security and data protection concept has been developed which is continuously checked for any need of adjustment. Amendments are documented and checked for their effectiveness at regular intervals.

B. Additional technical and organisational measures in the case of processing sensitive data according to Section 22 (2) of the Federal Data Protection Act (Bundesdatenschutzgesetz, BDSG) 2018:

The employees are regularly trained in the area of data protection regarding the current situation. A data protection officer has been appointed.

Taking into account the latest state of technology, implementation costs and type, scope and purpose of processing, as well as the different occurrence probability and seriousness of the processing risks related to the rights and freedoms of a natural person, the following other security measures are taken during the processing of sensitive data according to Art. 9 (1) of the EU GDPR considering the proportionality:

S1. Input control (Section 22 (2) (2) of the BDSG 2018)

The input, amendment and deletion of sensitive personal data is recorded, including the individualisable processor identification.

S2. Limitation of access to personal data (Section 22 (2)(5) of the BDSG 2018)

Personal data which do not require any access for lawful processing of data according to the principle of data minimisation according to Art. 5 (1)(c) of the EU GDPR are locked against the access by the employees of the controller or the processor. For this purpose, a role- and group-based authorisation concept has been developed (cf. A(3) and (8) above)

S3. Specific procedure regulations which ensure the compliance with requirements of this Act and Regulation (EU) 2016/679 in the case of transfer or processing for other purposes

In the case of special data protection requirements according to industry-specific legal or contractual provisions or articles of association, the protection measures are discussed with the controller and adjusted to the relevant necessary protection level in individual cases. This shall also include the compliance with specific data protection and data security norms and standards (ISO 27001, BSI Basic Protection Standard 200-1 through 200-3, the German Security Screening Act, protection category classification of documents in public service, etc.)

The other points of Section 22 (2) of the BDSG have already been covered by the provisions of the Regulation (see A (1) through (8) above).

Annex 2 to Agreement for order processing

Specification of data types, data categories and data subjects

1. Specification of data types and data categories:
- Customer master data (e.g. customer contact data, addresses, etc.)
- Reference data (e.g. terms of payment and delivery, bank accounts data, etc.)
- Company-wide structural data (e.g. products, services, responsibilities of employees, etc.)
- Transaction data (e.g. business activity, etc.)
2. Specification of data subjects:
- Customers and their employees (contact person)

Annex 3 to the Agreement for order processing

Approved subcontractors