Supplementary terms and conditions for the processing of data on behalf

within the meaning of Article 28 (3) of the EU General Data Protection Regulation ("GDPR") (hereinafter referred to as the "Data Processing Agreement") between Schwarz Druck GmbH, Industriestrasse 2, 83734 Hausham (hereinafter referred to as the "Processor") and the controller (hereinafter referred to as the "Controller"), the following Data Processing Agreement is concluded.

1. General

(1) The Processor shall process personal data on behalf of the Controller within the meaning of Art. 4 No. 8 and Art. 28 of Regulation (EU) 2016/679 - General Data Protection Regulation (GDPR). This contract regulates the rights and obligations of the parties in connection with the processing of personal data.

(2) Insofar as the term "data processing" or "processing" (of data) is used in this Agreement, the definition of "processing" as defined in Art. 4 No. 2 of the GDPR shall apply.

2. Conclusion of Contract, Purpose of Contract and Scope of Services

(1) The commissioned processing shall take place within the framework of the legal relationship (General Terms and Conditions, main contract, service agreement or the service certificate) and shall come into force upon commissioning of the same.

(2) The supplementary terms and conditions for the processing of data on behalf of the Controller shall be automatically accepted upon conclusion of the Terms and Conditions. An additional signature is not required.

(3) The subject of the processing, the type and purpose of the processing, the type of personal data and the categories of data subjects are specified in **Annex 1** to this Agreement.

(4) Commissioned processing within the meaning of Art. 28 GDPR shall only take place with the processing of personal data. The printing of prefabricated documents or graphics without their prior processing by the Processor, in which data processing is not the main focus, or in which data processing does not constitute at least an important (core) component, does not constitute commissioned processing in the sense of data protection law. The legal basis for data processing by the print shop is Art. 6 (1) letter f GDPR.

3. Rights and Obligations of the Controller

(1) The Controller is the responsible party within the meaning of Art. 4 No. 7 GDPR for the processing of data on behalf of the Processor. Pursuant to Section 4 (3), the Processor shall have the right to inform the Controller if it considers data processing to be legally inadmissible as part of the order and/or instructions.

(2) As the responsible party, the Controller shall be responsible for safeguarding the rights of the data subjects. The Processor shall inform the Controller without delay if data subjects assert their data subject rights against the Processor.

(3) The Controller shall have the right to issue supplementary instructions to the Processor at any time regarding the type, scope and procedure of data processing. Instructions must be given in text form (e.g., e-mail).

(4) Regulations on any remuneration of additional expenses incurred by the Processor due to supplementary instructions of the Controller shall remain unaffected.

(5) The Controller may appoint persons authorized to issue instructions. Insofar as persons authorized to issue instructions are to be named, they shall be named in **Annex 1**. If the persons authorized to give instructions to the Controller change, the Controller shall notify the Processor thereof in text form.

(6) The Controller shall inform the Processor without undue delay if it discovers errors or irregularities in connection with the processing of personal data by the Processor.

(7) In the event that there is an obligation to inform third parties pursuant to Art. 33, 34 GDPR or any other statutory notification obligation applicable to the Controller, the Controller shall be responsible for compliance therewith.

4. General Obligations of the Processor

(1) The Processor shall process personal data exclusively within the scope of the agreements made and/or in compliance with any supplementary instructions issued by the Controller. Excluded from this are legal regulations which may oblige the Processor to process data in a different manner. In such a case, the Processor shall notify the Controller of these legal requirements prior to processing, unless the relevant law prohibits such notification due to an important public interest. The purpose, nature and scope of the data processing shall otherwise be governed exclusively by this Agreement and/or the Controller's instructions. The Processor is prohibited from processing data in any other way unless the Controller has given its written consent.

(2) The Processor shall generally carry out data processing on behalf of the Controller in member states of the European Union (EU) or the European Economic Area (EEA). The Processor is also permitted to process data outside the EU or EEA if corresponding subprocessors are used in the third country in compliance with the requirements of Section 9 and the requirements of Art. 44-48 GDPR are met, or an exception as defined in Art. 49 GDPR exists.

(3) The Processor shall inform the Controller without undue delay if, in its opinion, an instruction issued by the Controller violates statutory provisions. The Processor shall be entitled to suspend the implementation of the relevant instruction until it is confirmed or amended by the Controller. If the Processor can demonstrate that processing in accordance with the Controller's instructions may lead to liability on the part of the Processor in accordance with Art. 82 GDPR, the Processor shall be entitled to suspend further processing in this respect until the liability between the parties has been clarified.

(4) The Processor may name to the Controller the person(s) authorized to receive instructions from the Controller. If persons authorized to receive instructions are to be named, they shall be named in **Annex 1**. If the persons authorized to receive instructions change at the Processor, the Processor shall notify the Controller thereof in text form.

5. Data Protection Officer of the Processor

(1) The Processor confirms that it has appointed a data protection officer in accordance with Art. 37 GDPR. The Processor shall ensure that the data protection officer has the required qualifications and expertise. The Processor shall inform the Controller of the name and contact details of its data protection officer separately in text form.

(2) The obligation to appoint a data protection officer pursuant to paragraph 1 may be waived at the discretion of the Controller if the Processor can prove that it is not required by law to appoint a data protection officer and the Processor can prove that operational regulations exist that ensure processing of personal data in compliance with the statutory provisions, the provisions of this Agreement and any further instructions of the Controller.

6. Reporting Obligations of the Processor

(1) The Processor shall be obliged to notify the Controller without undue delay of any infringement of data protection regulations or of the contractual agreements made and/or the instructions issued by the Controller which has occurred during the processing of data by the Processor or other persons involved in the processing. The same shall apply to any violation of the protection of personal data processed by the Processor on behalf of the Controller.

(2) Furthermore, the Processor shall inform the Controller without undue delay if a supervisory authority pursuant to Art. 58 GDPR acts against the Processor and this may also concern a control of the processing which the Processor performs on behalf of the Controller.

(3) The Processor is aware that the Controller may be subject to a notification obligation pursuant to Art. 33, 34 GDPR, which provides for notification to the supervisory authority within 72 hours of becoming known. The Processor shall support the Controller in implementing the reporting obligations. In particular, the Processor shall notify the Controller of any unauthorized access to personal data processed on behalf of the Controller without undue delay after becoming aware of such access. The Processor's notification to the Controller shall contain the following information:

– a description of the nature of the personal data breach, including, to the extent possible, the categories and approximate number of data subjects concerned, the categories concerned, and the approximate number of personal data records concerned.

– a description of the measures taken or proposed to be taken by the Processor to address the personal data breach and, where applicable, measures to mitigate its possible adverse effects.

7. Cooperation Obligations of the Processor

(1) The Processor shall support the Controller in its obligation to respond to requests for the exercise of data subject rights pursuant to Art. 12-23 GDPR. The provisions of Section 11 of this Agreement shall apply.

(2) The Processor shall cooperate in the preparation of directories of processing activities by the Controller. The Processor shall provide the Controller with the information required in this respect in an appropriate manner.

(3) The Processor shall support the Controller in complying with the obligations set out in Art. 32-36 GDPR, considering the type of processing and the information available to it.

8. Inspection authority

(1) The Controller shall have the right to monitor the Processor's compliance with the statutory provisions on data protection and/or compliance with the contractual provisions agreed between the parties and/or compliance with the Controller's instructions to the extent necessary.

(2) The Processor shall be obligated to provide the Controller with information to the extent that this is necessary to carry out the control within the meaning of paragraph 1.

(3) The Controller may carry out the inspection within the meaning of Paragraph 1 at the Processor's premises during normal business hours after prior notification with a reasonable period of notice. In doing so, the Controller shall ensure that the inspections are only carried out to the extent necessary in order not to disproportionately disrupt the Processor's business operations because of the inspections. The parties assume that an inspection is required no more than once a year. Further inspections shall be justified by the Controller stating the reason. In the case of on-site inspections, the Controller shall reimburse the Processor to a reasonable extent for the expenses incurred, including personnel costs for the supervision and support of the inspection personnel on site. The Processor shall inform the Controller of the basis of the cost calculation before the inspection is carried out.

(4) At the discretion of the Processor, proof of compliance with the technical and organizational measures may also be provided instead of an on-site inspection by submitting a suitable, current audit certificate, reports or report excerpts from independent bodies (e.g., auditors, auditing department, data protection officer, IT security department, data protection auditors or quality auditors) or a suitable certification, if the audit report enables the Controller to reasonably satisfy itself of compliance with the technical and organizational measures pursuant to **Annex 3** to this Agreement. If the Controller has reasonable doubts about the suitability of the test document within the meaning of clause 1, an on-site inspection may be carried out by the Controller. The Controller is aware that an on-site inspection in data centers is not possible or only possible in justified exceptional cases.

(5) In the event of measures by the supervisory authority vis-à-vis the Controller within the meaning of Art. 58 GDPR, in particular regarding information and control obligations, the Processor shall be obligated to provide the Controller with the necessary information and to enable the respective competent supervisory authority to

conduct an on-site inspection. The Controller shall be informed by the Processor about corresponding planned measures.

9. Sub Processors

(1) At the time of conclusion of the contract there are no sub processors. The commissioning of further sub processors may take place on an order-related basis and shall be permissible under the conditions specified in paragraph 2.

(2) The Processor shall carefully select the sub processor and, prior to commissioning, check that the sub processor is able to comply with the agreements made between the Controller and the Processor. In particular, the Processor shall check in advance and regularly during the term of the contract that the sub processor has taken the technical and organizational measures required under Art. 32 GDPR to protect personal data. In the event of a planned change of a sub processor or in the event of a planned commissioning of a new sub processor, the Processor shall inform the Controller in text form in good time, but no later than 4 weeks before the change or the new commissioning ("Information"). The Controller shall have the right to object to the change or the new assignment of the sub processor in text form within three weeks after receipt of the "Information", stating the reasons. The objection may be withdrawn by the Controller in text form at any time. In the event of an objection, the Processor may terminate the contractual relationship with the Controller with a notice period of at least 14 days to the end of a calendar month. The Processor shall reasonably consider the interests of the Controller in the notice period. If no objection is raised by the Controller within three weeks of receipt of the "Information", this shall be deemed to be the Controller's consent to the change or new commissioning of the sub processor concerned.

(3) The Processor shall be obliged to obtain confirmation from the sub processor that the latter has appointed a company data protection officer in accordance with Art. 37 GDPR, insofar as the sub processor is legally obliged to appoint a data protection officer.

(4) The Processor shall ensure that the regulations agreed in this Agreement and any supplementary instructions of the Controller also apply to the sub processor.

(5) The Processor shall conclude a contract processing agreement with the sub processor that complies with the requirements of Art. 28 GDPR. In addition, the Processor shall impose on the sub processor the same obligations for the protection of personal data that are specified between the Controller and the Processor. A copy of the commissioned data processing agreement shall be provided to the Controller upon request.

(6) The Processor shall be obliged to ensure by contractual provisions that the control authorities (Clause 8 of this Agreement) of the Controller and of supervisory authorities also apply to the sub processor and that corresponding control rights of the Controller and supervisory authorities are agreed. It shall also be contractually stipulated that the sub processor must tolerate these control measures and any on-site inspections.

(7) Services which the processor uses from third parties as purely ancillary services to carry out the business activity shall not be regarded as subcontracting relationships within the meaning of paragraphs 1 to 6. This includes, for example, cleaning services, pure telecommunication services without any specific reference to services provided by the Processor to the Controller, postal and courier services, transport services, security services. The Processor shall nevertheless be obliged, also in the case of ancillary services provided by third parties, to ensure that appropriate precautions and technical and organizational measures have been taken to guarantee the protection of personal data. The maintenance and servicing of IT systems or applications constitutes a subcontracting relationship requiring consent and commissioned processing within the meaning of Art. 28 GDPR if the maintenance and testing concern such IT systems that are also used in connection with the provision of services for the Controller and personal data processed on behalf of the Controller can be accessed during the maintenance.

10. Confidentiality Commitment

(1) When processing data for the Controller, the Processor shall be obliged to maintain confidentiality with regard to data which it receives or becomes aware of in connection with the order.

(2) The Processor has familiarized its employees with the provisions of data protection applicable to them and obligated them to maintain confidentiality.

(3) The obligation of the employees pursuant to paragraph 2 shall be proven to the Controller upon request.

11. Protection of Data Subject Rights

(1) The Controller shall be solely responsible for safeguarding the rights of data subjects. The Processor is obligated to support the Controller in its duty to process requests from data subjects pursuant to Art. 12-23 GDPR. In particular, the Processor shall ensure that the information required in this respect is provided to the Controller without delay so that the Controller can fulfill its obligations under Article 12 (3) GDPR.

(2) Insofar as the Processor's cooperation is required for the protection of data subject rights - for information, correction, blocking or deletion - by the Controller, the Processor shall take the measures required in each case in accordance with the Controller's instructions. The Processor shall support the Controller as far as possible with suitable technical and organizational measures in fulfilling its obligation to respond to requests for the exercise of data subject rights.

(3) This shall be without prejudice to any provisions regarding the remuneration of additional expenses incurred by the Processor because of cooperation services in connection with the assertion of data subject rights vis-à-vis the Controller.

12. Nondisclosure Agreements

(1) Both parties undertake to treat all information received in connection with the performance of this Agreement as confidential for an unlimited period and to use it only for the performance of the Agreement. Neither party shall be entitled to use this information in whole or in part for purposes other than those just mentioned or to make this information available to third parties.

(2) The above obligation shall not apply to information which one of the parties has demonstrably received from third parties without being obliged to maintain confidentiality or which is publicly known.

13. Payment

The payment of the Processor shall be agreed separately.

14. Technical and Organizational Measures for Data Security

(1) The Processor undertakes vis-à-vis the Controller to comply with the technical and organizational measures required to comply with the applicable data protection provisions. This includes the requirements of Art. 32 GDPR.

(2) The Processor confirms that a valid INTERGRAF certificate according to ISO 14298:2013 exists at the time of the conclusion of the contract. This certification includes extensive technical and organizational measures for controlling the security printing processes. The proof can be made available to the Controller if required. The parties agree that changes to the technical and organizational measures may be necessary to adapt to technical and legal circumstances. The Processor shall agree in advance with the Controller on any significant changes that may affect the integrity, confidentiality, or availability of the personal data. Measures that involve only minor technical or organizational changes and do not negatively affect the integrity, confidentiality and availability of the personal data can be implemented by the Processor without coordination with the Controller. The Controller may request an updated version of the technical and organizational measures taken by the Processor once a year or on justified occasions.

15. Duration of the Contract

(1) The contract shall commence upon signing and shall run for the duration of the main contract existing between the parties for the use of the Processor's services by the Controller.

(2) The Controller may terminate the contract at any time without notice if there is a serious breach by the Processor of the applicable data protection provisions or of obligations under this contract if the Processor cannot or will not carry out an instruction of the Controller or if the Processor refuses access by the Controller or the competent supervisory authority in breach of the contract.

16. Termination

(1) After termination of the contract, the Processor shall return to the Controller or delete, at the Controller's discretion, all documents, data and processing or utilization results created in its possession which are related to the contractual relationship. The deletion shall be documented in a suitable manner.

(2) The Processor may store personal data processed in connection with the order beyond the termination of the contract if and to the extent that the Processor has a legal obligation to retain such data. In such cases, the data may only be processed for the purpose of implementing the respective statutory retention obligations. After expiry of the retention obligation, the data must be deleted immediately.

17. Right of Retention

The parties agree that the defense of the right of retention by the Processor within the meaning of Art. 273 German Civil Code (BGB) is excluded regarding the processed data and the associated data carriers.

18. Final Provisions

(1) Should the property of the Controller with the Processor be endangered by measures of third parties (e.g., by attachment or seizure), by insolvency proceedings or by other events, the Processor shall inform the Controller without delay. The Processor shall inform the creditors without undue delay of the fact that data processed under the order is involved.

(2) Additional agreements must be made in writing.

(3) Should individually parts of this contract be invalid, this shall not affect the validity of the remaining provisions of the contract.

Annex 1 - Subject of the Agreement

1. Subject and Purpose of processing

The Controller's order to the Processor includes the following work and/or services:

- Processing and printing of data with personal reference

2. Type(s) of personal data

The following types of data are regularly subject to processing:

Selection	Data Category	Data Examples
X	Professional contact and (work) organization data	Name, first name, gender, address, e-mail address, telephone number, cell phone number, company, area, department, personnel numbers, responsibilities, functions, etc.
	IT usage data	User ID, roles, permissions, login times, computer name, IP address, software, virus protection, software update, etc.
	Contract and inventory data	Beauftragte Leistungen, gekaufte Produkte, Datum Kaufvertrag, Kaufpreis, Garantien, etc.
X	Communication data and their histories	Email history, call history, communication history of the CRM system, etc.
	Personnel data	Pay scale group, payroll accounting, special payments, garnishment, daily attendance times, reasons for absence, etc.
	Particularly sensitive personal data	Racial and ethnic origin, political opinions, religious or philosophical beliefs, trade union membership, genetic data, biometric data uniquely identifying a natural person, health data, or data concerning sex life or sexual orientation.
	Credit rating and bank data	Payment history, balance sheets, data from credit agencies, score values, asset ratios, bank account details, credit card numbers, etc.
X	Accounting data	Invoices, activity records, written orders, history data in ticket systems
X	Other data	Content data for the creation of the print job. This data is provided by the controller and compiled for printing.

3. Categories of person concerned

Group of persons affected by the data processing:

- Employees / staff of the Controller

- Business partners and end controllers of the Controller (third parties)

4. Instructions

(1) The Controller shall immediately confirm verbal instructions in writing (e.g., by e-mail).

(2) The Processor shall inform the Controller without delay if it is of the opinion that an instruction violates data protection regulations. The Processor shall be entitled to suspend the implementation of the corresponding instruction until it is confirmed and amended by the Controller.

5. Data Protection Officer of the Processor

The Processor has appointed the following as data protection officer Mr. Stephan Krischke, datenschutz@schwarz-druck.de. The Controller shall be notified immediately of any change in the data protection officer.