# AGREEMENT

REGARDING

THE PROCESSING OF PERSONAL DATA
IN ACCORDANCE WITH ART. 28 PARA. 3
OF THE EUROPEAN GENERAL DATA PROTECTION REGULATION 2016/679 ("GDPR")

**BETWEEN**

*Customer/User*

**- hereinafter referred to as the PRINCIPAL (CONTROLLER) -**

**AND**

*mediahelden GmbH*
*Theodpr-Lipps-Straße 4*
*80997 Munich, Germany*

**- hereinafter referred to as the CONTRACTOR (PROCESSOR) -**

## Preamble

This contract specifies the obligations of the contracting parties with regard to data protection that arise during the provision of the commissioned service. It applies to all activities in connection with the service in which employees of the contractor or other contractors commissioned by the contractor process personal data ("data") relating to the contract on behalf of the contracting authority within the meaning of Art. 4 No. 2 and 28 GDPR ("data processing").

## 1. Subject, Term and Specification of data processing

1.1. The subject, term, nature and purpose of the data processing, as well as the type of Data and categories of people affected, will result from the Main Contract. If such details are not specified in the Main Contract, this information should be listed in **no. I of Appendix 1** to this agreement. Changes to the subject of the processing and changes of processes must be made in writing or in a documented electronic format.

1.2. The services agreed upon in this agreement and in the Main Contract will only be provided in a member state of the European Union or in a country which is a signatory to the Agreement on the European Economic Area. Any relocation of services, or sub-operations thereof, to a third country ("Relocation") will require the Principal's prior consent and may only take place providing the special requirements set out in Article 44 et seq. of the GDPR are fulfilled (e.g. adequacy decision by the European Commission, standard data protection clauses, approved codes of conduct). Any relocations based on these principles and undertaken at the beginning of the processing are listed in **no. II of Appendix 1** to this agreement.

1.3. The term of this agreement and options for termination will be governed by the Main Contract unless otherwise specified in the provisions of this agreement.

The Principal may terminate this agreement, and the Main Contract – insofar as the latter relates to the services set out in more detail in this agreement – at any time without notice, (1) if the Contractor is in serious infringement of data protection rules or the provisions of this agreement, or (2) if the Contractor is unable or unwilling to comply with the Principal's instructions, or (3) if the Contractor denies the Principal's control and monitoring rights in contrary to the terms of the agreement. In particular, failure to comply with the obligations agreed upon in this agreement and arising from Art. 28 of the GDPR will constitute a serious infringement. Termination must be in writing, or in a documented electronic format ("special right of termination in the case of serious data protection infringements").

## 2. Rights and Obligations of the Contractor

2.1. The Contractor will only process the Data of subjects within the framework of the agreements entered into, and the documented instructions from the Principal, unless obligated to process said Data differently by European Union law or laws of member states to which the Processor is subject (e.g. investigation by law enforcement or state security authorities). In such cases, the Processor will notify the Principal of such legal requirements prior to the processing, provided that the right to such notification is not prohibited for important grounds of public interest (Art. 28(3) point (a) of the GDPR).

2.2. Subject to Art. 28(3) point (a) of the GDPR, the Contractor will notify the Principal immediately if he believes that an instruction breaches applicable legislation. In such cases, the Contractor will be entitled to suspend execution of the instruction until the parties have reached a mutually acceptable solution.

2.3. The Contractor will not use the Data provided for any other purpose and, in particular, not for its own purposes. The Data will not be copied or duplicated without the Principal's knowledge.

2.4. The Contractor commits to maintain confidentiality when processing the instruction-related Data and, in particular, to treat all knowledge of the Principal's trade secrets and data security measures gained during the course of the contractual relationship as confidential. This obligation will continue to apply even after completion of the execution or termination of the agreement. In this respect, the Contractor hereby warrants that the Data processed on behalf of the Principal will be kept entirely separate from other stored data. Storage devices originating from the Principal and used on the Principal's behalf will be specially identified. Actual use as well as receipt and dispatch thereof will be documented.

2.5. The Contractor assists the Principal by appropriate technical and organisational measures, insofar as this is possible, for the fulfilment of the Principal´s obligation to respond to requests for exercising the data subject´s rights laid down in Chapter III of the GDPR (Art. 28(3) point (e) of the GDPR).

2.6. The Contractor will provide the Principal with reasonable assistance in complying with the obligations set out in Articles 32 to 36 of the GDPR, for example with the creation of documentation of processing activities, or with carrying out the necessary data protection impact assessment by the Principal (Art. 28(3) point (f) of the GDPR). Any information needed for such purposes must be forwarded to the Principal immediately in each instance.

2.7. The Contractor will immediately notify the Principal of any incidents or breaches and violations of the data protection provisions or agreements entered into under this agreement by individuals employed by him or third parties engaged by him. This will apply as soon as such an incident is suspected and, in particular, with regard to the Principal's possible notification and reporting obligations pursuant to Articles 33 and 34 of the GDPR. In this respect, the Contractor hereby commits to provide the Principal with reasonable assistance as required for its obligations under Articles 33 and 34 of the GDPR (Art. 28(3) point (f) of the GDPR). The Contractor may only issue notifications pursuant to Article 33 or 34 of the GDPR on behalf of the Principal upon prior instruction. In each case however, the Contractor will take all necessary measures to safeguard the Data and avoid any possible detrimental consequences for the data subjects. Such measures will be agreed upon with the Principal.

2.8. The Contractor will provide the Principal with all necessary information to demonstrate compliance with the obligations set out for the data processing in Art. 28 of the GDPR and enable and contribute to audits and inspections – always by prior arrangement – to be performed by the Principal, or by another auditor commissioned by the latter (Art. 28(3) point (h) of the GDPR). Clauses 3.3 and 6 of this agreement shall additionally apply.

2.9. The Contractor confirms his awareness of the data protection rules of the GDPR applicable to him for data processing, and that he has instructed individuals charged with providing the service on data protection provisions applicable to them prior to commencing the data processing. The Contractor further commits to comply with the relevant rules on protecting secrecy relevant to this agreement and to which the Principal is subject. Where applicable, these secrecy rules will be listed in **no. III of Appendix 1** to this agreement.

2.10. The Contractor hereby warrants that he has prohibited the employees involved in processing the Data and other individuals working for the Contractor from processing the Data in other ways than instructed. Moreover, the Contractor hereby warrants that the persons authorised to process the Data have been obliged to confidentiality prior to the data processing or are subject to an adequate

legal confidentiality obligation (Art. 28(3) point (b) and Art. 29 of the GDPR), and that said confidentiality obligation will continue to be valid following termination of the agreement concluded with the parties charged with processing the data.

2.11. The Contractor will provide the Principal with details of a contact person for all matters regarding data protection arising in connection with this agreement, and as a specific recipient for instructions on the part of the Contractor. Said contact (and the specific party authorised to issue the Principal's instructions) will be listed in **no. IV of Appendix 1** to this agreement. In the case of a change, or the long-term incapacity of one of the specified contacts, the other party must be notified of a successor or substitute immediately in writing or in a documented electronic format.
Instructions must be retained for their entire period of validity and for a further three full calendar years afterwards.

2.12. The Contractor will correct, delete or limit the processing of data, if the Principal instructs him to.

2.13. Provided that the Contractor is legally required to do so, he must appoint a data protection officer. Further details of this, in particular the contact details of the data protection officer appointed, can be found in **no. V of Appendix 1** to this agreement. Any change to the the data protection officer or the fulfilment of legal requirements and the resulting appointment of a data protection officer must be reported to the Principal in writing or in a documented electronic format.

2.14. At the end of data processing, all Data, data mediums, documents and other materials, and in particular all results from the data processing and usage associated with the contractual relationship, received by the Contractor or by subcontractors, must either be returned to the Principal or deleted and destroyed in accordance with data protection legislation. This decision will be at the Principal's discretion. Further information on this can be found in **no. VI of Appendix 1** to this agreement.

## 3. Rights and Obligations of the Principal

3.1. The Principal alone will be responsible for assessing the permissibility of data processing in accordance with Art. 6(1) of the GDPR, and for safeguarding the rights of the data subjects pursuant to Articles 12 to 22 of the GDPR.

3.2. The Pricinipal has the right to assure itself of the compliance with the Contractor's technical and organisational measures before entering into this agreement and afterwards regularly in an appropriate way. This both applies to this agreement as well as the obligations from the Main Contract (see clause 2.8).

3.3. Where inspections by the Principal, or by an auditor commissioned by him, are necessary in individual cases, these will be generally performed during normal business hours without disruption to the business of the Contractor following a reasonable advance notice of 28 days as a minimum. However, in case of a personal data breach in accordance with Art. 4(12) GDPR or a serious infringement of the provisions of this agreement, the advance notice period may be reduced. The Contractor may execute such inspections dependent upon signature of a confidentiality declaration regarding data belonging to other clients or customers of him and the technical and organisational measures put in place. If the auditor commissioned by the Principal is in competition with the Contractor, the Contractor will have a right to object to said auditor.

3.4. The Principal must inform the Contractor immediately upon finding any problems or irregularities regarding data protection rules as a result of instructions in accordance to this agreement.

3.5. The Principal will provide the Contractor with details of a contact person that is authorised to execute all instructions regarding matters of data protection arising in connection with this agreement. Said contact will be listed in **no. IV of Appendix 1** to this agreement. In the case of a change, or the long-term incapacity, of one of the specified contacts, the other party must be notified of a successor or substitute immediately in writing or in a documented electronic format.

3.6. Instructions will initially be set out in the Main Contract or this agreement. Subsequent instructions must be given in writing or in a documented electronic format, submitted to the contact specified by the Contractor (see **no. IV of Appendix 1** to this agreement). In order to be valid, unwritten instructions must be confirmed in writing or in a documented electronic format. Instructions must be retained for the entire period of validity and for an additional three years from the end of the calendar year in which the validity of the instruction has expired.

3.7. The Principal will be obliged to treat all knowledge of the Contractor's trade secrets and data security measures gained during the course of the contractual relationship as confidential. This obligation will continue to exist even following termination of this agreement.

## 4. Enquiries from Data Subjects

4.1. In the case of claims laid against one of the parties by a data subject on the grounds of any claims pursuant to Art. 82 of the GDPR, the Contractor and the Principal mutually commit to assist one another to defend the claims to the best of their ability.

4.2. If a data subject contacts the Contractor with requests to correct or delete data or requests information, the Contractor will refer the data subject to the Principal and will immediately forward the data subject's request to the Principal if the assignment to the Principal is possible based on the details given by the data subject. The Contractor may only provide data, the processing of data or the contractual relationship to subjects or other third parties if the Principal has agreed before.

## 5. Technical and Organisational Measures

5.1. The Contractor will maintain a level of protection that is appropriate to the rights and freedom of persons subject to data processing. The Contractor will implement all technical and organisational measures required to protect the Principal's data. Such measures will meet the requirements of the General Data Protection Regulation, in particular those of Art. 32 of the GDPR. These technical and organisational measures ("TOMs") will be appended to this agreement as **Appendix 2**. They will contain a detailed description of all of the measures implemented, that are appropriate to the identified risk and take into account the protection objectives and the IT systems and processing operations implemented by the Contractor. In particular, the Contractor must take measures to ensure the ongoing confidentiality, integrity, availability and resilience of data processing systems and services.

5.2. The Contractor will monitor compliance with the data protection rules within its organisation.
The measures taken by the Contractor, or by a commissioned subcontractor, may be changed during the course of the contractual relationship in accordance with technical and organisational developments but may not fall short of the agreed standards and those required by law. Major decisions affecting of data processing and the related procedures must be agreed upon between the Contractor and the Principal. Major changes to the technical and organisational measures must be agreed upon by the Contractor with the Principal in writing or in a documented electronic format. Such agreements must be retained for the term of this agreement and for an additional three years from the end of the calendar year in which this agreement has expired.

5.3. The Contractor hereby assures to fulfil its obligations pursuant to Art. 32(1) point (d) of the GDPR and will adopt a process for regularly testing and assessing the effectiveness of technical and organisational measures for ensuring the security of the processing. The Principal must be notified of the results of such checks in each instance.

## 6. Guarantees, Evidence

6.1. The Contractor guarantees that suitable technical and organisational measures will be implemented such that the processing is done in compliance with the European General Data Protection Regulation and this agreement, and such that data subject's rights are ensured (Art. 28(1) of the GDPR). The Contractor further guarantees that, taking into account the current state of technology, the implementation costs and the nature, scope, circumstances and purpose of the processing along with different probabilities of occurrence and severity of risk, the technical and organisational measures taken will ensure a reasonable level of protection (Art. 32(1) of the GDPR). The Contractor will provide the Principal with evidence of compliance with these guarantees by suitable means (e.g. documents, certifications, audits and certificates, etc.). Further information on this can be found in **no. VII of Appendix 1** to this agreement.

6.2. If relevant, the Contractor commits to inform the Principal about the suspension or exclusion of approved codes of conduct pursuant to Art. 41(4) of the GDPR or the withdrawal of a certification in accordance with Art. 42(7) of the GDPR immediately.

## 7. Subcontractors (other Processors)

7.1. Commissioning subcontractors to process the Principal's Data will always require either the separate approval of the Principal in each individual case, or general authorisation (Art. 28(2) of the GDPR). In all cases the Contractor must ensure that the subcontractor is selected carefully giving special consideration to the suitability of the technical and organisational measures implemented by the latter as defined in Art. 32 of the GDPR. The relevant review documentation in this respect must be provided to the Principal upon request.

7.2. Subcontractors in third countries may only be commissioned if the special requirements set out in Articles 44 et seq. of the GDPR are met (e.g. adequacy decision by the Commission, standard data protection clauses, approved codes of conduct).

7.3. A subcontracting relationship subject to approval occurs if the Contractor commissions other contractors to carry out all or part of the service agreed upon in this agreement. Ancillary services such as telecommunication, cleaning staff, maintenance and user support (without ability to access the Principal's data) will not constitute a subcontracting relationship as defined in this clause. However, the commissioning of waste management companies is notifiable where such companies are primarily commissioned to dispose documents/data mediums which contain the Principal's Data. Even in the case of externally assigned ancillary services, the Contractor will enter into reasonable and lawful contractual agreements and will take all necessary supervisory measures to ensure the protection and security of the Principal's Data.

7.4. Upon commissioning subcontractors, the Contractor must contractually ensure that the regulations agreed upon between him and the Principal also apply to subcontractors. In the contract with the subcontractor, the details must be stipulated specifically so that the responsibilities of the Contractor and the subcontractor are clearly separated from one another. If multiple subcontractors are commissioned, this will also apply to the responsibilities between the subcontractors. In particular, the Principal must be entitled to carry out reasonable checks and inspections, as required, even on site, with subcontractors, or to have such checks and inspections carried out by a third party commissioned by him.

7.5. The agreement with the subcontractor must be in writing which can also be done in a documented electronic format (Art. 28(4) and (9) of the GDPR).

7.6. Forwarding Data to the subcontractor will only be permitted if the subcontractor has fulfilled the obligations set out in Art. 29 and Art. 32(4) of the GDPR in respect to his employees.

7.7. The Contractor will be liable to the Principal for the compliance with data protection obligations by its subcontractors. Such obligations will be imposed in a contract with said subcontractors in line with this section of the agreement.

7.8. Decisions regarding whether or not subcontractors may be commissioned and, where applicable, the processes that will then apply when commissioning subcontractors will be governed by **no. IX of Appendix 1** to this agreement.

7.9. By way of derogation, where necessary, from the specifications in **no. IX of Appendix 1** to this agreement, the subcontractors listed in **no. VIII of Appendix 1** to this agreement have already been engaged with processing Data for the Contractor within the scope specified therein upon conclusion of this agreement. In this respect, the Contractor hereby warrants that the requirements for commissioning said subcontractors set out in this clause 7 have been adhered to. Subject to the submission of review documentation in accordance with clause 5 of this agreement, the Principal hereby declares its consent to the commissioning of the subcontractors named in **no. VIII of Appendix 1**.

## 8. Liability and Compensation

8.1. The contracting parties will be liable to the data subjects in accordance with the relevant statutory provisions, particularly in accordance with Art. 82 of the GDPR.

8.2. In the event of claims being made against the Principal on the grounds of the unlawful processing of Data that falls under the Contractor's responsibility, or that of a third party commissioned by the latter (subcontractor), or the processing of the same in breach of data protection obligations, the Contractor will hold the Principal free and harmless from such claims.

## 9. Final Provisions

9.1. Where this agreement has been concluded prior to May 25th, 2018, and thus before the GDPR will start to apply, the contracting parties are in agreement that up to this point in time the respective applicable national data protection legislation is to be applied accordingly. This will apply in particular to those provisions which expressly make reference to the GDPR.

9.2. If the Principal's Data held by the Contractor is endangered by garnishment or seizure, insolvency or composition proceedings, or by other incidents or third-party measures, the Contractor must inform the Principal thereof immediately. The Contractor will immediately inform all responsible and interested parties in this respect that control and ownership of the Data rests solely with the Principal as the "Person Responsible" as defined in the General Data Protection Regulation.

9.3. The defence of the right of retention as defined in Section 273 of the German Civil Code is hereby excluded in respect of the Data processed for the Principal and the associated data media.

9.4. Technical and organisational measures, and any change thereto, plus inspection and audit documentation (including for subcontractors), must be retained for the entire term of this agreement and for an additional three years from the end of the calendar year in which this agreement has expired.

9.5. No oral subsidiary agreements to this contract, or regarding objects governed by this agreement, have been entered into. Where applicable, previous existing verbal agreements will be cancelled upon this agreement entering into force.

9.6. Amendments and supplements to this agreement, and all components thereof – including any assurances or guarantees given by the Principal – must be made in writing, which may include a documented electronic format, and must expressly state that they constitute an amendment or supplement to these terms and conditions. This will also apply to any waiver of this written form requirement.

9.7. In the event of any contradictions, the provisions of this agreement and its appendices will take precedence over the main agreement, and the appendices to this agreement will take precedence over the agreement.

9.8. In the event of individual provisions of this agreement or its appendices being or becoming invalid or unfeasible, in full or in part, this will not affect the validity of the remaining clauses. In such cases, the parties will mutually agree upon a new provision, or a supplement to the existing provisions, to

replace or supplement the invalid or unfeasible provision such that it most closely reflects the provision the parties would have intended upon concluding this agreement and its appendices had they considered the invalidity or unfeasibility. The same will apply to omissions.

9.9. This agreement and its appendices are subject to the law of the Federal Republic of Germany.

**This contract has been accepted electronically by both parties and is therefore valid without a signature.**

## Appendix 1

to the AGREEMENT REGARDING THE PROCESSING OF PERSONAL DATA IN ACCORDANCE WITH ART. 28 PARA. 3 OF THE EUROPEAN GENERAL DATA PROTECTION REGULATION 2016/679 (GDPR)

***I. Re. clause 1.1 -*** *Scope, nature and purpose of the Contract Processing, nature of the personal data and data subjects*

*Subject of the order:*

*Creation, distribution and administration/update of digital advertising material (Wallet passes) for smartphones.*

*Provisioning of landing pages for sale and for the creation of wallet passes.*

*Scope, nature and purpose of the Contract Processing (services commissioned):*

*- in accordance with the definition in Art. 4 no. 2 of the GDPR -*

*Digital advertising media (wallet passes) can contain individualized data, such as customer names, customer numbers, IDs, etc. In addition, log files with transaction data are generated and stored. The customer can define which personal data is contained. See also the valid terms and conditions.*

*Data types to be processed:*

*- in accordance with the definition in Art. 4 nos. 1, 9, 13, 14 and 15 of the GDPR -*

☒ Personnel master data (e.g. salutation, last name, first name, address, title, position)

☒ Communications data (phone number, email)

☒ Contract master data (e.g. contractual relationships, product and contractual interests)

☒ Customer history

☒ Contract billing and payment data

☒ Planning and control data

☐ Report data (from third parties, e.g. credit agencies or from public directories)

☒ Technical log data (e.g. login, IP address, time stamp)

☒ Data sent by users of their own accord in messages, free text fields or as content in files:

*Contextual content such as advertising statements, product information, calls, directions, contact information, URLs, loyalty programs.*

☐ Special categories of personal data as defined in Art. 9(1) of the GDPR (racial and ethnic origin, political opinions, religious and philosophical beliefs, trade union membership, information about a person's health or sex life, genetic data or biometric data for the purpose of uniquely identifying a natural person):

☐ Other Data:

*Geo localization*

## Appendix 1

to the AGREEMENT REGARDING THE PROCESSING OF PERSONAL DATA IN ACCORDANCE WITH ART. 28 PARA. 3 OF THE EUROPEAN GENERAL DATA PROTECTION REGULATION 2016/679 (GDPR)

*Data subjects:*

*- in accordance with the definition in Art. 4 no. 1 of the GDPR -*

- ☒ Principal's customers
- ☒ Customers of the Principal's customers
- ☒ Principal's employees
- ☒ Employees of the Principal's customers
- ☒ Contact persons at Principal's suppliers
- ☒ Contact persons at suppliers to the Principal's customers
- ☒ Principal's prospective customers
- ☒ Prospective customers of the Principal's customers
- ☐ Other

***II. Re. clause 1.2 –*** *Existing relocations of the contractually agreed service (or parts thereof) to a third country:*

| Service / Processing procedure | Details of third country | Special requirements as per Article 44 seq. of the GDPR |
|---|---|---|
| | | |
| | | |
| | | |
| | | |
| | | |

***III. Re. clause 2.9 –*** *Rules on protecting secrecy relevant to this order:*

*(e.g. banking secrecy, telecommunications confidentiality, secrecy of social data, business or trade secrets in accordance with Section 203 of the German Criminal Code etc.)*

## Appendix 1

to the AGREEMENT REGARDING THE PROCESSING OF PERSONAL DATA IN ACCORDANCE WITH ART. 28 PARA. 3 OF THE EUROPEAN GENERAL DATA PROTECTION REGULATION 2016/679 (GDPR)

### *IV. Re. clause 2.11 and clause 3.5 – Authority*

*Persons authorised by the Principal to issue instructions are:*

*Customer/User*

*Persons authorised by the Contractor to receive instructions are:*

*David Sporer, CEO, +4915122609871, david@passcreator.com*

*Communication channels to be used for instructions:*

*Theodor-Lipps-Str. 4, D-80997 Munich, privacy@passcreator.com, +498925007997*

### *V. Re. clause 2.13 – Data Protection Officer*

☒ Appointed as Data Protection Officer by the Contractor:

*Daniela Duda*
*Rehm Datenschutz GmbH*
*Eugen-Sänger-Ring 13*
*85649 Brunnthal*
*Germany*
*Phone: +49 89 6080 7600*
*E-Mail: kontakt@rehm-datenschutz.de*

☐ The Contractor has not appointed a Data Protection Officer since the legal requirements to appoint one did not exist at the time of concluding the agreement.

### *VI. Re. clause 2.14 – Obligations to delete*

☒ Immediately after completing an order, the Contractor will delete or destroy, or arrange to have destroyed, the Data processed within that individual order in accordance with data protection requirements.

☒ Following completion of the contractual tasks, and upon termination of the agreement, the Contractor must do the following with all Data, documents and results from the processing or usage in its possession, or provided to subcontractors, relating to the contractual relationship

☒ Hand back to the Principal.

☐ Delete or destroy/arrange to have destroyed as follows in accordance with data protection requirements:

Any deletion or destruction must be confirmed to the Principal in writing or in a documented electronic format specifying the date.

# Appendix 1

to the AGREEMENT REGARDING THE PROCESSING OF PERSONAL DATA IN ACCORDANCE WITH ART. 28 PARA. 3 OF THE EUROPEAN GENERAL DATA PROTECTION REGULATION 2016/679 (GDPR)

***VII. Re. clause 6 –*** *Evidence*

☐ Results of a self-audit (see Appendix *Appendix number* ).

☐ Data protection and / or information security certification (e.g. ISO 27001)
*(Specify certification and issue date and the Appendix number)*

☐ Approved codes of conduct (Art. 40 of the GDPR) including external evidence of compliance therewith.
As regards compliance with the agreed protective measures and their verified effectiveness, reference is hereby made to the approved codes of conduct in accordance with Art. 40 of the GDPR. The Contractor subscribed to these on (Date) and compliance with the same was checked and confirmed on *(Date)* (*see Appendix xx - Appendix number - )*.

☐ Binding internal data protection rules (Art. 47 of the GDPR) including external evidence of compliance therewith. As regards compliance with the agreed protective measures and their verified effectiveness, reference is hereby made to the binding internal data protection rules in accordance with Art. 47 of the GDPR. The Contractor subscribed to these on (Date) and compliance with the same was checked and confirmed on (Date) (*see Appendix xx - Appendix number -* ).

☐ Certifications in accordance with Art. 42 of the GDPR
As regards compliance with the agreed protective measures and their verified effectiveness, reference is hereby made to the existing certification in accordance with Art. 42 of the GDPR. Compliance with the same by the Contractor was checked and confirmed on (*see Appendix Appendix number* ).

☐ The Principal and the Contractor agree that the required evidence may also be provided by the following documents and certifications:
As regards compliance with the agreed protective measures and their verified effectiveness, reference is hereby made to the existing certification by [certification body], the presentation of which to the Principal will suffice as evidence of appropriate safeguards (see *Appendix number* ).

***VIII. Re. clause 7.9*** *– Subcontractors already engaged upon conclusion of the agreement:*

| Name and address | Description of services provided by the subcontractor |
|---|---|
| *Flownative GmbH, Arnimstraße 19c, 23566 Lübeck* | *Hosting* |
| *SMSAPI<br>ComVision sp. z o. o.<br>ul. Toszecka 101<br>44-100 Gliwice<br>Poland* | *Sending of SMS* |
| *Mailjet<br>Mailjet SAS (Global HQ)<br>13-13 bis, rue de l'Aubrac,<br>75012 Paris, France* | *Sending of E-Mails* |
| *Google<br>1600 Amphitheatre Parkway, Mountain View, CA, USA* | *Analysis of access to websites (Google Analytics)* |
| *Hubspot<br>25 First Street, 2nd Floor<br>Cambridge, MA 02141<br>United States* | *CRM system* |
| *Newsletter2Go<br>Newsletter2Go GmbH<br>Köpenicker Str. 126<br>10179 Berlin, Germany* | *Sending of Newsletter* |
| *MailChimp<br>The Rocket Science Group, LLC<br>675 Ponce de Leon Ave NE<br>Suite 5000<br>Atlanta, GA 30308 USA* | *Sending of Newsletter* |
| *Kayako<br>Sixth Floor<br>20 Ropemaker Street<br>London EC2Y 9AR<br>United Kingdom* | *Support system* |
| *FastBill GmbH<br>Wildunger Str. 6<br>60487 Frankfurt am Main, Germany* | *Financial accounting software* |
| *Functional Software, Inc. dba Sentry, 132 Hawthorne Street, San Francisco, CA 94107. USA* | *Error Tracking system* |

## Appendix 1

to the AGREEMENT REGARDING THE PROCESSING OF PERSONAL DATA IN ACCORDANCE WITH ART. 28 PARA. 3 OF THE EUROPEAN GENERAL DATA PROTECTION REGULATION 2016/679 (GDPR)

### ***IX. Re. clause 7 –*** *Rules on dealing with subcontractors*

☒ The Principal generally allows the Contractor to involve additional or different subcontractors, but the Contractor must inform the Principal in writing, or in a documented electronic format, about any intended change regarding enlisting or replacing a subcontractor. The Principal may object to any such changes. If there is good cause in terms of data protection law for the objection, and if the parties are unable to reach a mutual solution on how to proceed, the Principal will have a special right of termination without notice as regards the overall Contract Processing. In the absence of any objection by the Principal within 28 days of sending the notice, the change will be deemed approved.

☐ Prior to any change regarding enlisting or replacing a subcontractor, the Contractor must obtain the Principal's consent. Consent may only be granted if the Contractor informs the Principal of the subcontractor's name and address and details of the intended activity, and warrants that the principles for engaging subcontractors set out in clause 7 of this agreement have been complied with. The consent will only be valid when given in writing or in a documented electronic format. It may only be refused for good cause in terms of data protection law.

☐ The commissioning of subcontractors and, where applicable, changes to existing, approved subcontractor relationships (no. VIII of this appendix) by the Contractor to provide the services agreed upon in the agreement is not permitted.

**APPENDIX 2**

TO THE AGREEMENT REGARDING THE PROCESSING OF PERSONAL DATA IN ACCORDANCE WITH ART. 28 PARA. 3 OF THE EUROPEAN GENERAL DATA PROTECTION REGULATION 2016/679 (GDPR)

***Re. clause 5 of the agreement*** *– technical and organisational measures*

*At the time of concluding this agreement, the Contractor has implemented the following technical and organisational measures (TOMs):*

# Individual processing activities

| | |
|---|---|
| **Designated processing activity:** | ☒ Onlineshop.<br>☒ Website.<br>☒ Marketing activities.<br>☐ Personnel management.<br>☐ Accounting.<br>☒ Communication (E-Mail, Messenger, etc.).<br>☐ Security management.<br>☐ Administration of suppliers.<br>☒ Customer management.<br>☒ Processing of data on behalf of third parties (e.g. as a service provider).<br>☐ _____ |
| **Description of the processing activity (1-2 sets)** | Storage of data for billing, as well as marketing activities.<br>_ |
| **Type of data / data categories:** | ☒ Master data (names, addresses).☒ Kontaktdaten (E-Mail, Telefonnummern, Fax, Messenger).<br>☒ Content (text input, pictures, videos).<br>☒ Contract data (time, content, payment information, customer category).<br>☒ Usage data (interests, visited websites, purchasing behavior, login times).☒ Meta-/Kommunikationsdaten (Geräte-IDs, IP-Adressen, Standortdaten).<br>☐ Employee master data (names, addresses, wage group, tax characteristics).<br>☐ Employee data (names, addresses, qualifications).<br>☒ Loyalty program data._____ |
| **Special data categories:** | ☐ _____<br>(Art. 9 DSGVO, e.g. health data, genetic and biometric data, sexual orientation, political, religious, trade union membership, ethnic origin, etc.). |
| **Category of affected groups of persons:** | ☒ Customer.<br>☒ Users of Passcreator, Website visitors.<br>☒ Recipients of marketing activities.<br>☒ Suppliers, service providers, partner companies and their employees.<br>☒ Employees, applicants.<br>☐ _____ |
| **Sources of the data and description of the collection, transmission, etc.** | ☒ Online form.<br>☒ Voluntary self-declarations.<br>☐ Publicly accessible data.☐ Mittels von Onlinetools/Verfahren ermittelte Daten.<br>☒ Data from customer databases. |
| **Type of processing:** | ☒ Electronic processing.☐ Verarbeitung in analogen Systemen (Aktenablage, etc.).<br>☐ _____ |
| **Purposes of data processing:** | ☒ Establishment, execution and termination of purchase or service contracts.☐ Begründung, Durchführung und Beendigung von Kauf oder Beschäftigungsverträgen.<br>☒ Security measures.☐ market research.<br>☒ Marketing and advertising purposes.☒ Loyalitätsprogramme_____ |

| | |
|---|---|
| **Legal ground for processing:** | ☒ Art. 6 para. 1 a), Art. 7 GDPR (consent).<br>☐ Art. 6 para. 1 lit. 1/b, § 26 BDSG-New / § 32 BDSG "Employment".☒ Art. 6 Abs. 1 lit. b DSGVO (Vertragserfüllung).<br>☐ Art. 6 para. 1 lit. c GDPR (legal obligations).☒ Art. 6 Abs. 1 lit. f DSGVO (berechtigte Interessen).<br>☐ _____ |
| **Receiver internal:** | ☐ Human resources<br>☐ Financial accounting<br>☒ Marketing/PR<br>☒ IT<br>☐ Stock<br>☒ Business management |
| **Transmission/disclosure to third parties & purpose.** | ☒ Banks for the purpose of payment/collection of payment claims.☐ Parcel services<br>☒ Tracking provider for range analysis and online marketing.☒ Hosting provider |
| **Transfer to third country (outside EU/EEA)** | ☐ _____<br>☒<br>See III. |
| **Deletion periods** | ☒ Deletion with Termination of Contract/Cancellation.<br>☐ 6 years, in accordance with § 257 (1) HGB (trading books, inventories, opening balance sheets, annual financial statements, commercial letters, accounting documents, etc.).<br>☒ 10 years, in accordance with § 147 para. 1 AO (books, records, management reports, accounting documents, commercial and business letters, documents relevant for taxation, etc.).<br>☐ _____ |
| **Special security measures (if not already in the general security concept)** | ☒ See general security concept_____<br>☐ _____ |
| **Have the persons concerned been informed in a data protection declaration or similarly (how)?** | ☒ Privacy Policy.☐ Individuell (z.B. per E-Mail).<br>☐ None, information, because _____<br>☐ _____ |
| **Have the principles of Privacy by Design/ by Default been considered?** | _____<br>• Data at Rest – Data is stored encrypted if it is not accessed.<br>• Transparency of data for the customer - the customer has the possibility to see which data is stored in the system and is able to delete and change/correct this data at any time.<br>• Use of secure password encryption.<br>• Strict logical separation of data between clients<br>• Regular updates of the software used (including e.g. PHP frameworks, web servers) |
| **Is there a case of Art. 22 DSGVO Automated decisions in individual cases including profiling?** | ☐ _____<br>(if yes, please describe) |

| | |
|---|---|
| **DS Impact Assessment required?** | ☒ No, because no increased risk.<br>☐ _____ |
| **Notes/ Other** | _____ |

# Security concept

| | |
|---|---|
| **Data protection at employee level** | ☒ Confidence/confidentiality obligation .<br>☒ BYOD regulation.<br>☒ Homeoffice regulation.<br>☒ Regulation of business Internet/e-mail useage.<br>☐ Trainings.<br>☐ _____ |
| **Archiving, deletion, disposal and restriction of processing** | ☒ There is an archiving, deletion and disposal concept with defined responsibilities.<br>☒ Employees were informed about legal requirements, deletion periods and specifications for device disposal and disposal service providers .<br>☐ _____ |
| **Safeguarding the rights of those concerned** | ☒ There is a concept which guarantees the protection of the rights of the persons concerned (information, correction, data transfer, revocations & objections) within the legal deadlines.<br>☐ _____ |
| **Contingency plan** | ☐ A concept exists that guarantees an immediate reaction to violations of the protection of personal data (testing, documentation, reporting) in accordance with legal requirements.<br>☐ _____ |
| **Access control** | ☒ Door locks.<br>☐ Access regulations for external persons<br>☐ Chip card/transponder locking system .<br>☐ Security locks .<br>☐ Window protection .<br>☐ Video surveillance .<br>☐ Supervision of auxiliary personnel.<br>☐ _____<br>☐ _____ |
| **Access control** | ☒ Firewalls (Hardware/Software).<br>☒ Up-to-date Anti-Virus software.<br>☒ Up-to-date software versions.<br>☐ Authorization/authentication concepts with access regulations limited to the most necessary.<br>☒ Minimum password lengths and password manager.<br>☐ Use of VPN technology.<br>☐ Locking external interfaces (USB etc.).<br>☐ Use of intrusion detection systems .<br>☒ Encryption of mobile storage and devices .<br>☐ Use of central smartphone administration software .<br>☒ Logging access to data.<br>☐ Proper destruction of data carriers .<br>☐ _____<br>☐ _____ |

| | |
|---|---|
| **Handover control** | ☒ Determination and documentation of recipients.<br>☐ Pseudonymisation.<br>☒ Encryption of storage and connections.<br>☐ Dedicated permissions.<br>☒ The employees have undertaken in writing not to pass on data, unless this is necessary for the fulfilment of inquiries from governmental authorities on a legal basis. ☐<br>_____ |
| **Input control** | ☒ Logging of data entries, changes and deletions.<br>☐ Retention of forms from which data has been transferred to automated processing.<br>☒ Assignment of rights to enter, modify and delete data on the basis of an authorization concept.<br>☐ _____<br>☐ _____ |
| **Control of sub-contractors** | ☒ Selection of contractors based on due diligence.<br>☒ Determination of instructions in writing.<br>☒ Control of compliance with contractors.<br>☒ Ensuring the destruction of data after termination of the mandate.<br>☐ _____<br>☐ _____ |
| **Avialbility concept / Data integrity** | ☒ Contingency plan.<br>☒ Constantly controlled backup and recovery concept.<br>☒ Additional backup copies with storage in specially protected locations.<br>☒ Execution of load capacity tests.<br>☐ _____<br>☐ _____ |
| **Guarantee of the earmarking/division requirement** | ☐ Physical separation of clients (hardware).<br>☒ Logical separation of clients (software).<br>☒ Separation of production and test system.<br>☐ For pseudonymised data: Separation of the mapping file and storage on a separate, secure system.<br>☐ _____<br>☐ _____ |