Data Processing Agreement

This Data Processing Agreement is made and entered

Between:

Presspage B.V., a company incorporated in the Netherlands and having its registered office at Joan Muyskenweg 22, 1096 CJ Amsterdam ("Processor")

And

Customer ("Controller")

Together 'Parties'

Consider the following

- The Processor provides services for the benefit of the Controller;
- The Controller and the Processor concluded an agreement regarding the purchasing of Processor's services, of which this Data Processing Agreement is a part;
- Within the context of the performance of this contract, Presspage is deemed a processor within the meaning of Article 4(8) of the GDPR and Controller is deemed a controller within the meaning of Article 4(7) of the GDPR.
- The Parties wish to establish a number of conditions that apply to their relationship in connection with the processing of personal data for the Controller, partly in implementation of the provisions of Article 28, third paragraph of the GDPR.

Agree to the following

1. Definitions

1.1. In this Data Processing Agreement, the following terms shall have the meaning set out below:

Agreement	The Agreement concluded between the Controller and the Processor and on the basis of which the Processor processes Personal Data for the Controller for the purpose of the performance of this Agreement.
GDPR	Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the Processing of Personal Data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation).
Personal Data	All information relating to a Data Subject as referred to in Article 4(1) GDPR.
Personal Data Breach	A breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, Personal Data transmitted, stored or otherwise processed, as referred to in Article 4(12) GDPR.
Data Subject	The identified or identifiable natural person to whom the

	Personal Data pertain, as referred to in Article 4(1) GDPR.
Data Processing Agreement	This Data Processing Agreement and all appendices thereto, as referred to in Article 28(3) GDPR.
Processing	*As well as conjugations of this verb:* the processing of Personal Data as referred to in Article 4(2) GDPR.
Sub-processor	The subcontractor, engaged by the Processor to perform specific processing activities at the Controller's expense, as referred to in Article 28(4) GDPR.
Third-party	A natural or legal person, public authority, agency or body other than the Data Subject, the Controller or the Processor.

1.2. The provisions of the Agreement apply in full to the Data Processing Agreement. With regard to the processing of Personal Data, the provisions of this Data Processing Agreement prevail.

2. Applicability and duration

2.1. This Data Processing Agreement applies to all Processing of Personal Data carried out by the Processor on behalf of the Controller under the Agreement.

2.2. This Data Processing Agreement supplements the Agreement and supersedes any prior arrangements between the Parties with respect to the Processing of Personal Data.

2.3. This Data Processing Agreement enters into force on the effective date of the Agreement and shall remain in force until thirty (30) working days after the expiration or termination of the Agreement. During this period, the Processor shall cease all Processing of Personal Data unless otherwise instructed by the Controller or required by law. Within that same period, or such other timeframe as the Parties may agree, the Processor shall return or delete all Personal Data, the Account, and Customer Content in accordance with Article 10 of this Data Processing Agreement.

2.4. This Data Processing Agreement may not be terminated separately from the Agreement.

3. Processing of personal data

3.1. The Processor shall Process Personal Data solely for the purpose described in this Data Processing Agreement and the Agreement. Details regarding the categories of Data Subjects, types of Personal Data, and the nature and purpose of Processing are set out in **Appendix 1**.

3.2. The Processor shall not Process Personal Data for its own or third-party purposes without the prior written instruction of the Controller, unless legally required to do so. In such cases, the Processor shall notify the Controller prior to such Processing, unless prohibited by law.

3.3. The Processor may engage Sub-processors listed in **Appendix 2**. The Processor shall notify the Controller in advance of any intended changes to its Sub-processor list. The Controller may object in writing within five (5) working days of such notice, provided the objection is based on reasonable data protection grounds. Failure to object within this period shall be deemed as acceptance.

3.4. The Processor shall ensure that Sub-processors are bound by data protection obligations

substantially similar to those in this Data Processing Agreement, including appropriate technical and organization measures.

3.5. The Processor shall not transfer Personal Data outside of the European Economic Area unless such transfer complies with the applicable statutory obligations under the GDPR, including the use of Standard Contractual Clauses or other lawful mechanisms.

3.6. The Processor shall be responsible for Processing Personal Data in accordance with the Controller's documented instructions. The Controller retains full responsibility for the lawfulness of such instructions and for any Processing outside the scope of this Data Processing Agreement, including but not limited to the collection of Personal Data and the use of the Services in a manner not disclosed to the Processor.

4. Technical and organisational security measures

4.1. The Processor shall implement and maintain appropriate technical and organizational measures to ensure a level of security appropriate to the risks presented by the Processing of Personal Data, taking into account the state of the art, the costs of implementation, and the nature, scope, context, and purpose of Processing. These measures shall protect Personal Data against accidental or unlawful destruction, loss, alteration, unauthorized disclosure, or access.

4.2. The Processor has provided a description of its security measures in **Appendix 3** to this Data Processing Agreement. By signing this Agreement, the Controller acknowledges and agrees to the adequacy of these measures. The Processor may update or modify these measures from time to time, provided such modifications do not materially reduce the overall level of protection afforded to the Personal Data.

5. Audit

5.1. Upon written request, the Processor shall allow the Controller or its designated external auditors to conduct an audit of the Processor's compliance with this Data Processing Agreement, including security measures, no more than once per calendar year. Such audit shall be subject to reasonable advance notice, prior written permission and coordination with the Processor, and shall be conducted in a way that minimizes disruption to the Processor's business operations. All audit costs shall be borne by the Controller.

5.2. Before initiating an on-site audit, the Controller shall first review any relevant certifications or audit reports made available by the Processor (e.g. ISO 27001, TISAX). An on-site audit may be conducted only if, after such review, the Controller can demonstrate reasonable grounds to believe that the available documentation is insufficient to demonstrate compliance with this Data Processing Agreement.

5.3. If the Processor reasonably believes that any instruction related to the audit infringes the GDPR or other applicable data protection laws, it shall promptly notify the Controller.

6. Personal Data breach

6.1. In the event the Processor becomes aware of a Personal Data Breach involving Personal Data Processed on behalf of the Controller it shall i) notify the Controller without undue delay, and ii) take all reasonable measures to prevent or limit (further) violation of the GDPR.

6.2. The Processor shall, to the extent reasonably practicable, provide the Controller with

cooperation and assistance to enable the Controller to comply with its obligations under Articles 33 and 34 GDPR, including by providing relevant information about the nature and scope of the breach and any remedial actions taken.

6.3. The Processor is not responsible for notifying the Data Protection Authority or affected Data Subjects. Such notifications remain the sole responsibility of the Controller.

6.4. The Processor shall not be liable for any failure by the Controller to comply with its legal obligations under Articles 33 and 34 GDPR, including any delay or omission in breach notifications.

7. Confidentiality

7.1. The Processor will ensure that employees and contractors involved in the execution of the Agreement and this Data Processing Agreement are bound by a written confidentiality obligation – whether in their employment or contractor agreement or in a separate NDA – that includes an obligation to maintain strict confidentiality regarding the Personal Data and any other Confidential Information accessed in connection with the Agreement. These confidentiality obligations shall survive the termination of the Agreement. The Processor shall take appropriate measures to enforce these obligations.

8. Cooperation

8.1. The Processor will, insofar as reasonably possible, assist the Controller in responding to requests from Data Subjects to exercise their rights under the GDPR. The Processor shall forward any such request or complaint to the Controller without undue delay, and in any case within two (2) working days. The Controller remains solely responsible for handling such requests. The Processor may charge the Controller for excessive, repetitive, or non-standard assistance provided under this clause.

8.2. The Processor shall, upon reasonable request, assist the Controller with the performance of data protection impact assessments and prior consultations with supervisory authorities, in accordance with Articles 35 and 36 GDPR.

8.3. The Processor shall make available to the Controller, upon request and at the Processor's discretion, the information reasonably necessary to demonstrate compliance with this Data Processing Agreement and the GDPR. The Processor may charge the Controller for any assistance provided under this clause, including for time and resources spent gathering, compiling, or explaining such information.

9. Liability

9.1. The provisions in the Agreement regarding limitation of liability and indemnification shall apply in full to the Processor's liability under this Data Processing Agreement.

9.2. Without prejudice to Article 9.1 of this Data Processing Agreement, the Processor shall only be liable for damages suffered by the Controller or for third-party claims arising from Processing activities where the Processor has failed to comply with its specific obligations under the GDPR, or where it has acted outside or in violation of the documented instructions of the Controller. Any liability under this Article shall remain subject to the liability caps and exclusions agreed in the Agreement, unless such damage results from the Processor's gross negligence or willful misconduct.

10. Termination

10.1. Upon termination or expiration of this Data Processing Agreement and/or the Agreement, or upon the request of the Controller, the Processor shall, unless mandatory law provides otherwise and without prejudice to Article 2.3 of this Data Processing Agreement, cease all Processing of Personal Data and within thirty (30) working days or another period mutually agreed in writing:

a) return the Personal Data to the Controller in a standard, commercially reasonable format specified by the Processor; and/or
b) permanently delete or anonymize the Personal Data (including copies), at the Controller's written instruction, except where retention is required by law.

If the Controller does not provide written instructions within the timeframe specified above, the Processor shall be entitled to delete the Personal Data in accordance with its standard data retention schedule. Deletion of Personal Data from backups will be performed in accordance with the Processor's regular backup lifecycle.

11. Final provisions

11.1. In the event of any conflict between the provisions of this Data Processing Agreement and the Agreement or any other related terms, the provisions of this Data Processing Agreement shall prevail with respect to the Processing of Personal Data.

11.2. The provisions of this Data Processing Agreement that by their nature are intended to survive termination, including but not limited to those relating to confidentiality, liability, audit, cooperation with authorities, and data return or deletion, shall remain in effect after termination of this Data Processing Agreement.

Appendix 1: Personal Data

Subject matter and duration

The subject matter: providing the Processor's services to the Controller involves the Processing of Personal Data. The Personal Data will only be processed by the Processor for the purpose of the activities referred to in this Data Processing Agreement and/or the Agreement.

The duration of the Processing is for the term of the Agreement, and for up to thirty (30) working days following termination, as specified in Article 2.3 of this Data Processing Agreement.

The nature and purpose

The Processing activities include collection, structuring, storage, transmission, and deletion of Personal Data in connection with use of the Presspage platform and services (including Newsroom, Presspage Mail, and Media Database features), for the purpose of publishing, communication, media outreach, and support services.

The types of Personal Data to be processed

Data categories (not limitative):

- Contact data: name, email, address
- Content data: press release/article content and any personal information included therein
- Meta data: system logs, analytics, IP address
- All (other) data that is disclosed by the Controller to the Processor in using the Processor's services

The categories of Data Subjects to whom Personal Data relates

- Customers of the Services
- Employees or representatives of the Controller, to the extent their data is processed through user accounts or platform interactions
- Visitors of the Services
- Contact lists (PR related), journalist contacts from the Agility Media Database

Locations of data processing

Presspage Database:	Frankfurt, Germany
Mailgun:	European Region
Agility PR Solutions:	Canada

For detailed information on all Sub-processors, including their purpose, data types, and data locations, see Appendix 2.

Appendix 2: Sub-processors

The Processor makes use of the following sub-processors:

Company name	Purpose	Data types processed	Data location
Agility PR	Media Database Service	Name, email address	Canada
Amazon (AWS)	Hosting	All data uploaded by users	Germany, Ireland
Atlassian (Jira)	Issue tracking and support ticket resolution	Name, data required to resolve reported issues	Germany, Ireland
Chargebee	Payment processor	Name, email address, billing information	United States
Google Ireland Limited (Workspace)	Email, calendar, documents	Name, email address, data transmitted by users in email or document	Europe
Hotjar (Contentsquare)	Usage analytics	IP address, location data	Ireland
Hubspot	CRM	Name, email address, job title, telephone numbers, location data, IP address	United States
Mailgun	Presspage Mail Service	Name, email address, contents of email campaigns	Germany
OpenAI (ChatGPT)	AI functionality	Data the user inputs in AI features	United States
Productboard	Feedback collection	Name, email address	United States
Twilio (Sendgrid)	Transactional mails	Name, email address	United States
Userpilot	Product engagement tool	Name, email address	United States
Zendesk	Ticketing system	Name, email address, data included in support requests	Germany

All companies mentioned above that operate outside the EU — except for OpenAI — participate in the Data Privacy Framework Program. A data processing agreement is in place with all the

companies mentioned above. For OpenAI, the Processor relies on Standard Contractual Clauses (SCCs) for transfers to the United States.

Appendix 3: Technical and Organizational Measures

Pseudonymization and encryption of personal data
Measures:

- Pseudonymisation and encryption of personal data (TLS 1.2 and 1.3 for data in transit, AES-256 for data at rest)

Confidentiality
Physical Access Control
No unauthorized access to data processing facilities. Measures:

- Entrance security (opening doors by using security tags)
- Surveillance installation (e.g. alarm systems)
- Rules for visitors in place (e.g. register at the reception and escorting the visitors)

Electronic Access Control
No unauthorized persons can make use of the data processing systems. Measures:

- Authentication (e.g. password policy/ requirements/protection, two-factor authentication)
- Authorization (e.g. authorization concept for terminal devices and system, devices and systems can only be accessed by entering usernames and passwords, access attempts monitored, access authority specified and checked)
- Access on a need-to-know basis and reviewed periodically
- Automatic blocking/locking mechanisms
- Using security software (e.g. anti-malware, VPN, firewall) including automatic updates

Internal Access Control
No unauthorized reading, copying, changes or deletions of data within the system. Measures:

- Authorization and roles concept implemented for applications
- Rules for authorizing users and data access implemented
- Regular review of authorizations
- Need-based rights of access
- Access restrictions and limitations are imposed
- Administration of rights by system administrator
- Separation of test and productive environment
- Logging (e.g. write-access logged, unauthorized access attempts logged)
- Regular and ad hoc analyses carried out
- Integrity checks carried out
- Onboarding and offboarding procedures

Integrity
Data Transfer Control
No unauthorized Reading, Copying, Changes or Deletions of Data with electronic transfer or transport. Measures:

- Encryption

- Special security software (e.g. anti-malware, VPN, firewall)

Data Entry Control
Input control refers to the action taken to ensure that checks can be carried out, whether and by whom personal data is entered into a Data Processing System, is changed or deleted.
Measures:
- Regular review of logs
- Document Management

Availability and Resilience
Availability Control
Prevention of accidental or willful destruction or loss. Measures:
- Monitoring (system condition regularly checked)
- Backup and recovery plan
- Contingency plans including regularly tests
- Redundancy systems (servers, storage, etc.)
- Data archiving strategy implemented
- Fully operation physical protection systems in place (e.g. fire alarm system, emergency plan, A/C)
- Backup strategy (online/offline/on-site/off-site)
- Uninterruptible Power Supply (UPS)

Rapid Recovery
- Recovery plan is in place
- Regular tests of data recovery

Procedures for regularly testing, assessing and evaluating
- Data Protection Management
- Contract control
- Any employee of Presspage will sign a non-disclosure agreement
- Vulnerability scanning
- Penetration testing (annually conducted by independent third party)