

# Data Processing Agreement

**Effective Date: January 1, 2025**

This Data Processing Agreement ("DPA") forms part of the agreement between PDFBolt (the "Processor") and the Customer (the "Controller") for the provision of PDF generation services (the "Services") as described in the PDFBolt [Terms of Service](#).

## 1. Definitions

For the purposes of this DPA:

**"Controller"** means the entity that determines the purposes and means of processing Personal Data, as identified in the Agreement.

**"Data Protection Laws"** means all applicable laws and regulations relating to privacy and data protection, including but not limited to the General Data Protection Regulation (EU) 2016/679 ("GDPR"), the California Consumer Privacy Act ("CCPA"), and any successor legislation.

**"Data Subject"** means an identified or identifiable natural person whose Personal Data is processed.

**"Personal Data"** means any information relating to an identified or identifiable natural person that is processed by the Processor on behalf of the Controller in connection with the Services.

**"Processing"** has the meaning given in applicable Data Protection Laws and includes any operation performed on Personal Data.

**"Processor"** means Michał Szymanowski PDFBolt, a business entity registered in Poland (VAT EU: PL8121921097).

**"Agreement"** means the PDFBolt Terms of Service or the main agreement between the parties governing the provision of the Services.

**"Services"** means the PDF generation services provided through the PDFBolt API, including conversion of HTML content, URLs, and template-based document generation.

**"Sub-processor"** means any third party engaged by the Processor to process Personal Data on behalf of the Controller.

## 2. Scope and Application

---

### 2.1 Relationship of the Parties

The parties acknowledge that with regard to the processing of Personal Data, the Controller acts as the data controller and the Processor acts as the data processor under applicable Data Protection Laws.

### 2.2 DPA Precedence

This DPA supplements and forms an integral part of the Agreement. In the event of any conflict between this DPA and the Agreement, this DPA shall prevail with respect to matters concerning the processing of Personal Data.

## 3. Details of Processing

---

### 3.1 Subject Matter and Duration

The subject matter and duration of the processing are determined by the Agreement and the Controller's use of the Services for the term of the Agreement.

### 3.2 Nature and Purpose of Processing

The Processor processes Personal Data for the following purposes:

- Generation of PDF documents from HTML content, URLs, or templates with JSON data into PDF format.
- Storing generated PDFs temporarily (24 hours) unless the Controller uses custom S3 storage or direct endpoint.
- Processing API requests and maintaining request logs. Only request metadata is stored in the logs; Personal Data, specifically the HTML content used to generate the PDF and the JSON data for the template, is processed only for the duration of the PDF generation and deleted immediately afterward. The Controller can independently configure which request metadata is stored in the logs they access for analysis and debugging purposes.
- Processing support requests and Customer communications.
- Managing Customer accounts.
- Ensuring service security and preventing fraud.

### 3.3 Categories of Data Subjects

Personal Data processed may relate to the following categories of Data Subjects:

- End users of services provided by the Controller.
- Customers and clients of the Controller.
- Employees or contractors of the Controller.
- Any other individuals whose Personal Data is included in content submitted to the Services.

### 3.4 Types of Personal Data

The types of Personal Data processed may include:

- Email addresses.
- Templates and JSON data submitted by the Customer (which may contain Personal Data).
- HTML content and URLs submitted for PDF generation (which may contain Personal Data).
- Customer support communications, including chat transcripts and support requests.

The Processor does not determine which types of Personal Data are processed; this is solely within the Controller's discretion and responsibility.

## 4. Controller Obligations

---

The Controller warrants and undertakes that:

### 4.1 Lawful Basis

The Controller has established a lawful basis for processing Personal Data under applicable Data Protection Laws and has obtained all necessary consents, permissions, and authorizations required for such processing.

### 4.2 Instructions to Processor

All instructions provided to the Processor regarding the processing of Personal Data shall be documented and shall comply with applicable Data Protection Laws.

### 4.3 Data Minimization

The Controller shall submit to the Services only the Personal Data that is strictly necessary for the legitimate purposes of the processing and shall not submit Sensitive Personal Data (as defined in applicable Data Protection Laws) unless absolutely necessary and legally authorized.

### 4.4 Transparency

The Controller shall provide appropriate notice to Data Subjects regarding the processing of their Personal Data, including disclosure of the Processor's involvement and the general location of processing.

### 4.5 Compliance Responsibility

The Controller acknowledges sole responsibility for compliance with Data Protection Laws in relation to its use of the Services, including but not limited to conducting Data Protection Impact Assessments where required.

### 4.6 Accuracy of Data

The Controller is responsible for ensuring that all Personal Data provided to the Processor is accurate, complete, and up to date.

## 4.7 Temporary Processing Only

The Controller acknowledges that the Processor does not permanently store or retain the Personal Data submitted through the Services. The submitted data (HTML content and template JSON data) is processed transiently for the purpose of generating the requested output (a PDF file) and is automatically deleted after processing is completed.

The Processor also provides configurable privacy preferences that allow the Controller to redact specific parameters from logs, as described in Section 4.8.

## 4.8 Privacy Preferences and Redacted Parameters

- The Controller may configure [privacy preferences](#) within the Services to determine which parameters or data fields should be redacted.
- "Redacted" means that the values of such parameters will not be logged, stored, or otherwise retained by the Processor for privacy reasons.
- The Controller is responsible for selecting the appropriate parameters to redact in accordance with its data protection obligations.
- For privacy and security reasons, certain parameters – including HTML content and template JSON data - are always redacted by default and are never logged or stored by the Processor.

## 5. Processor Obligations

---

### 5.1 Compliance with Instructions

The Processor shall process Personal Data only on documented instructions from the Controller, unless required to do so by applicable law. The Processor shall immediately inform the Controller if it believes any instruction violates applicable Data Protection Laws.

### 5.2 Confidentiality

The Processor shall ensure that persons authorized to process Personal Data have committed themselves to confidentiality or are under an appropriate statutory obligation of confidentiality.

### 5.3 Security Measures

The Processor shall implement and maintain appropriate technical and organizational measures to ensure a level of security appropriate to the risk, including:

- Encryption of Personal Data in transit and at rest using industry-standard protocols.
- Regular security updates to security infrastructure.
- Access controls limit processing to authorized personnel only.
- Regular backup procedures and disaster recovery planning.

The Processor maintains technical and organizational measures to protect Personal Data against unauthorized access and accidental loss, consistent with industry standards.

## 5.4 Sub-processing

The Controller provides general authorization for the Processor to engage Sub-processors in accordance with Section 7 of this DPA. The Processor shall:

- Maintain a current list of Sub-processors (as detailed in Section 7);
- Ensure that Sub-processors implement appropriate data protection measures in line with the obligations set out in this DPA;
- Remain fully liable to the Controller for the performance of Sub-processors' obligations.

## 5.5 Data Subject Rights

The Processor shall, to the extent legally permitted and considering the nature of the processing, assist the Controller by implementing appropriate technical and organizational measures to fulfill the Controller's obligation to respond to requests from Data Subjects exercising their rights under Data Protection Laws, including rights of access, rectification, erasure, restriction, portability, and objection.

## 5.6 Data Breach Notification

Upon becoming aware of a Personal Data breach, the Processor shall, to the extent technically and operationally feasible, given the nature of the Services:

- Notify the Controller without undue delay and in any event within 72 hours;
- Provide reasonable information and cooperation to enable the Controller to fulfill any data breach reporting obligations;
- Take reasonable measures to remediate the breach and prevent future occurrences;
- Document all Personal Data breaches and make such documentation available to the Controller upon request.

## 5.7 Data Retention and Deletion

The Processor shall:

- Automatically delete generated PDF documents within 24 hours of creation, unless the Controller uses custom storage solutions or direct endpoint (in which case this does not apply), or earlier upon the Controller's request;
- Retain request logs only as necessary for service provision and troubleshooting, and only for parameters that have not been redacted;
- Delete all Personal Data upon the Controller's request, unless retention is required by applicable law.

## 6. Location of Processing

---

Personal Data related to PDF generation and any temporary storage of generated PDF documents in the Services shall be processed and stored exclusively within the European Union, using the following infrastructure:

- **Germany (Frankfurt)** – Koyeb infrastructure
- **Germany (Nuremberg)** – Hetzner infrastructure
- **European Union** – Cloudflare R2

## 7. Sub-processors

### 7.1 Authorized Sub-processors

The Controller authorizes the use of the following Sub-processors:

Entity Name	Service / Type	Purpose / Function
Koyeb SAS	Cloud Infrastructure	Infrastructure and hosting services
Hetzner Online GmbH	Cloud Infrastructure	Infrastructure and hosting services
Cloudflare, Inc.	Object Storage	Temporary storage of generated PDF documents for sync endpoints
Stripe, Inc.	Payment Processing	Payment and billing services; Stripe is the only entity that stores payment data
Crisp IM SAS	Customer Support	Customer support and communications
Google LLC (via Firebase)	Authentication Service	User authentication, including sending emails for authentication and security purposes
Plausible Insights OÜ	Analytics	Privacy-friendly website analytics (no cookies, aggregated data only)

### 7.2 Sub-processor Obligations

All Sub-processors are contractually bound to:

- Process Personal Data only for the purposes specified by the Processor;
- Implement appropriate technical and organizational security measures;
- Maintain confidentiality of Personal Data;
- Notify the Processor of any Personal Data breaches;
- Assist with Data Subject rights requests as applicable;
- Delete or return Personal Data upon termination.

## 8. Audit Rights

---

The Processor shall provide reasonable assistance to the Controller to demonstrate compliance with this DPA. This includes:

- Making relevant information and documentation available;
- Cooperating with any audits or requests related to data processing.

## 9. DPIA and Prior Consultation

---

Upon the Controller's written request, the Processor shall provide reasonable cooperation and assistance (at the Controller's expense) to enable the Controller to comply with its obligations under Articles 35 and 36 of the GDPR or equivalent provisions under other Data Protection Laws concerning: Data Protection Impact Assessments; prior consultation with supervisory authorities.

## 10. Records and Reporting

---

### 10.1 Processing Records

The Processor shall maintain accurate records of all processing activities carried out on behalf of the Controller, as required by Article 30(2) of the GDPR or equivalent provisions of other Data Protection Laws.

### 10.2 Cooperation with Authorities

The Processor shall cooperate with supervisory authorities in the performance of their tasks relating to this DPA, as required by applicable Data Protection Laws.

## 11. Term and Termination

---

### 11.1 Effective Date and Duration

This DPA takes effect on the date of the Agreement and continues for the duration of the Agreement and any renewal periods.

### 11.2 Survival

The provisions of this DPA that by their nature should survive termination shall survive, including obligations relating to data deletion, confidentiality, and liability.

### 11.3 Effect of Termination

Upon termination of the Agreement:

- The Processor shall cease all processing of Personal Data;
- The Processor shall delete all Personal Data if requested by the Controller.

## 12. General Provisions

---

### 12.1 Amendments

The Processor may amend this DPA as necessary to comply with changes in Data Protection Laws, provided that such amendments do not reduce the level of protection for Personal Data. The Processor shall provide reasonable notice of material amendments.

### 12.2 Severability

If any provision of this DPA is held to be invalid or unenforceable, the remaining provisions shall remain in full force and effect. The parties shall negotiate in good faith to replace any invalid provision with a valid provision that achieves the original intent.

### 12.3 Conflict

In the event of any conflict between this DPA and the Agreement, this DPA shall prevail with respect to the processing of Personal Data.

### 12.4 Governing Law

This DPA shall be governed by and construed in accordance with the laws governing the Agreement.

### 12.5 Notices

All notices under this DPA shall be delivered to the addresses specified in the Agreement or as otherwise notified by either party.

## 13. Contact Information

---

For questions or concerns regarding this DPA or data protection matters:

### **PDFBolt**

Email: [contact@pdfbolt.com](mailto:contact@pdfbolt.com)

Address: Przedpole 9/73, 02-241 Warsaw, Poland

---

**By using the Services, the Controller acknowledges having read and agreed to this Data Processing Agreement and confirms that it has the authority to bind its organization to these terms.**