Publitas.com
Consolidated Multibrand
Data Processing Agreement

This Data Processing Agreement, including all appendices, apply to all Customers who use the Services of Publitas.com B.V. and/ or any signing entity under Publitas.com Holding B.V., whose registered office and address for service are located at J.H. Oortweg 21, 2333 CH Leiden, Netherlands. This Policy applies to the extent relevant in the context of the specific Service or Product selected by the Customer.

PLEASE READ THESE CAREFULLY.

General Regulations

1. Introduction, Scope, and Definitions

1.1. This Data Processing Agreement ("DPA") governs the rights and obligations of the Controller and the Processor (collectively referred to as the "Parties") in the processing of personal data on behalf of the Controller, in accordance with the EU General Data Protection Regulation (GDPR).

1.2. Where the term "**Service Agreement**" is used, it refers to the contract entered into between the Processor and the Controller, which is an integral part of a free or paid user agreement, governed by the Processor's Terms of Service, Privacy Policy, or other contractual agreements between the Parties.

1.3. "**Publitas**" or the "**Software**" refers to any service of Publitas.com B.V. and/ or of any signing entity under Publitas.com Holding B.V.

1.4. This DPA applies to all activities in which the Processor, its employees, or Subprocessors process personal data of the Controller in accordance with the Service Agreement, as defined under Article 28 of the GDPR. All terms used in this DPA shall be interpreted in accordance with the definitions provided in the GDPR.

1.5. In the event of any conflict between this DPA and the Service Agreement (or any other agreement between the Parties), the provisions of this DPA shall prevail, as they address specific data protection requirements.

2. Scope of Processing, Categories of Data, and Data Subjects

2.1. The subject, scope, type, and purpose of data processing are outlined in this DPA and the Service Agreement. The Processor shall process personal data on behalf of the Controller for the following purposes:

- Collecting data related to the Controller's use of the Processor's products.
- Aggregating and analyzing data, as well as storing such data through Subprocessors. The data may be transferred to Subprocessors for processing.
- The Processor may access the data for maintenance, analytics, or support purposes, and, upon the Controller’s instruction, forward data to third parties designated by the Controller.

2.2. The Processor does not process sensitive personal data. The following categories of personal data may be processed on behalf of the Controller, as identified in the Subprocessor list attached as Annex 1:

- Email addresses (if used in the publications by the Controller)
- IP addresses

- Phone numbers (if used in the publications by the Controller)
- Other information associated with the above data, such as location data

2.3. While the Processor’s platform is open to allow the Controller to independently collect additional personal data, the Controller is prohibited from using the Processor's platform to collect sensitive personal data. Any such action will be considered a breach of this Agreement.

2.4. The data subjects affected by the processing include visitors to the Controller’s content, such as users interacting with the Controller’s content via websites, apps, or other platforms, who have provided personal data in the manner designated by the Controller.

2.5. All processing under this Agreement takes place exclusively in a Member State of the European Union, a state party to the European Economic Area Agreement, or a country recognized by the European Commission as providing an adequate level of data protection in accordance with Article 45 GDPR.

2.6. If the service is relocated to a third country outside the aforementioned regions, prior written consent of the Controller is required, and the Processor must ensure compliance with the requirements of Articles 44–50 GDPR. The Controller may withhold consent if there are significant data protection concerns.

3. Duration of Processing

The processing duration will not exceed what is necessary to fulfill the processing activities as outlined in this DPA and the Service Agreement. The processing term is aligned with the term of the Service Agreement, unless this DPA imposes additional obligations that extend beyond the Service Agreement's term. In such cases, the DPA will terminate once these additional obligations are fulfilled.

4. Confidentiality

The Processor commits to maintaining confidentiality in line with Articles 28(3)(b), 29, and 32(4) of the GDPR. Only employees bound by confidentiality agreements and trained in applicable data protection laws will have access to personal data. Data processing shall be carried out solely based on the Controller's instructions, as outlined in the Service Agreement and this DPA, unless legally obligated to act otherwise.

Obligations of the Parties

5. Responsibility of the Controller

The Controller remains responsible for compliance with data protection laws, including the legality of data transferred to the Processor and the overall lawfulness of the processing (as per Article 4(7) GDPR). This includes:

- Ensuring compliance with applicable technical and organizational measures for data protection.

- Informing the Processor of any personal data breaches without undue delay, and no later than 72 hours after becoming aware of such incidents.

- Providing a designated contact person for data protection issues, or, if unavailable, the Processor may contact the Controller via the details provided in the Publitas account.

- The Controller is also responsible for protecting the rights of data subjects and complying with the GDPR requirements relating to the processing activities defined in this DPA.

6. Instructions

6.1. The Processor may only process personal data based on the Controller's instructions, unless legally required to do otherwise. The Service Agreement and this DPA constitute the Controller's standing instructions regarding data processing. Additional instructions are permissible, but must be provided in writing or via the Processor's designated electronic format. Verbal instructions are only allowed in urgent cases and must be confirmed in writing promptly.

6.2. If the Processor believes that an instruction violates data protection laws, they will notify the Controller without undue delay. The Processor may suspend action on the instruction until confirmation or modification by the Controller. The Controller assumes full responsibility for any damages arising from instructions that violate applicable law, and will indemnify the Processor against third-party claims.

6.3. If instructions fall outside the agreed scope of services, they will be treated as a request for a change to the services. The Processor will inform the Controller about potential impacts on service delivery, deadlines, and fees. If the Processor cannot reasonably accommodate the instructions, they may reject them. If the Controller insists, the Processor reserves the right to terminate the Service Agreement and the DPA immediately.

6.4. Only individuals authorized by the Controller may issue instructions. If no authorized person is specified within the Publitas platform, the Controller must appoint an individual via email to the designated address (privacy@publitas.com). The Processor may suspend processing until the Controller verifies the authority of the designated individual.

7. General Obligations of the Processor

In addition to adhering to the terms of this DPA, the Processor must comply with Articles 28 to 33 GDPR. This includes:

- appointing a Data Protection Officer (DPO), if required by law, who will perform their duties as outlined in Articles 38 and 39 GDPR. The DPO's contact information will be readily accessible through Publitas.

- cooperate with supervisory authorities as required by law, including notifying the Controller of any investigations or actions taken by authorities concerning the processing under this DPA.

- assist the Controller in case of any investigations or proceedings initiated by supervisory authorities or other legal processes that may involve the personal data being processed.

8. Monitoring and Compliance

8.1. The Processor will continuously assess internal processes and technical and organizational measures to ensure data processing complies with the applicable data protection laws and that the rights of data subjects are protected.

8.2. The Processor shall provide the Controller with documentation regarding the technical and organizational measures (TOMs) implemented, including relevant certifications (e.g., ISO certifications) to demonstrate compliance with privacy and security standards.

9. Duty to Cooperate in Inspections

9.1. The Controller has the right to assign an independent party to inspect the Processor's compliance with data protection obligations concerning their data, provided that the inspection respects the Processor's legitimate interests, technical and organizational measures, and data protection regulations. The Controller must provide at least 14 days' notice before a routine inspection during business hours. The Controller bears all costs of such inspection.

9.2. In the event of a security incident or a significant violation of data protection provisions, the notice period for an inspection will be reduced to an appropriate period, no longer than 72 hours. Event-related inspections are not subject to the restrictions outlined above.

9.3. The Processor may require the inspector to sign a confidentiality agreement before permitting the inspection. If the inspector has a competitive relationship with the Processor or there are other reasonable concerns, the Processor has the right to object to the Controller's choice of inspector.

9.4. The Processor is only required to permit one non-event-related on-site inspection per calendar year, which should not exceed one day. The Controller will cover all costs related to the inspection, including travel, labor, and external audit fees.

9.5. The Processor may refuse a non-event-related inspection if it provides appropriate evidence of compliance, such as certifications, reports from independent bodies, or proof of adherence to recognized standards like Art. 40 or Art. 42 GDPR.

Technical and Organizational Measures

10. Implementation of security measures

10.1. The Processor is responsible for implementing and documenting technical and organizational measures to ensure the security of data processing, as per Articles 28(3)(c) and 32 of the GDPR. These measures must ensure data confidentiality, integrity, availability, and resilience, taking into account the nature, scope, and risks associated with data processing.

10.2. The Processor reserves the right to update and improve security measures over time, provided that the agreed-upon level of protection is not compromised. Significant changes to these measures must be documented.

10.3. The Processor must provide the Controller with documentation of these measures for inspection when requested.

11. Subprocessing Relationships

11.1. Subprocessors are only those who provide directly related services to the primary contract. Ancillary services are excluded. The Controller’s initial approval of Subprocessors is granted at the conclusion of this DPA. Third-country Subprocessors are permitted under the condition that their data processing activities comply with GDPR requirements for data transfers. This includes adherence to mechanisms such as Standard Contractual Clauses (SCCs), Binding Corporate Rules (BCRs), adequacy decisions, or other approved transfer safeguards under Chapter V of the GDPR.

11.2. The Processor must notify the Controller if any new Subprocessors are engaged or if existing Subprocessors are replaced. The Controller has 14 days from the notification to object for legitimate data protection reasons. In the case of an objection, the Processor may choose to proceed without the change or discontinue the service within four weeks if the objection makes the service provision unfeasible.

11.3. The Processor is required to ensure that Subprocessors comply with the same data protection obligations under the GDPR. This includes entering into contractual agreements with Subprocessors to ensure data security and compliance.

11.4. Inspections at Subprocessors' premises will only be conducted by the Processor, once annually at most. If required, these inspections can be substituted with documentation proving the Subprocessors' data protection compliance.

12. Rights of Data Subjects

12.1. When a data subject exercises their rights under Chapter III of the GDPR, the Processor must redirect the request to the Controller and notify the Controller promptly, no later than 74 hours after receiving the request.

12.2. The Platform empowers the Controller with comprehensive tools for independent data management and access control. This allows the Controller to directly address data subject requests under GDPR. If the Controller requires additional support from the Processor to respond to such requests, the Processor will provide assistance as reasonably feasible. However, the Controller remains primarily responsible for responding to these requests.

12.3. The Processor holds no liability for any failure on the part of the Controller to respond to a data subject's request, respond accurately, or respond within the required timeframe, provided such failure is attributable solely to the Controller's actions or omissions.

13. Information and Notification Obligations

The Processor must assist the Controller in meeting their obligations under Articles 32–36 of the GDPR, including reporting breaches, conducting impact assessments, and engaging with supervisory authorities when necessary. This includes:

- Reporting any data protection breaches related to the Controller's end-users without undue delay.
- Providing information and documentation necessary for the Controller's data protection impact assessments.
- Assisting in consultations with the supervisory authority prior to processing, if needed.
- The Processor may request appropriate remuneration for providing such support.

14. Disclosure and Deletion of Data

14.1. Upon termination of the data processing services, the Processor must disclose or delete personal data as per the Controller's instructions.

14.2. The Processor may be legally obligated to retain personal data for a certain period after the end of the contract. The Controller may request the disclosure or deletion of such data at any time within the retention period.

14.3. If the Controller requests the deletion of data prior to the expiration of the retention period, the Processor must comply, except for data that is legally required to be retained (e.g., security logs).

14.4. If the Controller does not request disclosure or deletion of data by the end of the retention period, the Processor is obligated to delete the data.

15. Anonymization

15.1. The Processor has the right to anonymize and aggregate personal data covered by this Agreement, and to use the anonymized data for their own purposes (e.g., statistical analysis, product development).

15.2. Anonymized data will no longer be considered personal data and will not be subject to the obligations of this DPA. The Processor may use and store anonymized data beyond the contract’s end.

Remaining Provisions

16. Liability

16.1. The Controller will be fully liable and must indemnify the Processor from any claims brought by third parties.

16.2. The Processor is liable for damages arising from a failure to comply with their obligations under the GDPR or this Agreement, or if the Processor fails to follow the lawful instructions of the Controller.

16.3. Exclusions of liability do not apply in cases of gross negligence, intent, or damage caused by harm to life, health, or limb.

17. Concluding Provisions

17.1. Both parties may confirm the conclusion of the contract in electronic format in accordance with Art. 28(9) of the GDPR.

17.2. Both parties agree to treat all business secrets and data security measures of the other party as confidential, even beyond the termination of this DPA.

17.3. Any provision deemed void or unenforceable will be removed, and the remaining provisions will remain in full effect. Any terms that by their nature survive termination or expiration of this DPA, will survive.

17.4. The Processor reserves the right to modify any part of this DPA at any time, and such changes will take effect upon posting the updated version on our website at https://www.publitas.com/. The Controller will be notified of significant changes via email, invoice or platform announcements.

17.5. This DPA is governed by the Laws of the Netherlands, without regard to the choice or conflicts of law provisions of any jurisdiction.

17.6. Any dispute arising out of or in connection with this DPA, including any disputes regarding the existence, validity or termination, shall be settled by competent Dutch court and in force at the time when such proceedings are commenced. The place of court will be Amsterdam, the Netherlands.

ANNEX 1: Subprocessor list - latest update 25-06-25

Personal Data from Customers as a Controller may only be processed by Subprocessors listed for the CMS server in use (Publitas.com, Spott.ai, or WePublish.com used for i.e. folders.nl, promobutler or promozilla.). The Subprocessor list applies only to CMS users, not to specific products or services for which we are Controller (i.e. uploading a PDF document to folders.nl). This ensures GDPR-compliant data handling as per our Data Processing Agreement.

CMS Server	Name & Address	Description of services	Where data is processed	Guarantees / Legal basis
Publitas, Spott	Amazon Web Services EMEA SARL, 38 avenue John F. Kennedy, L-1855 Luxembourg	Core infrastructure hosting for Publitas and related platforms. Stores consumer data for security, auditing, and accounting purposes, with a data retention period of 365 days. Processes IP addresses, cookies, personal identifiers, app-instance IDs, geo location, device/browser metadata, click IDs, conversion values.	Data is processed in Dublin, Ireland (EU).	Data processing complies with GDPR. AWS provides data privacy and security measures, including data retention policies and compliance with EU data protection laws.
WePublish	Microsoft Corporation, One Microsoft Way, Redmond, WA 98052, USA	Primary cloud hosting and infrastructure provider for folders.nl, promobutler, legacy WP, and related platforms. Provides cloud storage, compute, and related infrastructure services, processing essentially all customer data for these products.	Data for EU customers is stored and processed in Microsoft's EU-based data centers (e.g., Ireland, Netherlands, and other EU countries). Microsoft has committed to full EU data residency for EU clients; all operations are monitored and controlled by EU-based personnel. Remote access by non-EU engineers is tightly controlled and monitored.	Microsoft's Data Protection Addendum (DPA) incorporates the European Commission's Standard Contractual Clauses (SCCs) for any international transfers. Microsoft is contractually obligated to comply with GDPR, including all Article 28 processor requirements. Microsoft's EU data residency commitment ensures all EU customer data remains under EU jurisdiction and law. Additional technical and organizational measures, including the Microsoft Supplier Security and Privacy Assurance Program, are in place for GDPR compliance.

WePublish, Spott	Cloudflare, Inc., 101 Townsend St, San Francisco, CA 94107, USA	Content Delivery Network (CDN), DDoS protection, firewall, DNS, TLS, rate-limiting, and edge worker services for Publitas platforms. Cloudflare processes IP addresses, HTTP request metadata (user-agent, browser type, device, etc.) to deliver these services.	Data is processed in the EU, the US, and other global locations as part of Cloudflare's distributed network. For EU customers, data is stored and processed in both the EU and the US, and may be cached in any of Cloudflare's global edge locations.	Cloudflare's Data Processing Addendum (DPA) includes the European Commission's Standard Contractual Clauses (SCCs) for international transfers. Cloudflare is certified under the EU Cloud Code of Conduct for GDPR compliance. Cloudflare's privacy and security practices are externally validated and monitored for GDPR compliance. Supplementary technical and organizational measures are in place to ensure lawful and secure data transfers from the EU.
Publitas, Spott, WePublish	Google LLC / Google Ireland Ltd, 4 Barrow St, Grand Canal Dock, Dublin 4, D04 V4X7, Ireland	Google Analytics collects site statistics about consumers and customers. Processes IP addresses, cookies, personal identifiers, app-instance IDs, geo location, device/browser metadata, click IDs, conversion values.	This subprocessor is optional for Publitas. End users can opt out via a cookie banner. Data is processed globally. For EU customers, Google offers EU data residency options but some analytics data may be processed in the US or other locations.	Google complies with GDPR, including anonymization of IP addresses and browser data. Uses EU Standard Contractual Clauses (SCCs) and other privacy safeguards for international transfers. Certified under relevant privacy frameworks.
Publitas, Spott	Functional Software, Inc. d/b/a Sentry, 45 Fremont Street, 8th Floor, San Francisco, CA 94105, USA	Cloud-based real-time error monitoring platform. Anonymously collects errors and provides an interface to track errors generated by browsers of customers and consumers. Event data retained for up to 90 days.	Data is processed in the US (Google Cloud Platform), but for EU customers, efforts are made to process and store data in the EEA where possible.	Sentry's DPA includes SCCs for international transfers. Sentry is committed to GDPR compliance, with technical and organizational measures in place with an dequacy decision certification Non-HR.