

NewsIntel — Data Processing Agreement

Global Staffing Support B.V. (“GSS”) and the Client

Effective date: 1 September 2026

Contents

- Preamble
- 1. Definitions
- 2. Roles of the Parties
- 3. Scope and instructions
- 4. Confidentiality
- 5. Security
- 6. Personal Data Breach
- 7. Sub-processors
- 8. International transfers
- 9. Assistance to the Client
- 10. Audit and information
- 11. Retention, return and deletion
- 12. Liability
- 13. Term
- 14. Changes to this DPA
- 15. Miscellaneous
- Annex I — Details of the Processing
- Annex II — Technical and organizational measures
- Annex III — Sub-processors
- Annex IV — Joint-controller arrangement (Art. 26 GDPR)
- Annex V — Publishable summary of the joint-controller arrangement

Preamble

This Data Processing Agreement (“**DPA**”) forms an integral part of the Agreement between:

(1) **Global Staffing Support B.V.**, a private limited liability company incorporated under the laws of the Netherlands, registered with the Dutch Chamber of Commerce under number 09132165, VAT number NL811925225B01, with its registered office at Kraailandhof 63, 3828 JP Hoogland, the Netherlands, operating the NewsIntel service (“**GSS**”); and

(2) the Client identified in the order or onboarding confirmation (“**Client**”); each a “**Party**” and together the “**Parties**”.

Whereas GSS provides the NewsIntel news-generation service to the Client under the Terms of Service, and whereas the provision of that service involves the processing of personal data, the Parties enter into this DPA in order to comply with Article 28(3) of Regulation (EU) 2016/679 (“**GDPR**”) and, where applicable, Article 26 GDPR.

Acceptance. This DPA is accepted together with the Terms of Service on formation of the Agreement. The Client accepts this DPA by ticking the acceptance or consent box presented at registration, at checkout or during onboarding, by clicking a button marked “I agree”, “Accept” or equivalent, by signing or confirming an order, or by using the Service. Acceptance in any of those ways is given by a person authorized to bind

the Client, constitutes the Client's agreement to be bound by this DPA, and has the same effect as a handwritten signature. No separate signature is required for this DPA to be binding, including on completion of a self-service checkout. Where the Client requires a signed counterpart, GSS will provide one on request at info@newsintel.eu.

1. Definitions

Terms defined in the Terms of Service have the same meaning here. In addition:

- **"Controller", "Processor", "Sub-processor", "Data Subject", "Personal Data", "Processing", "Personal Data Breach", "Supervisory Authority"** have the meanings given in Art. 4 GDPR.
- **"Client Personal Data"** means Personal Data that GSS Processes on behalf of the Client under the Agreement, as further specified in **Annex I**.
- **"Applicable Data Protection Law"** means the GDPR, the Dutch GDPR Implementation Act (*Uitvoeringswet AVG*), the Dutch Telecommunications Act insofar as it concerns electronic communications and cookies, the UK GDPR and Data Protection Act 2018 where applicable, and any other data-protection law applicable to a Party's Processing under the Agreement.
- **"Standard Contractual Clauses" / "SCCs"** means the standard contractual clauses for the transfer of personal data to third countries adopted by the European Commission in Implementing Decision (EU) 2021/914, as amended or replaced.
- **"UK Addendum"** means the International Data Transfer Addendum to the SCCs issued by the UK Information Commissioner under s.119A of the Data Protection Act 2018.
- **"TOMs"** means the technical and organizational measures set out in **Annex II**.

2. Roles of the Parties

2.1 The Parties acknowledge that the Service involves several distinct Processing activities, to which different roles attach. The allocation is set out in **Annex I, Part D**, and is summarized as follows:

Processing activity	GSS	Client
(a) Newsletter recipient lists created, imported or collected by the Client	Processor	Controller
(b) Sources, keywords, project configuration and other content supplied or designated by the Client	Processor	Controller
(c) Delivery of Articles to the Client's Channels and any Personal Data contained in them once published	Processor in respect of the delivery; the Client is Controller of the publication	Controller
(d) Source monitoring, scraping, normalization, clustering, generation and validation within the GSS pipeline	Independent Controller	Not a Controller
(e) Editorial approval of an Article containing Personal Data, in so far as the Parties jointly determine purposes and means	Joint Controller (Art. 26)	Joint Controller (Art. 26)
(f) Client account, authentication, authorization, security, audit logging, support and billing data	Controller	Not a Controller

Processing activity	GSS	Client
(g) Research of the Client's own sources by GSS personnel, to the extent it involves Personal Data supplied or designated by the Client	Processor	Controller

2.2 Sections 3 to 15 of this DPA apply to the activities in which GSS acts as **Processor** — rows (a) to (c) and (g).

2.3 In respect of the activity in which GSS acts as **independent Controller** — row (d) — GSS Processes Personal Data for its own purposes and on its own legal basis, as described in the GSS Privacy Policy (<https://newsintel.eu/privacy.html>). Each Party is independently responsible for its compliance, and neither Party is liable for the other's compliance in respect of that activity.

2.4 In respect of the activity in which the Parties may qualify as **Joint Controllers** — row (e) — the arrangement required by Art. 26(1) GDPR is set out in **Annex IV**, and the essence of that arrangement, in the form made available to Data Subjects, is in **Annex V**. Notwithstanding any allocation between the Parties, a Data Subject may exercise their rights against either Party.

2.5 This DPA prevails over the Terms of Service on the subject of the qualification of roles and on all matters required to be agreed under Art. 28(3) GDPR. Terms of Service §2.2 reflects this expressly.

3. Scope and instructions

3.1 GSS shall Process Client Personal Data only:

- on the documented instructions of the Client;
- as necessary to provide, maintain, secure and support the Service in accordance with the Agreement; and
- as required by Union or Member State law to which GSS is subject, in which case GSS shall inform the Client of that legal requirement before Processing, unless that law prohibits such information on important grounds of public interest.

3.2 The Agreement, including this DPA, the Client's configuration of its Project, and the Client's use of the functions of the Service and the API constitute the Client's documented instructions. Additional or diverging instructions must be given in writing to info@newsintel.eu and may be subject to reasonable charges where they require material additional effort.

3.3 GSS shall inform the Client without undue delay if, in its opinion, an instruction infringes Applicable Data Protection Law. GSS may suspend the execution of that instruction until it is confirmed, amended or withdrawn.

3.4 No model training. GSS shall not Process Client Personal Data for its own purposes, and in particular shall not use it to train, fine-tune or improve artificial-intelligence or machine-learning models, whether its own or those of a third party.

3.5 The Client warrants that: (i) it has a valid legal basis for the Processing it instructs, including for the collection and use of newsletter recipient data and for the publication of Articles on its Channels; (ii) it has provided the information required by Art. 13 and 14 GDPR to the relevant Data Subjects; and (iii) its instructions do not require GSS to Process Personal Data unlawfully.

3.6 Data not designed for. The Service is not designed for, and is not warranted as suitable for, the Processing of: special categories of Personal Data within the meaning of Art. 9 GDPR; Personal Data relating to criminal convictions and offences within the meaning of Art. 10 GDPR; government identification numbers; payment-card data; or Personal Data of children. The Client shall not knowingly submit such data

and shall take reasonable steps to exclude it from material it supplies or designates. Where such data is nevertheless Processed through the Service, (i) the Client remains solely responsible for identifying the additional safeguards it requires and for its own lawful basis, including any condition under Art. 9(2) GDPR; (ii) GSS Processes it under this DPA on the same terms as other Client Personal Data; and (iii) GSS may, on becoming aware, suspend the relevant Processing under Terms of Service §6.6 and require the Client to remove the material.

4. Confidentiality

4.1 GSS shall treat Client Personal Data as confidential and shall not disclose it except as permitted by this DPA.

4.2 GSS shall ensure that persons authorized to Process Client Personal Data are bound by an enforceable obligation of confidentiality that survives the end of their engagement, have received appropriate data-protection training, and have access only to the extent necessary for their duties (least privilege).

4.3 GSS shall limit access to Client Personal Data to personnel who need it to perform the Agreement, including the News Master assigned to the Client's Project, and shall log administrative access.

5. Security

5.1 GSS shall implement and maintain the technical and organizational measures set out in **Annex II**, appropriate to the risk within the meaning of Art. 32 GDPR, taking into account the state of the art, the costs of implementation, and the nature, scope, context and purposes of the Processing.

5.2 GSS may update the TOMs from time to time, provided that the level of protection is not materially reduced. Where an update materially changes the TOMs, GSS shall notify the Client at least thirty (30) days in advance.

5.3 The Client is responsible for the secure configuration and use of its side of the integration, including the confidentiality and server-side storage of API keys, the roles it assigns to its users, and the security of the systems on which it publishes Articles.

6. Personal Data Breach

6.1 GSS shall notify the Client of a Personal Data Breach affecting Client Personal Data without undue delay and in any event within 72 hours of becoming aware of it.

6.2 The notification shall include, to the extent then known and thereafter as it becomes available: the nature of the breach; the categories and approximate number of Data Subjects and records concerned; the likely consequences; the measures taken or proposed to address the breach and mitigate its effects; and the name and contact details of a point of contact at GSS.

6.3 GSS shall document every Personal Data Breach, take reasonable steps to contain and remediate it, and provide the Client with the assistance the Client reasonably requires to meet its own obligations under Art. 33 and 34 GDPR.

6.4 GSS shall not notify a Supervisory Authority or Data Subjects on the Client's behalf in respect of Client Personal Data unless the Client instructs it to do so, or unless GSS is itself obliged to notify in its capacity as independent Controller.

7. Sub-processors

7.1 The Client gives GSS **general written authorization** to engage Sub-processors for the Processing of Client Personal Data. The Sub-processors currently engaged are listed in **Annex III**.

7.2 GSS shall impose on each Sub-processor, by way of a written contract, data-protection obligations that are no less protective than those in this DPA, in particular as regards security, confidentiality, the prohibition on model training in §3.4, assistance and transfer safeguards.

7.3 GSS remains fully liable to the Client for the performance of each Sub-processor's obligations.

7.4 Change notification. GSS shall notify the Client of any intended addition or replacement of a Sub-processor at least **thirty (30) days** in advance, by e-mail to the Client's registered administrative contact and by updating **Annex III** to this DPA, which is published at <https://newsintel.eu/subprocessors.html>.

7.5 Objection. The Client may object to an intended change on reasonable, documented data-protection grounds within fourteen (14) days of notification. The Parties shall then discuss the objection in good faith. If GSS cannot reasonably provide the Service without the Sub-processor, and the objection is not resolved within thirty (30) days, the Client may terminate the affected part of the Agreement, or the Agreement as a whole, without penalty, effective from the date the change takes effect.

7.6 Urgent changes. Where a Sub-processor must be replaced urgently for security, legal or continuity reasons, GSS may do so with shorter notice and shall inform the Client as soon as reasonably possible, stating the reason.

8. International transfers

8.1 GSS shall not transfer Client Personal Data outside the European Economic Area, nor permit a Sub-processor to do so, except where one of the following applies:

- an adequacy decision of the European Commission under Art. 45 GDPR covers the recipient, including certification under the EU-US Data Privacy Framework where applicable;
- the Standard Contractual Clauses are in place, supplemented by a documented transfer impact assessment and any additional technical, contractual and organizational measures the assessment identifies as necessary; or
- another valid transfer mechanism under Chapter V GDPR applies.

8.2 Which instrument applies.

Situation	Instrument
Client established in the EEA; recipient in a third country acting as processor	SCCs Module Two (Controller to Processor), Client as data exporter
GSS transfers as processor to a Sub-processor in a third country	SCCs Module Three (Processor to Processor)
Client established outside the EEA, receiving Personal Data from GSS as processor	SCCs Module Four (Processor to Controller), where the data originates in the EEA
Personal Data subject to UK GDPR	SCCs plus the UK Addendum
Personal Data subject to Swiss law	SCCs with the Swiss adaptations

For the purposes of the SCCs:

- the optional docking clause (Clause 7) **applies**;
- for Clause 9, **Option 2 (general written authorization)** applies, with the notification period in §7.4 of this DPA;
- for Clause 11, the optional independent dispute-resolution body **does not apply**;
- for Clause 17, the governing law is the law of **the Netherlands**;
- for Clause 18(b), the forum is the courts of **the Netherlands**;
- Annexes I, II and III to the SCCs are the corresponding Annexes to this DPA.

8.3 By entering into this DPA, the Client mandates GSS to enter into the SCCs with Sub-processors in the Client's name and on its behalf, and to make the corresponding onward-transfer arrangements. GSS shall make copies of the relevant clauses available to the Client on request, with commercially confidential terms redacted.

8.4 GSS maintains a record of the transfer mechanism applicable to each Sub-processor listed in **Annex III** and makes that record available to the Client on request.

9. Assistance to the Client

9.1 Data-subject requests. Taking into account the nature of the Processing, GSS shall assist the Client in fulfilling requests from Data Subjects to exercise their rights under Chapter III GDPR. GSS shall:

- (a) provide functionality in the Service enabling the Client to access, export, rectify, restrict and delete Client Personal Data itself;
- (b) not respond to a Data Subject request concerning Client Personal Data itself, but forward it to the Client without undue delay, unless the request concerns GSS's own Controller Processing; and
- (c) provide reasonable additional assistance where the Client cannot fulfil a request using the functionality of the Service.

9.2 Requests concerning Articles. Where a Data Subject request concerns an Article, the Parties shall coordinate under the procedure in Terms of Service §8 and **Annex IV** to this DPA. Neither Party shall unilaterally reject such a request without consulting the other. Where GSS assesses a request as justified after a documented balancing of interests, the Client shall remove or anonymize the Article from all Channels within **72 hours**, and GSS shall take the steps in Terms of Service §8.8 in its own systems.

9.3 DPIA and prior consultation. GSS shall provide the Client, on request, with the information reasonably necessary for the Client to carry out a data-protection impact assessment under Art. 35 GDPR or a prior consultation under Art. 36 GDPR in respect of the Service, including the data-flow documentation, the TOMs and the sub-processor mapping.

9.4 Regulatory enquiries. GSS shall provide reasonable assistance in relation to enquiries, investigations or enforcement action by a Supervisory Authority concerning Client Personal Data and shall inform the Client without undue delay of any legally binding request for disclosure of Client Personal Data by a public authority, unless prohibited from doing so.

9.5 Charges. Assistance under §9.1(c), §9.3 and §9.4 is provided free of charge to the extent it is proportionate and non-recurring. Where a request requires material additional effort, GSS may charge on a time-and-materials basis at its then-current rates, having first informed the Client.

10. Audit and information

10.1 GSS shall make available to the Client the information reasonably necessary to demonstrate compliance with Art. 28 GDPR, including the TOMs, the sub-processor list, the data-flow documentation and, where available, third-party audit reports and certifications.

10.2 The Client may audit GSS's compliance with this DPA. Audits shall:

- be conducted no more than once per twelve-month period, save where a Personal Data Breach has occurred or a Supervisory Authority requires it;
- be announced at least thirty (30) days in advance;
- take place during normal business hours, without unreasonable disruption to GSS's operations;
- be limited to information and systems relevant to the Processing of that Client's Personal Data, and shall not extend to other customers' data, to GSS's commercially confidential information, or to source code;
- be conducted by the Client or by an independent auditor bound by confidentiality and not being a competitor of GSS.

10.3 GSS may satisfy an audit request in the first instance by providing a current third-party audit report or certification, or by completing a reasonable security questionnaire. An on-site audit may proceed where the Client demonstrates that these do not adequately address its documented concern.

10.4 The Client bears the costs of an audit it initiates, unless the audit reveals a material breach of this DPA by GSS, in which case GSS bears the reasonable costs.

10.5 GSS is not currently certified under ISO/IEC 27001 or SOC 2.

11. Retention, return and deletion

11.1 GSS shall Process Client Personal Data only for as long as necessary for the purposes of the Agreement, and in accordance with the retention periods in **Annex I, Part C**.

11.2 The Client may configure a retention period for its Project within the limits offered by the Service.

11.3 Deletion and return on termination. On termination or expiry of the Agreement, GSS shall, at the Client's choice, delete or return Client Personal Data, and delete existing copies, within thirty (30) days of the end of the export window referred to in Terms of Service §7.6, unless Union or Member State law requires further storage. Articles already delivered to the Client are dealt with in §11.4 instead.

11.4 Delivered Articles after termination.

- **(a)** GSS retains each Article delivered to the Client during the term, together with its revisions, its published snapshot, its cover images and the associated editorial audit record, for twenty-four (24) months from the date of termination or expiry of the Agreement, and deletes them at the end of that period in accordance with §11.7.
- **(b)** That retention serves to demonstrate GSS's compliance with its editorial, source-selection and accountability obligations, and to allow the establishment, exercise or defense of legal claims. GSS Processes retained Articles for no other purpose, and §3.4 continues to apply to them.
- **(c)** Retention by GSS does not affect ownership of, or the licence granted in respect of, a delivered Article. The licence in Terms of Service §4.3 survives termination, and deletion of an Article from GSS's systems does not limit the Client's rights in it or its ability to keep, publish and use its own copies.
- **(d)** At any time during the retention period the Client may request an export of its delivered Articles in a structured, commonly used and machine-readable format. GSS provides one such export free of charge in any twelve-month period; further exports may be charged under §9.5. The Client is responsible for keeping its own copies, and after the end of the retention period GSS is no longer able to supply them.
- **(e)** The Client may request deletion of its delivered Articles before the end of the retention period. GSS shall comply within thirty (30) days, except to the extent that retention remains required by law or necessary for the purposes in (b).

11.5 Other retention after termination. Apart from §11.4, GSS may retain Client Personal Data after termination only to the extent and for as long as required by law, or as necessary for the establishment, exercise or defense of legal claims. Data retained under §11.4 or this §11.5 remains subject to this DPA for as long as it is retained.

11.6 Backups. Data deleted from the production environment is removed from backups in accordance with the backup rotation cycle, after which it is no longer recoverable.

11.7 Deletion completeness. Deletion of an Article or a record includes deletion of the derived artefacts associated with it, namely: Article revisions; the published snapshot; generated cover images and any other file held in object storage or as binary data; embeddings and vector representations; extracted and chunked text; scraped source records; and any material the Client has designated in connection with that Article together with the text retrieved from it.

11.8 GSS shall certify deletion in writing on request.

12. Liability

12.1 The liability regime in Terms of Service §12 applies to this DPA, subject to §12.2.

12.2 Nothing in this DPA or in the Terms of Service limits or excludes:

- either Party's liability towards a Data Subject under Art. 82 GDPR;
- either Party's liability for administrative fines imposed on it by a Supervisory Authority in respect of its own infringement; or
- liability that cannot be limited under mandatory law.

12.3 Where the Parties are Joint Controllers under **Annex IV** and one Party has paid compensation to a Data Subject in full, that Party may claim back from the other Party the part of the compensation corresponding to the other Party's share of responsibility for the damage, in accordance with Art. 82(5) GDPR.

12.4 Each Party shall indemnify the other against claims, fines and reasonable costs to the extent these result from that Party's own breach of Applicable Data Protection Law or of this DPA.

13. Term

13.1 This DPA takes effect on formation of the Agreement and remains in force for as long as GSS Processes Client Personal Data.

13.2 Provisions that by their nature are intended to survive — including §3 (Scope and instructions), §4 (Confidentiality), §8 (International transfers), §11 (Retention, return and deletion), §12 (Liability), **Annex IV** and **Annex V** — survive termination for as long as GSS retains any Client Personal Data.

14. Changes to this DPA

14.1 Reservation of right to amend. GSS reserves the right to amend this DPA, at its own initiative or where required by a change in Applicable Data Protection Law, in the guidance or decisions of a Supervisory Authority or a court, in a certification or code of conduct, or in the Service. No amendment shall reduce the level of protection of Client Personal Data below the standard required by Art. 28 GDPR, and no amendment shall relieve GSS of an obligation that Applicable Data Protection Law requires a processor to accept.

14.2 Non-material amendments — including corrections, clarifications, changes of contact details, and updates to **Annex II** and **Annex III** made in accordance with §5.2 and §7 — take effect on publication of the amended DPA, without further notice.

14.3 Material amendments will be notified in writing to the Client's registered administrative contact at least thirty (30) days before they take effect. An amendment is material where it appreciably changes the Client's rights or GSS's obligations under this DPA.

14.4 If the Client does not accept a material amendment, it may terminate the Agreement by written notice given before the amendment takes effect, effective as of the date the amendment takes effect. Continued use of the Service after a material amendment has taken effect constitutes acceptance of that amendment.

14.5 The Client is notified of and may accept an amendment in the same ways as set out under "Acceptance" in the Preamble.

15. Miscellaneous

15.1 This DPA is governed by the laws of the Netherlands. Disputes are subject to Terms of Service §15.2.

15.2 Where a provision of this DPA conflicts with the SCCs, the SCCs prevail.

15.3 Notices under this DPA are given to info@newsintel.eu for GSS, and to the administrative contact registered by the Client.

Annex I — Details of the Processing

Part A — Parties

	Data exporter / Controller	Data importer / Processor
Name	The Client, as identified in the order or onboarding confirmation	Global Staffing Support B.V.
Address	As registered by the Client	Kraailandhof 63, 3828 JP Hoogland, the Netherlands
Contact	The Client's administrative contact	info@newsintel.eu
Activities relevant to the transfer	Use of the NewsIntel Service; publication of Articles on its own Channels	Provision of the NewsIntel news-generation service
Role	Controller (see DPA §2)	Processor (see DPA §2)

Part B — Description of the Processing

B.1 Subject matter. Provision of the NewsIntel news-generation service: configuration of a Project, generation and human editorial review of Articles, delivery of Articles to the Client's Channels, and operation of newsletter distribution to the Client's own recipient lists.

B.2 Duration. For the term of the Agreement, plus the retention periods in Part C.

B.3 Nature and purpose of the Processing. Collection, recording, organization, structuring, storage, retrieval, consultation, use, indexing and vectorization, transmission by delivery to the Client's Channels, e-mail distribution, restriction, erasure and destruction — for the purpose of producing and delivering news content and operating the associated newsletter function.

B.4 Categories of Data Subject

Category	Notes
The Client's authorized users	Employees and contractors of the Client using the application
Newsletter recipients	Individuals on lists the Client creates, imports or collects through a subscription form connected to the public API
Individuals mentioned in source material or in Articles	Predominantly persons acting in a public, professional or corporate capacity
Individuals appearing in sources the Client supplies or designates	Any individual named in a source or in data the Client designates — the Client controls what it designates

B.5 Categories of Personal Data

Category	Fields
User account data	Name, work e-mail address, company, job title, language preference, hashed password, verification and session tokens, role and membership assignments

Category	Fields
Newsletter recipient data	E-mail address, optional name, active or inactive status, subscription and unsubscription timestamps, unsubscribe token, send and delivery outcomes
Content data	Names and information about identifiable individuals appearing in scraped source material, generated Articles, Article revisions, summaries, claims, metadata and AI-generated images
Client-designated source material	Sources and data the Client supplies or designates for the generation of Articles, and the text retrieved from them
Configuration data	Topics, categories, keywords, excluded topics, registered Channels, source and domain allowlists, quotas, prompt profiles and publishing policies — which may indirectly reveal information about individuals where a keyword is a person's name
Usage and audit data	User identifier, timestamps, action performed, object affected, IP address, user agent, request and response metadata
Support data	Subject, description, page URL, timestamp, user and workspace identifiers, e-mail address, attachments

B.6 Special categories of Personal Data. None are intended to be Processed. The Client is prohibited from submitting them under DPA §3.6. GSS's editorial guidelines prohibit the generation of Art. 9 and Art. 10 GDPR content about identified individuals.

B.7 Frequency of the transfer. Continuous, for the duration of the Agreement.

B.8 Sub-processing. As set out in **Annex III**.

B.9 Competent Supervisory Authority. Autoriteit Persoonsgegevens (the Netherlands), where the Client is established in the Netherlands or where GSS acts as the relevant establishment. Otherwise, the authority of the Client's main establishment.

Part C — Retention periods

Data	Retention	Notes
User account data	Term of the Agreement + 90 days	Deleted or returned per DPA §11.3
Newsletter recipient data	Until removed by the Client or unsubscribed by the recipient; a suppression record is then kept for 90 days and deleted	Suppression prevents re-adding by mistake
Articles and revisions	Term of the Agreement + the export window; delivered Articles, their revisions and the editorial audit record retained for 24 months from termination, then deleted	Per DPA §11.4; export available on request; the licence under Terms of Service §4.3 is unaffected
Scraped source records	90 days from scraping	
Client-designated source material	Until removed by the Client, or on termination per DPA §11.3	Client-controlled

Data	Retention	Notes
Embeddings and derived artefacts	Deleted together with the source record	See DPA §11.7
Editorial and generation audit logs	24 months	Required to demonstrate adherence to the source policy
Application and error logs	90 days	
AI-processing records	12 months	Model, tokens, latency; input text where logged
Support tickets	24 months after closure	

Part D — Role allocation per activity

As set out in DPA §2.1. **Annex IV** governs the joint-controller activity; **Annex V** is the publishable summary of it.

Annex II — Technical and organizational measures

Each section below distinguishes measures **in place** from measures **in development and not yet in effect**. Only the measures listed as in place are represented by GSS as implemented.

II.1 Pseudonymization and encryption

In place

- All data in transit is encrypted using TLS with modern cipher suites; HTTP is redirected to HTTPS; HSTS is enabled.
- Selected database fields are encrypted at the storage layer.
- Passwords are stored using a one-way hash. Public API keys are stored as a hash with a pepper and are displayed once, at creation.
- Logs are passed through a centralized sanitization layer that redacts passwords, tokens, API keys, authorization headers and e-mail addresses before storage.
- Secrets are held outside the source repository and injected at deployment; the commit history has been verified clean and production credentials are issued independently of the development environment.

In development — not yet in effect

- Encryption at rest across all stored data, including disk-level encryption and a managed key-management service.

II.2 Confidentiality, integrity, availability and resilience

Access control — in place

- Authentication by JWT with scoped sessions; e-mail verification on registration; single sign-on via Google where enabled.
- Role-based access control with workspace and project membership. Workspace roles: Workspace Owner, Workspace Member. Project roles: News Master, Viewer.
- Tenant scoping (workspace and project) enforced in queries, endpoints, background jobs and administrative screens, with the project identifier carried through every news-domain table.
- Least-privilege internal access; administrative actions logged with actor, timestamp and action.
- Public endpoints protected by per-project API keys with scoped permissions — separate scopes for feed reading and newsletter subscription — and per-key rate limiting.

Access control — in development

- A single, consistent access model for public Article retrieval.
- Rate limiting on the main authenticated API.

Input and application security — in place

- Server-side validation of inputs; output sanitization for rendered content; sanitized server-side Markdown rendering to prevent cross-site scripting.
- URL normalization and domain allowlisting in discovery.

Input and application security — in development

- A single validator for outbound URL fetching, to prevent server-side request forgery, unified across every place a URL enters the system.

Availability and resilience — in place

- Health-check endpoints and error and performance monitoring.

Availability and resilience — in development

- Backups and disaster recovery, to be established with the ICT manager.

No service level is committed during the Early Access phase.

II.3 Testing, assessing and evaluating effectiveness

In place

- Code review and automated test suites in the development pipeline.
- Dependency and vulnerability monitoring.

An independent penetration test will be completed on the production environment before the first external client is connected, and annually thereafter.

II.4 Organizational measures

In place

- Confidentiality undertakings for all personnel and contractors.
- Data-protection and security awareness training.
- Records of processing activities, a lawful-basis analysis and editorial guidelines restricting the unnecessary use of Personal Data of non-public individuals.
- A documented source-selection and compliance policy, including verification of lawful access to sources and honouring machine-readable text-and-data-mining reservations under Art. 4 of Directive (EU) 2019/790.
- Written agreements with Sub-processors, including the prohibition on model training.
- Change management, with material changes to the TOMs notified to Clients.

In development — not yet in effect

- A documented incident-response process with defined roles, escalation and notification paths.
- A documented log-retention policy.
- Per-project retention configuration and a scheduled purge.
- Complete deletion, including files in object storage and derived artefacts.

II.5 Content-specific safeguards

In place

- **Human editorial gate:** every Article is reviewed, approved or rejected by a News Master before delivery, and publication is blocked by policy where approval has not been given. No Article reaches a Client Channel without that review.
- **Allowlist enforcement** at discovery and before scraping, restricted to curated and verified sources.
- **Prompt-level grounding:** the actual content of the retrieved sources is supplied to the generating model.
- **Immutable revisions:** generation, regeneration and manual edits create revisions rather than overwriting published content, preserving an auditable editorial history, and publication is tied to a specific revision.
- **Quotas and crawl budgets** per project and per domain, enforced by the scheduler and by counters before costly steps.
- **Cover images** are produced by an illustration-oriented model that does not generate photorealistic depictions of people.
- **Event-level editorial logging** for Articles, recording actor, timestamp, action and payload.

In development — not yet in effect

- Bias, toxicity and defamation screening with quarantine.
- Recorded image provenance (model, prompt, timestamp) as an auditable record rather than a property of the model choice.
- Origin and authorship metadata returned to the Client consistently in the API response, to enable AI-transparency labelling.
- Field-level audit diffs and a platform-wide audit log.

II.6 Measures for onward transfers

Sub-processors are bound by written agreements incorporating obligations no less protective than this DPA, the Standard Contractual Clauses where applicable, and, for AI providers, contractual restrictions on retention and on the use of submitted data for model training.

Annex III — Sub-processors

The Sub-processors engaged by GSS are listed below. Changes are notified under DPA §7.4.

III.1 Infrastructure

Compute, database and object storage are operated by GSS on its own infrastructure; no third-party hosting provider Processes Client Personal Data.

Sub-processor	Legal entity & country	Service	Data categories
TransIP	TransIP B.V. — Netherlands	Verification e-mails, notifications and newsletter sending	Recipient e-mail address, name, message content

III.2 AI model providers

Sub-processor	Legal entity & country	Service	Data categories
OpenAI	OpenAI Ireland Limited — Ireland	Text generation; cover-image generation	Prompt content, source excerpts, configuration context

III.3 Operations, payments and analytics

Sub-processor	Legal entity & country	Service	Data categories
Stripe	Stripe Payments Europe, Limited — Ireland	Subscription billing, SEPA direct debit and card payments, invoicing	Billing contact, company, VAT number, payment status; card data collected directly by Stripe
Sentry	Functional Software, Inc. d/b/a Sentry — United States	Error and performance monitoring	Error traces, technical metadata, sanitized context
Amplitude	Amplitude, Inc. — United States	Product analytics (consent-gated)	Pseudonymous identifiers, event data, truncated IP
Cal.com	Cal.com, Inc. — United States	Demo and appointment scheduling (GSS-controller activity; listed for completeness)	Name, e-mail, booking details
DuckDuckGo	Duck Duck Go, Inc. — United States	Discovery of source material	Search queries derived from keywords

III.4 Client-enabled integrations

Where the Client registers a Channel or other delivery target operated by a third party, Articles and the Personal Data they contain flow to that system on the Client's instruction. That provider acts under the Client's own agreement with it and is not a Sub-processor of GSS; GSS Processes only the credentials necessary to operate the connection.

Annex IV — Joint-controller arrangement (Art. 26 GDPR)

IV.1 Scope

This Annex applies to the Processing activity in which the Parties jointly determine the purposes and means: **the editorial approval and delivery of an Article that contains Personal Data, and the subsequent coordinated handling of Data Subject requests, corrections and takedowns in respect of that Article.**

It does not apply to GSS's own generation pipeline (GSS acts as independent Controller), or to the Client's publication decisions on its own Channels beyond the coordination duties below (the Client acts as Controller).

IV.2 Allocation of responsibilities

Obligation	Responsible Party
Determining that an Article meets editorial and compliance standards before delivery	GSS
Determining whether, when and where to publish a delivered Article	Client
Providing information to Data Subjects under Art. 13–14 GDPR in respect of the generation pipeline	GSS, via its Privacy Policy
Providing information to readers and subscribers of the Client's Channels	Client, via its own privacy notice
Machine-readable marking of generated output (Art. 50(2))	GSS
Disclosure to end readers (Art. 50(4))	Client
Supplying origin and authorship metadata enabling that labelling	GSS
Receiving and logging a Data Subject request concerning an Article	Either Party; the receiving Party informs the other without undue delay
Assessing a request against a documented balancing of interests	GSS, in consultation with the Client
Executing removal, anonymization or correction on the Client's Channels within 72 hours	Client
Executing removal in GSS's own systems, clearing caches and preventing redelivery	GSS
Notifying a Supervisory Authority or Data Subjects of a Personal Data Breach concerning the joint activity	The Party in whose systems the breach originated, with the other Party's cooperation
Maintaining a record of the joint Processing activity	Each Party for its own record
Security of its own systems	Each Party

IV.3 Point of contact for Data Subjects

Data Subjects may address requests concerning an Article to info@newsintel.eu or support@newsintel.eu, or to the Client at the address published on the Client's Channels. Whichever Party receives the request:

- acknowledges it without undue delay;
- informs the other Party without undue delay;
- cooperates so that a substantive response is given within one month of receipt, extendable by two further months for complex requests, with the Data Subject informed of any extension.

Neither Party shall unilaterally reject a request concerning an Article without consulting the other. Regardless of this allocation, a Data Subject may exercise their rights against either Party (Art. 26(3) GDPR).

IV.4 Essence of the arrangement

The essence of this Annex is made available to Data Subjects through Section 8 of the GSS Privacy Policy and through the corresponding section of the Client's own privacy notice. **Annex V** contains the text the Client may use for that purpose.

IV.5 Allocation of liability between the Parties

Each Party bears the consequences of its own non-compliance. Where compensation is paid to a Data Subject by one Party, DPA §12.3 applies.

Annex V — Publishable summary of the joint-controller arrangement

The Client may reproduce the text below in its own privacy notice, adapted to its own house style. It is drafted to be read by a data subject rather than by a lawyer.

News content on this website

Some of the news articles on this website are produced for us by Global Staffing Support B.V. (“NewsIntel”), a Dutch company, using artificial intelligence. Every article is reviewed and approved by a human editor at NewsIntel before we receive it, and we then decide whether and where to publish it.

Where an article mentions a person, we and NewsIntel share responsibility for the approval and delivery of that article. NewsIntel is responsible for assessing whether an article meets its editorial and compliance standards, and for the systems that produce it. We are responsible for deciding to publish it, for how it appears on this website and in our newsletter, and for labelling it as AI-generated content.

If an article concerns you. You can contact either of us, and you do not have to contact both. Write to us at info@newsintel.eu or to support@newsintel.eu. Whoever receives your request will tell the other, and we will respond within one month — sooner where we can. If your request is justified, we will correct, anonymize or remove the article. E-mails we have already sent cannot be recalled, but we will remove the article from our online archive and from all future mailings.

You can also complain to a data-protection authority: in the Netherlands, the Autoriteit Persoonsgegevens, or the authority in your own country.