

Data Processing Agreement

One complete instrument: the selected Commission Article 28 clauses, Legiscope’s completed annexes and the supplementary terms that govern Customer Personal Data.

Status	DRAFT
Version	2026-09-02
Last reviewed	2 SEPTEMBER 2026
Accountable owner	PRIVACY AND LEGAL

PUBLICATION NOTE

This page is the canonical published DPA. When an Order Form is accepted, the DPA as published at acceptance automatically forms part of the Agreement whenever Legiscope processes Customer Personal Data. No separate DPA signature is required. Publication alone does not create acceptance.

OFFICIAL COMMISSION
SOURCE

Commission Implementing Decision (EU) 2021/915



01

Contract formation and selections

The Customer and Legiscope UAB (Parties) agree to the present Standard Contractual Clauses in the Annex to Commission Implementing Decision (EU) 2021/915 of 4 June 2021 under Article 28(7) GDPR (Commission Clauses), reproduced verbatim below, and to the Supplementary contractual terms that follow them. The applicable GDPR selections are highlighted, and the non-applicable alternatives and the non-retained optional clause are shown struck through.

The Customer’s role is determined by the relevant processing: Legiscope acts as processor where the Customer is controller, and as sub-processor where the Customer processes personal data on behalf of another controller. In the latter case, this DPA also constitutes the Parties’ sub-processing agreement under Article 28(4) and (6) GDPR. Option 1 in Clause 1(a), Article 28(3) and (4) GDPR, is selected. Clause 5, the optional docking clause, is not retained. Option 2 in Clause 7.7(a), general written authorisation, is selected with a 30-calendar-day notice period. The GDPR options in Clauses 8 and 9 are selected.

This DPA is published at www.legiscope.com/dpa.html as one complete canonical instrument. When an accepted Order Form applies, the DPA as published at acceptance automatically forms part of the Agreement; no separate DPA signature is required. The customer identity, role, service scope, effective date and any service-specific processing details stated in the Order Form complete Annexes I and II. A professional service is processed under this DPA; the Order Form records its particulars or any deviation before the engagement begins.

[COMMISSION DECISION \(EU\) 2021/915](#) [CURRENT SUBPROCESSOR REGISTER](#)

02

SECTION I – OBLIGATIONS OF THE PARTIES

EU

OFFICIAL COMMISSION TEXT • SELECTIONS OPEN

DECISION (EU) 2021/915 • ANNEX • SECTION I ↗

CLAUSE 1

Purpose and scope

- (a) The purpose of these Standard Contractual Clauses (the Clauses) is to ensure compliance with **OPTION 1:** Article 28(3) and (4) of 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) / [**OPTION 2:** Article 29(3) and (4) of Regulation (EU) 2018/1725 of the European Parliament and of the Council of 23 October 2018 on the protection of natural persons with regard to the processing of personal data by the Union institutions, bodies, offices and agencies and on the free movement of such data, and repealing Regulation (EC) No 45/2001 and Decision No 1247/2002/EC].
- (b) The controllers and processors listed in Annex I have agreed to these Clauses in order to ensure compliance with Article 28(3) and (4) of Regulation (EU) 2016/679 and/or Article 29(3) and (4) of Regulation (EU) 2018/1725.
- (c) These Clauses apply to the processing of personal data as specified in Annex II.
- (d) Annexes I to IV are an integral part of the Clauses.
- (e) These Clauses are without prejudice to obligations to which the controller is subject by virtue of Regulation (EU) 2016/679 and/or Regulation (EU) 2018/1725.
- (f) These Clauses do not by themselves ensure compliance with obligations related to international transfers in accordance with Chapter V of Regulation (EU) 2016/679 and/or Regulation (EU) 2018/1725.

CLAUSE 2

Invariability of the Clauses

- (a) The Parties undertake not to modify the Clauses, except for adding information to the Annexes or updating information in them.
- (b) This does not prevent the Parties from including the standard contractual clauses laid down in these Clauses in a broader contract, or from adding other clauses or additional safeguards provided that they do not directly or indirectly contradict the Clauses or detract from the fundamental rights or freedoms of data subjects.

CLAUSE 3

Interpretation

- (a) Where these Clauses use the terms defined in Regulation (EU) 2016/679 or Regulation (EU) 2018/1725 respectively, those terms shall have the same meaning as in that Regulation.
- (b) These Clauses shall be read and interpreted in the light of the provisions of Regulation (EU) 2016/679 or Regulation (EU) 2018/1725 respectively.
- (c) These Clauses shall not be interpreted in a way that runs counter to the rights and obligations provided for in Regulation (EU) 2016/679 / Regulation (EU) 2018/1725 or in a way that prejudices the fundamental rights or freedoms of the data subjects.

CLAUSE 4

Hierarchy

In the event of a contradiction between these Clauses and the provisions of related agreements between the Parties existing at the time when these Clauses are agreed or entered into thereafter, these Clauses shall prevail.

~~CLAUSE 5~~
~~OPTIONAL~~

~~Docking clause~~

- ~~(a) Any entity that is not a Party to these Clauses may, with the agreement of all the Parties, accede to these Clauses at any time as a controller or a processor by completing the Annexes and signing Annex I.~~
- ~~(b) Once the Annexes in (a) are completed and signed, the acceding entity shall be treated as a Party to these Clauses and have the rights and obligations of a controller or a processor, in accordance with its designation in Annex I.~~
- ~~(c) The acceding entity shall have no rights or obligations resulting from these Clauses from the period prior to becoming a Party.~~

03

SECTION II — OBLIGATIONS OF THE PARTIES



OFFICIAL COMMISSION TEXT • SELECTIONS OPEN

DECISION (EU) 2021/915 • ANNEX • SECTION II ➤

Description of processing(s)

The details of the processing operations, in particular the categories of personal data and the purposes of processing for which the personal data is processed on behalf of the controller, are specified in Annex II.

Obligations of the Parties

7.1 Instructions

- (a) The processor shall process personal data only on documented instructions from the controller, unless required to do so by Union or Member State law to which the processor is subject. In this case, the processor shall inform the controller of that legal requirement before processing, unless the law prohibits this on important grounds of public interest. Subsequent instructions may also be given by the controller throughout the duration of the processing of personal data. These instructions shall always be documented.
- (b) The processor shall immediately inform the controller if, in the processor's opinion, instructions given by the controller infringe Regulation (EU) 2016/679 / Regulation (EU) 2018/1725 or the applicable Union or Member State data protection provisions.

7.2 Purpose limitation

The processor shall process the personal data only for the specific purpose(s) of the processing, as set out in Annex II, unless it receives further instructions from the controller.

7.3 Duration of the processing of personal data

Processing by the processor shall only take place for the duration specified in Annex II.

7.4 Security of processing

- (a) The processor shall at least implement the technical and organisational measures specified in Annex III to ensure the security of the personal data. This includes protecting the data against a breach of security leading to accidental or unlawful destruction, loss, alteration, unauthorised disclosure or access to the data (personal data breach). In assessing the appropriate level of security, the Parties shall take due account of the state of the art, the costs of implementation, the nature, scope, context and purposes of processing and the risks involved for the data subjects.

- (b) The processor shall grant access to the personal data undergoing processing to members of its personnel only to the extent strictly necessary for implementing, managing and monitoring of the contract. The processor shall ensure that persons authorised to process the personal data received have committed themselves to confidentiality or are under an appropriate statutory obligation of confidentiality.

7.5 Sensitive data

If the processing involves personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade union membership, genetic data or biometric data for the purpose of uniquely identifying a natural person, data concerning health or a person's sex life or sexual orientation, or data relating to criminal convictions and offences ("sensitive data"), the processor shall apply specific restrictions and/or additional safeguards.

7.6 Documentation and compliance

- (a) The Parties shall be able to demonstrate compliance with these Clauses.
- (b) The processor shall deal promptly and adequately with inquiries from the controller about the processing of data in accordance with these Clauses.
- (c) The processor shall make available to the controller all information necessary to demonstrate compliance with the obligations that are set out in these Clauses and stem directly from Regulation (EU) 2016/679 and/or Regulation (EU) 2018/1725. At the controller's request, the processor shall also permit and contribute to audits of the processing activities covered by these Clauses, at reasonable intervals or if there are indications of non-compliance. In deciding on a review or an audit, the controller may take into account relevant certifications held by the processor.
- (d) The controller may choose to conduct the audit by itself or mandate an independent auditor. Audits may also include inspections at the premises or physical facilities of the processor and shall, where appropriate, be carried out with reasonable notice.
- (e) The Parties shall make the information referred to in this Clause, including the results of any audits, available to the competent supervisory authority/ies on request.

7.7 Use of sub-processors

- (a) **OPTION 1: PRIOR SPECIFIC AUTHORISATION:** ~~The processor shall not subcontract any of its processing operations performed on behalf of the controller in accordance with these Clauses to a sub-processor, without the controller's prior specific written authorisation. The processor shall submit the request for specific authorisation at least [SPECIFY TIME PERIOD] prior to the engagement of the sub-processor in question, together with the information necessary to enable the controller to decide on the authorisation. The list of sub-processors authorised by the controller can be found in Annex IV. The Parties shall keep Annex IV up to date.~~

OPTION 2: GENERAL WRITTEN AUTHORISATION: The processor has the controller's general authorisation for the engagement of sub-processors from an agreed list. The processor shall specifically inform in writing the controller of any intended changes of that list through the addition or replacement of sub-processors at least 30 calendar days in advance, thereby giving the controller sufficient time to be able to object to such changes prior to the engagement of the concerned sub-processor(s). The processor shall provide the controller with the information necessary to enable the controller to exercise the right to object.

- (b) Where the processor engages a sub-processor for carrying out specific processing activities (on behalf of the controller), it shall do so by way of a contract which imposes on the sub-processor, in substance, the same data protection obligations as the ones imposed on the data processor in accordance with these Clauses. The processor shall ensure that the sub-processor complies with the obligations to which the processor is subject pursuant to these Clauses and to Regulation (EU) 2016/679 and/or Regulation (EU) 2018/1725.
- (c) At the controller's request, the processor shall provide a copy of such a sub-processor agreement and any subsequent amendments to the controller. To the extent necessary to protect business secret or other confidential information, including personal data, the processor may redact the text of the agreement prior to sharing the copy.
- (d) The processor shall remain fully responsible to the controller for the performance of the sub-processor's obligations in accordance with its contract with the processor. The processor shall notify the controller of any failure by the sub-processor to fulfil its contractual obligations.
- (e) The processor shall agree a third party beneficiary clause with the sub-processor whereby - in the event the processor has factually disappeared, ceased to exist in law or has become insolvent - the controller shall have the right to terminate the sub-processor contract and to instruct the sub-processor to erase or return the personal data.

7.8 International transfers

- (a) Any transfer of data to a third country or an international organisation by the processor shall be done only on the basis of documented instructions from the controller or in order to fulfil a specific requirement under Union or Member State law to which the processor is subject and shall take place in compliance with Chapter V of Regulation (EU) 2016/679 or Regulation (EU) 2018/1725.
- (b) The controller agrees that where the processor engages a sub-processor in accordance with Clause 7.7. for carrying out specific processing activities (on behalf of the controller) and those processing activities involve a transfer of personal data within the meaning of Chapter V of Regulation (EU) 2016/679, the processor and the sub-processor can ensure compliance with Chapter V of Regulation (EU) 2016/679 by using standard contractual clauses adopted by the Commission in accordance with of Article 46(2) of Regulation (EU) 2016/679, provided the conditions for the use of those standard contractual clauses are met.

Assistance to the controller

- (a) The processor shall promptly notify the controller of any request it has received from the data subject. It shall not respond to the request itself, unless authorised to do so by the controller.
- (b) The processor shall assist the controller in fulfilling its obligations to respond to data subjects' requests to exercise their rights, taking into account the nature of the processing. In fulfilling its obligations in accordance with (a) and (b), the processor shall comply with the controller's instructions
- (c) In addition to the processor's obligation to assist the controller pursuant to Clause 8(b), the processor shall furthermore assist the controller in ensuring compliance with the following obligations, taking into account the nature of the data processing and the information available to the processor:
 - (1) the obligation to carry out an assessment of the impact of the envisaged processing operations on the protection of personal data (a 'data protection impact assessment') where a type of processing is likely to result in a high risk to the rights and freedoms of natural persons;
 - (2) the obligation to consult the competent supervisory authority/ies prior to processing where a data protection impact assessment indicates that the processing would result in a high risk in the absence of measures taken by the controller to mitigate the risk;
 - (3) the obligation to ensure that personal data is accurate and up to date, by informing the controller without delay if the processor becomes aware that the personal data it is processing is inaccurate or has become outdated;
 - (4) the obligations in **[OPTION 1]** Article 32 of Regulation (EU) 2016/679/ **[OPTION 2]** ~~Articles 33 and 36 to 38 of Regulation (EU) 2018/1725.~~
- (d) The Parties shall set out in Annex III the appropriate technical and organisational measures by which the processor is required to assist the controller in the application of this Clause as well as the scope and the extent of the assistance required.

Notification of personal data breach

In the event of a personal data breach, the processor shall cooperate with and assist the controller for the controller to comply with its obligations under Articles 33 and 34 of Regulation (EU) 2016/679 or under Articles 34 and 35 of Regulation (EU) 2018/1725, where applicable, taking into account the nature of processing and the information available to the processor.

9.1 Data breach concerning data processed by the controller

In the event of a personal data breach concerning data processed by the controller, the processor shall assist the controller:

- (a) in notifying the personal data breach to the competent supervisory authority/ies, without undue delay after the controller has become aware of it, where relevant/(unless the personal data breach is unlikely to result in a risk to the rights and freedoms of natural persons);
- (b) in obtaining the following information which, pursuant to **[OPTION 1]** Article 33(3) of Regulation (EU) 2016/679/ **[OPTION 2]** ~~Article 34(3) of Regulation (EU) 2018/1725~~, shall be stated in the controller's notification, and must at least include:
 - (1) the nature of the personal data including where possible, the categories and approximate number of data subjects concerned and the categories and approximate number of personal data records concerned;
 - (2) the likely consequences of the personal data breach;
 - (3) the measures taken or proposed to be taken by the controller to address the personal data breach, including, where appropriate, measures to mitigate its possible adverse effects.

Where, and insofar as, it is not possible to provide all this information at the same time, the initial notification shall contain the information then available and further information shall, as it becomes available, subsequently be provided without undue delay.

- (c) in complying, pursuant to **[OPTION 1]** Article 34 of Regulation (EU) 2016/679 / **[OPTION 2]** ~~Article 35 of Regulation (EU) 2018/1725~~, with the obligation to communicate without undue delay the personal data breach to the data subject, when the personal data breach is likely to result in a high risk to the rights and freedoms of natural persons.

9.2 Data breach concerning data processed by the processor

In the event of a personal data breach concerning data processed by the processor, the processor shall notify the controller without undue delay after the processor having become aware of the breach. Such notification shall contain, at least:

- (a) a description of the nature of the breach (including, where possible, the categories and approximate number of data subjects and data records concerned);
- (b) the details of a contact point where more information concerning the personal data breach can be obtained;
- (c) its likely consequences and the measures taken or proposed to be taken to address the breach, including to mitigate its possible adverse effects.

Where, and insofar as, it is not possible to provide all this information at the same time, the initial notification shall contain the information then available and further information shall, as it becomes available, subsequently be provided without undue delay.

The Parties shall set out in Annex III all other elements to be provided by the processor when assisting the controller in the compliance with the controller's obligations under **[OPTION 1]** Articles 33 and 34 of Regulation (EU) 2016/679 / **[OPTION 2]** ~~Articles 34 and 35 of Regulation (EU) 2018/1725.~~

04

SECTION III — FINAL PROVISIONS



OFFICIAL COMMISSION TEXT • SELECTIONS OPEN

DECISION (EU) 2021/915 • ANNEX • SECTION III ↗

CLAUSE 10

Non-compliance with the Clauses and termination

- (a) Without prejudice to any provisions of Regulation (EU) 2016/679 and/or Regulation (EU) 2018/1725, in the event that the processor is in breach of its obligations under these Clauses, the controller may instruct the processor to suspend the processing of personal data until the latter complies with these Clauses or the contract is terminated. The processor shall promptly inform the controller in case it is unable to comply with these Clauses, for whatever reason.
- (b) The controller shall be entitled to terminate the contract insofar as it concerns processing of personal data in accordance with these Clauses if:
 - (1) the processing of personal data by the processor has been suspended by the controller pursuant to point (a) and if compliance with these Clauses is not restored within a reasonable time and in any event within one month following suspension;
 - (2) the processor is in substantial or persistent breach of these Clauses or its obligations under Regulation (EU) 2016/679 and/or Regulation (EU) 2018/1725;
 - (3) the processor fails to comply with a binding decision of a competent court or the competent supervisory authority/ies regarding its obligations pursuant to these Clauses or to Regulation (EU) 2016/679 and/or Regulation (EU) 2018/1725.
- (c) The processor shall be entitled to terminate the contract insofar as it concerns processing of personal data under these Clauses where, after having informed the controller that its instructions infringe applicable legal requirements in accordance with Clause 7.1 (b), the controller insists on compliance with the instructions.
- (d) Following termination of the contract, the processor shall, at the choice of the controller, delete all personal data processed on behalf of the controller and certify to the controller that it has done so, or, return all the personal data to the controller and delete existing copies unless Union or Member

State law requires storage of the personal data. Until the data is deleted or returned, the processor shall continue to ensure compliance with these Clauses.

05

Annex I – List of parties

COMPLETED SCHEDULE

- **Controller party:** The Customer identified in the accepted Order Form, for processing for which it acts as controller. Its identity, address, privacy or DPO contact and authorised signatory are the corresponding particulars recorded in that Order Form.
- **Processor parties:** Legiscope UAB, company code 304581221, Laisvės pr. 60-1107, LT-05120 Vilnius, Lithuania. Privacy contact: contact@legiscope.com. Activities relevant to the data: provision, security, support and administration of the purchased Legiscope Service. Where the Customer acts as processor, the Customer identified in the accepted Order Form is also a contracting processor, with the identity and contact particulars recorded there, and Legiscope acts as its sub-processor.
- **Contracting capacity:** The Customer contracts in its own name. Its upstream controllers are not Parties to this DPA. Customer acceptance does not constitute acceptance in an upstream controller's name.
- **Signature and date:** The effective date and acceptance evidence recorded in the applicable Order Form. No separate signature on this Annex is required.

06

Annex II – Description of processing

COMPLETED SCHEDULE

Every processing activity under this DPA is performed by Legiscope as processor or, where the Customer acts for another controller, as sub-processor; Legiscope does operate independent-controller activities that are outside this DPA and are described separately in the Terms.

- **Subject matter:** Processing Customer Personal Data to provide, operate, secure, support and administer the Legiscope Service and professional services selected in the applicable Order Form, in accordance with the Customer's documented instructions and configuration.
- **Categories of data subjects:** Customer personnel and authorised users; the Customer's clients, suppliers, processors, sub-processors and business contacts; applicants, employees, contractors, complainants and data-rights requesters; persons described in processing activities, DPIAs, transfer assessments, incidents, audits, evidence or other Customer compliance records; and other individuals whose personal data the Customer lawfully submits.
- **Categories of personal data:** identity, contact, account and professional details; employment and organisational information; online and technical identifiers; access, role and activity information; correspondence; contractual and supplier information; data-rights and complaint information; incident and security information; processing, retention, recipient and transfer information; uploaded documents, evidence, prompts and customer-specific generated output; and any other category deliberately included by the Customer within purchased scope.

- Sensitive data and safeguards: The Service is not designed for unrestricted processing of underlying identifiable special-category or criminal-conviction data. Whether particular data may be processed lawfully and appropriately depends on the data category, purpose, jurisdiction, provider service and route, configuration, contractual terms, scale and safeguards. Health, genetic, biometric and similarly regulated data may be subject to sector- or country-specific rules that do not apply in the same way to other categories, such as trade-union membership. Before submitting such data, the Customer must determine that the use is lawful, necessary, proportionate and compatible with the selected workflow and provider route, minimise the data and use non-identifying descriptions where sufficient. For example, AWS or an AI provider may be suitable for a particular category and use in one jurisdiction but not another. Legiscope has not assessed the Customer's sector- or country-specific requirements and does not represent that the standard Service or every provider route satisfies them.
- Nature of processing: collect, receive, host, store, organise, retrieve, consult, display, transmit, structure, compare, analyse, generate customer-specific output, export, secure, back up, support and delete Customer Personal Data solely to provide the instructed Service.
- Purpose: provide, secure, support and administer the hosted Legiscope privacy and compliance platform, its purchased modules, organisations, integrations and professional services as identified in the Order Form and documented Customer instructions.
- Duration of the processing: the Agreement term; the post-termination retention-for-restorability period of up to 12 months described in the supplementary terms; active-system deletion without undue delay on the applicable instruction or election; and the backup retention and deletion process described under "Backups" in the supplementary terms. Independent-controller records are outside this DPA.
- Frequency: continuous hosting and security processing during the term; user-initiated or scheduled processing when an authorised workflow, integration, support action, provider operation or export is performed.
- Sub-processor processing: each authorised sub-processor's subject matter, purpose, data scope, processing context and transfer basis are identified in Annex IV.

07

Annex III – Technical and organisational measures

COMPLETED SCHEDULE

These measures apply according to the processing in scope. The current public Security record supplies the concrete control descriptions and evidence boundaries referenced by this Annex; it does not replace the contractual measures below.

- Pseudonymisation and minimisation: tenant and record identifiers rather than customer names address primary records, storage prefixes and security events; uploaded filenames are normalised; provider inputs are limited to the material required for an authorised operation.
- Encryption and transmission: customer-facing endpoints use HTTPS/TLS; production database tables and private customer object storage use AWS server-side encryption at rest; storage policies reject insecure transport and public access is blocked.

- Identity and authorisation: authenticated individual accounts, role-based permissions, tenant-scoped record and object access, administrative access controls, TOTP MFA capability and periodic personnel access review.
- Confidentiality, integrity and tenant isolation: authorised personnel are bound by confidentiality; point reads and list queries enforce the authenticated account boundary; allow-listed fields, typed validation and conditional writes protect integrity.
- Availability and recovery: monitored managed infrastructure, point-in-time and versioned recovery controls, encrypted private recovery copies in a geographically separate EU region, documented restoration procedures and protected recovery retention.
- Logging and detection: privacy-controlled application diagnostics, security events, managed service logs and distributed traces; relevant identifiers are pseudonymised or omitted; access to logging systems is restricted and incidents follow documented triage and escalation.
- Development and change: separated development, pre-production and production paths; source control, reviewed changes, automated packaging, dependency and vulnerability management, source-bound release evidence and MFA-protected production approval.
- Assistance and effectiveness: controlled export and deletion procedures, incident investigation, data-subject-request assistance, DPIA and prior-consultation support, periodic control review and proportionate audit cooperation.
- Return and erasure: active-system deletion without undue delay following the applicable instruction; encrypted, access-restricted disaster-recovery copies subject to the scheduled expiry and subsequent deletion process stated under “Backups” in the supplementary terms; restored copies have recorded deletion instructions re-applied before ordinary use.

[DETAILED ARTICLE 32 SECURITY RECORD➔](#)

08

Annex IV — List of sub-processors COMPLETED SCHEDULE

The Customer gives general written authorisation for the sub-processors below to the extent they apply to the purchased Service. The register below, as published at acceptance, forms the agreed list for that Order and identifies each sub-processor’s contracting entity and transfer basis. The current online register is maintained at <https://www.legiscope.com/subprocessors.html>.

The listed AI providers are each authorised for any AI-assisted operation of the purchased Service; Legiscope determines the provider or providers used for ai operations according to capability, performance, cost, security and risk profile. A provider not on the agreed list is engaged only through the Clause 7.7(a) change process.

A provider used solely for Legiscope’s independent-controller contracting, billing or business-communication activity is not an Annex IV sub-processor unless it also processes Customer Personal Data on the Customer’s behalf.

AWS · EU APPLICATION CLOUD INFRASTRUCTURE

CORE PROVIDER

Amazon Web Services

CONTRACTING ENTITY	Amazon Web Services EMEA SARL, 38 avenue John F. Kennedy, L-1855 Luxembourg, Grand Duchy of Luxembourg — the AWS contracting entity for the EU-hosted services.
PURPOSE	EU application hosting, identity, storage, security, recovery and supporting infrastructure.
DATA IN SCOPE	Customer Content, account and authentication data, service records, uploaded files, job data, and proportionate security and diagnostic metadata.
PROCESSING CONTEXT	The primary customer application is hosted in the European Union (Ireland), with a protected customer-object recovery copy in France. The applicable AWS DPA includes transfer safeguards for restricted transfers.
TRANSFER BASIS	Standard processing is EEA-only (Ireland, with recovery in France) and involves no restricted transfer. A residual restricted transfer — such as non-EEA support access — is covered by the EU Standard Contractual Clauses (Commission Decision (EU) 2021/914, processor-to-processor module) incorporated in the AWS Data Processing Addendum and by Amazon Web Services, Inc.’s certification under the EU–US Data Privacy Framework.

[AWS DPA OVERVIEW](#)

[AWS SERVICE TERMS](#)

COMMERCIAL API · AI-ASSISTED PROCESSING		AI PROVIDER
OpenAI		
CONTRACTING ENTITY	OpenAI Ireland Ltd, 1st Floor, The Liffey Trust Centre, 117–126 Sheriff Street Upper, Dublin 1, D01 YC43, Ireland — the API contracting entity for EEA-based customers under the OpenAI data processing addendum.	
PURPOSE	One selectable commercial API route for user-invoked AI-assisted operations.	
DATA IN SCOPE	When selected: minimum source material or Customer Content, task instructions, workflow context and generated output required for the invoked operation.	

PROCESSING CONTEXT	Legiscope uses OpenAI through commercial API routes. Model selection may vary by task and configuration. For Customer Content, Legiscope enables only a contracted route under which inputs and outputs are not used to train, fine-tune or improve a general-purpose or cross-customer model. Processing and retention follow the contracted API service, DPA and enabled controls; processing may involve the United States.
TRANSFER BASIS	Legiscope contracts with OpenAI Ireland Ltd. Processing may involve OpenAI's United States entities as a restricted transfer, covered by the EU Standard Contractual Clauses (Commission Decision (EU) 2021/914, processor-to-processor module) incorporated in the OpenAI Data Processing Addendum and, where held by the importing entity, its certification under the EU-US Data Privacy Framework.
OPENAI DATA PROCESSING ADDENDUM ENTERPRISE PRIVACY	

COMMERCIAL API · AI-ASSISTED PROCESSING		AI PROVIDER
Anthropic		
CONTRACTING ENTITY	Anthropic Ireland, Limited, 6th Floor, South Bank House, Barrow Street, Dublin 4, Ireland — the commercial API contracting entity for EEA-based customers under the Anthropic data processing addendum.	
PURPOSE	One selectable commercial API route for user-invoked AI-assisted operations.	
DATA IN SCOPE	When selected: minimum source material or Customer Content, task instructions, workflow context and generated output required for the invoked operation.	
PROCESSING CONTEXT	Legiscope uses Anthropic as a commercial AI provider and may route a bounded operation to an Anthropic model. For Customer Content, Legiscope enables only a contracted route under which inputs and outputs are not used to train, fine-tune or improve a general-purpose or cross-customer model; the applicable DPA governs commercial processing and transfers.	
TRANSFER BASIS	Legiscope contracts with Anthropic Ireland, Limited. Processing may involve Anthropic’s United States entities as a restricted transfer, covered by the EU Standard Contractual Clauses (Commission Decision (EU) 2021/914, processor-to-processor module) incorporated in the Anthropic Data Processing Addendum and, where held by the importing entity, its certification under the EU–US Data Privacy Framework.	
ANTHROPIC DPA INFORMATION↗ COMMERCIAL PROCESSING ROLE↗		

Google Gemini

CONTRACTING ENTITY	Google Ireland Limited, Gordon House, Barrow Street, Dublin 4, Ireland — the provider of the Gemini API paid services to customers based in the EEA.
PURPOSE	One selectable paid commercial API route for user-invoked AI-assisted operations.
DATA IN SCOPE	When selected: minimum source material or Customer Content, task instructions, workflow context and generated output required for the invoked operation.
PROCESSING CONTEXT	Legiscope uses Google Gemini as a commercial AI provider and may route a bounded operation to a Gemini model. For Customer Content, Legiscope enables only a paid contracted route under which inputs and outputs are not used to train, fine-tune or improve a general-purpose or cross-customer model. Global processing and limited abuse-monitoring logs are governed by the applicable terms and DPA.
TRANSFER BASIS	Legiscope contracts with Google Ireland Limited. The paid Gemini API involves global processing as a restricted transfer, covered by the EU Standard Contractual Clauses (Commission Decision (EU) 2021/914, processor-to-processor module) incorporated in the applicable Google data-processing terms and by Google LLC’s certification under the EU-US Data Privacy Framework.

[GEMINI API TERMS↗](#) [GEMINI DATA-USE CONTROLS↗](#)

SECTION IV — SUPPLEMENTARY CONTRACTUAL TERMS

The provisions that follow supplement the Commission Clauses and the completed Annexes with Service-specific rules for consultancies and DPO services, sub-processor changes and objections, audits, assistance, personal data breaches, deletion and restorability, backups, and public-authority access requests. They must be read together with the Commission Clauses and do not replace, restrict or override them; if a supplementary term conflicts with the Commission Clauses, the Commission Clauses prevail.

Consultancies and DPO services

- (a) Where the Customer acts as processor for a client, that client is the controller referred to in the Commission Clauses, and Legiscope is the sub-processor. Under this DPA, Legiscope also agrees directly with the Customer to comply with the processor obligations in those Clauses for that processing. The Customer may enforce these obligations directly against Legiscope under this sub-processing agreement, made pursuant to Article 28(4) and (6) GDPR. The Commission Clauses remain unchanged and prevail over conflicting supplementary terms.
- (b) The Customer must have its client's documented instructions and all required authorisations and agreements, including under Clauses 7.7 and 7.8, before processing starts. It must promptly relay instructions, requests, decisions, notices, information and assistance between the client and Legiscope in time to meet deadlines and allow objections.
- (c) The Customer must ensure, before processing starts, that this DPA imposes the applicable data-protection obligations from its client contract under Article 28(4) GDPR. Additional obligations for Legiscope require its prior written agreement. The Customer remains responsible to its client under Article 28(4).
- (d) In cases Legiscope is legally required to identify the controllers for which it processes data — for example where a supervisory authority requires that information under Articles 30(4) or 58 GDPR - Legiscope may request the information from the Customer, or provide it directly from the programmes the Customer administers in its tenant as the identification of the clients for which it acts.
- (e) Each client controller may enforce the controller rights in the Commission Clauses for its data as an intended third-party beneficiary. If the Customer disappears, ceases to exist legally or becomes insolvent, the client may terminate the affected sub-processing and require Legiscope to return or erase its data.

Sub-processor changes and objections

- (a) Legiscope gives the written notice required by Clause 7.7(a) by email to the Customer's contract or privacy contact recorded in the Order Form, and records the change in a dated update to the register at www.legiscope.com/subprocessors.html.
- (b) The notice identifies the intended sub-processor, its service and purpose, the categories of data concerned, the processing locations and transfer mechanism, and the intended effective date.
- (c) If the Customer objects to an intended sub-processor change on reasonable documented data-protection grounds during the Clause 7.7(a) notice period, the Parties will work in good faith on a commercially reasonable alternative.

- (d) If none is available, the Customer may stop using the affected feature or terminate the affected Service and receive a pro-rata refund of prepaid unused fees for it.

CLAUSE 13

Audits and compliance information

- (a) Legiscope documents its security and compliance posture publicly and in detail: the technical and organisational measures protecting the Service, with the related policies and control descriptions, at www.legiscope.com/security.html; the subprocessor register at www.legiscope.com/subprocessors.html; hosting, data-residency and transfer information at www.legiscope.com/hosting-residency-transfers.html; and the use of AI providers at www.legiscope.com/ai-usage.html.
- (b) This published record, together with written answers to targeted questions it does not already address, is Legiscope's standing compliance information under Clause 7.6 and is provided without charge.
- (c) In accordance with Article 28(3)(h) GDPR and Clause 7.6, Legiscope allows for and contributes to audits, including inspections, conducted by the Customer or another auditor mandated by the Customer.
- (d) The Parties organise each audit through a specific audit agreement, concluded in good faith and within reasonable time limits before the audit begins. The audit agreement defines the scope, timing, methods, auditor, confidentiality, results-sharing and conditions of the audit, together with the costs borne by the Customer, including the documented working time of Legiscope personnel.
- (e) The audit agreement may not be used to unreasonably delay or prevent an audit.

CLAUSE 14

Assistance to the Customer

- (a) The Service is the first level of assistance: its search, export, correction, deletion, register and evidence functions let the Customer answer most data-subject requests, assessments and authority enquiries directly.
- (b) Legiscope promptly forwards to the Customer any request it receives directly from a data subject or a supervisory authority concerning Customer Personal Data, unless prohibited by law.
- (c) Assistance under Clauses 8 and 9 that cannot be self-served is requested through the published support channel, stating the affected records, the right or request concerned, the action requested and the applicable deadline.
- (d) Legiscope responds under the support terms of the purchased Plan, and in time for the Customer's statutory deadline where one reasonably applies.

- (e) Work beyond that assistance — analysis, drafting or any bespoke engagement — is a professional service recorded in the Order Form.

CLAUSE 15

Personal data breaches

- (a) Legiscope notifies the Customer of a personal data breach affecting Customer Personal Data under Clause 9.2 by email to the privacy or security contact recorded in the Order Form, without undue delay and, where feasible, within 48 hours of becoming aware of the breach.
- (b) For a suspected event likely to have a high impact, Legiscope sends an early holding notice where waiting for confirmation could impair the Customer's own 72-hour assessment under Article 33 GDPR.
- (c) A notification is not an admission of fault or liability.

CLAUSE 16

Deletion and restorability

- (a) When the Agreement expires or terminates, the Customer chooses, in accordance with Clause 10(d), between return of its data, erasure, or retention for restorability. Absent an election, and if available - retention for restorability applies as the Customer's standing instruction, so that the account and the work it contains are not lost while the role responsible for it might be vacant.
- (b) The Customer may change its election, request return or instruct erasure at any time, without restriction, charge or condition.
- (c) Retention for restorability is a courtesy service provided without additional charge: Legiscope keeps the account and Customer Personal Data in an access-disabled, restorable state for up to 12 months after the end of the Agreement, during which the Customer may reactivate the account and recover its data.
- (d) The retention for restorability service is available in limited quantities for Legiscope Customers and is not a guaranteed service: after the end of the applicable retrieval period, if allocated space for the service is not sufficient, Legiscope may delete the account and data at any time, and at its own discretion, in particular where the volume or cost of retention becomes significant. The service operates as a limited space pooled for Legiscope Customers. If the space is full, the service will not be available.
- (e) At the latest, the account and data are deleted automatically 12 months after the end of the Agreement, unless a legal obligation requires longer storage. This DPA continues to apply to retained data for as long as it is held.

Backups

- (a) As part of the Service, the Customer instructs Legiscope to maintain encrypted, access-restricted backups solely for disaster recovery. Copies held in retention-locked vaults cannot be altered or deleted, nor can their retention period be shortened, before scheduled expiry. Residual backup copies are scheduled to expire no later than 90 days after active-system deletion and are automatically deleted without undue delay following expiry.
- (b) A deletion instruction is executed on active systems without undue delay. Deletion of residual backup copies completes through their automatic deletion following expiry. If a backup is restored, recorded deletion instructions are re-applied before the restored data returns to ordinary use.

Public authority and third-country access requests

- (a) If Legiscope receives a request from a public authority — including a law-enforcement, national-security or other third-country authority — for access to Customer Personal Data, it promptly notifies the Customer and redirects the authority to the Customer, unless and only to the extent legally prohibited from doing so.
- (b) Before any disclosure, Legiscope reviews the legal validity of the request, including whether Article 48 GDPR and Chapter V permit it, and challenges or seeks to narrow a request that is overbroad, unlawful or in conflict with Union or Member State law, where reasonable grounds exist.
- (c) Legiscope discloses only the minimum data legally required, documents each request and its handling, and informs the Customer of what was disclosed as soon as any prohibition on doing so is lifted.
- (d) A demand addressed to a sub-processor is handled under that sub-processor's data-processing terms and transparency commitments; Legiscope enforces the protections contractually available to it.