ARTICLE 28 · COMPLETE STANDARD FORM

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	CURRENT STANDARD DPA
Version	2026-08-26
Last reviewed	26 AUGUST 2026
Accountable owner	PRIVACY AND LEGAL

PUBLICATION NOTE

When an accepted Order Form or other Agreement identifies version 2026-08-26, this DPA automatically forms part of the Agreement whenever Legiscope processes Customer Personal Data. No separate DPA signature is required. Publication alone does not create acceptance.

Skip to content

01

Contract formation and selections

The Customer and Legiscope UAB (Parties) agree to the 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 in full below with the applicable GDPR selections completed and the non-applicable EUDPR alternatives omitted.

The Customer is the controller and Legiscope is the processor unless the Order Form states that the Customer acts as processor for another controller, in which case Legiscope is the sub-processor. Option 1 in Clause 1(a), Article 28(3) and (4) GDPR, is selected. Clause 5, the optional docking clause, is 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.

An Order Form or other Agreement accepted by authorised signatories automatically incorporates the DPA version it identifies. The customer identity, role, service scope, effective date and any service-specific processing details stated there complete Annexes I and II. No separate DPA signature is required. Each party receives or can reproduce the incorporated version, and the contract record retains its exact PDF and SHA-256 hash.

The Commission Clauses prevail over any conflicting supplementary term. This DPA prevails over the Terms of Service for processing Customer Personal Data, and an applicable Chapter V transfer instrument prevails for a restricted international transfer. This DPA does not itself provide a Chapter V transfer mechanism.

COMMISSION DECISION (EU) 2021/915↗ CURRENT SUBPROCESSOR REGISTER→

02

Section I — Commission clauses

EU COMMISSION TEXT · GDPR OPTIONS COMPLETED 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 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).

(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.

(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.

(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.

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, 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.

(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 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 — Commission clauses

EU COMMISSION TEXT · GDPR OPTIONS COMPLETED DECISION (EU) 2021/915 · ANNEX · SECTION II ↗

CLAUSE 6

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.

CLAUSE 7

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 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. 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 · general written authorisation

(a) 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.

(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.

(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.

CLAUSE 8

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 Article 32 of Regulation (EU) 2016/679.

(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.

CLAUSE 9

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, 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 Article 33(3) of Regulation (EU) 2016/679, 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 Article 34 of Regulation (EU) 2016/679, 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 Articles 33 and 34 of Regulation (EU) 2016/679.

04

Section III — Commission clauses

EU COMMISSION TEXT · GDPR OPTIONS COMPLETED

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, 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;
>
> (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.

(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: the Customer legal entity identified in the Order Form. Its registered address, registration information, privacy or DPO contact, role, authorised signatory and signature or accession date are the corresponding details recorded in the accepted Order Form or accession document. Activities relevant to the data: use and administration of the purchased Legiscope compliance workflows.
- Processor: Legiscope UAB, company code 304581221, Laisvės pr. 60-1107, LT-05120 Vilnius, Lithuania. Privacy contact: privacy@legiscope.com. Activities relevant to the data: provision, security, support and administration of the purchased Legiscope Service.
- Signature and accession date: the effective date and acceptance evidence recorded in the applicable Order Form or signed accession document. No separate signature on this Annex is required unless a party uses Clause 5 to accede after the Agreement takes effect.

06

Annex II — Description of processing

COMPLETED SCHEDULE

- 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 does not require special-category or criminal-conviction data by default. Where the Customer lawfully includes it, the Order Form identifies material or systematic categories and workflows. Applicable safeguards include strict purpose limitation, least-privilege role access, confidentiality, encryption in transit and at rest, access and security logging, onward-transfer restrictions, provider-input minimisation and competent human review of legally significant AI-assisted output.
- 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: the Agreement term, applicable Data Act transition and retrieval periods, active-system deletion without undue delay, and the bounded 90-day technically immutable backup cycle described 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 and processing context are identified in Annex IV and the service-specific snapshot incorporated into the Agreement.

Skip to content

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 and technically immutable disaster-recovery copies automatically purge no later than 90 days after active deletion; restored copies have recorded deletion instructions re-applied before ordinary use.

Skip to content

DETAILED ARTICLE 32 SECURITY RECORD→

Skip to content

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 service-specific snapshot of the Subprocessor Register incorporated on the effective date identifies the applicable contracting entity and forms the agreed list for that Order. The current online register is maintained at https://www.legiscope.com/subprocessors.html.

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.

- Amazon Web Services (AWS) — cloud infrastructure and transactional email. Processing: host, secure, back up, monitor and transmit Customer Personal Data and service records required for the application. Primary application processing is in AWS eu-west-1 (Ireland), with protected customer-object recovery in eu-west-3 (France); the incorporated snapshot identifies the applicable AWS contracting entity and any service-specific transfer context.
- OpenAI — commercial API, when selected for an authorised AI-assisted workflow. Processing: receive the minimum source material, Customer Content, task instructions and workflow context required to generate structured analysis, drafting or decision-support output. The incorporated snapshot records whether this provider is enabled and the applicable contracting and transfer position.
- Anthropic — commercial API, when selected for an authorised AI-assisted workflow. Processing: receive the minimum source material, Customer Content, task instructions and workflow context required to generate structured analysis, drafting or decision-support output. The incorporated snapshot records whether this provider is enabled and the applicable contracting and transfer position.
- Google Gemini — paid Gemini API services, when selected for an authorised AI-assisted workflow. Processing: receive the minimum source material, Customer Content, task instructions and workflow context required to generate structured analysis, drafting or decision-support output. The incorporated snapshot records whether this provider is enabled and the applicable Google contracting and transfer position.

REVIEW CURRENT SUB-PROCESSORS→

09

Supplementary terms — instructions and assistance

The Agreement, authorised user actions in the Service, support requests and documented configuration choices are the Customer's instructions. Legiscope may suspend affected processing while an instruction that it reasonably believes infringes applicable data-protection law is confirmed, modified or withdrawn.

Taking account of the nature of processing and information available, Legiscope will reasonably assist the Customer with data-subject requests, security obligations, breach notifications, DPIAs and prior consultation. The Customer remains responsible for decisions and communications legally assigned to it.

Legiscope will notify the Customer without undue delay after becoming aware of a personal data breach affecting Customer Personal Data and provide information available for the Customer's assessment and notifications. Notification is not an admission of fault or liability.

10

Supplementary terms — sub-processors and transfers

The Customer generally authorises the sub-processors in Annex IV. Legiscope will give at least 30 calendar days' advance written notice of an intended addition or replacement unless an emergency necessary to protect the Service or personal data makes shorter notice necessary.

The Customer may object during the notice period on reasonable documented data-protection grounds. The Parties will work in good faith on a commercially reasonable alternative. If none is available, the Customer may stop the affected feature or terminate the affected Service and receive a pro-rata refund of prepaid unused fees for it.

Legiscope remains responsible for each sub-processor's performance of the applicable data-protection obligations. Restricted transfers must use an applicable adequacy decision, the relevant module of Commission Implementing Decision (EU) 2021/914 or another lawful Chapter V mechanism, together with supplementary measures where required.

11

Supplementary terms — audits and confidentiality

Legiscope will make available information reasonably necessary to demonstrate compliance with the Commission Clauses, including appropriate control summaries and relevant independent assurance that it is lawfully permitted to share. Public trust material is not a substitute for information required by Clause 7.6.

The Customer may audit itself or through an independent auditor bound by confidentiality. Except after a material incident, on reasonable indications of non-compliance or where an authority requires otherwise, an audit will occur no more than once in 12 months, during business hours and on reasonable advance notice, and will avoid another customer's data and material security secrets. The Customer bears reasonable audit costs unless the audit identifies a material breach by Legiscope.

Personnel authorised to process Customer Personal Data are bound by confidentiality and receive instructions appropriate to their role. Nothing restricts mandatory supervisory-authority powers.

12

Supplementary terms — deletion and immutable backups

At the Customer's choice, Legiscope will return or delete Customer Personal Data after the relevant services end in accordance with Clause 10(d) and the Data Act exit process. Data selected for deletion is removed from active systems without undue delay and put beyond ordinary use.

Residual copies may remain only in encrypted, access-restricted and technically immutable rolling backups used solely for disaster recovery. They cannot be selectively altered during the protected cycle and are automatically purged no later than 90 days after active-system deletion. Until purge, the Commission Clauses protect those copies and Legiscope will not process them for another purpose.

Legiscope records each deletion instruction. If a backup is restored, Legiscope re-applies the instruction before the restored data returns to ordinary operation. On request, Legiscope will certify active-system deletion and, after the cycle expires, final backup purge. A legal retention requirement is documented and disclosed unless law prohibits disclosure.

13

Supplementary terms — liability and termination

Without prejudice to data-subject rights and supervisory-authority powers, liability between the Parties is governed by the Agreement's single global liability cap. Nothing relieves either Party of its own responsibilities under the GDPR.

The Customer may exercise the suspension and termination rights in Clause 10. Legiscope may terminate processing only as permitted by Clause 10(c) or other controlling law.

The governing law and jurisdiction stated in the Terms apply only to supplementary contractual matters. Mandatory data-protection law and the Commission Clauses remain controlling within their scope.