LONIA AI / PALLAS

Standard Contractual Clauses (Module Two)

Commission Implementing Decision (EU) 2021/914, controller to processor, with Appendix completed for Pallas

The EU Standard Contractual Clauses as adopted by the European Commission, with Module Two selected and the Appendix completed for transfers of personal data from the EEA, the United Kingdom, and Switzerland to Pallas by Lonia AI in the United States. Clauses 1 to 18 are reproduced from the Official Journal and are not modified. Annexes I, II, and III are ours.

Version. 1.0. Published 2026-08-30 by Lonia AI.

Jurisdictions addressed. European Union (GDPR Article 46(2)(c)), United Kingdom (UK GDPR, subject to the UK Addendum), Switzerland (revised FADP)

Every control claim in this document is rendered from the Pallas control inventory at src/data/control-inventory.ts, with its status, its evidence basis, and its disclosure text unaltered. Appendix A lists every control cited.

This render is informational; signable version issued on request. Request one at support@lonia.ai, giving your legal entity name and the jurisdiction of your establishment.

This document is provided for procurement and vendor-onboarding review. It is not legal advice, and both parties should have any contractual artifact reviewed by counsel before execution. Questions: support@lonia.ai

Contents

1. What this document is

This document is a completed pack of the European Union Standard Contractual Clauses. It has two parts, and the difference between them is the most important thing on this page.

Sections 4 and 5 are the Clauses themselves: the Annex to Commission Implementing Decision (EU) 2021/914 of 4 June 2021. That text is adopted law. Clause 2 of the Clauses provides that the parties undertake not to modify them. Nothing in this document modifies them, and the way this document is produced is designed so that nobody can. Clauses 1 to 18 and the twelve footnotes in section 4 are reproduced from https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=CELEX:32021D0914, retrieved 2026-09-06T02:08:35Z, extract SHA-256 19add20b38dba13bf5791627d9447c00d185e2ef655178a3d47ec614612e9ba3. They are not edited here and cannot be: they are read at build time from a stored reference file whose hash is recorded in this document's build manifest and checked by a release gate. Five characters outside printable ASCII were transliterated to their ASCII equivalents (no-break space to space, single quotation marks to the apostrophe, en dash to the hyphen, ellipsis to three full stops). No word, number, or clause reference differs from the Official Journal text.

Sections 6, 7, and 8 are the Appendix: Annex I, Annex II, and Annex III. The Appendix is the part the Clauses require the parties to complete, and it is the part that describes Pallas specifically. Every technical measure listed in Annex II is rendered from the Pallas control inventory with its implementation status and its disclosure text unaltered, so a measure that is partial says partial in the place a reviewer will read it.

Pallas by Lonia AI is the data importer. It processes personal data on behalf of its customers, who are the controllers, so Module Two (transfer controller to processor) is the applicable module and the one selected here. The other three modules are omitted from sections 4 and 5 rather than reproduced, which is how a completed pack is normally presented.

2. What this document does not do

No counsel has reviewed this pack. Lonia AI operates without a legal budget. Every part of this document that is not the Union's own text is either rendered from the control inventory or written by the operator. The selections recorded in section 3, including the choice of Ireland as the governing law and the forum, are the operator's selections and are subject to legal correction on request. If your counsel needs a different selection, that is a conversation to have before execution, and it is the reason the signable render is issued on request rather than published.

This pack is not a transfer impact assessment. Clause 14 requires the parties to warrant that they have no reason to believe the laws of the third country of destination prevent the importer from complying. Pallas publishes its own assessment supporting that warranty at /documents/pallas-tia.pdf. That document is the importer's input to the exporter's assessment. It is not a substitute for the exporter carrying out its own, and an exporter that adopts it without reading it has not done what Clause 14(b) asks of it.

Executing these Clauses is not the whole mechanism. The Clauses operate alongside the Data Processing Agreement at /documents/pallas-dpa.pdf, which carries the Article 28 terms. Where the two documents address the same subject, the Clauses prevail, as Clause 5 requires.

The blanks in the Clauses are not filled in. The Union's text carries blanks and bracketed alternatives, and section 3 below records what the parties select. They are recorded there rather than typed into the clause text, so that a reviewer comparing sections 4 and 5 against the Official Journal finds them character for character. A pack whose clause text has been helpfully tidied is a pack whose reviewer has to diff it before they can trust it.

3. Options and selections

The Clauses offer the parties several choices. These are the data importer's selections. They take effect only on execution of the signable render by both parties.

- **Module.** Module Two, transfer controller to processor. Pallas processes customer personal data on the customer's documented instructions and is a processor for that data.
- **Clause 7, the docking clause.** Included, and offered as available. An affiliate or a further party may accede to these Clauses by completing the Appendix and signing Annex I.A, without a fresh negotiation. Clause 7 is optional in the Union's text; the data importer's position is that it is enabled by default.
- **Clause 9(a), sub-processors.** OPTION 2, general written authorisation, with a notice period of thirty days. The data importer maintains a published list of sub-processors and gives thirty days' advance notice before a new sub-processor processes any customer personal data, which is the same commitment the sub-processor control below records and the same one the published list carries.
- **Clause 11(a), redress.** The optional independent dispute resolution paragraph is NOT selected. Pallas has not engaged an arbitration body. Data subjects retain every route Clause 11 gives them without it, including complaint to a supervisory authority and proceedings before the courts identified in Clause 18. Saying this plainly is better than leaving a reviewer to infer it from a paragraph's absence.
- **Clause 13(a), supervision.** The competent supervisory authority is the Data Protection Commission of Ireland, on the basis set out in Annex I.C.
- **Clause 17, governing law.** OPTION 1, the law of Ireland.
- **Clause 18(b), forum.** The courts of Ireland.

The full subprocessor list is published, with each provider purpose, data categories, processing location, and published certifications.

> Control subprocessors-published-list. Status: Implemented. Demonstrated in the pallas-marketing repository and checked by a release gate.
>
> Disclosure. The 2026-08-30 inventory record names four subprocessors in use: Supabase, Cloudflare, Stripe, and Resend. The published page carries six operative entries, adding Google and Microsoft as OAuth identity providers. Both are accurate about different things: Google and Microsoft receive an authentication assertion at sign-in and store no Pallas customer data. Procurement artifacts should carry all six operative entries, because a buyer assessing identity provider dependency needs to see the two that the four-entry description omits.
>
> Implementation. marketing: src/pages/legal/subprocessors.astro.
>
> Verification. marketing: src/pages/trust.astro, Sub-processors section.

A new subprocessor is published with 30 days advance notice before it processes any customer data.

Control subprocessors-change-notice. Status: Implemented. A commitment the operator makes contractually. No code enforces it.

Disclosure. This is a contractual commitment by the operator, not a technical control. Nothing in either repository enforces the notice period, and no new subprocessor has yet been added under it.

Implementation. marketing: src/pages/legal/subprocessors.astro, Change Notification section.

Certifications listed against each subprocessor are those published by that provider.

Control subprocessors-certifications-are-theirs. Status: Implemented. A statement by a subprocessor. Pallas configures and relies on it; no Pallas code implements it and neither Pallas repository can demonstrate it.

Disclosure. Pallas holds no SOC 2, ISO 27001, or PCI DSS certification of its own. Every certification named on the subprocessor list belongs to the named provider and covers that provider infrastructure, not the Pallas application built on top of it. A procurement document must never present a subprocessor certification in a way that could be read as a Pallas certification. This is the single most consequential misreading available in this inventory, so the distinction is stated wherever the certifications appear.

Implementation. marketing: src/pages/legal/subprocessors.astro.

Pallas operates no data centre, server cage, office server room, or other facility in which institutional data is held. Physical and environmental security for every system that holds institutional data belongs to Supabase and Cloudflare.

Control physical-security-subprocessor-operated. Status: Implemented. A statement by a subprocessor. Pallas configures and relies on it; no Pallas code implements it and neither Pallas repository can demonstrate it.

Disclosure. Every physical-security control a questionnaire asks about, including staffed facilities, cages, enclosing barriers, redundant and tested power, cooling, fire suppression, and carrier diversity, belongs to Supabase or Cloudflare. Pallas can neither demonstrate nor test any of them, and does not inherit them as its own controls. Answers to physical-security questions state reliance and name the provider. A buyer who needs evidence should read the provider audit reports; a Pallas assertion is not evidence of a provider control.

Implementation. vendor: Supabase and Cloudflare published data centre physical and environmental security programmes.

Verification. marketing: src/pages/trust.astro, subprocessor list with per-provider processing locations.

Pallas operates no network perimeter, no host, and no network monitoring of its own. Edge filtering, DDoS mitigation, and TLS termination are Cloudflare functions, and the database network boundary is operated by Supabase.

Control network-perimeter-subprocessor-operated. Status: Implemented. A statement by a subprocessor. Pallas configures and relies on it; no Pallas code implements it and neither Pallas repository can demonstrate it.

Disclosure. Pallas runs no firewall of its own, no network intrusion detection or prevention system, and no host-based agent, because it operates no hosts. Stateful filtering, DDoS mitigation, and TLS termination happen at the Cloudflare edge and are answered as provider-operated. Intrusion detection, intrusion prevention tuned by Pallas, next-generation persistent threat monitoring, and 24x7 intrusion monitoring are answered no: no such capability is operated by Pallas or configured by Pallas at a provider. A buyer requiring a monitored perimeter under vendor control, or a staffed security operations centre, should treat this as an open item.

Implementation. vendor: Cloudflare edge network, web application firewall and DDoS mitigation; Supabase managed database network boundary.

Verification. marketing: workers/, whose Workers execute on the Cloudflare edge rather than on any Pallas-operated host.

Where the transfer originates outside the Union. For personal data subject to the UK GDPR, these Clauses operate with the International Data Transfer Addendum issued by the UK Information Commissioner under section 119A of the Data Protection Act 2018. Pallas does not yet issue that Addendum with the signable render; a UK buyer should treat it as an open item to be executed with the Clauses, and raise it before signature. For personal data subject to the revised Swiss Federal Act on Data Protection, references to the GDPR are read as references to the FADP, the Swiss Federal Data Protection and Information Commissioner is an additional competent supervisory authority, and the term "member state" is read so as not to deprive a data subject in Switzerland of the right to sue in their place of habitual residence.

4. The Clauses

The text from here to the end of section 5 is reproduced from the Official Journal without modification. Section headings, clause headings, and clause numbering are the Union's. Where a clause carries a Module heading, the Module Two text is the text reproduced.

SECTION I

Clause 1: Purpose and scope

(a) The purpose of these standard contractual clauses is to ensure compliance with the requirements 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 (General Data Protection Regulation) (1) for the transfer of personal data to a third country.

(b) The Parties:

(i) the natural or legal person(s), public authority/ies, agency/ies or other body/ies (hereinafter 'entity/ies') transferring the personal data, as listed in Annex I.A (hereinafter each 'data exporter'), and

(ii) the entity/ies in a third country receiving the personal data from the data exporter, directly or indirectly via another entity also Party to these Clauses, as listed in Annex I.A (hereinafter each 'data importer')

have agreed to these standard contractual clauses (hereinafter: 'Clauses').

(c) These Clauses apply with respect to the transfer of personal data as specified in Annex I.B.

(d) The Appendix to these Clauses containing the Annexes referred to therein forms an integral part of these Clauses.

Clause 2: Effect and invariability of the Clauses

(a) These Clauses set out appropriate safeguards, including enforceable data subject rights and effective legal remedies, pursuant to Article 46(1) and Article 46(2)(c) of Regulation (EU) 2016/679 and, with respect to data transfers from controllers to processors and/or processors to processors, standard contractual

clauses pursuant to Article 28(7) of Regulation (EU) 2016/679, provided they are not modified, except to select the appropriate Module(s) or to add or update information in the Appendix. This does not prevent the Parties from including the standard contractual clauses laid down in these Clauses in a wider contract and/or to add other clauses or additional safeguards, provided that they do not contradict, directly or indirectly, these Clauses or prejudice the fundamental rights or freedoms of data subjects.

(b) These Clauses are without prejudice to obligations to which the data exporter is subject by virtue of Regulation (EU) 2016/679.

Clause 3: Third-party beneficiaries

(a) Data subjects may invoke and enforce these Clauses, as third-party beneficiaries, against the data exporter and/or data importer, with the following exceptions:

(i) Clause 1, Clause 2, Clause 3, Clause 6, Clause 7;

(ii) Clause 8 - Module One: Clause 8.5 (e) and Clause 8.9(b); Module Two: Clause 8.1(b), 8.9(a), (c), (d) and (e); Module Three: Clause 8.1(a), (c) and (d) and Clause 8.9(a), (c), (d), (e), (f) and (g); Module Four: Clause 8.1 (b) and Clause 8.3(b);

(iii) Clause 9 - Module Two: Clause 9(a), (c), (d) and (e); Module Three: Clause 9(a), (c), (d) and (e);

(iv) Clause 12 - Module One: Clause 12(a) and (d); Modules Two and Three: Clause 12(a), (d) and (f);

(v) Clause 13;

(vi) Clause 15.1(c), (d) and (e);

(vii) Clause 16(e);

(viii) Clause 18 - Modules One, Two and Three: Clause 18(a) and (b); Module Four: Clause 18.

(b) Paragraph (a) is without prejudice to rights of data subjects under Regulation (EU) 2016/679.

Clause 4: Interpretation

(a) Where these Clauses use terms that are 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 conflicts with rights and obligations provided for in Regulation (EU) 2016/679.

Clause 5: Hierarchy

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

Clause 6: Description of the transfer(s)

The details of the transfer(s), and in particular the categories of personal data that are transferred and the purpose(s) for which they are transferred, are specified in Annex I.B.

Clause 7 - Optional: Docking clause

(a) An entity that is not a Party to these Clauses may, with the agreement of the Parties, accede to these Clauses at any time, either as a data exporter or as a data importer, by completing the Appendix and signing Annex I.A.

(b) Once it has completed the Appendix and signed Annex I.A, the acceding entity shall become a Party to these Clauses and have the rights and obligations of a data exporter or data importer in accordance with its designation in Annex I.A.

(c) The acceding entity shall have no rights or obligations arising under these Clauses from the period prior to becoming a Party.

SECTION II - OBLIGATIONS OF THE PARTIES

Clause 8: Data protection safeguards

The data exporter warrants that it has used reasonable efforts to determine that the data importer is able, through the implementation of appropriate technical and organisational measures, to satisfy its obligations under these Clauses.

MODULE TWO: Transfer controller to processor

8.1 Instructions

(a) The data importer shall process the personal data only on documented instructions from the data exporter. The data exporter may give such instructions throughout the duration of the contract.

(b) The data importer shall immediately inform the data exporter if it is unable to follow those instructions.

8.2 Purpose limitation

The data importer shall process the personal data only for the specific purpose(s) of the transfer, as set out in Annex I.B, unless on further instructions from the data exporter.

8.3 Transparency

On request, the data exporter shall make a copy of these Clauses, including the Appendix as completed by the Parties, available to the data subject free of charge. To the extent necessary to protect business secrets or other confidential information, including the measures described in Annex II and personal data, the data exporter may redact part of the text of the Appendix to these Clauses prior to sharing a copy, but shall provide a meaningful summary where the data subject would otherwise not be able to understand the its content or exercise his/her rights. On request, the Parties shall provide the data subject with the reasons for the redactions, to the extent possible without revealing the redacted information. This Clause is without prejudice to the obligations of the data exporter under Articles 13 and 14 of Regulation (EU) 2016/679.

8.4 Accuracy

If the data importer becomes aware that the personal data it has received is inaccurate, or has become outdated, it shall inform the data exporter without undue delay. In this case, the data importer shall cooperate with the data exporter to erase or rectify the data.

8.5 Duration of processing and erasure or return of data

Processing by the data importer shall only take place for the duration specified in Annex I.B. After the end of the provision of the processing services, the data importer shall, at the choice of the data exporter, delete all personal data processed on behalf of the data exporter and certify to the data exporter that it has done so, or return to the data exporter all personal data processed on its behalf and delete existing copies. Until the data is deleted or returned, the data importer shall continue to ensure compliance with these Clauses. In case of local laws applicable to the data importer that prohibit return or deletion of the personal data, the data importer warrants that it will continue to ensure compliance with these Clauses and will only process it to the extent and for as long as required under that local law. This is without prejudice to Clause 14, in particular the requirement for the data importer under Clause 14(e) to notify the data exporter throughout the duration of the contract if it has reason to believe that it is or has become subject to laws or practices not in line with the requirements under Clause 14(a).

8.6 Security of processing

(a) The data importer and, during transmission, also the data exporter shall implement appropriate technical and organisational measures to ensure the security of the data, including protection against a breach of security leading to accidental or unlawful destruction, loss, alteration, unauthorised disclosure or access to that data (hereinafter '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 purpose(s) of processing and the risks involved in the processing for the data subjects. The Parties shall in particular consider having recourse to encryption or pseudonymisation, including during transmission, where the purpose of processing can be fulfilled in that manner. In case of pseudonymisation, the additional information for attributing the personal data to a specific data subject shall, where possible, remain under the exclusive control of the data exporter. In complying with its obligations under this paragraph, the data importer shall at least implement the technical and organisational measures specified in Annex II. The data importer shall carry out regular checks to ensure that these measures continue to provide an appropriate level of security.

(b) The data importer shall grant access to the personal data to members of its personnel only to the extent strictly necessary for the implementation, management and monitoring of the contract. It shall ensure that persons authorised to process the personal data have committed themselves to confidentiality or are under an appropriate statutory obligation of confidentiality.

(c) In the event of a personal data breach concerning personal data processed by the data importer under these Clauses, the data importer shall take appropriate measures to address the breach, including measures to mitigate its adverse effects. The data importer shall also notify the data exporter without undue delay after having become aware of the breach. Such notification shall contain the details of a contact point where more information can be obtained, a description of the nature of the breach (including, where possible, categories and approximate number of data subjects and personal data records concerned), its likely consequences and the measures taken or proposed to address the breach including, where appropriate, measures to mitigate its possible adverse effects. Where, and in so far as, it is not possible to provide all 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.

(d) The data importer shall cooperate with and assist the data exporter to enable the data exporter to comply with its obligations under Regulation (EU) 2016/679, in particular to notify the competent supervisory authority and the affected data subjects, taking into account the nature of processing and the information available to the data importer.

8.7 Sensitive data

Where the transfer 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 (hereinafter 'sensitive data'), the data importer shall apply the specific restrictions and/or additional safeguards described in Annex I.B.

8.8 Onward transfers

The data importer shall only disclose the personal data to a third party on documented instructions from the data exporter. In addition, the data may only be disclosed to a third party located outside the European Union (4) (in the same country as the data importer or in another third country, hereinafter 'onward transfer') if the third party is or agrees to be bound by these Clauses, under the appropriate Module, or if:

(i) the onward transfer is to a country benefitting from an adequacy decision pursuant to Article 45 of Regulation (EU) 2016/679 that covers the onward transfer;

(ii) the third party otherwise ensures appropriate safeguards pursuant to Articles 46 or 47 Regulation of (EU) 2016/679 with respect to the processing in question;

(iii) the onward transfer is necessary for the establishment, exercise or defence of legal claims in the context of specific administrative, regulatory or judicial proceedings; or

(iv) the onward transfer is necessary in order to protect the vital interests of the data subject or of another natural person.

Any onward transfer is subject to compliance by the data importer with all the other safeguards under these Clauses, in particular purpose limitation.

8.9 Documentation and compliance

(a) The data importer shall promptly and adequately deal with enquiries from the data exporter that relate to the processing under these Clauses.

(b) The Parties shall be able to demonstrate compliance with these Clauses. In particular, the data importer shall keep appropriate documentation on the processing activities carried out on behalf of the data exporter.

(c) The data importer shall make available to the data exporter all information necessary to demonstrate compliance with the obligations set out in these Clauses and at the data exporter's request, allow for 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 audit, the data exporter may take into account relevant certifications held by the data importer.

(d) The data exporter may choose to conduct the audit by itself or mandate an independent auditor. Audits may include inspections at the premises or physical facilities of the data importer and shall, where appropriate, be carried out with reasonable notice.

(e) The Parties shall make the information referred to in paragraphs (b) and (c), including the results of any audits, available to the competent supervisory authority on request.

Clause 9: Use of sub-processors

MODULE TWO: Transfer controller to processor

(a) OPTION 1: SPECIFIC PRIOR AUTHORISATION The data importer shall not sub-contract any of its processing activities performed on behalf of the data exporter under these Clauses to a sub-processor without the data exporter's prior specific written authorisation. The data importer shall submit the request for specific authorisation at least [Specify time period] prior to the engagement of the sub-processor, together with the information necessary to enable the data exporter to decide on the authorisation. The list of sub-processors already authorised by the data exporter can be found in Annex III. The Parties shall keep Annex III up to date.

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

(b) Where the data importer engages a sub-processor to carry out specific processing activities (on behalf of the data exporter), it shall do so by way of a written contract that provides for, in substance, the same data protection obligations as those binding the data importer under these Clauses, including in terms of third-party beneficiary rights for data subjects. (8) The Parties agree that, by complying with this Clause, the data importer fulfils its obligations under Clause 8.8. The data importer shall ensure that the sub-processor complies with the obligations to which the data importer is subject pursuant to these Clauses.

(c) The data importer shall provide, at the data exporter's request, a copy of such a sub-processor agreement and any subsequent amendments to the data exporter. To the extent necessary to protect business secrets or other confidential information, including personal data, the data importer may redact the text of the agreement prior to sharing a copy.

(d) The data importer shall remain fully responsible to the data exporter for the performance of the sub-processor's obligations under its contract with the data importer. The data importer shall notify the data exporter of any failure by the sub-processor to fulfil its obligations under that contract.

(e) The data importer shall agree a third-party beneficiary clause with the sub-processor whereby - in the event the data importer has factually disappeared, ceased to exist in law or has become insolvent - the data exporter shall have the right to terminate the sub-processor contract and to instruct the sub-processor to erase or return the personal data.

Clause 10: Data subject rights

MODULE TWO: Transfer controller to processor

(a) The data importer shall promptly notify the data exporter of any request it has received from a data subject. It shall not respond to that request itself unless it has been authorised to do so by the data exporter.

(b) The data importer shall assist the data exporter in fulfilling its obligations to respond to data subjects' requests for the exercise of their rights under Regulation (EU) 2016/679. In this regard, the Parties shall set

out in Annex II the appropriate technical and organisational measures, taking into account the nature of the processing, by which the assistance shall be provided, as well as the scope and the extent of the assistance required.

(c) In fulfilling its obligations under paragraphs (a) and (b), the data importer shall comply with the instructions from the data exporter.

Clause 11: Redress

(a) The data importer shall inform data subjects in a transparent and easily accessible format, through individual notice or on its website, of a contact point authorised to handle complaints. It shall deal promptly with any complaints it receives from a data subject.

[OPTION: The data importer agrees that data subjects may also lodge a complaint with an independent dispute resolution body (11) at no cost to the data subject. It shall inform the data subjects, in the manner set out in paragraph (a), of such redress mechanism and that they are not required to use it, or follow a particular sequence in seeking redress.]

MODULE TWO: Transfer controller to processor

(b) In case of a dispute between a data subject and one of the Parties as regards compliance with these Clauses, that Party shall use its best efforts to resolve the issue amicably in a timely fashion. The Parties shall keep each other informed about such disputes and, where appropriate, cooperate in resolving them.

(c) Where the data subject invokes a third-party beneficiary right pursuant to Clause 3, the data importer shall accept the decision of the data subject to:

(i) lodge a complaint with the supervisory authority in the Member State of his/her habitual residence or place of work, or the competent supervisory authority pursuant to Clause 13;

(ii) refer the dispute to the competent courts within the meaning of Clause 18.

(d) The Parties accept that the data subject may be represented by a not-for-profit body, organisation or association under the conditions set out in Article 80(1) of Regulation (EU) 2016/679.

(e) The data importer shall abide by a decision that is binding under the applicable EU or Member State law.

(f) The data importer agrees that the choice made by the data subject will not prejudice his/her substantive and procedural rights to seek remedies in accordance with applicable laws.

Clause 12: Liability

MODULE TWO: Transfer controller to processor

(a) Each Party shall be liable to the other Party/ies for any damages it causes the other Party/ies by any breach of these Clauses.

(b) The data importer shall be liable to the data subject, and the data subject shall be entitled to receive compensation, for any material or non-material damages the data importer or its sub-processor causes the data subject by breaching the third-party beneficiary rights under these Clauses.

(c) Notwithstanding paragraph (b), the data exporter shall be liable to the data subject, and the data subject shall be entitled to receive compensation, for any material or non-material damages the data exporter or the data importer (or its sub-processor) causes the data subject by breaching the third-party beneficiary rights

under these Clauses. This is without prejudice to the liability of the data exporter and, where the data exporter is a processor acting on behalf of a controller, to the liability of the controller under Regulation (EU) 2016/679 or Regulation (EU) 2018/1725, as applicable.

(d) The Parties agree that if the data exporter is held liable under paragraph (c) for damages caused by the data importer (or its sub-processor), it shall be entitled to claim back from the data importer that part of the compensation corresponding to the data importer's responsibility for the damage.

(e) Where more than one Party is responsible for any damage caused to the data subject as a result of a breach of these Clauses, all responsible Parties shall be jointly and severally liable and the data subject is entitled to bring an action in court against any of these Parties.

(f) The Parties agree that if one Party is held liable under paragraph (e), it shall be entitled to claim back from the other Party/ies that part of the compensation corresponding to its/their responsibility for the damage.

(g) The data importer may not invoke the conduct of a sub-processor to avoid its own liability.

Clause 13: Supervision

MODULE TWO: Transfer controller to processor

(a) [Where the data exporter is established in an EU Member State:] The supervisory authority with responsibility for ensuring compliance by the data exporter with Regulation (EU) 2016/679 as regards the data transfer, as indicated in Annex I.C, shall act as competent supervisory authority.

[Where the data exporter is not established in an EU Member State, but falls within the territorial scope of application of Regulation (EU) 2016/679 in accordance with its Article 3(2) and has appointed a representative pursuant to Article 27(1) of Regulation (EU) 2016/679:] The supervisory authority of the Member State in which the representative within the meaning of Article 27(1) of Regulation (EU) 2016/679 is established, as indicated in Annex I.C, shall act as competent supervisory authority.

[Where the data exporter is not established in an EU Member State, but falls within the territorial scope of application of Regulation (EU) 2016/679 in accordance with its Article 3(2) without however having to appoint a representative pursuant to Article 27(2) of Regulation (EU) 2016/679:] The supervisory authority of one of the Member States in which the data subjects whose personal data is transferred under these Clauses in relation to the offering of goods or services to them, or whose behaviour is monitored, are located, as indicated in Annex I.C, shall act as competent supervisory authority.

(b) The data importer agrees to submit itself to the jurisdiction of and cooperate with the competent supervisory authority in any procedures aimed at ensuring compliance with these Clauses. In particular, the data importer agrees to respond to enquiries, submit to audits and comply with the measures adopted by the supervisory authority, including remedial and compensatory measures. It shall provide the supervisory authority with written confirmation that the necessary actions have been taken.

SECTION III - LOCAL LAWS AND OBLIGATIONS IN CASE OF ACCESS BY PUBLIC AUTHORITIES

Clause 14: Local laws and practices affecting compliance with the Clauses

MODULE TWO: Transfer controller to processor

(where the EU processor combines the personal data received from the third country-controller with personal data collected by the processor in the EU)

(a) The Parties warrant that they have no reason to believe that the laws and practices in the third country of destination applicable to the processing of the personal data by the data importer, including any requirements to disclose personal data or measures authorising access by public authorities, prevent the data importer from fulfilling its obligations under these Clauses. This is based on the understanding that laws and practices that respect the essence of the fundamental rights and freedoms and do not exceed what is necessary and proportionate in a democratic society to safeguard one of the objectives listed in Article 23(1) of Regulation (EU) 2016/679, are not in contradiction with these Clauses.

(b) The Parties declare that in providing the warranty in paragraph (a), they have taken due account in particular of the following elements:

(i) the specific circumstances of the transfer, including the length of the processing chain, the number of actors involved and the transmission channels used; intended onward transfers; the type of recipient; the purpose of processing; the categories and format of the transferred personal data; the economic sector in which the transfer occurs; the storage location of the data transferred;

(ii) the laws and practices of the third country of destination- including those requiring the disclosure of data to public authorities or authorising access by such authorities - relevant in light of the specific circumstances of the transfer, and the applicable limitations and safeguards (12);

(iii) any relevant contractual, technical or organisational safeguards put in place to supplement the safeguards under these Clauses, including measures applied during transmission and to the processing of the personal data in the country of destination.

(c) The data importer warrants that, in carrying out the assessment under paragraph (b), it has made its best efforts to provide the data exporter with relevant information and agrees that it will continue to cooperate with the data exporter in ensuring compliance with these Clauses.

(d) The Parties agree to document the assessment under paragraph (b) and make it available to the competent supervisory authority on request.

(e) The data importer agrees to notify the data exporter promptly if, after having agreed to these Clauses and for the duration of the contract, it has reason to believe that it is or has become subject to laws or practices not in line with the requirements under paragraph (a), including following a change in the laws of the third country or a measure (such as a disclosure request) indicating an application of such laws in practice that is not in line with the requirements in paragraph (a). [For Module Three: The data exporter shall forward the notification to the controller.]

(f) Following a notification pursuant to paragraph (e), or if the data exporter otherwise has reason to believe that the data importer can no longer fulfil its obligations under these Clauses, the data exporter shall promptly identify appropriate measures (e.g. technical or organisational measures to ensure security and confidentiality) to be adopted by the data exporter and/or data importer to address the situation [for Module Three:, if appropriate in consultation with the controller]. The data exporter shall suspend the data transfer if it considers that no appropriate safeguards for such transfer can be ensured, or if instructed by [for Module

Three: the controller or] the competent supervisory authority to do so. In this case, the data exporter shall be entitled to terminate the contract, insofar as it concerns the processing of personal data under these Clauses. If the contract involves more than two Parties, the data exporter may exercise this right to termination only with respect to the relevant Party, unless the Parties have agreed otherwise. Where the contract is terminated pursuant to this Clause, Clause 16(d) and (e) shall apply.

Clause 15: Obligations of the data importer in case of access by public authorities

MODULE TWO: Transfer controller to processor

(where the EU processor combines the personal data received from the third country-controller with personal data collected by the processor in the EU)

15.1 Notification

(a) The data importer agrees to notify the data exporter and, where possible, the data subject promptly (if necessary with the help of the data exporter) if it:

(i) receives a legally binding request from a public authority, including judicial authorities, under the laws of the country of destination for the disclosure of personal data transferred pursuant to these Clauses; such notification shall include information about the personal data requested, the requesting authority, the legal basis for the request and the response provided; or

(ii) becomes aware of any direct access by public authorities to personal data transferred pursuant to these Clauses in accordance with the laws of the country of destination; such notification shall include all information available to the importer.

[For Module Three: The data exporter shall forward the notification to the controller.]

(b) If the data importer is prohibited from notifying the data exporter and/or the data subject under the laws of the country of destination, the data importer agrees to use its best efforts to obtain a waiver of the prohibition, with a view to communicating as much information as possible, as soon as possible. The data importer agrees to document its best efforts in order to be able to demonstrate them on request of the data exporter.

(c) Where permissible under the laws of the country of destination, the data importer agrees to provide the data exporter, at regular intervals for the duration of the contract, with as much relevant information as possible on the requests received (in particular, number of requests, type of data requested, requesting authority/ies, whether requests have been challenged and the outcome of such challenges, etc.). [For Module Three: The data exporter shall forward the information to the controller.]

(d) The data importer agrees to preserve the information pursuant to paragraphs (a) to (c) for the duration of the contract and make it available to the competent supervisory authority on request.

(e) Paragraphs (a) to (c) are without prejudice to the obligation of the data importer pursuant to Clause 14(e) and Clause 16 to inform the data exporter promptly where it is unable to comply with these Clauses.

15.2 Review of legality and data minimisation

(a) The data importer agrees to review the legality of the request for disclosure, in particular whether it remains within the powers granted to the requesting public authority, and to challenge the request if, after careful assessment, it concludes that there are reasonable grounds to consider that the request is unlawful under the laws of the country of destination, applicable obligations under international law and principles of international comity. The data importer shall, under the same conditions, pursue possibilities of appeal. When

challenging a request, the data importer shall seek interim measures with a view to suspending the effects of the request until the competent judicial authority has decided on its merits. It shall not disclose the personal data requested until required to do so under the applicable procedural rules. These requirements are without prejudice to the obligations of the data importer under Clause 14(e).

(b) The data importer agrees to document its legal assessment and any challenge to the request for disclosure and, to the extent permissible under the laws of the country of destination, make the documentation available to the data exporter. It shall also make it available to the competent supervisory authority on request. [For Module Three: The data exporter shall make the assessment available to the controller.]

(c) The data importer agrees to provide the minimum amount of information permissible when responding to a request for disclosure, based on a reasonable interpretation of the request.

SECTION IV - FINAL PROVISIONS

Clause 16: Non-compliance with the Clauses and termination

(a) The data importer shall promptly inform the data exporter if it is unable to comply with these Clauses, for whatever reason.

(b) In the event that the data importer is in breach of these Clauses or unable to comply with these Clauses, the data exporter shall suspend the transfer of personal data to the data importer until compliance is again ensured or the contract is terminated. This is without prejudice to Clause 14(f).

(c) The data exporter shall be entitled to terminate the contract, insofar as it concerns the processing of personal data under these Clauses, where:

(i) the data exporter has suspended the transfer of personal data to the data importer pursuant to paragraph (b) and compliance with these Clauses is not restored within a reasonable time and in any event within one month of suspension;

(ii) the data importer is in substantial or persistent breach of these Clauses; or

(iii) the data importer fails to comply with a binding decision of a competent court or supervisory authority regarding its obligations under these Clauses.

In these cases, it shall inform the competent supervisory authority [for Module Three: and the controller] of such non-compliance. Where the contract involves more than two Parties, the data exporter may exercise this right to termination only with respect to the relevant Party, unless the Parties have agreed otherwise.

(d) [For Modules One, Two and Three: Personal data that has been transferred prior to the termination of the contract pursuant to paragraph (c) shall at the choice of the data exporter immediately be returned to the data exporter or deleted in its entirety. The same shall apply to any copies of the data.] [For Module Four: Personal data collected by the data exporter in the EU that has been transferred prior to the termination of the contract pursuant to paragraph (c) shall immediately be deleted in its entirety, including any copy thereof.] The data importer shall certify the deletion of the data to the data exporter. Until the data is deleted or returned, the data importer shall continue to ensure compliance with these Clauses. In case of local laws applicable to the data importer that prohibit the return or deletion of the transferred personal data, the data importer warrants that it will continue to ensure compliance with these Clauses and will only process the data

to the extent and for as long as required under that local law.

(e) Either Party may revoke its agreement to be bound by these Clauses where (i) the European Commission adopts a decision pursuant to Article 45(3) of Regulation (EU) 2016/679 that covers the transfer of personal data to which these Clauses apply; or (ii) Regulation (EU) 2016/679 becomes part of the legal framework of the country to which the personal data is transferred. This is without prejudice to other obligations applying to the processing in question under Regulation (EU) 2016/679.

Clause 17: Governing law

MODULE TWO: Transfer controller to processor

[OPTION 1: These Clauses shall be governed by the law of one of the EU Member States, provided such law allows for third-party beneficiary rights. The Parties agree that this shall be the law of _____ (specify Member State).]

[OPTION 2 (for Modules Two and Three): These Clauses shall be governed by the law of the EU Member State in which the data exporter is established. Where such law does not allow for third-party beneficiary rights, they shall be governed by the law of another EU Member State that does allow for third-party beneficiary rights. The Parties agree that this shall be the law of _____ (specify Member State).]

Clause 18: Choice of forum and jurisdiction

MODULE TWO: Transfer controller to processor

(a) Any dispute arising from these Clauses shall be resolved by the courts of an EU Member State.

(b) The Parties agree that those shall be the courts of _____ (specify Member State).

(c) A data subject may also bring legal proceedings against the data exporter and/or data importer before the courts of the Member State in which he/she has his/her habitual residence.

(d) The Parties agree to submit themselves to the jurisdiction of such courts.

Footnotes to the Clauses

The twelve footnotes below are part of the Annex as published and are reproduced with it. Their numbers are the numbers used in the clause text above.

(1) Where the data exporter is a processor subject to Regulation (EU) 2016/679 acting on behalf of a Union institution or body as controller, reliance on these Clauses when engaging another processor (sub-processing) not subject to Regulation (EU) 2016/679 also ensures compliance with Article 29(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 (OJ L 295, 21.11.2018, p. 39), to the extent these Clauses and the data protection obligations as set out in the contract or other legal act between the controller and the processor pursuant to Article 29(3) of Regulation (EU) 2018/1725 are aligned. This will in particular be the case where the controller and processor rely on the standard contractual clauses included in Decision 2021/915.

(2) This requires rendering the data anonymous in such a way that the individual is no longer identifiable by anyone, in line with recital 26 of Regulation (EU) 2016/679, and that this process is irreversible.

(3) The Agreement on the European Economic Area (EEA Agreement) provides for the extension of the European Union's internal market to the three EEA States Iceland, Liechtenstein and Norway. The Union data protection legislation, including Regulation (EU) 2016/679, is covered by the EEA Agreement and has been incorporated into Annex XI thereto. Therefore, any disclosure by the data importer to a third party located in the EEA does not qualify as an onward transfer for the purpose of these Clauses.

(4) The Agreement on the European Economic Area (EEA Agreement) provides for the extension of the European Union's internal market to the three EEA States Iceland, Liechtenstein and Norway. The Union data protection legislation, including Regulation (EU) 2016/679, is covered by the EEA Agreement and has been incorporated into Annex XI thereto. Therefore, any disclosure by the data importer to a third party located in the EEA does not qualify as an onward transfer for the purpose of these Clauses.

(5) See Article 28(4) of Regulation (EU) 2016/679 and, where the controller is an EU institution or body, Article 29(4) of Regulation (EU) 2018/1725.

(6) The Agreement on the European Economic Area (EEA Agreement) provides for the extension of the European Union's internal market to the three EEA States Iceland, Liechtenstein and Norway. The Union data protection legislation, including Regulation (EU) 2016/679, is covered by the EEA Agreement and has been incorporated into Annex XI thereto. Therefore, any disclosure by the data importer to a third party located in the EEA does not qualify as an onward transfer for the purposes of these Clauses.

(7) This includes whether the transfer and further 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 or offences.

(8) This requirement may be satisfied by the sub-processor acceding to these Clauses under the appropriate Module, in accordance with Clause 7.

(9) This requirement may be satisfied by the sub-processor acceding to these Clauses under the appropriate Module, in accordance with Clause 7.

(10) That period may be extended by a maximum of two more months, to the extent necessary taking into account the complexity and number of requests. The data importer shall duly and promptly inform the data subject of any such extension.

(11) The data importer may offer independent dispute resolution through an arbitration body only if it is established in a country that has ratified the New York Convention on Enforcement of Arbitration Awards.

(12) As regards the impact of such laws and practices on compliance with these Clauses, different elements may be considered as part of an overall assessment. Such elements may include relevant and documented practical experience with prior instances of requests for disclosure from public authorities, or the absence of such requests, covering a sufficiently representative time-frame. This refers in particular to internal records or other documentation, drawn up on a continuous basis in accordance with due diligence and certified at senior management level, provided that this information can be lawfully shared with third parties. Where this practical experience is relied upon to conclude that the data importer will not be prevented from complying with these Clauses, it needs to be supported by other relevant, objective elements, and it is for the Parties to consider carefully whether these elements together carry sufficient weight, in terms of their reliability and representativeness, to support this conclusion. In particular, the Parties have to take into account whether their practical experience is corroborated and not contradicted by publicly available or otherwise accessible,

reliable information on the existence or absence of requests within the same sector and/or the application of the law in practice, such as case law and reports by independent oversight bodies.

5. Appendix

The Clauses require the parties to complete an Appendix in three annexes. Annexes I, II, and III follow. They are the data importer's, not the Union's.

6. Annex I

A. List of parties

Data exporter.

The Customer, being the entity that has entered into an agreement with the data importer for the provision of the Pallas service, acting as controller in respect of the personal data it submits to the service. Name, address, contact person, activities relevant to the transfer, and signature are completed on the signature page of the executed pack.

Role: controller.

Data importer.

Lonia AI

Contact person for data protection matters: support@lonia.ai.

Activities relevant to the data transferred: provision of the Pallas accessibility scanning, monitoring, remediation-tracking, and reporting service to the data exporter, including hosting of the data exporter's account and organisation records, scan findings, generated reports, and audit records.

Role: processor.

This informational render carries the party block in the trade name only and is not executable. Request the signable render at support@lonia.ai.

B. Description of transfer

Categories of data subjects. Individuals whom the data exporter authorises to use the Pallas service: the data exporter's employees, contractors, and other personnel who hold an account or an organisation membership. Where the data exporter uploads or submits content for scanning that itself contains personal data relating to other individuals, those individuals are also data subjects of the transfer, and the data exporter is responsible for determining what it submits.

Categories of personal data transferred. The classes below are the enumerated data classes from the Pallas control inventory. Nothing outside them is transferred.

Pallas holds account identity, organisation records, scan findings, generated reports, transiently uploaded source files, audit events, and marketing list membership. It holds no payment card data, no special category data by design, and no health or student records.

Control data-classes-enumerated. Status: Implemented. Backed by a file in the pallas-app repository, verified

read-only on 2026-08-30, not gated from the marketing repository.

Disclosure. Pallas does not collect special category data as a matter of design, but it scans customer-supplied URLs and accepts customer-uploaded documents. Content a customer submits is outside Pallas control, so the accurate statement is that Pallas does not solicit or intentionally process special category data, not that none can ever transit the system. Uploaded source files carry a 7 day default retention precisely because they are the class most likely to contain something unintended.

Implementation. app: The 29 tables enumerated in tenant-rls-every-table, plus the three Storage buckets in migration 020.

Verification. marketing: src/pages/trust.astro, What Pallas holds and What Pallas never collects.

Account identity data comprises the name, email address, and profile photograph asserted by the data exporter's chosen identity provider at sign-in. Pallas does not collect or store passwords, because it does not accept them.

Pallas authenticates users through Google and Microsoft OAuth only. It stores no passwords, offers no password login, and has no password reset flow.

Control auth-oauth-only. Status: Implemented. Backed by a file in the pallas-app repository, verified read-only on 2026-08-30, not gated from the marketing repository.

Implementation. app: src/contexts/AuthContext.tsx:172 and :181; app: src/pages/Onboarding.tsx:123.

Verification. app: Search src/ for signInWithPassword and signUp(.

Sensitive data. Pallas does not request, require, or make provision for special categories of personal data within the meaning of Article 9, nor for personal data relating to criminal convictions and offences within the meaning of Article 10. The service is an accessibility scanner and no feature of it calls for such data. Where the data exporter nonetheless submits content that contains it, no additional restriction or safeguard beyond the measures in Annex II is applied to it, because none is implemented. The data exporter should treat that as a limitation on what it submits rather than as an assurance.

Frequency of the transfer. Continuous, for the duration of the agreement between the parties.

Nature and purpose of the processing. Hosting, storage, automated analysis of submitted web content against accessibility success criteria, generation of reports and remediation records, transmission of transactional email relating to the service, retention and deletion in accordance with the data exporter's configured policies, and the maintenance of an audit record of actions taken in the service.

Period of retention. Determined by the data exporter through per-organisation retention settings, subject to the floors and sweeps below.

Retention is configured per organisation, with defaults of 365 days for scan data, 7 days for uploaded source files, 730 days for reports, and 2555 days (seven years) for the audit log.

Control retention-per-org-policies. Status: Implemented. Backed by a file in the pallas-app repository, verified read-only on 2026-08-30, not gated from the marketing repository.

Implementation. app: pallas_retention_policies, migration 002:374.

Verification. app: uq_pallas_retention_org, migration 002:385.

A scheduled job applies retention policies daily at 03:00 UTC for every organisation with automatic deletion enabled.

Control retention-daily-sweep. Status: Implemented. True of the migration file set. Live database state is not provable from source, and the operator pre-check that resolves it is named in the disclosure.

Disclosure. The job is scheduled by a DO block that catches its own exception, so a database on which pg_cron was not enabled at migration time has no job and the migration still reported success. Whether the job exists and is running on the live database is an operator check against the cron.job and cron.job_run_details tables. This repository can show what was intended to be scheduled; it cannot show what is scheduled.

Implementation. app: pallas-daily-retention, '0 3 * * *', scheduled at migration 021:238; app: pallas_apply_retention_policies, migration 021:197, rebuilt 029:629, migration 041, and migration 042.

Verification. app: supabase/migrations/042_restore_retention_sweeps_and_gaps.sql.

Archived audit events past their retention window are purged nightly at 04:00 UTC, and each purge run is logged.

Control retention-audit-purge. Status: Implemented. True of the migration file set. Live database state is not provable from source, and the operator pre-check that resolves it is named in the disclosure.

Disclosure. Scheduled by the same self-catching DO block pattern as the 03:00 UTC sweep. Existence of the live job is an operator check against cron.job.

Implementation. app: pallas_nightly_retention_purge, '0 4 * * *', scheduled at migration 034:581; app: pallas_purge_expired_retained_audit_events, migration 034:460; app: pallas_retention_purge_log, migration 034:405, RLS enabled 034:416.

Verification. app: supabase/migrations/034_enforce_finding_limit_and_retention_purge.sql section 9.

Uploaded source files are purged from Storage daily at 05:00 UTC by a Supabase Edge Function invoked from the database.

Control retention-source-file-purge. Status: Partial. True of the migration file set. Live database state is not provable from source, and the operator pre-check that resolves it is named in the disclosure.

Disclosure. This job does no work unless two database settings are present: app.settings.functions_base_url and app.settings.cron_secret. When either is missing the job raises a warning and returns, so source files are NOT purged and nothing fails loudly. Migration 035:619 states this in the job body. The operator must confirm both settings are set on the live database before this control is claimed to a buyer. Separately, the 2026-08-30 inventory record describes this credential as being held in Supabase Vault under the name pallas_enforce_retention_bearer. No file in either repository references Vault or that name; the mechanism on disk is a Supabase Edge Function secret named CRON_SECRET plus a database setting named app.settings.cron_secret. The inventory description and the file set disagree, and the file set is what these repositories can show.

Implementation. app: pallas_daily_source_file_retention, '0 5 * * *', scheduled at migration 035:609; app: supabase/functions/enforce-retention/index.ts.

Verification. app: supabase/functions/enforce-retention/index.ts:239 to :252.

Retention settings cause actual deletion rather than being stored as a preference. The sweep issues DELETE statements against the tables it governs.

Control retention-deletion-actually-deletes. Status: Implemented. Backed by a file in the pallas-app repository, verified read-only on 2026-08-30, not gated from the marketing repository.

Implementation. app: pallas_apply_retention_policies, migration 042.

Verification. app: migration 041, which enumerates the three code paths that lawfully remove audit rows.

Place of processing. The default processing location is the United States. This is the fact that makes these Clauses necessary.

The default processing location is the United States. Supabase hosts the database and Storage in us-east-1; Cloudflare serves from its global edge network.

Control data-location-default-us. Status: Implemented. A statement by a subprocessor. Pallas configures and relies on it; no Pallas code implements it and neither Pallas repository can demonstrate it.

Implementation. vendor: Supabase project region us-east-1; marketing: src/pages/legal/subprocessors.astro.

Verification. marketing: src/pages/trust.astro, Data residency options.

Processing takes place in the United States only. No European Union hosting exists and none is offered.

Control data-location-eu-option. Status: Not implemented. A commitment the operator makes contractually. No code enforces it.

Disclosure. No customer data is processed in the European Union and no EU infrastructure subprocessor is engaged or planned. Any procurement document, questionnaire response, or sales conversation must present United States processing as the only option and must not present EU hosting as available, on request, or on a roadmap.

Implementation. marketing: src/pages/trust.astro, Data residency options; marketing: src/pages/legal/subprocessors.astro, six operative entries and no planned entry.

Transfers to sub-processors. Subject matter, nature, and duration of processing by each sub-processor are as set out in Annex III.

C. Competent supervisory authority

The Data Protection Commission of Ireland, 21 Fitzwilliam Square South, Dublin 2, D02 RD28, Ireland.

Clause 13(a) requires the supervisory authority to be identified by reference to the data exporter's establishment. Where the data exporter is established in an EU Member State, the competent authority is that of the Member State of establishment, and this Annex is completed on execution to name it. Where the data exporter is not established in the Union but falls within the territorial scope of the GDPR under Article 3(2) and has designated a representative under Article 27, the competent authority is that of the Member State in which the representative is established. Where the data exporter is not established in the Union, falls within the territorial scope of Article 3(2), and has not designated a representative, the parties select the Data Protection Commission of Ireland, being the supervisory authority of the Member State in which the data subjects whose personal data is transferred under these Clauses in relation to the offering of goods or services to them are located.

The Data Protection Commission of Ireland is also the authority to which the data importer directs breach notification where the jurisdiction of the affected data subjects is the Union.

Authority notification follows the jurisdiction: Ireland DPC, UK ICO, and EU supervisory authorities within 72 hours; Canada OPC under PIPEDA; Australia OAIC under the Notifiable Data Breaches scheme.

> Control incident-authority-notification. Status: Implemented. A commitment the operator makes contractually. No code enforces it.
>
> Disclosure. A contractual and regulatory commitment rather than a technical control. Pallas has not been required to make such a notification, so there is no track record to evidence.
>
> Implementation. marketing: src/pages/trust.astro, Breach commitments, Authority notification.

7. Annex II. Technical and organisational measures

Clause 8.6 requires the data importer to implement appropriate technical and organisational measures to ensure the security of the data, and this Annex is where those measures are described.

Every measure below is rendered from the Pallas control inventory at src/data/control-inventory.ts with its claim, its implementation status, the basis of the evidence behind it, and its disclosure text reproduced without alteration. A measure marked Partial says Partial here. A measure that rests on a sub-processor's assertion rather than on Pallas code says so. This is deliberate and it is the point of rendering the annex from the inventory rather than writing it: an Annex II that describes measures more favourably than the system implements them is a warranty the importer cannot meet, and Clause 8.6 is the clause under which that would be tested.

The measures are grouped as the Clauses' own Annex II example list groups them.

Measures of user identification and authorisation

Pallas authenticates users through Google and Microsoft OAuth only. It stores no passwords, offers no password login, and has no password reset flow.

> Control auth-oauth-only. Status: Implemented. Backed by a file in the pallas-app repository, verified read-only on 2026-08-30, not gated from the marketing repository.
>
> Implementation. app: src/contexts/AuthContext.tsx:172 and :181; app: src/pages/Onboarding.tsx:123.
>
> Verification. app: Search src/ for signInWithPassword and signUp(.

The trigger that provisions a Pallas profile on first sign-in cannot block a sign-in if it fails.

> Control auth-profile-trigger-fail-safe. Status: Implemented. Backed by a file in the pallas-app repository, verified read-only on 2026-08-30, not gated from the marketing repository.
>
> Implementation. app: handle_pallas_new_user, migration 001:105, corrected in 003 and 021:260.
>
> Verification. app: supabase/migrations/021_reconcile_live_state.sql section 5.

Sessions are JWT-based through Supabase Auth, and refresh tokens rotate on use.

> Control auth-session-jwt. Status: Implemented. A statement by a subprocessor. Pallas configures and relies on it; no Pallas code implements it and neither Pallas repository can demonstrate it.

Disclosure. Token rotation behaviour is a property of Supabase Auth. Pallas configures it and relies on it; no Pallas code implements it, and neither Pallas repository can demonstrate it independently.

Implementation. vendor: Supabase Auth refresh token rotation.

Verification. marketing: src/pages/trust.astro, Security posture, Session security.

No authentication state, entitlement, or quota is trusted from browser storage. Authorisation decisions are made server side.

Control auth-no-browser-storage-for-entitlements. Status: Implemented. Backed by a file in the pallas-app repository, verified read-only on 2026-08-30, not gated from the marketing repository.

Implementation. app: Row-Level Security policies on every pallas_ table, enumerated in the tenant-isolation rows below; app: pallas-app-api.

Verification. marketing: Rule sweep for browser storage API calls across src/.

Organisation membership carries one of four roles: org_admin, manager, contributor, viewer. Read is available to any member; write and update require contributor or above; delete requires org_admin.

Control access-org-roles. Status: Implemented. Backed by a file in the pallas-app repository, verified read-only on 2026-08-30, not gated from the marketing repository.

Implementation. app: pallas_organization_users.role, migration 001:30; app: supabase/migrations/020_storage_bucket_rls.sql, role model section.

Verification. app: pallas_user_org_role, migration 002:17 hardened 031:68.

An organisation cannot be left without an administrator. Removing or demoting the last org_admin is refused at the database layer.

Control access-last-admin-guard. Status: Implemented. Backed by a file in the pallas-app repository, verified read-only on 2026-08-30, not gated from the marketing repository.

Implementation. app: pallas_guard_last_admin, migration 010:106, rebuilt 025:162.

Verification. app: supabase/migrations/015_drop_duplicate_last_admin_trigger.sql.

When a user loses the privilege that let them invite others, their outstanding invitations are revoked.

Control access-privilege-loss-revokes-invites. Status: Implemented. Backed by a file in the pallas-app repository, verified read-only on 2026-08-30, not gated from the marketing repository.

Implementation. app: pallas_revoke_invites_on_privilege_loss, migration 029:266, rebuilt 040:260.

Verification. app: supabase/migrations/029_medium_security_hardening.sql.

Authenticated endpoints carry per-user rate limits. Endpoints that move or expose data fail closed when the limiter is unavailable; read-only endpoints degrade to load.

Control access-rate-limiting-authenticated. Status: Implemented. Backed by a file in the pallas-app repository, verified read-only on 2026-08-30, not gated from the marketing repository.

Disclosure. Cloudflare Workers KV is eventually consistent across colocations, so a KV-backed counter is a burst

guard rather than a hard ceiling: concurrent requests can each read the same value before any write lands. Where a hard ceiling was required, the limit is transactional in PostgreSQL instead, as with the 50 invitations per organisation per 24 hours enforced by pallas_org_invites_today. Pallas does not claim KV-backed limits are exact.

Implementation. app: pallas-app-api, checkRateLimit() over the RATE_LIMIT_KV namespace.

Verification. app: workers/pallas-app-api/wrangler.toml, rate limiting comment block.

Unauthenticated marketing endpoints are rate limited. The newsletter and resource gate endpoint carries a per-IP burst ceiling of 12 per 60 seconds and a per-email burst ceiling of 5 per 60 seconds, keyed on the normalised address; the anonymous checkout endpoint carries 5 per 60 seconds.

Control access-rate-limiting-anonymous. Status: Partial. Demonstrated in the pallas-marketing repository and checked by a release gate.

Disclosure. The Cloudflare native rate limiting binding supports a 10 second or 60 second period only. The email gate therefore carries per-IP and per-email burst ceilings and nothing else: there is no daily global signup ceiling on that endpoint and none is claimed. What bounds abuse there is the Turnstile gate plus the unique constraint on (email, source) in pallas_subscribers, which makes a repeat submission of the same pair produce no new row. A daily ceiling would require a Durable Object binding the operator has not provisioned.

Implementation. marketing: workers/pallas-email-gate/wrangler.toml, native SIGNUP_RATE_LIMIT binding, 12 per 60 seconds; marketing: workers/pallas-email-gate/wrangler.toml, native SIGNUP_EMAIL_RATE_LIMIT binding, 5 per 60 seconds, keyed on the trimmed and lowercased email; the Worker refuses with a 500 if either binding is absent; app: workers/pallas-checkout/wrangler.toml, native PURCHASE_LIMITER binding, 5 per 60 seconds, Worker returns 503 if the binding is absent.

Verification. marketing: tests/email-gate.test.ts.

Every unauthenticated write endpoint verifies a Cloudflare Turnstile token and refuses the request when the verification secret is unset, rather than running with the bot gate off.

Control access-turnstile-fails-closed. Status: Implemented. Demonstrated in the pallas-marketing repository and checked by a release gate.

Implementation. marketing: src/lib/turnstile.ts; marketing: pallas-scan-email and pallas-email-gate, both returning 500 when TURNSTILE_SECRET_KEY is unset.

Verification. marketing: tests/turnstile.test.ts; marketing: scripts/test-turnstile.mjs.

Pallas does not operate a documented background-screening programme, a security-awareness programme, or a recurring mandatory security or privacy training programme for personnel.

Control personnel-no-formal-screening-program. Status: Not implemented. A commitment the operator makes contractually. No code enforces it.

Disclosure. Pallas is operated by a small team and publishes no background-screening programme, no recurring security-awareness curriculum, and no annual training record. Personnel questions on a vendor questionnaire are answered as not formalised rather than answered yes from intent. What limits operator access instead is technical and is inventoried separately: OAuth-only sign-in with no password to share or leak, least-privilege service roles, and a tamper-evident audit trail over administrative actions that the operator cannot silently alter.

Verification. marketing: src/pages/trust.astro, Personnel screening and security training, status Not yet formalized.

Measures for ensuring data segregation and multi-tenancy isolation

Row-Level Security is enabled on every Pallas application table. Twenty-nine tables carry it in the migration file set.

Control tenant-rls-every-table. Status: Implemented. True of the migration file set. Live database state is not provable from source, and the operator pre-check that resolves it is named in the disclosure.

Disclosure. Twenty-nine tables carry RLS in the migration file set (twenty-four before migrations 057 and 059 added the digest-run and rule-override tables on 2026-09-16, twenty-six before migration 067 added the two crawl-state tables on 2026-09-17, and twenty-eight before migration 072 added the API-token table). Two of them, pallas_subscribers and pallas_subscriber_suppression, were created directly on the live database on 2026-08-30 and captured into migration 046 only afterwards, so any count taken before that migration was written disagrees with this one. The 2026-08-30 inventory pass recorded twenty-two on the live project. That difference has not been reconciled against the live database, because code in these repositories does not execute SQL. Before this claim is stated to a buyer with a number attached, the operator should run a live count of pg_tables joined to pg_class.relrowsecurity for tables matching pallas_%, and either correct this row or correct the 2026-08-30 inventory record. Until then the safe published form of this claim omits the count and states only that RLS is enabled on every application table.

Implementation. app: ENABLE ROW LEVEL SECURITY on 29 tables across migrations 001, 002, 005, 010, 017, 021, 024, 029, 034, 041, 046, 057, 059, 067, 072.

Verification. app: Search supabase/migrations/*.sql for ENABLE ROW LEVEL SECURITY and compare the count against CREATE TABLE.

Every tenant-scoped policy resolves membership through two SECURITY DEFINER helpers with a pinned search_path, rather than by re-entering the membership table under its own RLS.

Control tenant-org-scoping-helpers. Status: Implemented. Backed by a file in the pallas-app repository, verified read-only on 2026-08-30, not gated from the marketing repository.

Implementation. app: pallas_user_has_org_access, migration 002:8, hardened in 031:54; app: pallas_user_org_role, migration 002:17, hardened in 031:68.

Verification. app: supabase/migrations/031_low_severity_hardening.sql.

The evidence, source-files, and reports Storage buckets are private and carry per-organisation RLS policies on storage.objects, with read, write, update, and delete scoped to organisation role.

Control tenant-storage-per-org. Status: Implemented. Backed by a file in the pallas-app repository, verified read-only on 2026-08-30, not gated from the marketing repository.

Implementation. app: supabase/migrations/020_storage_bucket_rls.sql; app: pallas_storage_org_access, migration 020:50.

Verification. app: supabase/migrations/020_storage_bucket_rls.sql header.

Server-side operator functions run under service credentials that bypass Row-Level Security by necessity. Their scope is limited, they are versioned in source, and their actions are covered by the audit trail.

Control tenant-service-role-bypass-disclosed. Status: Implemented. Backed by a file in the pallas-app repository, verified read-only on 2026-08-30, not gated from the marketing repository.

Disclosure. Service-role credentials bypass Row-Level Security. This is a property of PostgreSQL and Supabase, not a Pallas design choice, and it means tenant isolation for service-role code paths rests on the correctness of those code paths rather than on the database refusing them. The mitigating controls are that the paths are few, versioned, and audit-logged, not that they are constrained by RLS.

Implementation. app: pallas-app-api; app: supabase/functions/enforce-retention/index.ts.

Verification. marketing: src/pages/trust.astro, Security posture, Tenant isolation.

Measures of pseudonymisation and encryption of personal data

Data is encrypted at rest with AES-256 through Supabase-managed infrastructure.

Control encryption-at-rest. Status: Implemented. A statement by a subprocessor. Pallas configures and relies on it; no Pallas code implements it and neither Pallas repository can demonstrate it.

Disclosure. Encryption at rest is provided and attested by Supabase. No Pallas code implements it and neither Pallas repository can demonstrate it. A buyer who requires independent evidence should request the Supabase SOC 2 Type II report rather than a Pallas assertion.

Implementation. vendor: Supabase managed PostgreSQL and Storage encryption at rest.

Verification. vendor: Supabase SOC 2 Type II report, available to the operator under NDA.

All connections are TLS 1.3, enforced by Cloudflare and Supabase.

Control encryption-in-transit. Status: Implemented. A statement by a subprocessor. Pallas configures and relies on it; no Pallas code implements it and neither Pallas repository can demonstrate it.

Disclosure. TLS termination and version are properties of Cloudflare and Supabase. What this repository demonstrates is the header set and the build gate that refuses to ship without it, not the negotiated cipher.

Implementation. vendor: Cloudflare edge TLS and Supabase connection TLS; marketing: public/_headers.

Verification. marketing: scripts/csp-hashes.mjs.

Production secrets are held in the platform secret store and never in either repository. Worker configuration files carry variable names only.

Control encryption-no-secrets-in-repo. Status: Implemented. Demonstrated in the pallas-marketing repository and checked by a release gate.

Disclosure. Two Cloudflare KV namespace identifiers are committed, at workers/pallas-scan-email/wrangler.toml and in the pallas-app Workers. A KV namespace id is an identifier rather than a credential: reaching the namespace still requires authenticated access to the Cloudflare account. This is recorded as a deliberate decision, with the note that the ids should move to deploy-time values if either repository is shared with a buyer, an auditor, or a contractor.

Implementation. marketing: workers/pallas-scan-email/.dev.vars.example and workers/pallas-email-gate/.dev.vars.example; marketing: .gitignore.

Verification. marketing: Rule sweep for key, token, price identifier, and webhook secret strings.

Finding comments, evidence descriptions and code snippets, and evidence files are encrypted at rest by the database and storage provider under a key the provider holds, and in transit by TLS. They are

not client-side encrypted: every member of the organization can read them, they are included in the organization's data export, and the Processor can read them as any SaaS operator can.

Control encryption-member-prose-provider-held-key. Status: Implemented. Backed by a file in the pallas-app repository, verified read-only on 2026-08-30, not gated from the marketing repository.

Implementation. app: docs/DATABASE_ENFORCEMENT.md:86, What is and is not encrypted; app: src/audit/auditMetadataKeys.ts, AUDIT_METADATA_KEYS.

Verification. app: tests/audit/auditMetadataKeys.test.ts.

Measures for ensuring events logging and accountability

Every audit event appends an entry to a SHA-256 hash chain. Each entry is hashed together with the previous entry hash, so modification, deletion, or reordering of historical events breaks the chain and is detectable.

Control audit-sha256-ledger. Status: Implemented. Observed in the production database by catalog query on 2026-09-16 and recorded in the pallas-app deployed-objects manifest. The migration that created the object is held out of the repository as a trade secret, so the observation, not a file, is the evidence; objects are cited by name only.

Implementation. app: supabase/migrations/041_audit_tamper_evidence.sql; app: hashing helpers inside migration 041; row_hash and prev_row_hash columns on pallas_audit_events; app: insert trigger on pallas_audit_events, migration 041.

Verification. app: pallas_verify_audit_chain, migration 041; app: pallas_verify_audit_row, migration 041.

The ledger table is append-only in the strong sense: Row-Level Security is enabled with zero policies, and INSERT, UPDATE, DELETE, and TRUNCATE are revoked from every role including service_role. Only SECURITY DEFINER trigger functions can write to it.

Control audit-ledger-append-only. Status: Implemented. Observed in the production database by catalog query on 2026-09-16 and recorded in the pallas-app deployed-objects manifest. The migration that created the object is held out of the repository as a trade secret, so the observation, not a file, is the evidence; objects are cited by name only.

Implementation. app: pallas_audit_chain, created by migration 041 with Row-Level Security enabled; app: SECURITY DEFINER trigger functions inside migration 041.

Verification. app: pallas_audit_chain, migration 041; the table answers permission denied to the anon role through the API.

Lawful removal of an audit row, whether under a retention policy or under GDPR Article 17, appends a redaction entry recording the sequence number, the hash before, the hash after, the reason, and the timestamp. The ledger outlives the row it describes, so a reviewer can distinguish a lawful purge from a concealment.

Control audit-lawful-redaction-recorded. Status: Implemented. Observed in the production database by catalog query on 2026-09-16 and recorded in the pallas-app deployed-objects manifest. The migration that created the object is held out of the repository as a trade secret, so the observation, not a file, is the evidence; objects are cited by name only.

Disclosure. The delete allowlist is a declaration, not an authorisation control. Anything holding service_role and a SQL connection can set the redaction reason. The control is not that setting it is hard; the control is that setting it does not

buy silence, because the redaction entry lands in a table that role cannot subsequently edit or truncate. An audit row can be deleted. It cannot be deleted quietly. This distinction is stated here because a reviewer will press on it, and a document that presented the flag as an access control would be overclaiming.

Implementation. app: pallas_audit_delete_reason_allowed, migration 041; the redaction hash is computed inside the same migration; app: update and delete triggers on pallas_audit_events, migration 041.

Verification. app: migration 041, which carries the update and delete allowlists.

A daily anchor snapshot of the chain tip is taken at 06:00 UTC and retained. Any anchor can be exported for independent verification on request.

Control audit-daily-anchors. Status: Partial. True of the migration file set. Live database state is not provable from source, and the operator pre-check that resolves it is named in the disclosure.

Disclosure. Anchor creation is automated. External publication of anchors is an operator action and not an automated feed, so Pallas does not claim an automated external anchoring service. Until external publication begins, an anchor proves the chain was in a given state at a given time only to a party who trusts the Pallas database clock. Additionally, the cron job schedules itself inside a DO block that catches its own exception: if pg_cron was not enabled at migration time, the job was never created and the migration still reported success. Whether the job exists on the live database is an operator check against cron.job, not a fact this repository can assert.

Implementation. app: pg_cron job at '0 6 * * *', scheduled by migration 041; app: pallas_create_audit_anchor, pallas_verify_audit_anchors, pallas_list_audit_anchors, pallas_mark_audit_anchor_exported, migration 041; app: pallas-app-api, POST /audit-chain/anchor, /anchors, /verify-anchors, /anchor-exported.

Verification. app: pallas_verify_audit_anchors, migration 041.

Attempts to modify or delete an audit event are refused with specific error codes: PA030 for update, PA031 for delete, PA032 for forged chain metadata on insert.

Control audit-error-codes. Status: Implemented. Observed in the production database by catalog query on 2026-09-16 and recorded in the pallas-app deployed-objects manifest. The migration that created the object is held out of the repository as a trade secret, so the observation, not a file, is the evidence; objects are cited by name only.

Implementation. app: migration 041, immutability triggers on pallas_audit_events.

Verification. marketing: src/pages/trust.astro, Security posture, Audit trail.

Audit rows carry a seven-year (2555 day) retention floor enforced by a database CHECK constraint. An administrator cannot configure a shorter audit retention than the regulatory minimum.

Control audit-seven-year-floor. Status: Implemented. Backed by a file in the pallas-app repository, verified read-only on 2026-08-30, not gated from the marketing repository.

Implementation. app: chk_audit_log_retention_min_2555 on pallas_retention_policies, migration 016:34; app: pallas_apply_retention_policies, migration 042.

Verification. app: supabase/migrations/016_audit_retention_floor_check.sql.

Audit action names are validated against a registry table rather than accepted as free text, so an unrecognised action cannot be written.

Control audit-action-registry. Status: Implemented. Backed by a file in the pallas-app repository, verified read-only on

2026-08-30, not gated from the marketing repository.

Implementation. app: pallas_audit_action_registry, created migration 024:143, RLS enabled 024:164; app: pallas_assert_audit_action, migration 024:431.

Verification. app: supabase/migrations/043_audit_action_registry_documentation.sql.

Audit attribution survives user erasure. Actor name and email are snapshotted onto the audit row at write time, so severing the identity link under Article 17 does not orphan the audit trail.

Control audit-actor-attribution-survives-erasure. Status: Implemented. Backed by a file in the pallas-app repository, verified read-only on 2026-08-30, not gated from the marketing repository.

Implementation. app: pallas_actor_snapshot 024:379, pallas_fill_audit_actor_snapshot 040:195; app: supabase/migrations/040_user_fk_set_null.sql.

Verification. app: migration 041, whose update allowlist requires actor_name_snapshot and actor_email_snapshot unchanged.

Measures of system, application, and process security

The public scan tool validates every submitted URL against a hostname and IP-literal denylist before fetching it, blocking loopback, link-local, unique-local, IPv4-mapped private addresses, cloud metadata endpoints, and the private, CGNAT, and multicast IPv4 ranges.

Control appsec-ssrf-guard. Status: Implemented. Demonstrated in the pallas-marketing repository and checked by a release gate.

Implementation. marketing: src/lib/ssrf-guard.ts; app: workers/pallas-cors-proxy/src/index.ts, isBlockedHost and isBlockedIpv4.

Verification. marketing: tests/ssrf-guard.test.ts.

The scan proxy cannot fully defend against DNS rebinding. This is disclosed publicly rather than omitted.

Control appsec-dns-rebinding-limitation. Status: Partial. Backed by a file in the pallas-app repository, verified read-only on 2026-08-30, not gated from the marketing repository.

Disclosure. A Cloudflare Worker resolves DNS inside fetch(). The runtime exposes no hook to read the address a hostname resolved to and no way to pin a connection to an already-validated address, so there is no point at which the Worker can compare the address it approved against the address it connected to. This is a property of the runtime rather than a gap in the guard. What limits the blast radius is that the Worker egresses from Cloudflare edge to the public internet: it is not inside a private network, no Pallas internal service is reachable from it, and Workers have no cloud instance metadata service. Mitigations in place are the denylist, a 10 MB response cap enforced against both the declared Content-Length and the bytes actually received, and rendering of fetched markup on a dedicated origin with empty storage pinned shut by Content-Security-Policy. A full fix requires a resolving egress proxy, which is new infrastructure rather than an edit to this Worker.

Implementation. app: workers/pallas-cors-proxy/src/index.ts:56; marketing: src/pages/trust.astro:388, Known limitations section.

Verification. app: docs/OPERATOR_ACTIONS.md section 1.1.

Fetched third-party responses are capped at 10 MB, enforced against the declared Content-Length and again against the bytes actually received.

Control appsec-response-cap. Status: Implemented. Demonstrated in the pallas-marketing repository and checked by a release gate.

Implementation. marketing: src/lib/response-cap.ts; app: workers/pallas-cors-proxy/src/index.ts:261, MAX_RESPONSE_BYTES.

Verification. marketing: tests/response-cap.test.ts.

Scanned third-party markup renders on a dedicated origin with nothing in its storage, pinned shut with Content-Security-Policy, so retrieved markup cannot reach the application session, cookies, or IndexedDB.

Control appsec-sandboxed-rendering. Status: Implemented. Backed by a file in the pallas-app repository, verified read-only on 2026-08-30, not gated from the marketing repository.

Implementation. app: workers/pallas-scanner-sandbox/src/index.ts.

Verification. app: docs/OPERATOR_ACTIONS.md section 1.1, mitigations table.

Untrusted content is escaped before it reaches HTML or email. The only place untrusted input meets raw HTML on the marketing site is JSON-LD, fed exclusively by a serializer that escapes the closing angle bracket and the U+2028 and U+2029 line separators.

Control appsec-output-escaping. Status: Implemented. Demonstrated in the pallas-marketing repository and checked by a release gate.

Implementation. marketing: src/lib/jsonld.ts, serializeJsonLd(); marketing: src/lib/html-escape.ts; marketing: src/lib/safe-url.ts.

Verification. marketing: tests/safe-url.test.ts and tests/scan-report.test.ts; marketing: SECURITY_ADVISORY_TRIAGE.md, section titled The one place untrusted input meets HTML.

The build command itself runs every gate: a type check, the typography and published-document freshness checks, the six written-claim verification gates, the unit test suite over the security and validation code, the build, an automated accessibility test against every built page, a Turnstile configuration check against the built artifact, and a sweep of the built output for forbidden claims. The hosting platform runs that command on every push, so a non-zero exit at any step fails the build and nothing deploys; the failing guards remove the dist directory so a failed build leaves nothing to deploy.

Control appsec-release-gate-fails-closed. Status: Implemented. Demonstrated in the pallas-marketing repository and checked by a release gate.

Implementation. marketing: package.json, the build script.

Verification. marketing: scripts/test-a11y.mjs, scripts/test-turnstile.mjs, scripts/check-dashes.mjs, scripts/verify-doc-artifact-freshness.mjs.

Measures for ensuring limited data retention

Retention is configured per organisation, with defaults of 365 days for scan data, 7 days for uploaded source files, 730 days for reports, and 2555 days (seven years) for the audit log.

Control retention-per-org-policies. Status: Implemented. Backed by a file in the pallas-app repository, verified read-only on 2026-08-30, not gated from the marketing repository.

Implementation. app: pallas_retention_policies, migration 002:374.

Verification. app: uq_pallas_retention_org, migration 002:385.

A scheduled job applies retention policies daily at 03:00 UTC for every organisation with automatic deletion enabled.

Control retention-daily-sweep. Status: Implemented. True of the migration file set. Live database state is not provable from source, and the operator pre-check that resolves it is named in the disclosure.

Disclosure. The job is scheduled by a DO block that catches its own exception, so a database on which pg_cron was not enabled at migration time has no job and the migration still reported success. Whether the job exists and is running on the live database is an operator check against the cron.job and cron.job_run_details tables. This repository can show what was intended to be scheduled; it cannot show what is scheduled.

Implementation. app: pallas-daily-retention, '0 3 * * *', scheduled at migration 021:238; app: pallas_apply_retention_policies, migration 021:197, rebuilt 029:629, migration 041, and migration 042.

Verification. app: supabase/migrations/042_restore_retention_sweeps_and_gaps.sql.

Archived audit events past their retention window are purged nightly at 04:00 UTC, and each purge run is logged.

Control retention-audit-purge. Status: Implemented. True of the migration file set. Live database state is not provable from source, and the operator pre-check that resolves it is named in the disclosure.

Disclosure. Scheduled by the same self-catching DO block pattern as the 03:00 UTC sweep. Existence of the live job is an operator check against cron.job.

Implementation. app: pallas_nightly_retention_purge, '0 4 * * *', scheduled at migration 034:581; app: pallas_purge_expired_retained_audit_events, migration 034:460; app: pallas_retention_purge_log, migration 034:405, RLS enabled 034:416.

Verification. app: supabase/migrations/034_enforce_finding_limit_and_retention_purge.sql section 9.

Uploaded source files are purged from Storage daily at 05:00 UTC by a Supabase Edge Function invoked from the database.

Control retention-source-file-purge. Status: Partial. True of the migration file set. Live database state is not provable from source, and the operator pre-check that resolves it is named in the disclosure.

Disclosure. This job does no work unless two database settings are present: app.settings.functions_base_url and app.settings.cron_secret. When either is missing the job raises a warning and returns, so source files are NOT purged and nothing fails loudly. Migration 035:619 states this in the job body. The operator must confirm both settings are set on the live database before this control is claimed to a buyer. Separately, the 2026-08-30 inventory record describes

this credential as being held in Supabase Vault under the name pallas_enforce_retention_bearer. No file in either repository references Vault or that name; the mechanism on disk is a Supabase Edge Function secret named CRON_SECRET plus a database setting named app.settings.cron_secret. The inventory description and the file set disagree, and the file set is what these repositories can show.

Implementation. app: pallas_daily_source_file_retention, '0 5 * * *', scheduled at migration 035:609; app: supabase/functions/enforce-retention/index.ts.

Verification. app: supabase/functions/enforce-retention/index.ts:239 to :252.

Retention settings cause actual deletion rather than being stored as a preference. The sweep issues DELETE statements against the tables it governs.

Control retention-deletion-actually-deletes. Status: Implemented. Backed by a file in the pallas-app repository, verified read-only on 2026-08-30, not gated from the marketing repository.

Implementation. app: pallas_apply_retention_policies, migration 042.

Verification. app: migration 041, which enumerates the three code paths that lawfully remove audit rows.

Measures for ensuring the ability to restore availability and access

Application data is held in Supabase managed PostgreSQL with provider-operated automated backups and point-in-time recovery. The recoverable window is set by the provider tier.

Control backup-provider-operated. Status: Implemented. A statement by a subprocessor. Pallas configures and relies on it; no Pallas code implements it and neither Pallas repository can demonstrate it.

Disclosure. Pallas runs no backup schedule of its own. The backup posture is entirely the Supabase provider tier posture, and the operator has not customised it.

Implementation. vendor: Supabase automated backups and point-in-time recovery.

Verification. marketing: src/pages/trust.astro, Backup and disaster recovery questionnaire answer.

Pallas does not publish a recovery time objective or a recovery point objective.

Control backup-no-published-rto-rpo. Status: Not implemented. A commitment the operator makes contractually. No code enforces it.

Disclosure. No RTO or RPO is published, because a number that cannot be evidenced from a restore test is worth nothing on a questionnaire. No restore test has been performed. A negotiated RTO and RPO with service credits is an Enterprise onboarding item. Any questionnaire field asking for an RTO or RPO must be answered as not published rather than filled with an estimate.

Verification. marketing: src/pages/trust.astro:126.

Pallas has not performed a documented restore test.

Control backup-no-restore-test. Status: Not implemented. A commitment the operator makes contractually. No code enforces it.

Disclosure. No restore test has been carried out, so the recoverability of the backups is a provider assertion rather than a demonstrated property. This is a genuine gap and it is listed as one. A buyer for whom tested recoverability is a

control requirement should treat this as an open item, and the operator should schedule a restore test into a non-production project as the remediation.

Pallas does not maintain a business continuity plan or a disaster recovery plan that is documented, assigned to a named owner, and exercised annually.

Control continuity-no-tested-bcp-drp. Status: Not implemented. A commitment the operator makes contractually. No code enforces it.

Disclosure. There is no annually tested BCP or DRP with a named owner. Continuity rests on the managed platform underneath: Supabase provider backups with point-in-time recovery, and Cloudflare for edge and Pages hosting. Because no restore test has been performed, recoverability is a provider assertion rather than a demonstrated property. A questionnaire item asking for a documented and tested plan is answered no, not answered yes from the existence of provider backups.

Verification. marketing: src/pages/trust.astro, Backup and disaster recovery questionnaire answer.

Measures for certification, assurance, and process for regularly testing and evaluating

Dependency advisories are triaged by whether a request path actually reaches the affected code, and the triage is recorded in version control with a review date and the reasoning rather than the conclusion alone.

Control vuln-advisory-triage-artifact. Status: Implemented. Demonstrated in the pallas-marketing repository and checked by a release gate.

Disclosure. Three advisories are currently open in npm audit, reported as one low and two high. All ten individual advisories were assessed as unreachable in this build configuration, on the basis that the site is a fully static build with no server runtime, no client hydration, and no build-time image processing. The advisories remain open rather than fixed: the proposed remediation is a two major version Astro upgrade that npm audit labels breaking, and that upgrade is scheduled on its own timeline rather than taken as an emergency for unreachable findings. A buyer running npm audit against this repository will see the counts, and this file is the answer to what they mean.

Implementation. marketing: SECURITY_ADVISORY_TRIAGE.md.

Verification. marketing: SECURITY_ADVISORY_TRIAGE.md, section titled What would invalidate this triage.

Pallas has not commissioned an independent penetration test.

Control vuln-no-penetration-test. Status: Not implemented. A commitment the operator makes contractually. No code enforces it.

Disclosure. No third party penetration test has been performed and no report exists. Security review to date has been internal, through repeated structured audits recorded in this repository. Any questionnaire field asking for the date of the last penetration test or for a report must be answered as none performed. This is a real gap for institutional buyers and it should be presented as one rather than deflected to the internal audit history.

Verification. marketing: src/pages/trust.astro, questionnaire answers section.

Pallas holds no SOC 2, ISO 27001, or other independent security certification.

Control vuln-no-independent-certification. Status: Not implemented. A commitment the operator makes contractually. No code enforces it.

Disclosure. Pallas holds no certification of its own. Certifications named anywhere in Pallas materials belong to subprocessors. Where a buyer requires a converted assurance rather than an assertion, the mechanism is a contractual term in the Institutional Terms of Service, the signable agreement, not a certificate Pallas can produce. There is no separate master services agreement.

Verification. marketing: src/pages/trust.astro, Compliance frameworks, Planned.

Every change reaches production through version control, and the build fails closed rather than degrading.

Control vuln-version-control-and-review. Status: Implemented. Demonstrated in the pallas-marketing repository and checked by a release gate.

Disclosure. Pallas is built and operated by a single operator, so there is no second-party code review before merge and no segregation of duties between the person who writes a change and the person who deploys it. The compensating control is the automated build chain, which the hosting platform runs on every push, is identical for every change, and cannot be selectively skipped. Any questionnaire asking about mandatory peer review or segregation of duties must be answered no.

Implementation. marketing: package.json build script; marketing: scripts/csp-hashes.mjs and scripts/test-turnstile.mjs.

Verification. marketing: src/pages/trust.astro:121.

Deployment to Cloudflare Pages and to every Worker is a deliberate manual operator step, not an automatic consequence of a merge.

Control vuln-deploys-are-manual. Status: Implemented. Backed by a file in the pallas-app repository, verified read-only on 2026-08-30, not gated from the marketing repository.

Disclosure. Manual deployment is a deliberate choice rather than a missing pipeline: it means a malformed build cannot ship silently. It also means deployment timing depends on operator availability, which a buyer assessing change velocity or emergency patch turnaround should know.

Implementation. app: docs/OPERATOR_ACTIONS.md section 2, standing operator steps.

Verification. app: docs/OPERATOR_ACTIONS.md, items 1 through 4.

Measures for internal IT and security governance and management, and incident handling

Pallas notifies affected customers without undue delay and in any event within 72 hours of becoming aware of a breach affecting their data. The clock starts on awareness, not on confirmation.

Control incident-72-hour-notification. Status: Implemented. A commitment the operator makes contractually. No code enforces it.

Disclosure. This is a contractual commitment. No technical control enforces it and no artifact in either repository can demonstrate it has been met, because no breach has occurred. A buyer should treat it as a term to be captured in the Data Processing Agreement rather than as a verified capability.

Implementation. marketing: src/pages/trust.astro, Breach commitments, Customer notification; marketing: src/pages/legal/dpa.astro.

Authority notification follows the jurisdiction: Ireland DPC, UK ICO, and EU supervisory authorities within 72 hours; Canada OPC under PIPEDA; Australia OAIC under the Notifiable Data Breaches scheme.

Control incident-authority-notification. Status: Implemented. A commitment the operator makes contractually. No code enforces it.

Disclosure. A contractual and regulatory commitment rather than a technical control. Pallas has not been required to make such a notification, so there is no track record to evidence.

Implementation. marketing: src/pages/trust.astro, Breach commitments, Authority notification.

Worker observability and logging are enabled on every deployed Worker so that failures surface rather than passing silently.

Control incident-detection-monitoring. Status: Partial. Demonstrated in the pallas-marketing repository and checked by a release gate.

Disclosure. Observability is enabled and logs are collected. There is no security information and event management system, no alerting pipeline, no on-call rotation, and no documented incident response runbook with named roles. Detection today means an operator reading the Cloudflare dashboard. Any questionnaire asking about 24 by 7 monitoring, SIEM, or a tested incident response plan must be answered no. Pallas is operated by a single operator and a procurement document that implied a staffed security operations centre would be false.

Implementation. marketing: workers/pallas-scan-email/wrangler.toml and workers/pallas-email-gate/wrangler.toml, observability and observability.logs enabled; app: All six pallas-app Workers, observability enabled in wrangler.toml.

Verification. marketing: workers/pallas-email-gate/wrangler.toml observability comment.

A full technical postmortem is provided to affected customers within 30 days.

Control incident-post-incident-report. Status: Implemented. A commitment the operator makes contractually. No code enforces it.

Implementation. marketing: src/pages/trust.astro, Breach commitments, Post-incident report.

A subprocessor breach triggers the same 72 hour notification cascade, from the subprocessor to Pallas to the customer.

Control incident-subprocessor-cascade. Status: Partial. A commitment the operator makes contractually. No code enforces it.

Disclosure. The Pallas leg of this cascade is a commitment Pallas controls. The subprocessor leg depends on each provider notifying Pallas, which is governed by that provider terms and is outside Pallas control. The end-to-end 72 hours is therefore contingent on subprocessor performance, and a buyer requiring a guaranteed end-to-end window should raise it during Enterprise contracting rather than rely on this statement.

Implementation. marketing: src/pages/trust.astro, Breach commitments.

Pallas does not publish a cyber liability insurance policy or a certificate of cover.

Control insurance-no-published-cover. Status: Not implemented. A commitment the operator makes contractually. No code enforces it.

Disclosure. No cyber liability certificate is published. A questionnaire field asking for evidence of cover is answered as not published rather than left blank or answered from intent, and where a contract requires evidence of cover the matter is addressed in the agreement during procurement.

Verification. marketing: src/pages/trust.astro, Cyber liability insurance, status Not yet formalized.

Measures to be taken by sub-processors

The sub-processors listed in Annex III are engaged under written agreements imposing data protection obligations equivalent to those in these Clauses, as Clause 9(b) requires. Pallas relies on the certifications each sub-processor publishes and does not independently audit them.

The full subprocessor list is published, with each provider purpose, data categories, processing location, and published certifications.

Control subprocessors-published-list. Status: Implemented. Demonstrated in the pallas-marketing repository and checked by a release gate.

Disclosure. The 2026-08-30 inventory record names four subprocessors in use: Supabase, Cloudflare, Stripe, and Resend. The published page carries six operative entries, adding Google and Microsoft as OAuth identity providers. Both are accurate about different things: Google and Microsoft receive an authentication assertion at sign-in and store no Pallas customer data. Procurement artifacts should carry all six operative entries, because a buyer assessing identity provider dependency needs to see the two that the four-entry description omits.

Implementation. marketing: src/pages/legal/subprocessors.astro.

Verification. marketing: src/pages/trust.astro, Sub-processors section.

A new subprocessor is published with 30 days advance notice before it processes any customer data.

Control subprocessors-change-notice. Status: Implemented. A commitment the operator makes contractually. No code enforces it.

Disclosure. This is a contractual commitment by the operator, not a technical control. Nothing in either repository enforces the notice period, and no new subprocessor has yet been added under it.

Implementation. marketing: src/pages/legal/subprocessors.astro, Change Notification section.

Certifications listed against each subprocessor are those published by that provider.

Control subprocessors-certifications-are-theirs. Status: Implemented. A statement by a subprocessor. Pallas configures and relies on it; no Pallas code implements it and neither Pallas repository can demonstrate it.

Disclosure. Pallas holds no SOC 2, ISO 27001, or PCI DSS certification of its own. Every certification named on the subprocessor list belongs to the named provider and covers that provider infrastructure, not the Pallas application built on top of it. A procurement document must never present a subprocessor certification in a way that could be read as a Pallas certification. This is the single most consequential misreading available in this inventory, so the distinction is stated wherever the certifications appear.

Implementation. marketing: src/pages/legal/subprocessors.astro.

Pallas operates no data centre, server cage, office server room, or other facility in which institutional data is held. Physical and environmental security for every system that holds institutional data

belongs to Supabase and Cloudflare.

Control physical-security-subprocessor-operated. Status: Implemented. A statement by a subprocessor. Pallas configures and relies on it; no Pallas code implements it and neither Pallas repository can demonstrate it.

Disclosure. Every physical-security control a questionnaire asks about, including staffed facilities, cages, enclosing barriers, redundant and tested power, cooling, fire suppression, and carrier diversity, belongs to Supabase or Cloudflare. Pallas can neither demonstrate nor test any of them, and does not inherit them as its own controls. Answers to physical-security questions state reliance and name the provider. A buyer who needs evidence should read the provider audit reports; a Pallas assertion is not evidence of a provider control.

Implementation. vendor: Supabase and Cloudflare published data centre physical and environmental security programmes.

Verification. marketing: src/pages/trust.astro, subprocessor list with per-provider processing locations.

Pallas operates no network perimeter, no host, and no network monitoring of its own. Edge filtering, DDoS mitigation, and TLS termination are Cloudflare functions, and the database network boundary is operated by Supabase.

Control network-perimeter-subprocessor-operated. Status: Implemented. A statement by a subprocessor. Pallas configures and relies on it; no Pallas code implements it and neither Pallas repository can demonstrate it.

Disclosure. Pallas runs no firewall of its own, no network intrusion detection or prevention system, and no host-based agent, because it operates no hosts. Stateful filtering, DDoS mitigation, and TLS termination happen at the Cloudflare edge and are answered as provider-operated. Intrusion detection, intrusion prevention tuned by Pallas, next-generation persistent threat monitoring, and 24x7 intrusion monitoring are answered no: no such capability is operated by Pallas or configured by Pallas at a provider. A buyer requiring a monitored perimeter under vendor control, or a staffed security operations centre, should treat this as an open item.

Implementation. vendor: Cloudflare edge network, web application firewall and DDoS mitigation; Supabase managed database network boundary.

Verification. marketing: workers/, whose Workers execute on the Cloudflare edge rather than on any Pallas-operated host.

8. Annex III. List of sub-processors

Clause 9 of Module Two requires the data exporter's authorisation for sub-processors and, under OPTION 2 as selected in section 3, a list of the sub-processors the general authorisation covers.

The authoritative and current list is published at pallas.lonia.ai/legal/subprocessors, which carries the full data categories, processing locations, and published certifications for each provider. The list below is that list as at the date on the title page of this document. Where the two differ, the published page is the more recent and governs, and the thirty-day advance notice commitment in section 3 applies to any addition.

Sub-processors processing customer personal data.

- Cloudflare. Hosting, content delivery, and edge security: Workers, Pages, R2 object storage, and Turnstile challenge protection. Processing location: United States, with global edge distribution.

- Supabase. Application data: the PostgreSQL database, authentication, and object storage. Processing location: United States by default.
- Stripe. Payments and invoicing: billing, tax calculation, and the customer billing portal. Processing location: United States.
- Resend. Transactional email: invitation emails and data-request notifications. Processing location: United States.
- Google. OAuth sign-in provider. Processes the authentication assertion (name, email address, profile photograph) at sign-in. No customer personal data is stored with Google by Pallas.
- Microsoft. OAuth sign-in provider (Azure AD). Processes the authentication assertion (name, email address) at sign-in. No customer personal data is stored with Microsoft by Pallas.

Processing location. All sub-processors above process in the locations stated; none processes customer personal data in the European Union.

Processing takes place in the United States only. No European Union hosting exists and none is offered.

> Control data-location-eu-option. Status: Not implemented. A commitment the operator makes contractually. No code enforces it.
>
> Disclosure. No customer data is processed in the European Union and no EU infrastructure subprocessor is engaged or planned. Any procurement document, questionnaire response, or sales conversation must present United States processing as the only option and must not present EU hosting as available, on request, or on a roadmap.
>
> Implementation. marketing: src/pages/trust.astro, Data residency options; marketing: src/pages/legal/subprocessors.astro, six operative entries and no planned entry.

9. Execution

These Clauses take effect on signature by both parties. Annex I.A is completed with the data exporter's details on execution.

Data exporter: _____

Name and position: _____

Date: _____

Data importer: Lonia AI

Name and position: _____

Date: _____

The signature lines above are reproduced so that a reviewer can see the shape of the instrument they would be asked to sign. This render is informational and must not be executed: the data importer party block above names a trade name, and a trade name cannot execute a contract on its own. Clauses executed by a party that cannot be bound by them are not an Article 46 safeguard at all, which is why this render says so twice. Request the signable render at support@lonia.ai.

Appendix A. Controls cited

This document cites 61 of the 84 rows in the Pallas control inventory. Each is listed below with the status and evidence basis it carried at the 2026-08-30 inventory pass. A row absent from this list is not claimed by this document.

- **auth-oauth-only** (Authentication). Implemented.
- **auth-profile-trigger-fail-safe** (Authentication). Implemented.
- **auth-session-jwt** (Authentication). Implemented.
- **auth-no-browser-storage-for-entitlements** (Authentication). Implemented.
- **tenant-rls-every-table** (Multi-tenancy isolation). Implemented.
- **tenant-org-scoping-helpers** (Multi-tenancy isolation). Implemented.
- **tenant-storage-per-org** (Multi-tenancy isolation). Implemented.
- **tenant-service-role-bypass-disclosed** (Multi-tenancy isolation). Implemented.
- **audit-sha256-ledger** (Tamper-evident audit chain). Implemented.
- **audit-ledger-append-only** (Tamper-evident audit chain). Implemented.
- **audit-lawful-redaction-recorded** (Tamper-evident audit chain). Implemented.
- **audit-daily-anchors** (Tamper-evident audit chain). Partial.
- **audit-error-codes** (Tamper-evident audit chain). Implemented.
- **audit-seven-year-floor** (Tamper-evident audit chain). Implemented.
- **audit-action-registry** (Tamper-evident audit chain). Implemented.
- **audit-actor-attribution-survives-erasure** (Tamper-evident audit chain). Implemented.
- **retention-per-org-policies** (Retention and deletion). Implemented.
- **retention-daily-sweep** (Retention and deletion). Implemented.
- **retention-audit-purge** (Retention and deletion). Implemented.
- **retention-source-file-purge** (Retention and deletion). Partial.
- **retention-deletion-actually-deletes** (Retention and deletion). Implemented.
- **encryption-at-rest** (Encryption). Implemented.
- **encryption-in-transit** (Encryption). Implemented.
- **encryption-no-secrets-in-repo** (Encryption). Implemented.
- **encryption-member-prose-provider-held-key** (Encryption). Implemented.
- **access-org-roles** (Access control). Implemented.
- **access-last-admin-guard** (Access control). Implemented.
- **access-privilege-loss-revokes-invites** (Access control). Implemented.
- **access-rate-limiting-authenticated** (Access control). Implemented.
- **access-rate-limiting-anonymous** (Access control). Partial.
- **access-turnstile-fails-closed** (Access control). Implemented.
- **personnel-no-formal-screening-program** (Access control). Not implemented.
- **appsec-ssrf-guard** (Application security). Implemented.
- **appsec-dns-rebinding-limitation** (Application security). Partial.

- **appsec-response-cap** (Application security). Implemented.
- **appsec-sandboxed-rendering** (Application security). Implemented.
- **appsec-output-escaping** (Application security). Implemented.
- **appsec-release-gate-fails-closed** (Application security). Implemented.
- **data-classes-enumerated** (Data classes and processing location). Implemented.
- **data-location-default-us** (Data classes and processing location). Implemented.
- **data-location-eu-option** (Data classes and processing location). Not implemented.
- **subprocessors-published-list** (Subprocessors). Implemented.
- **subprocessors-change-notice** (Subprocessors). Implemented.
- **subprocessors-certifications-are-theirs** (Subprocessors). Implemented.
- **physical-security-subprocessor-operated** (Subprocessors). Implemented.
- **network-perimeter-subprocessor-operated** (Subprocessors). Implemented.
- **incident-72-hour-notification** (Incident response). Implemented.
- **incident-authority-notification** (Incident response). Implemented.
- **incident-detection-monitoring** (Incident response). Partial.
- **incident-post-incident-report** (Incident response). Implemented.
- **incident-subprocessor-cascade** (Incident response). Partial.
- **insurance-no-published-cover** (Incident response). Not implemented.
- **backup-provider-operated** (Backup and recovery). Implemented.
- **backup-no-published-rto-rpo** (Backup and recovery). Not implemented.
- **backup-no-restore-test** (Backup and recovery). Not implemented.
- **continuity-no-tested-bcp-drp** (Backup and recovery). Not implemented.
- **vuln-advisory-triage-artifact** (Vulnerability management). Implemented.
- **vuln-no-penetration-test** (Vulnerability management). Not implemented.
- **vuln-no-independent-certification** (Vulnerability management). Not implemented.
- **vuln-version-control-and-review** (Vulnerability management). Implemented.
- **vuln-deploys-are-manual** (Vulnerability management). Implemented.