



ОТЧЁТ ОБ УЧАСТИИ В МЕЖДУНАРОДНЫХ ПУБЛИЧНЫХ КОНСУЛЬТАЦИЯХ

ARGA - Asylum Research & Global Assistance

21 октября 2026 года

ARGA подготовила пять экспертных позиций по вопросам защиты персональных данных, регулирования искусственного интеллекта и авторского права. Четыре позиции направлены в рамках публичных консультаций: три - Европейскому совету по защите данных (EDPB), одна - Департаменту защиты персональных данных Малайзии (JPDP). По консультациям Европейской комиссии подготовлены документ и ответы на анкету.

Участие объединяет европейскую и азиатскую регуляторную повестку вокруг практического вопроса: как обеспечить проверяемую ответственность за использование данных и действенную защиту человека при применении новых технологий.

1. Веб-скрейпинг и генеративный искусственный интеллект

EDPB, Guidelines 03/2026. Консультация затрагивает массовый сбор информации из открытых источников для систем генеративного ИИ. Для ARGA особое значение имеет риск распространения устаревших обвинений и чувствительных сведений вне первоначального контекста, в том числе информации, связанной с убежищем и уголовным преследованием.

Позиция ARGA: прослеживаемость происхождения данных и их последующего использования; оценка правомерности до сбора; сохранение существенного контекста; доступный механизм исправления и удаления. Удаление записи из исходного массива должно отличаться от проверки того, продолжает ли модель воспроизводить спорную информацию.

Результат: подача подтверждена на экране и письмом EDPB от 21 октября 2026 года, 16:57. Публикация предусмотрена после проверки EDPB.

2. Анонимизация и риск повторной идентификации

EDPB, Guidelines 02/2026. Значение консультации состоит в разграничении реальной анонимности и формального удаления идентификаторов. Сочетание дат, мест, семейных обстоятельств и событий может раскрывать личность даже без имени.

Позиция ARGA: оценка должна учитывать конкретный набор данных, получателей и условия доступа, подтверждаться тестами и пересматриваться при изменении обстоятельств. Особое внимание уделено малым группам, чувствительным историям и безопасным условиям тестирования повторной идентификации.

Результат: подача подтверждена на экране и письмом EDPB от 21 октября 2026 года, 17:03.



3. Административные штрафы и иные корректирующие меры

EDPB, Guidelines 04/2026. Консультация касается соотношения штрафов и иных полномочий надзорных органов по GDPR. Её практическое значение - в обеспечении соразмерного правоприменения, которое одновременно устанавливает ответственность и прекращает последствия нарушения для человека.

Позиция ARGА: нарушение, роль конкретного участника, умысел или неосторожность и выбор санкции требуют самостоятельного обоснования. Масштаб последствий нельзя оценивать только числом затронутых лиц: раскрытие данных одного человека может существенно повлиять на его безопасность, репутацию и доступ к необходимым услугам.

ARGA предложила связывать оценку исправительных действий с проверяемыми результатами: какие операции прекращены, какие данные исправлены и каким образом установлена эффективность мер. Штраф не должен подменять устранение нарушения, а обещание улучшений - доказательство фактического исправления. Отдельно подчеркнуты понятность решений, возможность их оспаривания и защита заявителей от повторного раскрытия данных.

Результат: подача подтверждена на экране и письмом EDPB от 21 октября 2026 года, 17:08.

4. Искусственный интеллект и защита персональных данных в Малайзии

JPDP, Public Consultation Paper No. 1/2026. Обсуждение AI and Personal Data Protection Framework посвящено управлению обработкой данных на всех стадиях жизненного цикла ИИ. Участие в этой консультации расширяет географию экспертной работы ARGА и позволяет представить подход к защите уязвимых лиц в самостоятельном национальном правовом контексте.

Позиция ARGА: ясное распределение ответственности между разработчиком, поставщиком и пользователем системы; документирование источников и целей обработки; контроль изменений моделей и условий использования данных. Для решений с существенными последствиями предложены содержательный человеческий пересмотр и доступная процедура оспаривания результата.

В ответах также предложены практические инструменты: карта ролей, реестр источников данных, вопросы для проверки поставщиков, процедуры исправления ошибок и соразмерная проверка систем. Международные стандарты рассматриваются как организационные ориентиры, которые должны соотноситься с требованиями малайзийского права, а не заменять их.

Результат: ответы направлены, успешная отправка подтверждена сообщением «Your response has been recorded». В приложении приведены подготовленная письменная позиция, использованная для ответов, и скриншот подтверждения.

Общее значение представленных предложений

Четыре завершённые подачи формируют согласованную экспертную позицию ARGА: защита прав должна опираться на проверяемые факты, понятное распределение ответственности и доступные средства исправления. Подход отражает профиль ARGА в сфере трансграничной защиты прав.



5. Технологии, авторское право и генеративный ИИ

Европейская комиссия. Targeted consultation on a potential initiative for a better copyright environment for European creativity and innovation. Консультация посвящена условиям использования охраняемых материалов в ИИ, защите правообладателей, цифровым имитациям исполнителей и исследовательскому доступу.

Подготовленная позиция ARGА: документирование происхождения обучающих материалов, понятные условия лицензирования и оговорок правообладателей, соразмерный доступ к доказательствам при споре. Публичная прозрачность должна сочетаться с защищёнными каналами раскрытия, чтобы не создавать новых рисков для персональных данных и конфиденциальной информации.

В части цифровых имитаций предложены адресные и оспоримые меры защиты, учитывающие контекст и законные формы выражения. В исследовательской части - предсказуемые правила доступа, безопасные среды и соразмерная документация, позволяющие проводить независимую проверку систем ИИ.

Документальное подтверждение и состав приложений

Получение трёх позиций EDPB подтверждено автоматическими письмами EDPB. Подтверждение получения не означает принятия предложений регулятором; письма предусматривают проверку перед публикацией. По Малайзии основанием для фиксации отправки служит сохранённый экран подтверждения. Время писем приведено так, как оно отображено в предоставленных копиях.

Ниже включены полные тексты позиций и подтверждающие материалы. Исходные документы сохранены без изменения содержания. Общая цепочка писем и отдельно предоставленные сообщения включены полностью; повторяющиеся письма относятся к тем же подачам и не увеличивают их количество.

Приложение 1. Веб-скрейпинг: позиция ARGА и подтверждение отправки - стр. 4-6.

Приложение 2. Анонимизация: позиция ARGА и подтверждение отправки - стр. 7-9.

Приложение 3. Административные штрафы: позиция ARGА и подтверждение отправки - стр. 10-12.

Приложение 4. Малайзия: позиция ARGА и подтверждение отправки ответов - стр. 13-16.

Приложение 5. Европейская комиссия: позиция и ответы на анкету - стр. 17-23.

Приложение 6. Письма EDPB: общая цепочка и отдельные копии подтверждений - стр. 24-26.



Web scraping and generative AI

Response to EDPB Guidelines 03/2026

European Data Protection Board

21 October 2026 | France

ARGA — Asylum Research & Global Assistance submits this position from a fundamental-rights and access-to-remedy perspective. Our central concern is the loss of context when information about identifiable people is collected, combined and reused by generative AI systems. The recommendations below concern the consultation draft and are proposals for clarification, not assertions that every suggested measure is already mandatory.

1 Make provenance operational

We support clearer accountability for the acquisition and reuse of personal data. The final guidance should connect the allocation of responsibilities in paragraphs 17–20 with a practical evidence trail. A controller should be able to link a training-data collection to its source, collection date, stated purpose, assessed legal basis, relevant restrictions and subsequent dataset versions. The level of detail should reflect risk and avoid retaining unnecessary personal data solely to document compliance.

We recommend a minimum provenance record covering the collecting entity, source categories, acquisition method, relevant filtering decisions, transfers and the training runs or model versions that used the material. For purchased datasets, a supplier warranty alone should not close the inquiry. A proportionate verification process should test the supplier's account, record unresolved gaps and identify circumstances requiring exclusion or further investigation.

The guidance should explain how responsibility follows actual decisions about purposes and means. Contractual labels must not obscure a developer's own decisions about selection, combination or reuse. An upstream breach should not automatically be attributed to every downstream actor without examining that actor's processing and applicable duties.

2 Assess lawfulness before collection

Public availability does not resolve lawfulness, necessity or fairness. Where legitimate interests are relied upon, the assessment should identify a concrete interest, examine less intrusive means and address reasonable expectations in the original publication context. A general aspiration to improve a model should not substitute for that analysis. The assessment should be revisited when the intended use or affected population changes materially.

We recommend clearer examples involving asylum-related narratives, humanitarian assistance pages, allegations of crime and information about children. These are illustrative risk scenarios, not client case studies. The same passage can acquire a substantially different impact when detached from its date, procedural status or original audience.

The guidance should distinguish special-category data under Article 9 GDPR from data concerning criminal convictions and offences under Article 10. A balancing exercise under Article 6(1)(f) does not itself satisfy those separate conditions. Controllers should identify whether such material is likely to be collected and adopt source selection, exclusion and handling measures before ingestion, with a documented response to residual collection.

3 Preserve context and enable correction

The minimisation and accuracy discussion should address outdated or contested allegations. A withdrawn notice, an acquittal or a correction can be lost when a dataset retains only an earlier

report. Where personal data are retained, provenance and update mechanisms should make the date, source and relevant status discoverable without indiscriminately expanding the data collected.

We recommend an escalation procedure for credible reports of serious inaccuracies: assess the report, identify affected dataset versions, restrict further reuse where justified, implement the applicable correction or deletion and document verification. The final guidance should distinguish action on a source corpus from action on a trained model and on generated outputs. Removing a row from a dataset does not demonstrate that the model has ceased reproducing it.

Controllers should explain the capabilities and limits of their remediation method. Technical difficulty should be evidenced, not used as a generic exemption. Tests should examine whether relevant output risks persist, while preventing the testing process from exposing the affected person's data more widely.

4 Make transparency and remedies usable

For paragraphs 24–34, we recommend concrete criteria for assessing and documenting any Article 14 exception. Scale alone should not be presented as an automatic justification. Where an exception applies, alternative information should be specific enough to help people understand the processing and locate a usable contact point.

A searchable source register can be useful, but a public register of exact URLs may itself expose vulnerable people. The guidance should permit layered disclosure: meaningful public information on source categories and periods, a protected request route, and fuller evidence available to competent authorities. It should not require fresh identifying data solely to make an anonymous or unidentifiable record attributable to a person.

Rights procedures should accept reasonably sufficient evidence and provide a reasoned outcome. A request should be traceable across the collecting entity, dataset supplier and model provider where relevant responsibilities exist. Referral between organisations must not become an endless loop. Any communication of rectification or erasure should follow the applicable GDPR requirements and protect the requester's identity.

5 Require evidence proportionate to risk

ARGA recommends a concise accountability annex covering provenance, the lawfulness assessment, source exclusions, impact assessment where required, rights handling, remediation tests and material changes. For particularly consequential processing, suitably independent review can improve confidence; the guidance should explain when such review is useful without presenting universal external certification as a legal requirement.

Reviewers should have relevant expertise, access sufficient to test claims, and safeguards against conflicts of interest. Published findings should describe scope and limitations. Neither an audit label nor a supplier assurance should create immunity from responsibility. Our priority is verifiable prevention and effective correction, rather than documentation that cannot be tested.

References

[1] EDPB Guidelines 03/2026, consultation draft, version 1.0, adopted 7 July 2026. Principal references: paragraphs 17–20, 24–34 and the sections on minimisation, accuracy and lawfulness. Official source

[2] Regulation (EU) 2016/679, in particular Articles 5, 6, 9–11, 14, 16–19, 21, 24, 25 and 35. Official source

EDPB: веб-скрейпинг и генеративный ИИ

21 октября 2026 года | Сохранённый экран подтверждения отправки

The EDPB Secretariat staff screens all replies provided before publication (only for the purpose of blocking unauthorised submissions, such as spam), after which the replies are made available to the public directly on the EDPB public consultations' page. Unauthorised submissions are immediately deleted. The attached files are not altered in any way by the EDPB.

Please note that your contribution may be subject to a request for access to documents under [Regulation 1049/2001](#) on public access to European Parliament, Council and Commission documents. In this case the request will be assessed against the conditions set out in the Regulation and in accordance with applicable data protection rules.

All legal details can be found in our [Specific Privacy Statement \(SPS\)](#).

Your contribution has been submitted.



Topics

Documents

Task and duties

Our members





Anonymisation and reidentification risk

Response to EDPB Guidelines 02/2026

European Data Protection Board

21 October 2026 | France

ARGA — Asylum Research & Global Assistance welcomes guidance that makes anonymisation assessments explainable and reviewable. Our perspective is the protection of people whose identification can expose them to serious consequences and whose access to correction or redress may be limited. We propose practical additions to the consultation draft while preserving the GDPR test of identifiability.

1 Document the context of the assessment

The final guidance should provide a short assessment template stating the dataset and version, intended recipients, release environment, relevant actors, reasonably available auxiliary information, likely means of identification and review horizon. An anonymity claim should identify the perspective and circumstances to which it applies. A result established for restricted access should not be carried over automatically to unrestricted publication.

The analysis should consider realistic cooperation between recipients or other actors where relevant, without assuming an omnipotent adversary with unlimited resources. Conversely, contractual prohibitions should not be treated as conclusive where practical access, incentives or weak enforcement make identification reasonably likely. The record should show why assumptions about access and capabilities are credible.

We support the distinction between anonymisation and pseudonymisation. Replacing direct identifiers, hashing a field or calling data “synthetic” does not by itself establish anonymity. Data-processing steps undertaken to achieve anonymisation remain subject to the applicable GDPR requirements while personal data are being processed.

2 Explain the three criteria and their limits

Paragraphs 52–53 and section 3.5.3 should be accompanied by a worked decision record showing how the three criteria — No Record Isolation, No Linkage and No Inference — feed into the overall assessment. The guidance should make clear both the significance of satisfying all three and the need for further analysis when a criterion is not met. Failure of a screening criterion should not be reduced to an unexplained automatic verdict.

We recommend examples involving small populations, longitudinal records and unstructured narratives. Removing a name may leave a distinctive combination of location, dates, family circumstances or procedural events. An assessment limited to individual database columns can miss the identifying effect of the combined record or of linked releases.

Tests should report the attack or inference attempted, auxiliary data used, success definition, false positives, uncertainty and limits of the evaluation. A low average success rate may conceal a readily identifiable subgroup. No single numerical threshold should be presented as a universal safe harbour across datasets, recipients and release conditions.

3 Protect people during reidentification testing

Reidentification testing should not create an avoidable new disclosure. We recommend controlled environments, authorised access, minimisation of test outputs, separation of identifiers where appropriate and documented deletion or restricted retention of test material. External evaluators should be bound by suitable confidentiality and security arrangements.

The likelihood of identification and the severity of its consequences should be recorded separately. Vulnerability does not replace or redefine the legal test of identifiability. It should nevertheless inform the safeguards, release design and scrutiny of assumptions. For sensitive narratives, aggregate publication or controlled access may be preferable to releasing granular records.

The final guidance should include a decision point for uncertainty. Where the evidence does not substantiate anonymity in the planned context, the organisation should continue to apply the relevant personal-data protections or change the release design. An unresolved assessment should not be converted into an anonymity claim merely because further testing is inconvenient.

4 Treat anonymity as a maintained conclusion

We recommend explicit review triggers: new auxiliary datasets, changes in access conditions or recipients, improved identification techniques, additional releases that can be combined, and credible reports of identification. The initial decision should name a review owner and record the rationale for the review interval. Periodic reassessment should be proportionate and should not imply that every previous assessment is automatically invalid.

A response plan should describe how to investigate a credible reidentification report, preserve necessary evidence, contain further access where possible and reassess the processing under the applicable law. If public release cannot be reversed, that limitation should be acknowledged before publication and reflected in the initial decision.

We also recommend separate assessment of source data, transformed data and any model produced from them. A conclusion that a released table is anonymous does not establish that a model trained on identifiable source material is anonymous. Testing and documentation should identify the particular artefact and use context to which the conclusion applies.

5 Retain accountability and access to remedy

The draft should retain the distinction between anonymisation for a recipient and the obligations of a controller that collected identifiable data. Later anonymisation must not be used to retroactively erase transparency obligations that arose at collection. Retention of original identifiable data should be justified separately; anonymising one copy does not resolve the storage limitation assessment for all other copies.

ARGA proposes a proportionate evidence package comprising the assessment record, test results, access controls, residual uncertainties and review triggers. In cases presenting substantial consequences for individuals, independent scrutiny may be appropriate. It should test the stated assumptions and methods, not merely certify that a checklist exists.

A public explanation can describe the purpose, techniques, release context and limitations without disclosing an attack recipe or personal information. A confidential channel should allow people and qualified researchers to report credible weaknesses. The objective is an anonymity claim that remains defensible in practice and can be challenged responsibly.

References

[1] EDPB Guidelines 02/2026, consultation draft, version 1.0, adopted 7 July 2026. Principal references: paragraphs 3, 6–14 and 52–53; sections 2.4, 2.5 and 3.5.3. Official source

[2] Regulation (EU) 2016/679, in particular Recital 26 and Articles 4, 5, 13, 14, 24, 25 and 32. Official source

EDPB: анонимизация

21 октября 2026 года | Сохранённый экран подтверждения отправки

The EDPB Secretariat staff screens all replies provided before publication (only for the purpose of blocking unauthorised submissions, such as spam), after which the replies are made available to the public directly on the EDPB public consultations' page. Unauthorised submissions are immediately deleted. The attached files are not altered in any way by the EDPB.

Please note that your contribution may be subject to a request for access to documents under [Regulation 1049/2001](#) on public access to European Parliament, Council and Commission documents. In this case the request will be assessed against the conditions set out in the Regulation and in accordance with applicable data protection rules.

All legal details can be found in our [Specific Privacy Statement \(SPS\)](#).

Your contribution has been submitted.



Topics

Documents

Task and duties

Our members





Administrative fines and effective remedies

Response to EDPB Guidelines 04/2026

European Data Protection Board

21 October 2026 | France

ARGA — Asylum Research & Global Assistance supports enforcement that is effective, proportionate and dissuasive, with reasoned decisions and meaningful procedural safeguards. Our contribution concerns the impact of data misuse on individuals, attribution of responsibility, evidentiary quality and the relationship between sanctions and corrective action. The recommendations address the consultation draft adopted on 17 September 2026.

1 Preserve the sequence of the assessment

The five-step structure is useful if each step remains distinct. The final guidance should make explicit that establishing an infringement, identifying the appropriate addressee, establishing intention or negligence and deciding on a sanction require their own reasons. The desirability of deterrence must not substitute for evidence of the relevant infringement and responsibility.

For complex processing chains, the decision should identify the actor's actual role, the processing operation, the breached duty and the evidence connecting that actor to the breach. Paragraphs 42–43 should be illustrated with cases distinguishing a processor acting within instructions, a processor exceeding them and a controller's separate failures of selection or oversight. Contractual labels should neither shield actual responsibility nor justify automatic liability for every participant.

We recommend examples involving AI-assisted systems, but the mere use of AI should not be treated as an infringement or an aggravating factor in itself. The authority should establish the relevant facts: for example, the actual collection, use, disclosure, accuracy failure or failure to honour an applicable right.

2 Keep culpability and individual assessment explicit

We support the requirement to establish intention or negligence. The final guidance should explain the evidential reasoning required when awareness, organisational omissions or ignored warnings are relied upon. A documented compliance system can be relevant evidence, but its existence alone does not prove reasonable conduct; nor does a failed control automatically establish intentional misconduct.

The strong presumption discussed in paragraphs 55–57 for non-minor infringements should be accompanied by an express safeguard that it does not reverse the burden of establishing the infringement or culpability. The authority should still give an individualised explanation of why a fine is appropriate, taking account of the relevant Article 83 factors and the available corrective powers.

ARGA recommends separating three questions in the reasons: why the infringement is or is not minor; why a fine or another measure is appropriate; and how the amount is determined under the applicable framework. This would improve reviewability and avoid collapsing distinct assessments into a single conclusion about severity.

3 Assess consequences beyond aggregate numbers

A small number of affected people does not necessarily indicate minor consequences. The guidance should include examples where inaccurate or improperly disclosed information can have substantial effects on a person's safety, reputation or access to essential services. Examples concerning contested criminal allegations or asylum-related information would illuminate the importance of context without creating automatic sanction categories.

The assessment should distinguish established harm, a substantiated risk of harm and unsupported speculation. It should consider duration, exposure, accessibility of the information, reversibility and barriers to obtaining a remedy. Evidence should make clear whether harm is widespread, concentrated in a vulnerable subgroup or particularly serious for one person.

The nature of the data and the context of its use can inform gravity under the GDPR framework, but should not become a mechanical score that replaces judgment. A transparent explanation is preferable to an undisclosed risk model or a proprietary blacklist of supposedly high-risk actors.

4 Connect sanctions to verified correction

We support distinguishing ordinary compliance from exceptional mitigating conduct, as discussed in paragraphs 77–78. An organisation should not receive automatic mitigation merely for doing what the law already required. At the same time, prompt, evidenced action that genuinely limits harm should be assessed on its merits under the applicable factors.

The guidance should identify useful evidence of remediation: when the organisation became aware, what it stopped or restricted, which recipients or systems were affected, which corrections were completed and how effectiveness was tested. A promise to improve, an unverified vendor assurance or a newly purchased audit should not carry the same weight as a demonstrated result.

For AI-related processing, deletion from one training corpus does not establish correction across model versions or generated outputs. The authority should examine the scope and limits of the action actually taken. Corrective orders should specify a measurable objective, a proportionate timetable and suitable verification while remaining grounded in the authority's legal powers.

Remediation should not create immunity from a fine, and a fine should not be treated as permission to continue unlawful processing. Where necessary and lawful, sanctions and corrective measures should work together to stop the infringement and reduce continuing harm.

5 Make enforcement reviewable and accountable

The procedural safeguards referenced in paragraph 12 should be reflected throughout the guidance. The addressee should be able to understand and challenge the material evidence, attribution, technical methods and conclusions, subject to the applicable procedural rules and legitimate protections for confidential information. A technically complex investigation must remain intelligible enough for effective review.

Independent expert assessment can be valuable when it tests a contested technical claim. Its scope, assumptions, conflicts of interest and limitations should be disclosed as appropriate. An audit should be evidence to assess, not a substitute for the authority's judgment or a presumption that all processing is compliant.

When several authorities or legal regimes address related conduct, the guidance should encourage coordination and an explicit explanation of how applicable safeguards against duplicative punishment are respected. This should not be framed as a blanket exemption from distinct lawful proceedings.

Finally, public decisions should explain the infringement and outcome while protecting complainants and third parties from unnecessary reidentification. ARGAs recommends publishing meaningful reasoning and verified corrective outcomes, with appropriate redaction. Effective enforcement should improve the individual's practical position as well as deter future violations.

References

[1] EDPB Guidelines 04/2026, consultation draft, version 1.0, adopted 17 September 2026. Principal references: paragraphs 9, 12, 42–43, 48–57 and 77–78; section 5.2. Official source

[2] Regulation (EU) 2016/679, in particular Articles 58, 78 and 83 and Recital 148. Official source

EDPB: административные штрафы

21 октября 2026 года | Сохранённый экран подтверждения отправки

The EDPB Secretariat staff screens all replies provided before publication (only for the purpose of blocking unauthorised submissions, such as spam), after which the replies are made available to the public directly on the EDPB public consultations' page. Unauthorised submissions are immediately deleted. The attached files are not altered in any way by the EDPB.

Please note that your contribution may be subject to a request for access to documents under [Regulation 1049/2001](#) on public access to European Parliament, Council and Commission documents. In this case the request will be assessed against the conditions set out in the Regulation and in accordance with applicable data protection rules.

All legal details can be found in our [Specific Privacy Statement \(SPS\)](#).

Your contribution has been submitted.



Topics

Documents

Task and duties

Our members





AI and personal data protection

Response to JPDP Public Consultation Paper No. 1/2026

Department of Personal Data Protection, Malaysia

21 October 2026 | France

ARGA — Asylum Research & Global Assistance submits the following responses to questions 4.1.1–4.1.7 of the consultation paper dated 5 October 2026. Our contribution concerns accountable AI governance, protection of vulnerable individuals and practical access to remedies. Recommendations for additions to the proposed Framework are identified as proposals; references to Malaysian law remain governed by Act 709 and the applicable Malaysian legal framework.

4.1.1 Adequacy of Act 709 compliance

The proposed lifecycle approach is useful, particularly the treatment of lawful data sources, documentation, review and continuing oversight. ARGA recommends an accompanying compliance map connecting each operative requirement to Act 709, applicable subsidiary instruments or a clearly identified new recommendation. This would help organisations distinguish existing legal duties from suggested governance practice.

Paragraph 5.1 correctly states that using AI does not create a separate legal basis. The final Framework should give worked examples of selecting and recording the applicable Malaysian condition for processing at collection, training, testing, deployment and reuse. Concepts from foreign regimes should not be imported as if they were independent permissions under Act 709. Publicly accessible or purchased data should not be presumed authorised for any AI purpose.

4.1.2 Scope terms and exemptions

The final text should preserve the statutory scope and distinguish the responsibilities of controllers and processors wherever Act 709 allocates them differently. A glossary should explain the relationship between an AI developer, service provider, deployer and these legal roles. Actual processing decisions and the applicable law, rather than a supplier's product label, should determine the analysis.

For own systems, third-party services and APIs, organisations should map who receives personal data, who can reuse it for training, retention periods and relevant onward transfers. The guidance should explain how exclusions or exemptions apply by reference to their legal source. It should not appear to create new statutory exemptions, offences or extraterritorial powers through guidance alone.

4.1.3 AI lifecycle principles

We recommend a maintained record linking intended purpose, source and acquisition conditions, relevant processing justification, dataset versions, material model changes and deployment context. Before a material change, the organisation should assess whether the original justification and safeguards remain adequate. This should include a change from internal assistance to a system used in decisions with significant effects on people.

For consequential uses, we propose meaningful human review, an accessible route to question an outcome and a record of the role automation played. This is a recommendation for the Framework, not a claim that every proposed safeguard is already a freestanding statutory right. Review should be capable of changing the outcome and should address erroneous inputs and unsupported inferences.

Withdrawal, correction or deletion workflows should distinguish the source dataset, vendor copies, the deployed system and model outputs. A claim that a correction is complete should identify the action taken and the evidence supporting it. Where a technical limitation remains, the controller

should evaluate other effective measures under the applicable law rather than rely on a generic statement that AI cannot be corrected.

4.1.4 Governance and feasibility

For paragraphs 35–43, we recommend a named accountable owner, documented approval for consequential uses, an escalation route and change-control records. Existing governance structures can perform these functions where they have adequate authority and expertise. Smaller organisations should be able to use concise templates and shared technical resources without losing accountability.

The proportionality approach to review and audit in paragraph 41 should be retained. Internal review may be adequate for some uses; materially higher-risk processing may justify independent evaluation. The guidance should describe competence, access to relevant evidence and conflict-of-interest safeguards. It should not imply that purchasing an external certificate discharges statutory responsibilities.

Minimum vendor terms should address permitted processing, reuse for training, retention and deletion, incident cooperation, material changes and evidence needed to assess compliance. A controller should record what it has verified and what remains uncertain. Where the evidence is insufficient, the response may require limiting or suspending the proposed use rather than relying exclusively on a contractual assurance.

4.1.5 Constraints and enforcement challenges

Key practical constraints include opaque suppliers, incomplete provenance, changing models, limited technical expertise and the difficulty of tracing a harmful output back to relevant processing. ARGA recommends standard evidence requests and a staged escalation process so that organisations and the regulator can distinguish missing documentation, failed controls and demonstrated unlawful processing.

Records under paragraphs 40–42 should support investigation without becoming an unlimited archive of personal data. Access controls, retention rules and secure review arrangements should be specified. Confidential examination can protect trade secrets while allowing the regulator to test a claim. Commercial confidentiality should not be treated as a blanket reason to withhold evidence that must lawfully be provided.

Cross-border processing should be assessed under the applicable Act 709 requirements. Vendor assurances should be connected to actual data flows, recipient roles and safeguards. Guidance should explain practical escalation where a provider changes location, subprocessors or reuse terms.

4.1.6 Industry readiness and regulatory support

We recommend a starter pack containing a role-mapping worksheet, data-source register, vendor questionnaire, material-change checklist, rights-request workflow and proportionate audit record. Sector examples should include smaller organisations and cases involving sensitive or vulnerable populations. Templates should show the reasoning required, not just boxes to tick.

Training, published questions and answers, and suitably governed testing environments could improve implementation. Any transition period for new guidance should be clearly distinguished from existing statutory obligations. JPDP could publish anonymised implementation examples and recurring deficiencies without disclosing complainants' identities or confidential business information.

4.1.7 International references and standards

International risk-management and management-system frameworks, including NIST AI RMF and ISO/IEC 42001, can offer useful terminology and organisational methods. Their use should be mapped to Malaysian requirements rather than presented as legal equivalence. Certification, where relevant, should identify its scope, version, limitations and the processing actually assessed.

ARGA recommends a functional comparison: which Malaysian obligation a control supports, what evidence it generates and what remains unaddressed. The Framework should preserve local legal requirements while encouraging interoperable records and evaluation methods. The final objective should be demonstrable protection and a usable remedy, not a compliance label detached from actual system behaviour.

References

- [1] JPDP Public Consultation Paper No. 1/2026, AI and Personal Data Protection Framework, dated 5 October 2026. Questions: Part 3, 4.1.1–4.1.7. Draft Framework: paragraphs 5–6, 21–23, 29 and 35–43. Official source
- [2] Official Unified Public Consultation portal for this consultation. Submission route identified in Part 4 of the consultation paper. Official source
- [3] NIST AI Risk Management Framework. Voluntary framework for AI risk management. Official source
- [4] ISO/IEC 42001:2023. AI management systems. Official overview of the standard. Official source

Малайзия: ИИ и персональные данные

21 октября 2026 года | Сохранённый экран подтверждения отправки



**KERTAS KONSULTASI AWAM BIL.
1/2026: KERANGKA KECERDASAN
BUATAN (AI) DAN PERLINDUNGAN
DATA PERIBADI**
*PUBLIC CONSULTATION PAPER NO.
01/2026: ARTIFICIAL INTELLIGENCE (AI)
AND PERSONAL DATA PROTECTION
FRAMEWORK*

Your response has been recorded

[Изменить ответ](#)

[Отправить ещё один ответ](#)

Форма создана в домене MyGovUC. - [Связаться с владельцем формы](#)

Эта форма кажется вам подозрительной? [Пожаловаться](#)



Google Формы



Technology and copyright

Supplementary position paper for the European Commission

Targeted consultation on a potential initiative for a better copyright environment for European creativity and innovation

21 October 2026 | France

ARGA — Asylum Research & Global Assistance offers a fundamental-rights and accountability perspective on generative AI and copyright. This paper supplements the consultation questionnaire. It focuses on training-data provenance, licensing, enforcement, AI-generated imitations and research. It does not claim to represent a collecting society, a model developer or a particular creative industry, and does not provide market estimates.

1 Make copyright compliance verifiable

A workable copyright environment requires both respect for rights and a practical way to establish what a system has done. ARGA recommends a proportionate provenance framework linking the acquisition of training material, relevant permissions or exceptions, rights reservations and subsequent dataset versions. The purpose is to support a reasoned compliance assessment, not to presume that all AI training is unlawful or that every use requires a new licence.

The framework should distinguish public transparency from evidence held for competent authorities or lawful dispute resolution. A useful public summary can describe sources, periods, categories and acquisition channels. More granular records may be necessary to investigate a specific claim, but publication of an unrestricted source inventory may expose personal data, confidential material or security-sensitive information.

The Commission should build coherently on the copyright-policy and training-content-summary obligations for general-purpose AI providers under Article 53 of the AI Act. A summary is an information instrument; it should not be treated as proof that every use was lawful. Conversely, a limitation in a public summary should not automatically establish infringement. The evidence needed for each legal question should be identified.

2 Clarify rights reservations and licensing

For text and data mining, guidance should clearly distinguish the research exception in Article 3 of Directive (EU) 2019/790 from the framework in Article 4, including lawful-access and rights-reservation questions. It should not merge these regimes into a single universal opt-out rule or imply that one technical signal settles every copyright issue.

We recommend interoperable, reasonably accessible ways to express and record relevant rights reservations. A practical implementation record should capture the signal encountered, the time of collection, the version of the interpretation method and the decision taken. Future guidance should address conflicting signals, changes over time, intermediaries and erroneous reservations without retrospectively inventing permissions or obligations.

Licensing options should be intelligible for smaller rights holders and smaller developers. Model terms could identify the material covered, permitted uses, duration, territorial scope, downstream use and complaint route. Any collective mechanism should have clear authority, governance and safeguards for those who are not represented. ARGA does not propose an unverified remuneration formula or a compulsory licensing model in this submission.

3 Provide a usable and fair evidence route

Rights holders need a practical channel to raise a sufficiently specific concern. We recommend a structured process allowing them to identify the work or relevant rights, describe the suspected use

and receive a reasoned response. Evidence requirements should be proportionate to information realistically available to the claimant, while protecting against unsupported or abusive demands.

A graduated disclosure process could begin with a bounded search of relevant provenance records and, where legally justified, proceed to confidential inspection or expert review. Access should be limited to what is necessary for the dispute and should protect third-party rights. The applicable legal rules should govern disclosure and burdens of proof; a voluntary audit should not silently reverse them.

Technical similarity, evidence of collection, evidence of training and evidence of an infringing output answer different questions. The Commission should encourage methods that distinguish them and explain false positives and uncertainty. Compliance statements should identify their scope and the model or dataset version assessed. Neither an audit label nor a generic assertion of confidentiality should end the inquiry.

4 Address imitations with targeted remedies

AI-generated imitations of a performer can involve copyright or related rights alongside personality, privacy, consumer-protection and other interests. The consultation should preserve those distinctions. A technical resemblance should not be treated as conclusive proof of a particular legal violation, and a copyright licence should not be assumed to resolve every other affected right.

ARGA recommends accessible notice and review mechanisms for credible claims of unauthorised imitation, with proportionate interim measures where serious harm is plausibly demonstrated. Review should consider the relevant legal basis, context and legitimate expression, including applicable exceptions. Decisions should be reasoned, challengeable and implemented without demanding unnecessary identity documents.

Where a response is justified, it should identify the affected content, account, functionality or dataset as precisely as practicable. A general filter should not become a mechanism for suppressing criticism or lawful research. Human review is particularly important where automated detection cannot reliably distinguish an imitation from lawful quotation, parody or coincidental similarity.

5 Preserve research and protect sensitive material

Research access should be legally predictable and operationally feasible. The Commission should support secure environments and proportionate documentation that enable eligible research uses while respecting applicable conditions. A research label should not be used to conceal a different commercial purpose, and compliance requirements should not unnecessarily prevent independent scrutiny of AI systems.

Copyright transparency must be coordinated with data protection. For example, disclosure of exact sources may reveal a person's asylum narrative or sensitive allegations. We recommend layered access, minimised public explanations and protected evidentiary channels. Copyright compliance does not itself establish a lawful basis for processing personal data, and data-protection compliance does not itself confer copyright permission.

ARGA's priority is an enforceable chain of accountability: identifiable decisions, relevant records, proportionate access to evidence and remedies that can be tested. Before adopting new requirements, the Commission should examine their practical burden, accessibility to smaller organisations and interaction with existing EU instruments. Any proposed new duty should be clearly separated from guidance explaining existing law.

References

[1] European Commission, consultation announcement and official questionnaire, including the Additional documents section. Consulted 21 October 2026. Official source

[2] Official consultation questionnaire. Official source

[3] Directive (EU) 2019/790, in particular Articles 3 and 4. Official source

[4] European Commission, General-purpose AI obligations under the AI Act, including the copyright policy and training-content summary requirements. Official source



Targeted consultation on a potential initiative for a better copyright environment for European creativity and innovation

Copyright and generative AI: licensing and enforcement

Question 1. Приоритетные проблемы: выбранные места

1. Difficulties in enforcing exclusive rights provided under EU copyright law due to limited transparency on the use of copyright-protected content by AI model or system providers.
2. Practical challenges in expressing, identifying, and respecting rights reservations, including lack of standardised opt-out technical protocols that can be operationalised at scale.
3. Legal uncertainty on the applicable copyright rules, including with regard to the application of the text-and data mining exception.

Question 5. Выбран вариант Other: please specify

Combine clear guidance, interoperable rights reservations, proportionate provenance records and protected access to evidence; assess any new duties against existing law and burdens on smaller actors.

Question 6. Пояснение к механизмам защиты прав

ARGA recommends proportionate provenance records linking acquisition, permissions or exceptions, rights reservations and dataset versions. Public summaries should be distinguished from granular evidence held for competent authorities or lawful dispute resolution. Build coherently on Article 53 of the AI Act: a summary does not prove that every use was lawful, and a limitation in it should not automatically establish infringement. A structured complaint route should allow a sufficiently specific claim and a reasoned response. Graduated disclosure can begin with a bounded search and, where legally justified, proceed to confidential inspection or expert review. Protect personal data, trade secrets and third-party rights; retain records only for justified periods. Distinguish collection, training, similarity and infringing output. Neither an audit label nor a generic confidentiality claim should end the inquiry. Any new duty must be distinguished from guidance on existing law and assessed for proportionality. See sections 1–3 of the attached paper.



Copyright and generative AI: licensing and enforcement

Question 8. Выбранные меры по лицензированию

Develop model contractual clauses for licenses covering AI uses. Выбраны все три стадии: For training of generative AI; For inference-time use; For output.

Question 8. Пояснение к выбранным мерам

Model terms should identify the material covered, permitted uses at the relevant lifecycle stage, duration, territorial scope, downstream use and complaint route. They should be intelligible to smaller rights holders and developers. A licence should be required only where the applicable law requires authorisation; model terms must not displace exceptions. Guidance must distinguish Article 3 research TDM from Article 4 of Directive (EU) 2019/790, including lawful access and rights reservations. Interoperable reservation methods should address conflicting signals, changes over time and errors without retrospectively inventing permissions or duties. Any collective mechanism needs clear authority, governance and safeguards for unrepresented persons. ARGAs does not propose a compulsory licensing model or an unverified remuneration formula. See section 2 of the attached paper.

Описание охвата позиции: поле Other

Cross-sector perspective on copyright-protected training and research material, and AI-generated imitations; no representation of a particular creative industry.



Copyright and generative AI: AI generated imitations of performers

Question 1. In your view, how can AI be used to support creative processes, including through the use of digitally generated imitations of performers, in a balanced and fair manner?

ARGA recommends clear permissions for the relevant use, transparency about synthetic content and accessible notice and review mechanisms for credible claims of unauthorised imitation. Copyright, related rights, personality rights and privacy must be assessed separately. Review should consider context and legitimate expression, including applicable exceptions, and provide reasoned, challengeable decisions. Proportionate interim measures may be justified where serious harm is plausibly demonstrated. Responses should target the affected content, account or functionality precisely, with human review where detection cannot distinguish imitation from lawful quotation, parody or coincidental similarity. Avoid unnecessary identity-document collection. See section 4 of the attached paper.

Question 5. Taking into account the rationale, nature and scope of copyright protection, do you think that EU copyright legislation would be appropriate to address these issues or that this issue should be addressed through other legal means?

Copyright and related rights should address protected works and performances within their proper scope. AI-generated likeness can also engage personality, privacy, consumer-protection and other rights; a copyright licence does not resolve all these interests. The EU should preserve these distinctions and assess gaps across the relevant legal instruments before creating new duties. Technical resemblance is not conclusive evidence of a specific violation. Remedies must be proportionate, reasoned and open to challenge, with safeguards for lawful expression and research. A general filter must not suppress criticism or lawful research. See section 4 of the attached paper.



Copyright and research

Question 2. Пояснение об исключении для научных исследований

ARGA recommends legally predictable and operationally feasible research access, including across borders. Clear guidance should identify eligible beneficiaries, permitted uses and applicable conditions, while supporting secure research environments and proportionate documentation. Requirements should enable independent scrutiny of AI systems without treating a research label as sufficient justification for a different commercial purpose. ARGA does not provide an empirical assessment of national implementation or claim that a single yes/no answer captures the adequacy of the existing exception. See section 5 of the attached paper.

Question 3. Выбранный подход на уровне ЕС

Work on increasing awareness on allowed uses and developing guidelines.

Question 4. Пояснение о возможных изменениях и последствиях

Clearer beneficiaries, permitted uses and cross-border conditions should be assessed for their ability to enable lawful independent research and reduce avoidable compliance burdens. Secure environments and proportionate records can support access while respecting copyright conditions. Transparency must also protect personal data: exact sources may expose asylum narratives or sensitive allegations. Use layered access, minimised public explanations and protected evidentiary channels. Copyright permission and a lawful basis for processing personal data remain separate requirements. ARGA does not estimate business impacts or endorse every possible legislative option; any new duty should be assessed for practical burden and interaction with existing EU instruments.



Ekaterina Khomutinnikova <ekaterina@arga.world>

Your feedback on EDPB Public Consultation

3 messages

European Data Protection Board <no-reply@web.edpb.europa.eu>
Reply-To: European Data Protection Board <no-reply@web.edpb.europa.eu>
To: ekaterina@arga.world

21 October 2026 at 16:57

Dear Sergey Khrabrykh,

Thank you for your contribution to the public consultation "[Guidelines 03/2026 on web scraping in the context of generative AI](#)".

Your feedback has been sent to the EDPB, which will screen it and publish it. The file will be available on the website immediately after screening. Please note that this may mean that your contribution may not be immediately visible. We may also contact you concerning your submission, if necessary.

For more information about how your personal data is processed in the context of our public consultations, you can check our privacy statement for public consultations here: https://www.edpb.europa.eu/edpb-specific-privacy-statements_en

Kind regards,
The EDPB Secretariat

European Data Protection Board <no-reply@web.edpb.europa.eu>
Reply-To: European Data Protection Board <no-reply@web.edpb.europa.eu>
To: ekaterina@arga.world

21 October 2026 at 17:03

Dear Sergey Khrabrykh,

Thank you for your contribution to the public consultation "[Guidelines 02/2026 on Anonymisation](#)".

[Quoted text hidden]

European Data Protection Board <no-reply@web.edpb.europa.eu>
Reply-To: European Data Protection Board <no-reply@web.edpb.europa.eu>
To: ekaterina@arga.world

21 October 2026 at 17:08

Dear Sergey Khrabrykh,

Thank you for your contribution to the public consultation "[Guidelines 04/2026 on the application of the power to impose administrative fines in relation to other corrective powers under the GDPR](#)".

[Quoted text hidden]



Ekaterina Khomutinnikova <ekaterina@arga.world>

Your feedback on EDPB Public Consultation

European Data Protection Board <no-reply@web.edpb.europa.eu>
Reply-To: European Data Protection Board <no-reply@web.edpb.europa.eu>
To: ekaterina@arga.world

21 October 2026 at 17:03

Dear Sergey Khrabrykh,

Thank you for your contribution to the public consultation "[Guidelines 02/2026 on Anonymisation](#)".

Your feedback has been sent to the EDPB, which will screen it and publish it. The file will be available on the website immediately after screening. Please note that this may mean that your contribution may not be immediately visible. We may also contact you concerning your submission, if necessary.

For more information about how your personal data is processed in the context of our public consultations, you can check our privacy statement for public consultations here: https://www.edpb.europa.eu/edpb-specific-privacy-statements_en

Kind regards,
The EDPB Secretariat



Ekaterina Khomutinnikova <ekaterina@arga.world>

Your feedback on EDPB Public Consultation

European Data Protection Board <no-reply@web.edpb.europa.eu>
Reply-To: European Data Protection Board <no-reply@web.edpb.europa.eu>
To: ekaterina@arga.world

21 October 2026 at 17:08

Dear Sergey Khrabrykh,

Thank you for your contribution to the public consultation "[Guidelines 04/2026 on the application of the power to impose administrative fines in relation to other corrective powers under the GDPR](#)".

[Quoted text hidden]