ACT Association for Competitive Technology

10 September 2026

Mr. Nenad Vujić
Minister of Justice
Ministry of Justice of the Republic of Serbia
Nemanjina 22-26, 11000 Belgrade, Republic of Serbia

cc: Commissioner for Information of Public Importance and Personal Data Protection
Ministry of Science, Technological Development and Innovation

Re: Comments of ACT on the Draft Law on Personal Data Protection (Public Consultation, 30 July to 10 September 2026)

The Association for Competitive Technology (ACT) appreciates the opportunity to comment on the Draft Law on Personal Data Protection (the Draft Law) that the Ministry of Justice has published for public consultation,[1] and we are submitting these comments to konsultacije@mpravde.gov.rs. We commend the Ministry for undertaking a full revision of the 2018 Law on Personal Data Protection,[2] for keeping the Draft Law anchored in the concepts of the EU General Data Protection Regulation (GDPR)[3] that Serbian businesses and their foreign partners already apply, for extending standard contractual clauses to all four transfer relationships, for introducing a structured test for further processing (Art. 31), and for declining to adopt fines calculated as a percentage of global turnover. These choices are consistent with the approach ACT recommends to governments around the world, and our recommendations below are intended to help the Draft Law meet its objectives without raising the cost of compliance for the small firms that build and sell software in and into Serbia.

I. Introduction and Statement of Interest

ACT is a not-for-profit global trade association representing the global small business technology developer community. Our members are entrepreneurs, independent developers, and small firms that build software applications and connected devices used by consumers and businesses in nearly every sector of the economy, including health, education, financial services, and public services, and many of them either operate in Serbia or serve Serbian users from abroad. Small developers depend on clear rules, predictable enforcement, and the ability to move data across borders in order to reach customers and to use cloud services, and they are also the firms least

[1] Ministry of Justice of the Republic of Serbia, public consultation on the Draft Law on Personal Data Protection (30 July to 10 September 2026), https://mpravde.gov.rs/javne-rasprave; see also Paragraf, Rasprava će trajati do 10. septembra 2026. godine, https://www.paragraf.rs/dnevne-vesti/310726/310726-vest8.html. The text of the consultation draft is reproduced at https://www.paragraf.rs/dnevne-vesti/310726/310726-vest13.html, and article references in these comments are to that draft.
[2] Law on Personal Data Protection, Official Gazette of the Republic of Serbia No. 87/2018.
[3] Regulation (EU) 2016/679 (General Data Protection Regulation), https://eur-lex.europa.eu/eli/reg/2016/679/oj.

able to absorb compliance costs that are not matched to real risks or to maintain one set of practices for Serbia and another for the European Union.

We have organised our specific comments to follow the order of the Draft Law, and we have preceded them with a summary of our recommendations and the general principles ACT applies to data protection frameworks everywhere.

II. Summary of Recommendations

For ease of reference in compiling stakeholder views, our principal recommendations are set out below, each of which is developed in the sections that follow.

1. Limit the AI section of the Draft Law to the legal basis for using personal data to develop and operate AI systems and the way individual rights apply to trained models, and leave any question of AI-specific classification, disclosure, or labelling duties to the separate process on artificial intelligence, which should first establish how existing law already applies (Arts. 52-53).
2. Recognise legitimate interest as an ordinary legal basis for developing and operating AI systems, subject to the same balancing test that applies to other processing under Article 20, rather than as a basis available only in exceptional cases, and permit the incidental processing of special categories of data in training datasets where the developer takes reasonable steps to avoid and remove it (Arts. 32 and 52(1)).
3. Retain the recognition in Article 52 that certain rights cannot be applied to trained models in the ordinary way, explain its technical basis in the explanatory memorandum, and clarify that the deletion duty on completion of the purpose applies to training data rather than to the model itself (Art. 52(3)-(5)).
4. Rely on the general rules on impact assessments and prior consultation for AI processing rather than requiring a Commissioner opinion on every high-risk system, and remove the AI interaction disclosure and labelling duties from the Draft Law or, if they are retained, allocate them by role with the exemptions found in comparable rules (Art. 53).
5. Rely on Article 62 alone for decisions based solely on automated processing, whether or not AI is involved, and limit Article 53(4)-(5) accordingly (Arts. 53, 62).
6. Remove the requirement of an established relationship from the definition of legitimate interest, and restore the word “automated” to the definition of profiling, so that both terms follow the GDPR (Art. 4).
7. Define the territorial scope for foreign controllers using the criteria of the 2018 Law and the GDPR of offering goods or services to, or monitoring the behaviour of, individuals in Serbia, and retain the exemption from appointing a representative for occasional, low-risk processing (Art. 3 and the provisions on representatives).
8. Clarify that an app relying on a device’s built-in biometric authentication, which never receives the biometric data, does not process biometric data, and that a PIN or password satisfies the duty to offer an alternative (Art. 32).
9. Clarify that suppliers of cameras, software, and storage that customers use to run their own video surveillance are not controllers of that surveillance (Arts. 45-51).

10. Allow parties to meet the Serbian standard contractual clauses by using the European Commission's clauses with a short Serbian addendum, and recognise adequacy decisions, binding corporate rules, and certifications recognised in other trusted systems (Arts. 103-108).
11. Adopt a risk-based threshold for notifying breaches to the Commissioner, have the Commissioner publish impact-assessment lists and templates aligned with those used in the EU, and publish the method for calculating the new proportional fines.
12. Provide a transition period of at least 18 months before the substantive obligations apply, with application of the AI provisions tied to the AI law and continued validity for transfer instruments already in place.

III. ACT's General Views on Data Protection

ACT supports strong and enforceable privacy protections, because the small developers we represent succeed only when their customers trust them with personal data. We encourage the Ministry to test the Draft Law against the following principles, which ACT applies to data protection frameworks in every jurisdiction.

- **Interoperability.** Serbia is a candidate for membership of the European Union, and many Serbian firms serve customers in the EU, so the practical value of the Draft Law depends on how closely it follows the GDPR and the direction of EU reform. Where definitions or legal bases diverge, small firms must run separate compliance programmes for closely linked markets, a cost that larger firms can absorb and small ones cannot.
- **Risk-based and scalable obligations.** Obligations should be proportionate to the risk of the processing and the size of the organisation, and documentation, assessment, and notification duties should be concentrated where harm is likely.
- **Trusted data flows.** Small developers rely on cloud services and international partners and cannot afford to duplicate storage and processing in every market in which they acquire a user, so data localisation requirements fall hardest on them, and a data protection framework should offer several lawful routes for cross-border transfers.[4] We welcome the fact that the Draft Law does not impose localisation, and we encourage the Ministry to keep it that way.
- **Clear rules for data used in AI.** Data protection law should protect personal data while avoiding undue barriers to the collection and processing of data on which AI development depends, applying reasonable data minimisation, consent, and consumer rights requirements and giving developers clear guidance on the legal bases, including legitimate interest, on which they may rely.[5]

[4] See ACT, Digital Trade for Small Tech, https://actonline.org/wp-content/uploads/Digital-Trade.pdf.
[5] See ACT, Policy Principles for Artificial Intelligence (Nov. 16, 2023), https://actonline.org/wp-content/uploads/2023-11-16-ACT-AI-Policy-Principles-FINAL.pdf; ACT, Digital Omnibus, https://actonline.org/digital-omnibus/.

- **Responsibility assigned by role.** Obligations should attach to the party that is actually able to meet them, so a small firm that builds an app on a model or platform supplied by others should not inherit duties that only the supplier can perform.[6]
- **Predictable enforcement and adequate time to comply.** Small firms comply best when guidance, standard clauses, and templates are available before obligations apply, and when regulators use corrective measures for first, good-faith errors.

IV. ACT's Specific Input on the Draft Law

1. Scope of the AI Provisions (Arts. 52-53)

The Draft Law introduces a section on AI-based processing that distinguishes high-risk systems, systems that communicate directly with individuals, and minimal-risk systems, and that requires the labelling of synthetic audio and video content. At the same time, a working group under the Ministry of Science, Technological Development and Innovation is preparing a separate Law on Artificial Intelligence with its own risk categories and transparency obligations.[7] If two statutes classify the same systems by risk, using different definitions and overseen by different authorities, developers will not know which classification applies and may have to assess a single product twice.

Much of what Articles 52 and 53 address is already governed by the general provisions of the Draft Law, which apply to personal data processed by an AI system in the same way as to any other processing, including the rules on legal bases, impact assessments, and automated decisions. We therefore encourage the Ministry to confine the AI section to the questions that are specific to data protection and that developers need answered, namely the legal basis for using personal data to develop and operate AI systems and the way individual rights apply to trained models, and to remove the classification of AI systems, the interaction disclosure duties, and the labelling requirement from the Draft Law. Whether Serbia needs AI-specific obligations of that kind at all is a question for the separate process on artificial intelligence, which should begin by establishing how consumer protection, product safety, data protection, and other existing laws already apply to the conduct concerned.[8]

2. Legal Basis and Individual Rights in AI Development (Art. 52)

Article 52(1) permits processing to develop, test, and apply AI systems where it is compatible with the original purpose of collection and, exceptionally, on the basis of a legitimate interest of the controller or a third party that outweighs the rights and freedoms of data subjects. As we read it, this reverses the ordinary test in Article 20, under which

[6] See ACT, AI Roles & Interdependency Framework, appended to Comments of ACT on the Development of an Artificial Intelligence Action Plan (Mar. 14, 2025), https://actonline.org/wp-content/uploads/ACT-Comment-re-AI-Action-Plan-14-Mar-2025-w-appendix.pdf.

[7] NALED, Srbija dobija Zakon o veštačkoj inteligenciji – Balans između inovacija i odgovornosti (11 June 2026), https://naled.rs/vest-srbija-dobija-zakon-o-vestackoj-inteligenciji-balans-izmedju-inovacija-i-odgovornosti-12196.

[8] ACT, Policy Principles for Artificial Intelligence, supra note 5 (recommending that policymakers understand how existing law already applies before adopting AI-specific rules).

processing is lawful unless the data subject's interests or fundamental rights override the controller's interest, and it would make legitimate interest harder to rely on for AI than for any other kind of processing. The European Data Protection Board has concluded that legitimate interest can serve as a legal basis for the development and deployment of AI models where the controller identifies a legitimate interest, shows that the processing is necessary to pursue it, and completes a balancing test that takes account of the reasonable expectations of data subjects and the safeguards applied,[9] and the European Commission's Digital Omnibus proposal would confirm in the GDPR itself that controllers may rely on legitimate interest to process personal data for the development and operation of AI systems, subject to safeguards,[10] a change that the EDPB and the European Data Protection Supervisor described as unnecessary because the GDPR already allows it.[11]

We encourage the Ministry to align Article 52(1) with that approach by deleting the word "exceptionally" and the requirement that the interest outweigh the rights of data subjects, and by applying the ordinary test in Article 20 together with the safeguards already listed in Article 52(2), such as pseudonymisation and data minimisation. The difference matters to small developers because consent is rarely workable for training data drawn from many sources, and a developer that can rely on legitimate interest in the EU but not in Serbia is likely to carry out its development work elsewhere. For the same reason, we encourage the Ministry to address special categories of data that appear incidentally in large training datasets despite a developer's efforts to exclude them, by permitting their processing where the developer takes appropriate measures to avoid collecting such data, removes it once identified unless removal would require disproportionate effort, and otherwise prevents it from being used in outputs, which is the approach the European Commission has proposed in the Digital Omnibus and with which the EDPB and EDPS have partly agreed.[12] Without such a provision, the general prohibition in Article 32 could make it very difficult to train a model on the large and varied datasets that many applications need.

Article 52(4) provides that rectification, erasure, restriction of processing, portability, and the protection against automated decisions do not apply to AI-based processing, and Article 52(3) allows access and objection to be refused where they would significantly impair the purpose of the processing. We support the Ministry's recognition that personal data often cannot be isolated and removed from a trained model, and that rights designed for records held in a database cannot always be applied to a model's parameters in the same way, a point reinforced by the EDPB's view that a model trained on personal data may

[9] European Data Protection Board, Opinion 28/2024 on certain data protection aspects related to the processing of personal data in the context of AI models (Dec. 2024), https://www.edpb.europa.eu/our-work-tools/our-documents/opinion-board-art-64/opinion-282024-certain-data-protection-aspects_en.
[10] European Commission, Proposal for a Regulation amending, among others, Regulation (EU) 2016/679 (Digital Omnibus), COM(2025) 837 final (19 Nov. 2025), proposed Art. 88c and amendments to Arts. 33 and 35. See European Parliament, Legislative Train Schedule, The Digital Omnibus Regulation Proposal, https://www.europarl.europa.eu/legislative-train/theme-a-new-plan-for-europe-s-sustainable-prosperity-and-competitiveness/file-digital-package.
[11] EDPB-EDPS Joint Opinion 2/2026 on the Proposal for a Regulation as regards the simplification of the digital legislative framework (Digital Omnibus) (Feb. 2026), https://www.edpb.europa.eu/our-work-tools/our-documents/edpbedps-joint-opinion/edpb-edps-joint-opinion-22026-proposal_en.
[12] Digital Omnibus proposal, supra note 10, proposed Art. 9(2)(k) and (5); EDPB-EDPS Joint Opinion 2/2026, supra note 11.

itself be anonymous where the likelihood of extracting personal data from it is insignificant.[13] Because a provision of this kind is likely to attract scrutiny, we encourage the Ministry to retain it, to set out its technical basis in the explanatory memorandum, and to confirm that controllers remain free to respond to requests through practical measures, such as excluding data from future training or filtering outputs, where they are able to do so. The protection against decisions based solely on automated processing is different in kind, because it concerns decisions taken about a person rather than the model, and we encourage the Ministry to leave that protection to Article 62, which applies whether or not AI is involved, as we explain in section 3.

Article 52(5) requires personal data to be deleted once the purpose of the AI processing is complete. We encourage the Ministry to clarify that this duty applies to training, validation, and testing datasets rather than to the trained model, and to permit controllers to keep data for as long as needed to document, audit, and monitor a system for accuracy and harmful bias, and to confirm in Article 31 that further processing to test, evaluate, and secure an AI system, including testing it for bias, is compatible with the purpose for which the data were collected.

3. AI Risk Categories, Transparency, and Automated Decisions (Arts. 53 and 62)

Article 53(1) requires an impact assessment for every high-risk AI system and makes each such assessment subject to an opinion of the Commissioner. The general rules of the Draft Law already require an impact assessment for processing likely to result in a high risk, whether or not AI is involved, and reserve prior consultation with the Commissioner for cases in which the assessment shows a high residual risk that the controller cannot mitigate (Art. 85). A separate AI-specific requirement would create a queue for every deployment classed as high-risk, including deployments by small firms of well-understood tools, and would draw the Commissioner's resources away from the cases that need them. We encourage the Ministry to delete the AI-specific assessment and opinion requirement and to rely on the general rules in Articles 84 to 87, and to provide that the Commissioner will take account of a controller's implementation of ISO/IEC 42001[14] when assessing the organisational measures described in an impact assessment, so that a certified firm does not have to document the same practices twice.

Article 53(2), (3), and (6) would require controllers to tell individuals when they are interacting with an AI system and to label synthetic audio and video content. These duties apply whether or not personal data are processed, and transparency mandates of this kind should follow evidence about the circumstances in which they actually help address a risk,[15] so we encourage the Ministry to remove them from the Draft Law for the reasons given in section 1. If the Ministry nonetheless retains them, we encourage it to allocate them by role, so that a small developer that builds an app on a general-purpose model is

[13] EDPB Opinion 28/2024, supra note 9.
[14] ISO/IEC 42001:2023, Artificial intelligence management systems, https://www.iso.org/standard/81230.html.
[15] ACT, Policy Principles for Artificial Intelligence, supra note 5 (calling for research on the costs and benefits of transparency to determine how and under which circumstances transparency mandates would help address risks).

responsible for telling its own users that they are dealing with AI while the model provider is responsible for any marking of the model's outputs, and to remove the notification duty for general-purpose AI models, which do not themselves interact with individuals. In that case we also encourage the Ministry to exempt situations in which the use of AI is obvious from the context, systems that perform an assistive editing function or do not substantially alter the input, and evidently artistic, satirical, or fictional works, to accept machine-readable marking based on open technical standards for content provenance rather than a visible label on every output, and to limit any labelling duty to content that could mislead a reasonable person about its authenticity. Each of these limits appears in Article 50 of the EU AI Act,[16] and a Serbian rule without them would be stricter than the EU's own.

Article 53(4) restates, in different words, the rule in Article 62 on decisions based solely on automated processing that produce legal or similarly significant effects, and Article 53(5) appears to permit fully automated AI processing only for statistical, scientific, or historical purposes. If Article 53(5) were read to cover all fully automated processing rather than only such decisions, it would prohibit routine functions such as spam filtering, fraud detection, and security monitoring, and we doubt that is the Ministry's intention. We encourage the Ministry to rely on Article 62 alone for automated decisions, applying it in the same way whether or not AI is involved, and to delete Article 53(4)-(5) or limit it expressly to decisions producing legal or similarly significant effects.

4. Definitions and Legal Bases (Arts. 4, 14, and 20)

We welcome the Ministry's decision to define legitimate interest by reference to necessity, suitability, proportionality, and the reasonable expectations of data subjects, which reflects the way the GDPR test is applied in practice. As drafted, however, the definition applies only to processing carried out within a relationship already established with the data subject. That condition would exclude many cases in which no prior relationship exists, including some of the purposes the definition itself gives as examples, since fraud prevention and information security often involve people who have no relationship with the controller, as well as checks carried out before a contract is concluded and the development of AI models on data drawn from many sources, all of which the GDPR recognises as capable of resting on legitimate interest (Recitals 47 to 49). We encourage the Ministry to delete the reference to an established relationship and to treat the existence and nature of any relationship as a factor in the balancing test rather than as a precondition. Because the Draft Law also reorders the legal bases in Article 14, we encourage the Ministry to add a sentence to Article 14 stating that each of the listed bases is of equal standing and that the order in which they appear establishes no priority among them.

The definition of profiling in Article 4 no longer refers to automated processing and would therefore capture[17] any evaluation of personal aspects, including an ordinary manual

[16] Regulation (EU) 2024/1689 (Artificial Intelligence Act), Art. 50, https://eur-lex.europa.eu/eli/reg/2024/1689/oj.

[17] Draft Law, Art. 4 ("profilisanje je svaki oblik obrade koji se koristi da bi se ocenilo određeno svojstvo ličnosti"). Compare GDPR, Art. 4(4) ("any form of automated processing of personal data consisting of the use of personal data to evaluate certain personal aspects relating to a natural person").

review of a job application or a loan file. Because profiling triggers the protections of Article 62 and related transparency duties, we encourage the Ministry to restore the word "automated", consistent with Article 4(4) of the GDPR and the 2018 Law, so that these protections continue to apply where they were designed to apply.

5. Territorial Scope and Representatives (Art. 3)

Article 3 applies the Draft Law to controllers and processors established in Serbia and, for those established elsewhere, to the processing of data of persons resident in Serbia where the processing is carried out "within activities on the territory of the Republic of Serbia." That phrase could be read either to require an operational presence in Serbia or to reach any service that Serbian residents use, and a small developer outside Serbia whose app is downloaded by a handful of Serbian users cannot tell from it whether it is covered. We encourage the Ministry to return to the criteria used in the 2018 Law and in Article 3(2) of the GDPR, under which a foreign controller is covered where it offers goods or services to individuals in Serbia or monitors their behaviour in Serbia, since these criteria are familiar to firms worldwide and have been clarified by guidance and case law. We also encourage the Ministry to retain the exemption, found in the 2018 Law and in Article 27(2) of the GDPR, from the duty to appoint a representative in Serbia for processing that is occasional, does not involve special categories of data on a large scale, and is unlikely to result in a risk to individuals.

6. Special Categories and Biometric Data (Art. 32)

Article 32 provides that where biometric data are processed on the basis of consent for identification, the individual must be offered a less intrusive alternative. Many apps allow users to sign in using the biometric authentication built into their phone or computer, in which the fingerprint or facial template remains on the device under the user's control and the app receives only a confirmation that authentication succeeded. We encourage the Ministry to clarify that an app using such a feature does not process biometric data for the purposes of the Draft Law, and that for any controller a PIN, password, or passcode is a sufficient alternative. This clarification would encourage the use of authentication methods that are both more secure and more private than passwords alone.

7. Video Surveillance (Arts. 45-51)

The new video surveillance chapter places its obligations for signage, written decisions, records, and retention on the person who decides to install and operate a system, which we support. Many small firms supply the cameras, apps, and cloud storage that households and businesses use to run their own systems, and we encourage the Ministry to state expressly that a supplier of hardware, software, or storage that processes footage only on its customer's instructions acts as a processor, or falls outside the Draft Law where it has no access to the footage, and does not bear the controller's obligations under Articles 45 to 51.

8. Cross-Border Transfers (Arts. 103-108)

We welcome the extension of standard contractual clauses to controller-to-controller, controller-to-processor, processor-to-processor, and processor-to-controller transfers, and the express duty on the Commissioner to prepare and publish them. Most Serbian firms that transfer data abroad, and most foreign firms that receive it, already use the European Commission's standard contractual clauses,[18] and a second set of clauses with different wording would add cost without adding protection. We encourage the Ministry to provide that parties may meet the Serbian requirement by using the Commission's clauses together with a short Serbian addendum, as the United Kingdom has done with its addendum to the EU clauses.[19]

We also encourage the Ministry to confirm that jurisdictions and frameworks covered by an adequacy decision of the European Commission, including organisations certified under the EU-U.S. Data Privacy Framework,[20] are treated as providing an adequate level of protection without the need for a separate national listing, to recognise binding corporate rules approved by EU supervisory authorities, and to allow certification mechanisms, including the Global Cross-Border Privacy Rules system,[21] to serve as a basis for transfer. On the derogation for occasional transfers based on a compelling legitimate interest (Art. 108), we encourage the Commissioner to publish guidance on when a transfer is "not repetitive" and what the required notification must contain, since the meaning of "not repetitive" under the corresponding GDPR provision has caused uncertainty for small firms.[22]

9. Breach Notification and Impact Assessments (Arts. 82 and 84-87)

The Draft Law retains the duty to notify the Commissioner of a personal data breach within 72 hours. Notification of low-risk breaches consumes the time of small firms and regulators alike without improving outcomes for individuals, and the European Commission has proposed in the Digital Omnibus to require notification to the supervisory authority only for breaches likely to result in a high risk and to allow more time to prepare it.[23] We encourage the Ministry to adopt the same threshold and timeline, so that a firm operating in both markets can follow a single incident response plan.

For impact assessments, we encourage the Commissioner to publish lists of processing operations that do and do not require an assessment, aligned with the EU-level lists the

[18] Commission Implementing Decision (EU) 2021/914 of 4 June 2021 on standard contractual clauses for the transfer of personal data to third countries, https://eur-lex.europa.eu/eli/dec_impl/2021/914/oj.
[19] Information Commissioner's Office, What are standard data protection clauses (the UK IDTA and the Addendum)?, https://ico.org.uk/for-organisations/uk-gdpr-guidance-and-resources/international-transfers/appropriate-safeguards/what-are-standard-data-protection-clauses-the-uk-idta-and-the-addendum/.
[20] Commission Implementing Decision (EU) 2023/1795 of 10 July 2023 on the adequate level of protection of personal data under the EU-US Data Privacy Framework, https://eur-lex.europa.eu/eli/dec_impl/2023/1795/oj.
[21] Global Cross-Border Privacy Rules Forum, https://www.globalcbpr.org/.
[22] See ACT, Comments to the Article 29 Working Party re Guidelines on Article 49 of Regulation 2016/679 (Mar. 26, 2018), https://actonline.org/wp-content/uploads/03262018_ACT_Filing_WP29_Art49-FINAL.pdf.
[23] Digital Omnibus proposal, supra note 10, proposed amendments to Art. 33; see also EDPB-EDPS Joint Opinion 2/2026, supra note 11 (agreeing with the higher threshold and the longer deadline).

Digital Omnibus would introduce, together with a short template suited to small enterprises. Clear lists reduce both over-compliance by cautious firms and under-compliance by firms that do not know the rules apply to them.

10. Penalties

We support the Ministry's decision to keep the maximum fine for legal entities at its current level and not to introduce fines based on global turnover. The Draft Law also introduces a proportional fine of up to twenty times the value of the damage caused or the obligation not performed, capped at five times the highest prescribed fine.[24] We encourage the Ministry to set out in the law, or to require the Commissioner to publish, the method for valuing damage and unperformed obligations, making clear that damage means damage established in the proceedings rather than harm that is merely alleged, and to require that the size of the enterprise, good faith, and cooperation be taken into account. We also encourage the Ministry to give the Commissioner an express power to issue a warning or corrective order instead of a fine for a first, unintentional violation by a micro or small enterprise, which would direct enforcement toward compliance rather than punishment where that is the better outcome.

11. Entry into Force and Transition

As we understand it, the Draft Law would enter into force eight days after publication, with no transition period for the substantive obligations and with nine months allowed for secondary legislation. Controllers would therefore be required to comply with new obligations, including video surveillance records, AI impact assessments, and new transfer clauses, before the Commissioner has published the clauses, lists, and guidance on which compliance depends, whereas the 2018 Law allowed nine months and the GDPR allowed two years before their obligations applied.

We encourage the Ministry to provide a transition period of at least 18 months before the substantive obligations apply, to tie the application of the AI provisions to the corresponding obligations of the AI law, and to provide that contracts and transfer clauses concluded under the 2018 Law remain valid for a reasonable period, such as 12 months, after the Commissioner publishes the new clauses. We also encourage the Ministry to ask the Commissioner to publish guidance on the principal new obligations before they apply.

V. Conclusion

ACT supports the Ministry's aim of a modern data protection law that protects individuals, supports Serbia's digital economy, and brings Serbian law closer to that of the European Union. We encourage the Ministry to carry the recommendations above into the final text, in particular by limiting the AI provisions to questions of data protection, recognising legitimate interest as an ordinary basis for AI development, keeping definitions and transfer tools aligned with the GDPR, and allowing enough time for small firms to comply. We appreciate the opportunity to contribute to

[24] Petar Mijatović, Serbia's draft Personal Data Protection Law: What changes are on the table, IAPP (6 Aug. 2026), https://iapp.org/news/a/serbia-s-draft-personal-data-protection-law-what-changes-are-on-the-table.

this consultation, and we would welcome the chance to discuss these comments with the Ministry and to share the experience of small developers in other markets that have implemented comparable frameworks.

Sincerely,

Brian Scarpelli
Senior Global Policy Counsel

Chapin Gregor
Policy Counsel

Association for Competitive Technology