

Designing Olivia AI: User Expectations for a Trustworthy GDPR Compliance Assistant

Anamarija Mladinić

University of Zagreb

Faculty of Organization and Informatics

Pavlinka 2, 42000 Varaždin, Croatia

amladinic25@student.foi.hr

Abstract. *This paper examines whether Olivia, a Croatian GDPR compliance platform, should evolve into an AI-assisted compliance assistant. Based on 686 responses from registered Olivia users, the study analyses satisfaction with the existing tool, expectations for AI-supported GDPR guidance, and the need for a module assessing GDPR compliance in concrete AI tool use. The results show strong demand for such a module and confirm that trust safeguards, especially official sources and clear limitations, are essential for adoption. The paper argues that Olivia AI should be designed as a controlled, source-based compliance workflow, not as a generic chatbot.*

Keywords. GDPR, artificial intelligence, AI governance, data protection, SMEs

1 Introduction

Since 25 May 2018, the General Data Protection Regulation (GDPR) has been fully applicable across the European Economic Area (European Parliament and Council, 2016). For many smaller organisations, the difficult part has never been merely reading the Regulation, but translating it into everyday work: choosing a lawful basis, informing data subjects, keeping records, assessing risks, managing processors and reacting to data breaches. This is particularly relevant in Croatia, where micro, small and medium-sized enterprises (SMEs) dominate the economy and crafts also represent a large part of business activity. These organisations often process personal data daily, but do not necessarily have internal legal, IT or data protection capacity.

Earlier Croatian evidence already pointed to an implementation gap. In the EU-funded Awareness Raising Campaign for SMEs (ARC I) project, aimed at supporting Croatian SMEs in their efforts to comply with the GDPR, many SMEs recognised that GDPR compliance mattered for business, but far fewer had reviewed their processing activities or felt confident

that their staff had enough information to act in line with GDPR obligations. The same study also showed strong demand for a practical and free digital tool (Mladinić, Vukić, & Rončević, 2023). Olivia was developed in that context by the Croatian Personal Data Protection Agency (AZOP) and the Faculty of Organization and Informatics (FOI) as part of the ARC II project.

Olivia is a web-based GDPR tool designed as a free and practical platform for GDPR awareness, e-learning and compliance support, primarily for SMEs (Olivia GDPR ARC, 2025). The current platform includes GDPR learning modules, quizzes, certificates, self-assessment questionnaires, practical templates and tools supporting the preparation of privacy notices, consent forms, legitimate interest assessments, records of processing activities, templates and other compliance documents. However, the platform is still largely modular and user-driven: users must know which topic is relevant, which module to open and how to connect different outputs into a coherent compliance workflow.

This limitation becomes particularly relevant in the context of tools based on artificial intelligence (AI). Organisations using AI need to assess several connected GDPR questions at once, including whether personal data are processed, which legal basis applies, whether data subjects are informed, whether profiling or automated decision-making is involved, whether a data protection impact assessment is required and which safeguards should be documented. This raises the question of whether Olivia should evolve from a digital GDPR support tool into a more interactive, AI-assisted compliance assistant.

Since 2025, the regulatory and technological context has shifted substantially, particularly due to the wider adoption of AI tools and the evolving EU digital regulatory framework. Organisations that still struggle with basic GDPR questions increasingly use AI tools for analytics, automation, customer interaction or internal productivity (Croatian Employers' Association, 2025; Croatian Chamber of Economy, 2024). This creates a more specific compliance

problem: not simply how to comply with the GDPR, but how to understand GDPR duties when a concrete AI tool processes, stores or helps generate information about individuals. The key issue is therefore not whether Olivia should use AI, but under what governance conditions users would trust such support.

The aim of this paper is to determine the extent to which users recognise the need for a tool that would help organisations understand and assess GDPR obligations linked to concrete AI tools or AI systems, and which elements of usefulness, trust and regulatory assurance should be embedded in its design so that Olivia can become a responsible digital innovation in the field of GDPR and AI compliance.

Accordingly, the main research question is: to what extent do users of the Olivia platform recognise the need to develop an AI/GDPR self-assessment tool that would help organisations understand and verify GDPR obligations related to the use of specific AI tools or artificial intelligence systems? The study tests four hypotheses focused on users' need for an AI/GDPR self-assessment module, its relationship with adoption readiness, and the role of trust safeguards:

H1: Users of the Olivia platform express a high need for an AI/GDPR self-assessment module that supports both understanding GDPR obligations related to AI tools and assessing GDPR compliance in concrete AI tool use.

H2: A higher need for an AI/GDPR self-assessment module is positively associated with users' readiness to use AI Olivia.

H3: The need for an AI/GDPR self-assessment module significantly predicts users' readiness to use AI Olivia, even after controlling for organisational and user-related characteristics.

H4: Trust safeguards, particularly the inclusion of official sources, relevant GDPR provisions and clear limitations of the tool, are positively associated with users' readiness to use AI Olivia.

The rest of the paper is structured as follows. Section 2 presents the theoretical and regulatory background, focusing on the relationship between GDPR, AI governance and technology acceptance. Section 3 describes the methodology, including the survey design, sample, variables and statistical methods. Section 4 presents the results of the descriptive, correlational, regression and thematic analyses. Section 5 discusses the findings in relation to the hypotheses and derives design implications for Olivia AI. Section 6 concludes the paper by summarising the scientific and practical contribution of the study.

2 Theoretical Background and Research Context

The European Union (EU) digital regulatory environment is dense and still moving. Alongside the GDPR, organisations must now consider the AI Act, the Data Act, the Data Governance Act, the Digital Services Act, the NIS2 Directive and sector-specific rules, creating an increasingly complex compliance environment (Graux et al., 2025). The Digital Omnibus package confirms that the EU is trying to simplify and clarify this regulatory environment, but it does not remove organisational responsibility (European Commission, 2025). Simplification does not mean that controllers may stop assessing legal basis, transparency, data subject rights, data protection impact assessment (DPIA) requirements or security measures. On the contrary, clearer rules increase the expectation that organisations will be able to operationalise them.

This question is central for AI use. If personal data are used in the development or operation of AI systems, organisations need to understand the purpose of processing, lawful basis, transparency duties, possible rights of objection, risks to data subjects and the need for technical and organisational safeguards (European Data Protection Board, 2024; Sartor & Lagioia, 2020). The AI Act adds further obligations, especially for high-risk systems, but it does not replace the GDPR; rather, the two regimes operate as complementary layers of EU digital governance (European Parliament and Council, 2024; Hohmann & Kollár, 2025; Holtz & Ledendal, 2026; Sartor & Lagioia, 2020). A tool such as Olivia could be particularly important for Croatian startups and other organisations developing high-risk AI systems, since bringing such products to the EU market requires not only demonstrating compliance with the AI Act, but also ensuring and documenting compliance with the GDPR whenever the system involves the processing of personal data. A compliance tool dealing with AI cannot be limited to AI Act classification; it must also ask whether and how personal data are processed, because GDPR obligations apply whenever AI development or deployment involves personal data (European Data Protection Board, 2024; Croatian Personal Data Protection Agency, 2025).

For SMEs and other smaller organisations this is a practical problem. They may use commercially available AI tools without fully understanding whether prompts, documents, customer records or employee data are processed, stored or reused for model improvement. They may also rely on vendors without sufficiently assessing controller-processor roles, transfers outside the EEA, retention periods or contractual safeguards. A general statement that AI must be used lawfully is not operationally useful. What smaller organisations need is a sequence of concrete questions that translates legal requirements into an assessment workflow.

The survey instrument partly follows the logic of the Technology Acceptance Model, especially perceived usefulness and behavioural intention to use

(Davis, 1989; Venkatesh & Davis, 2000). However, a GDPR/AI assistant is a legally sensitive tool, so usefulness alone is insufficient. Trust, source reliability and clear limitations are part of adoption. This is consistent with work on trust in automation and intelligent systems acceptance, as well as broader discussions on transparency and the black-box problem in AI (Lee & See, 2004; Vorm & Combs, 2022; Zerilli et al., 2022; von Eschenbach, 2021). In the context of regulatory compliance, a wrong but confident answer, or an explanation that appears convincing but is misleading, can create legal risk (Lakkaraju & Bastani, 2020). Therefore, adoption readiness must be analysed together with governance safeguards.

The point of Olivia AI should not be to make the existing platform sound more like a chatbot. Its value would be in helping users move from general GDPR information to a structured assessment of what they actually need to check when using AI tools. For that reason, the system should be based on verified sources, clear limits, traceable outputs and safeguards against overconfident legal answers. The paper therefore connects three issues that cannot be separated in this context: whether users would accept such a tool, whether it would support GDPR compliance in practice, and whether it could be governed responsibly. In this sense, the research links technology acceptance, data protection compliance and AI governance (Batool et al., 2024; Papagiannidis et al., 2025; Raji et al., 2020).

This approach also reflects a broader shift in digital regulation. The EU increasingly expects organisations to translate abstract legal requirements into documented governance processes. In the GDPR, this is visible through accountability, records of processing activities, data protection impact assessment, processor management and breach documentation. In the AI Act, the same logic appears through risk classification, transparency duties, technical documentation, human oversight and post-market monitoring for higher-risk systems. Although Olivia AI would not itself be designed as a high-risk AI system, its subject matter is high-stakes because it guides users through legal and organisational choices. The design must therefore make legal uncertainty visible rather than hide it behind a fluent answer, and should be aligned with responsible AI governance and auditability practices (Papagiannidis et al., 2025; Raji et al., 2020).

For that reason, the proposed module is not a substitute for legal advice. Its value lies in helping non-expert users identify the relevant issues before they make decisions. In practice, this means asking better questions: Is personal data entered into the tool? Is the AI provider a processor, controller or independent controller? Are prompts stored? Are they used to train the model? Is there a transfer outside the EEA? Is the output used to make decisions about individuals? These questions are the entry points for GDPR analysis and for deciding whether additional expert review is required.

3 Methodology

An online questionnaire was conducted through the European Commission's EU Survey platform from 11 to 20 May 2026. The invitation was sent to 7,314 registered active Olivia users, with a reminder sent on 18 May. In total, 686 valid responses were collected, corresponding to a response rate of 9.38%. All closed questions were mandatory, so questions 1 to 19 had no missing answers. The sample is sufficiently large for descriptive and inferential statistical analysis; however, it should be interpreted as a sample of responding Olivia users rather than a representative sample of all Croatian organisations. The survey data used in this paper are based on the Olivia User Survey conducted in 2026 (Olivia User Survey, 2026). The questionnaire included 20 questions organised into several blocks. The first block covered respondent and organisational profile: type of organisation, role of the respondent, existence of a data protection officer (DPO) or other GDPR support and frequency of Olivia use. The second block examined the purposes for which Olivia had been used, such as understanding GDPR obligations, lawful bases, data subject rights, records of processing activities, security measures, privacy notices, video surveillance, cookies and webinars. The third block measured satisfaction with the existing Olivia platform. The fourth block measured perceived usefulness of a future AI version of Olivia. The final block measured trust safeguards, concern about incorrect or oversimplified AI answers and readiness to use AI Olivia.

Likert-scale answers were coded from 1 to 5. Data preparation and manual coding of open-ended answers were conducted in Microsoft Excel. Quantitative analyses were conducted in jamovi Desktop 2.7.30. The analyses included descriptive statistics, reliability analysis using Cronbach's alpha, Spearman correlations, Kruskal-Wallis and Mann-Whitney tests, and binary logistic regression. Statistical significance was assessed at the 5% level ($p < 0.05$).

Several composite variables were created. Satisfaction with the existing Olivia platform was measured through six items. Perceived usefulness of AI Olivia was measured through items addressing AI-supported guidance, search time, tailored recommendations, checklists, forms and DPIA screening. Trust in safeguards was measured through items addressing official sources, GDPR provisions, links to official materials and clear limits of the tool. Questions 14 and 15 were combined into a two-item construct measuring the need for a module assessing GDPR compliance in the use of AI tools. Question 19 was used as the main dependent variable for adoption readiness.

Because Likert items are ordinal, Spearman's rho was used to test associations between the need construct, trust safeguards, concern about incorrect answers and readiness to use AI Olivia. Group differences were examined with non-parametric tests.

A binary logistic regression was then used to test whether the need for the AI-tool GDPR compliance module predicts readiness to use AI Olivia. Answers 4 and 5 on Question 19 were coded as readiness to use, while answers 1 to 3 were coded as neutral or negative. The model included organisational type, GDPR support, frequency of use, respondent role, trust safeguards and concern about incorrect answers as controls.

The open-ended Question 20 asked respondents to provide additional suggestions for improving Olivia or developing the future AI virtual assistant. Responses were coded manually using thematic coding. Empty or non-substantive answers were removed. The unit of analysis was the individual comment. A primary thematic code was assigned to each substantive comment, with additional codes used where comments covered more than one theme. This qualitative component was used to interpret and deepen the quantitative findings.

The coding was used as an interpretative layer to help identify whether the numerical support for AI Olivia was unconditional or whether users attached specific expectations to it. The latter proved to be the case. The most frequent themes were not novelty, automation or speed, but trust, accuracy, official sources, human oversight and practical guidance. This qualitative evidence is important because it prevents overinterpreting high agreement with AI functionality as unqualified enthusiasm for automation.

4 Results

The respondent structure shows that Olivia is used both by its original target group and by a wider range of organisations. When micro, small and medium-sized enterprises are grouped together, SMEs represent the largest share of respondents, with 250 responses, or 36.45% of the sample. Large enterprises account for 28.72%, while public authorities represent 24.93%. Crafts and self-employed activities account for 3.64%, non-profit organisations for 3.35%, and other organisations for 2.92%. This confirms that Olivia is relevant for SMEs, but also that its use extends well beyond them.

Data protection officers represented the largest respondent group (30.61%), followed by employees (23.03%), administrative or business staff (13.41%) and lawyers (13.27%). Most respondents came from organisations with an appointed DPO (67.93%) or another legal/GDPR support function (17.49%). This suggests that the sample includes many users who are already aware of data protection obligations.

Olivia is most often used occasionally. Almost half of the respondents used it several times per year (47.23%), while 34.69% had used it only once. The most common reason for using Olivia was understanding basic GDPR obligations (60.50%), followed by viewing webinars or presentations

(36.88%) and support in determining the lawful basis for processing (27.41%). Other reported purposes included data subject rights, records of processing activities, security measures, privacy notices, breaches and specific topics such as video surveillance or cookies. This confirms that Olivia functions both as an awareness tool and as practical compliance support.

Satisfaction with the existing platform was high. A total of 87.61% agreed that Olivia is useful as a digital tool for GDPR information, 86.30% agreed that it is easy to use and 80.91% agreed that it helps them understand what their organisation should do to comply with the GDPR. The somewhat lower, but still positive, score for everyday practical usefulness for small and medium-sized organisations (72.74%) indicates room for improvement. The satisfaction scale had a mean of 4.12, median of 4.17, standard deviation of 0.69 and Cronbach's alpha of 0.920, indicating very high internal consistency.

Expectations for AI Olivia were also high. Users supported functions that would reduce search time (83.67%), provide guidance adapted to organisation type and processing context (83.24%), support basic forms (83.23%), support DPIA screening (82.66%) and provide interactive GDPR checklists (80.32%). The perceived usefulness scale had a mean of 4.19, median of 4.22, standard deviation of 0.76 and Cronbach's alpha of 0.964. This very high reliability suggests that users see these AI functions as connected elements of a broader AI-assisted compliance tool.

The strongest result for the research question comes from Questions 14 and 15. A total of 79.44% agreed that Olivia support would be useful for understanding GDPR obligations related to AI systems or AI tools, including lawful basis, transparency, data subject rights and security. Similarly, 78.86% agreed that an interactive assessment of GDPR compliance in the use of a concrete AI tool would be useful. These two items formed a reliable two-item construct, with a mean of 4.13, median of 4.00, standard deviation of 0.82 and Cronbach's alpha of 0.905. The result shows that users do not only want general AI guidance; they want a concrete module for assessing GDPR obligations in specific AI tool use.

Trust was the most emphatic user requirement. The highest agreement in the whole questionnaire concerned official sources: 86.74% would trust AI Olivia more if answers included official sources, relevant GDPR provisions or links to additional official materials. In addition, 72.31% would trust the tool more if it clearly stated that it provides general information rather than individual legal advice. Concern about incorrect or oversimplified answers was also substantial: 52.63% agreed that such concern could deter them from using AI Olivia. Nevertheless, 82.36% stated that they would be ready to use AI Olivia if it had useful functionalities and clear safeguards. The key descriptive findings are summarised in Table 1.

Table 1. Key descriptive findings on existing Olivia and expected AI support

Item	% Agreement (4 or 5)	Mean
Existing Olivia is useful as a digital GDPR information tool	87.61%	4.33
An AI upgrade of Olivia would be useful	78.28%	4.18
Need for support in understanding GDPR obligations related to AI tools (Q14)	79.44%	4.14
Need for an interactive assessment of concrete AI tool use (Q15)	78.86%	4.13
More trust if answers include official sources and GDPR provisions	86.74%	4.43
Readiness to use AI Olivia (Q19)	82.36%	4.15

Spearman correlations confirmed the link between module need and adoption readiness. The need construct was positively and significantly associated with readiness to use AI Olivia ($\rho = 0.585$, $p < 0.001$). Questions 14 and 15 were also individually associated with readiness ($\rho = 0.559$ and $\rho = 0.568$, both $p < 0.001$). The need construct was positively associated with trust safeguards ($\rho = 0.497$, $p < 0.001$), but it was not significantly associated with concern about incorrect answers ($\rho = -0.036$, $p = 0.352$). Group comparisons showed that the need for the module did not significantly differ by organisation type. The need was present across SMEs, large enterprises, public authorities and other organisations. A statistically significant but small difference was found according to GDPR support in the organisation ($H = 11.954$, $p = 0.018$), with the lowest need among respondents who were unsure whether their organisation had GDPR support. Frequency of Olivia use mattered more clearly: occasional and regular users expressed a higher need for the module than one-time users ($H = 15.969$, $p < 0.001$). Differences by respondent role were not statistically significant ($H = 10.996$, $p = 0.089$).

Binary logistic regression showed that need for the AI-tool GDPR compliance module significantly predicted readiness to use AI Olivia (OR = 3.69, 95% CI: 2.55-5.34, $p < 0.001$), controlling for organisational and user-related characteristics. Trust safeguards were also a significant predictor (OR = 2.20, 95% CI: 1.53-3.16, $p < 0.001$). Concern about incorrect or oversimplified answers was not significant (OR = 1.06, $p = 0.682$). Model quality was good, with AUC = 0.853 and Nagelkerke $R^2 = 0.403$. Predicted probabilities illustrate the effect: when module need is at level 3, readiness is about 57%; at level 4, about 83%; and at level 5, about 95%. The main regression estimates are presented in Table 2.

Table 2. Binary logistic regression predicting readiness to use AI Olivia

Predictor	OR = odds ratio	95% CI = confidence interval	p
AI/GDPR self-assessment need (Q14+Q15)	3.69	2.55-5.34	<0.001
Governance trust (Q16+Q17)	2.20	1.53-3.16	<0.001
Risk concern (Q18)	1.06	0.82-1.36	0.682

The open-ended comments supported the quantitative findings. Of 686 respondents, 174 left some response to Question 20; after removing non-substantive answers, 85 substantive comments remained. The most frequent theme was trust, sources, accuracy and human oversight (36.5% of coded comments). Other themes included guided procedures, self-assessment and documents (16.5%), practical examples and concrete interpretations (12.9%), AI functionalities and contextual adaptation (10.6%), and scepticism or risks linked to AI (10.6%). One comment was particularly important because it suggested documenting and publishing the development of Olivia AI as an example of compliance for other AI deployers and providers. This expands Olivia's relevance beyond a user-facing tool: it could also serve as a demonstrator of responsible AI governance in the public interest. The distribution of primary qualitative themes is shown in Table 3.

Table 3. Main themes from open-ended responses

Code	Main theme	Frequency	% of substantive comments
T4	Trust, sources, accuracy and human oversight	31	36.47%
T2	Guided procedures, self-assessment and documents	14	16.47%
T1	Practical examples and concrete interpretations	11	12.94%
T3	AI functionality and adaptation to user context	9	10.59%
T7	Scepticism and AI-related risks	9	10.59%
T5	Education, webinars, updates and continuous support	6	7.06%

T6	User experience and technical improvements	5	5.88%
----	--	---	-------

Taken together, the descriptive, inferential and qualitative results point in the same direction. Users want structured support for decisions that are currently difficult to make, especially when AI tools are involved. The strongest demand is therefore located at the intersection of practical usefulness and governance safeguards.

5 Discussion

The findings support all four hypotheses. H1 is supported by strong agreement with the two items measuring the need for AI/GDPR support: 79.44% of respondents agreed that Olivia support would be useful for understanding GDPR obligations related to AI systems or AI tools, and 78.86% agreed that an interactive assessment of GDPR compliance in concrete AI tool use would be useful. H2 is supported by the significant positive correlation between the AI/GDPR self-assessment need construct and readiness to use AI Olivia ($\rho = 0.585$, $p < 0.001$). H3 is supported by the binary logistic regression model, where the need for the module remains a significant predictor of adoption readiness after controls ($OR = 3.69$, $p < 0.001$). H4 is supported by the significant role of trust safeguards in predicting readiness to use AI Olivia ($OR = 2.20$, $p < 0.001$). The empirical answer to the research question is therefore clear: Olivia users strongly recognise the need for a module that helps organisations understand and assess GDPR obligations related to concrete AI tools or AI systems. At the same time, the results draw an important boundary. Users do not want a confident but uncontrolled chatbot. They want a tool that cites official sources, explains its limits, avoids false legal certainty and supports structured assessment. This is not a minor design preference. In a regulatory domain, a convincing but wrong answer can mislead the user into non-compliance. The future system therefore needs to be designed around legal reliability, not only conversational convenience.

The findings also fit an extended technology-acceptance logic. Perceived usefulness clearly matters, as shown by the strong support for AI functions and the predictive effect of the AI-tool assessment need. However, usefulness is not enough. Users are willing to adopt AI support when usefulness is combined with safeguards: official sources, GDPR references, links to additional materials and clear limits. This is especially relevant because more than half of respondents expressed concern that incorrect or oversimplified answers could deter them from using AI Olivia. Users are not rejecting AI; they are asking for controlled AI.

These results have direct implications for the design of Olivia AI. The upgrade should turn Olivia into a guided compliance workflow. The system could

first ask users about the organisation, sector, role in processing and type of processing activity, and then direct them to relevant compliance steps. If the user does not inform data subjects, Olivia should lead to the privacy notice module. If legitimate interest is used, it should trigger the legitimate interest assessment. If AI or high-risk processing is involved, it should trigger DPIA-related questions.

The most distinctive functionality should be a module assessing GDPR compliance in the use of AI tools. The proposed workflow is shown in Fig. 1.

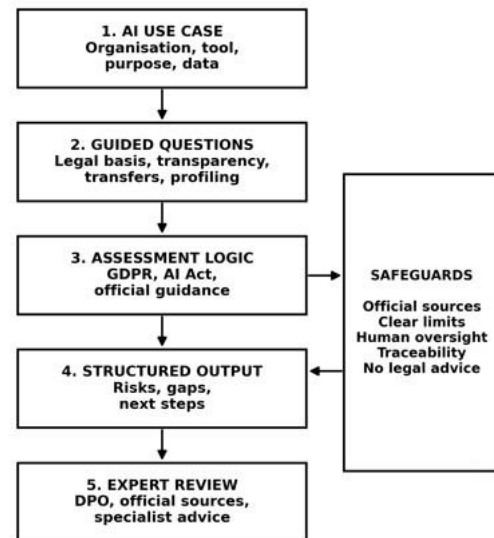


Figure 1. Proposed Olivia AI self-assessment workflow

This module should not assess “AI” in general, but a specific use of a specific AI tool in a specific organisational context. It should ask whether personal data are entered into the tool, which categories of data are processed, whether special categories of data are involved, whether the tool is used for profiling or decision-making, whether input data are used for model training, where data are stored, which provider is involved, whether transfers outside the European Economic Area (EEA) occur and whether data subjects are properly informed. The output should not state that the user is “GDPR compliant”. It should provide a structured overview of risks, missing information and recommended next steps.

Technically, the findings support a hybrid model rather than a general-purpose generative chatbot. Such a system should combine a curated and versioned knowledge base, retrieval-augmented generation, rule-based decision logic, structured questionnaires, controlled templates, document analysis and human oversight. The language model should help explain, navigate and communicate, but it should not be treated as the source of legal truth. If the system cannot identify a reliable source or if the case is too complex, the safer response is to state the limitation and refer the user to official sources, a DPO or expert advice. This

is consistent with the need for traceability, internal auditing and governance controls in AI systems (Papagiannidis et al., 2025; Raji et al., 2020).

The study also indicates that Olivia AI could have a broader role. If its development process is documented, including risk assessment, DPIA, AI Act classification, knowledge-based governance, red-teaming, hallucination testing, prompt-injection controls, versioning and incident handling, Olivia could become a practical example of governance-by-design. This would be particularly valuable because many organisations are being told to govern AI responsibly, but lack examples of how to document and operationalise such governance in practice (Batool et al., 2024; Papagiannidis et al., 2025; Raji et al., 2020).

Such documentation would also be aligned with the expectations users expressed in the survey. If users expect official sources, clear limits and human oversight in the answers they receive, the same standards should apply to the system behind those answers. The governance of the tool should therefore be visible at least at a high level: what sources are used, how they are updated, when the system refuses to answer, how errors are reported and how sensitive user inputs are protected. This would reduce the risk of automation bias and make the platform more credible for both SMEs and more mature organisations.

A further implication concerns the role of public institutions in digital innovation. Olivia was developed by a supervisory authority and an academic partner, not by a commercial vendor. That gives the compliance tool a different legitimacy, but also creates higher expectations. A public-interest AI compliance assistant should be more conservative than a commercial productivity chatbot. It should prefer a limited but reliable answer to a broad but unsupported one.

The study has limitations. Respondents were registered Olivia users and participation was voluntary, so the findings cannot be generalised to all Croatian organisations. Many respondents already came from organisations with a DPO or another GDPR support function, which may increase the level of awareness in the sample. The survey measures expectations and readiness, not actual behaviour after deployment. Future research should therefore include prototype testing, usability testing, analysis of real user behaviour and evaluation of whether the module improves concrete compliance decisions.

6 Conclusion

The study shows that Olivia has a strong basis for further development. Users value the existing platform and clearly support AI-assisted GDPR guidance. The most important finding is the demand for a module that helps assess GDPR compliance in the use of concrete AI tools. This need is strongly associated with, and significantly predicts, readiness to use AI Olivia.

However, adoption depends on trust. Users expect official sources, GDPR references, clear limitations and safeguards against incorrect or oversimplified answers. The future Olivia AI should therefore be designed as a hybrid compliance system with a controlled knowledge base, RAG, structured questions, rule-based logic, validated templates, human oversight and clear boundaries.

The scientific contribution of this paper lies in connecting technology acceptance, GDPR compliance and AI governance in the specific context of an AI-assisted compliance tool. The study provides empirical evidence that users recognise a specific need for a module assessing GDPR compliance in the use of concrete AI tools. It further shows that adoption readiness is shaped by perceived usefulness and by trust safeguards, including official sources, GDPR references and clear limitations of the tool.

The practical contribution lies in translating these findings into design requirements for Olivia AI. The results suggest that Olivia AI should be developed as a controlled, source-based compliance workflow combining structured questions, verified legal sources, rule-based logic, validated templates, human oversight and clear boundaries. If developed transparently and properly documented, Olivia AI could serve both as a support tool for organisations and as a practical example of responsible AI governance in public interest.

References

- Batool, A., Zowghi, D., & Bano, M. (2024). *Responsible AI governance: A systematic literature review*. arXiv. <https://arxiv.org/abs/2401.10896>
- Croatian Chamber of Economy. (2024). *Analysis of the perception and use of artificial intelligence in the Croatian economy*. Retrieved from <https://hgk.hr/documents/f2024-ai-studija-baf674e1e6c8c834.pdf>
- Croatian Employers' Association. (2025). *How the Croatian economy perceives and uses artificial intelligence?* Retrieved from <https://www.hup.hr/EasyEdit/UserFiles/2025/a1/hup-b2b-ai-istrzivanje-2025.pdf>
- Croatian Personal Data Protection Agency. (2025). *Data Protection and Artificial Intelligence: Frequently Asked Questions*. Retrieved from <https://azop.hr/umjetna-inteligencija-i-zastita-osobnih-podataka/>
- Davis, F. D. (1989). Perceived usefulness, perceived ease of use, and user acceptance of information technology. *MIS Quarterly*, 13(3), 319-340. <https://doi.org/10.2307/249008>
- European Commission. (2025). *Digital Omnibus Regulation Proposal*. Retrieved from

- <https://digital-strategy.ec.europa.eu/en/library/digital-omnibus-regulation-proposal>
- European Data Protection Board. (2024). Opinion 28/2024 on certain data protection aspects related to processing personal data in the context of AI models. Retrieved from https://www.edpb.europa.eu/system/files/2024-12/edpb_opinion_202428_ai-models_en.pdf
- European Parliament and Council. (2016). Regulation (EU) 2016/679 of the European Parliament and of the Council (General Data Protection Regulation). Official Journal of the European Union, L 119. Retrieved from <https://eur-lex.europa.eu/eli/reg/2016/679/oj/eng>
- European Parliament and Council. (2024). Regulation (EU) 2024/1689 laying down harmonised rules on artificial intelligence (Artificial Intelligence Act). Official Journal of the European Union. Retrieved from <https://eur-lex.europa.eu/eli/reg/2024/1689/oj/eng>
- Graux, H., Garstka, K., Murali, N., Cave, J., & Botterman, M. (2025). *Interplay between the AI Act and the EU digital legislative framework*. European Parliament. Retrieved from [https://www.europarl.europa.eu/thinktank/en/document/ECTI_STU\(2025\)778575](https://www.europarl.europa.eu/thinktank/en/document/ECTI_STU(2025)778575)
- Hohmann, B., & Kollár, G. (2025). Reflections on the data protection compliance of AI systems under the EU AI Act. *Cogent Social Sciences*, 11(1), 2560654. <https://doi.org/10.1080/23311886.2025.2560654>
- Holtz, H. M., & Ledendal, J. (2026). AI data governance—overlaps between the AI Act and the GDPR. *Law, Innovation and Technology*, 18(1), 380–409. <https://doi.org/10.1080/17579961.2026.2633677>
- Lakkaraju, H., & Bastani, O. (2020). “How do I fool you?” Manipulating user trust via misleading black-box explanations. In *Proceedings of the AAAI/ACM Conference on Artificial Intelligence, Ethics, and Society* (pp. 79-85). <https://doi.org/10.1145/3375627.3375833>
- Lee, J. D., & See, K. A. (2004). Trust in automation: Designing for appropriate reliance. *Human Factors*, 46(1), 50-80. https://doi.org/10.1518/hfes.46.1.50_303
- Mladinić, A., Vukić, Z., & Rončević, A. (2023). GDPR compliance challenges in Croatian micro, small and medium-sized enterprises. *Pravni vjesnik*, 39(3-4), 53-75. <https://doi.org/10.25234/pv/23972>
- Olivia GDPR ARC. (2025). *Olivia – web tool for GDPR compliance*. Retrieved from <https://olivia-gdpr-arc.eu/hr>
- Olivia User Survey. (2026). *Questionnaire on the use of Olivia and users’ needs for the development of an AI virtual assistant for GDPR compliance*. Retrieved from <https://arc-rec-project.eu/istrazivanje-olivia/>
- Papagiannidis, E., Mikalef, P., & Conboy, K. (2025). Responsible artificial intelligence governance: A review and research framework. *The Journal of Strategic Information Systems*, 34(2), 101885. <https://doi.org/10.1016/j.jsis.2024.101885>
- Raji, I. D., Smart, A., White, R. N., Mitchell, M., Gebru, T., Hutchinson, B., Smith-Loud, J., Theron, D., & Barnes, P. (2020). Closing the AI accountability gap: Defining an end-to-end framework for internal algorithmic auditing. *Proceedings of the 2020 Conference on Fairness, Accountability, and Transparency*, 33-44. <https://doi.org/10.1145/3351095.3372873>
- Sartor, G., & Lagioia, F. (2020). *The impact of the General Data Protection Regulation (GDPR) on artificial intelligence*. European Parliament. Retrieved from [https://www.europarl.europa.eu/thinktank/en/document/EPRS_STU\(2020\)641530](https://www.europarl.europa.eu/thinktank/en/document/EPRS_STU(2020)641530)
- Venkatesh, V., & Davis, F. D. (2000). A theoretical extension of the Technology Acceptance Model: Four longitudinal field studies. *Management Science*, 46(2), 186-204. <https://doi.org/10.1287/mnsc.46.2.186.11926>
- von Eschenbach, W. J. (2021). Transparency and the black box problem: Why we do not trust AI. *Philosophy & Technology*, 34(4), 1607-1622. <https://doi.org/10.1007/s13347-021-00477-0>
- Vorm, E. S., & Combs, D. J. Y. (2022). Integrating transparency, trust, and acceptance: The Intelligent Systems Technology Acceptance Model (ISTAM). *International Journal of Human-Computer Interaction*, 38, 1828-1845. <https://doi.org/10.1080/10447318.2022.2070107>
- Zerilli, J., Bhatt, U., & Weller, A. (2022). How transparency modulates trust in artificial intelligence. *Patterns*, 3(4), 100455. <https://doi.org/10.1016/j.patter.2022.100455>