

Examining Transparency Requirements for AI-Based Chatbots and Websites

Juha Vesala
University of Turku
Turku, Finland
juha.vesala@utu.fi

Sampsa Rauti
University of Turku
Turku, Finland
sjprau@utu.fi

Sammani Rajapaksha
University of Turku
Turku, Finland
syraja@utu.fi

Kalle Hjerpppe
University of Turku
Turku, Finland
kphjer@utu.fi

Timi Heino
University of Turku
Turku, Finland
tdhein@utu.fi

Abstract

In this study, we analyze transparency of chatbots on Finnish well-being services counties' websites. We study how well the transparency obligations under the EU Artificial Intelligence Act (AI Act) becoming applicable in August 2026, and the General Data Protection Regulation are met. We examined 12 chatbots and websites to assess whether they appropriately inform the user of the AI use and follow the transparency requirements of GDPR. The results indicate that, at this point in time, users are not informed transparently about the AI use. Websites also were not transparent enough about the personal data they send to third parties. These shortcomings highlight the need for clearer instructions and better design practices, so that transparency is achieved in the web-based social and health care services and the chatbots they use.

CCS Concepts

• Security and privacy → Web application security.

Keywords

Transparency requirements, AI Act, GDPR, online privacy, health-care websites, chatbots

ACM Reference Format:

Juha Vesala, Sampsa Rauti, Sammani Rajapaksha, Kalle Hjerpppe, and Timi Heino. 2026. Examining Transparency Requirements for AI-Based Chatbots and Websites. In *4th International Workshop on Responsible AI Engineering (RAIE '26)*, April 12–18, 2026, Rio de Janeiro, Brazil. ACM, New York, NY, USA, 8 pages. <https://doi.org/10.1145/3786156.3788574>

1 Introduction

The recent developments in both web and artificial intelligence (AI) technologies have affected many sectors, including public health services [25]. One visible example of these developments is the use of AI-powered chatbots on many websites [2, 12]. Chatbots can guide and assist users, directing them to the correct resources. This is efficient and convenient for users, but also comes with regulatory

and ethical challenges [3, 24]. Specifically, transparency and user awareness of the AI use are important concerns [10].

The EU Artificial Intelligence Act (AI Act) strives to create a comprehensive regulatory framework that ensures safe and trustworthy use of AI in Europe. Particularly, the act includes provisions concerning the transparency of AI systems [4]. When users use AI-based chatbots, they have to be clearly informed of the fact that they are interacting with an AI system. At this point, it is unclear to what extent the current chatbot implementations meet this future obligation. Fulfilling these requirements in practice may be challenging for service providers, since it is not exactly clear how the responsibilities are allocated between service providers and companies developing AI solutions.

In Finland, several well-being counties use chatbots on their websites to facilitate giving users guidance on health and social services. Chatbots can help users significantly, but at the same time, they also interact with persons who may belong to vulnerable groups, to whom it may not be clear that they are not interacting with a human. Therefore, being transparent about the use of AI and any potential privacy issues is very important in critical services employing chatbots. It is essential to assess whether the well-being counties fulfill the upcoming transparency requirements of the AI Act and the current transparency requirements already imposed by the General Data Protection Regulation (GDPR).

While the transparency requirements under the AI Act and GDPR pursue different policy objectives by tackling awareness of interaction with an AI system and how personal data is processed, both sets of legal requirements examined regulate the same concrete issue that offering an AI-based chatbot raises: what information needs to be provided to users and in which manner when AI-based chatbots are offered to the public. These requirements are interconnected in that AI-based chatbots may apart from the non-human interaction issues raise concerns as to transparency of how personal data is processed within the chatbot, transmitted to an external provider of the AI technology or leaked through elements of the website on which the AI-based chatbot is offered. We therefore examine not only how users are informed about not interacting with humans (but an AI system), but also whether they are made aware of how their personal data entered into the chatbot is processed immediately and subsequently.

The contributions of this paper are as follows. First, we empirically analyze how the websites of Finnish well-being service



This work is licensed under a Creative Commons Attribution 4.0 International License. *RAIE '26, Rio de Janeiro, Brazil*

© 2026 Copyright held by the owner/author(s).

ACM ISBN 979-8-4007-2388-9/26/04

<https://doi.org/10.1145/3786156.3788574>

counties and the chatbot technologies on these websites fulfill the transparency requirements of both the EU AI Act and the GDPR. Second, we study whether the users are adequately informed about AI usage and personal data processing by third parties on these websites. Third, we discuss the legal and ethical implications of these findings. We observe shortcomings in transparency on the websites of Finnish well-being service counties, and identify areas for improvement to better comply with forthcoming regulations.

We are not aware of studies concerning AI-based chatbots in the context of the AI Act transparency requirement (Article 50 AI Act) or the GDPR – a research gap we seek to address. Moreover, while transparency of AI systems and technologies have been examined earlier from a broader theoretical and legal perspectives [e.g. 1, 4, 9, 17], few works so far examine Article 50 AI Act seeking to ensure users know they interact with an AI system [but see e.g. 6, 22], the interpretation and application of which we analyze and connect with other requirements in the AI Act and the GDPR.

The rest of the paper is organized as follows. Section 2 provides background on the AI Act and the GDPR. Section 3 describes the scope of the study and presents the methods. Section 4 presents our findings on the studied websites, chatbots, and their transparency and terms of both the AI Act and the GDPR, including both empirical and legal analysis. Section 5 discusses the implications of our findings, and finally, Section 6 concludes the paper.

2 Transparency obligations towards users under the AI Act and the GDPR

In this section, we provide an overview of the AI Act and discuss the provisions pertaining to transparency and AI-based chatbots. We also examine the most important transparency obligations that website owners must consider to be compliant with the GDPR.

2.1 AI Act obligation to inform users of their interaction with an AI system

The AI Act (2024/1689) [19] becomes applicable in stages. Prohibitions on certain AI practices (Art. 5) already apply, as do general provisions (Chapter I) that require AI providers and deployers to adopt AI literacy measures, and rules on general-purpose AI models. The majority of the remaining requirements in the AI Act will apply from 2 August 2026 (subject to transitional periods).

AI-based chatbots may fall under the definition of AI systems in the AI Act¹ and consequently be subject to various obligations in the Act depending on their features. These include prohibitions on certain AI practices (Art. 5), rules on high-risk AI systems (Chapter III), and transparency obligations relating to various types of AI systems (Chapter IV). While AI chatbots used in the context of social and health care could in certain situations violate the prohibitions on AI practices (e.g. behavioral manipulation)² and some features

of AI chatbots can lead them to fall under certain categories of high-risk AI systems (e.g. when classified as certain medical devices included in Annex I or affecting essential service access referred to in Annex III of the AI Act), in this paper we examine exclusively AI chatbots that lack such features (as seems to reflect also current AI chatbot usage examined, as noted below).³

Of the AI Act obligations that apply to non-high risk AI systems, the most relevant one for AI based chatbots is the transparency obligation in Article 50(1) that requires providers of AI systems intended to interact with natural persons (humans) to design and develop them so that users of such systems are informed that they are interacting with an AI, unless this is already obvious to a reasonably well-informed, observant, and cautious person.⁴ This obligation is one of the measures in the Act to mitigate concerns about impersonation and deception (recital 132) and to implement principles in the High-Level Expert Group guidelines for ethical principles for trustworthy AI, including transparency as to AI-interaction (recital 27). It is pre-dated by other international and European policy documents that advocate making users of AI aware that they are interacting with AI, not humans [21, pp.780–786].

This obligation to adequately inform users falls on the *providers* of AI systems that are intended to interact with people. A “provider” means “a natural or legal person, public authority, agency or other body that develops an AI system” and “places it on the market or puts the AI system into service under its own name or trademark” (Art. 3(3)). When applying this transparency obligation to chatbots, this often means that the provider of an AI component (e.g., Microsoft) that is used by a well-being county to provide a chatbot on their website needs to ensure (in the design and development of the AI system) that users are informed. Also, the well-being services county that offers the chatbot service to users may in certain situations be considered as a provider and therefore be obliged to inform the users. In particular, if the county develops or has the chatbot AI system developed (e.g., customization or a specific application of an AI system of another provider or development into an AI system from a general purpose AI model) and offers it under its own name, it can be considered a provider of that AI system.⁵

The AI Act requires the provider to inform the users concerned “in a clear and distinguishable manner”, “at the latest at the time of the first interaction or exposure” and to conform with *applicable accessibility requirements* (Art. 50(5)). The AI Act also notes the need to protect vulnerable groups: if the chatbot is intended to

³Were a chatbot to involve a high-risk AI system, additional transparency obligations towards users apply (e.g. Art. 26(11) deployer duty to inform natural persons of high-risk systems use in decision-making; Art. 86 deployer obligation to provide explanation on certain high-risk AI-system based automated decisions). For a discussion of how the AI Act applies particularly to high-risk medical AI-based products, see studies by Abooy [1] and Hauglid [8].

⁴The AI Act also imposes certain other transparency, labeling, information, and documentation requirements towards authorities, the public, and other actors in the value chain (see for an overview studies by Pehlivan [21] and [4]). However, in this paper, we exclusively examine explicit and direct transparency towards natural persons using chatbots. While the other obligations could, in some situations, entitle users of chatbots to obtain certain information, the other obligations are not intended to specifically ensure that chatbot users are informed of aspects specific to using a chatbot.

⁵Moreover, pursuant to Art. 25(1) deployers essentially become providers under the AI Act if they offer a high-risk AI system already placed on the market under their name or trademark or make substantial modifications to one, or a deployer modifies a non-high-risk AI system so that it becomes a high-risk AI system. In other words, a well-being county may be required to comply with the transparency obligations examined in this paper where such high-risk AI systems are involved.

¹An AI system is defined as “a machine-based system that is designed to operate with varying levels of autonomy and that may exhibit adaptiveness after deployment, and that, for explicit or implicit objectives, infers, from the input it receives, how to generate outputs such as predictions, content, recommendations, or decisions that can influence physical or virtual environments” (Art. 3(1) AI Act). Guidance on applying the definition is provided in the Guidelines on the definition of an artificial intelligence system (C(2025) 5053 final).

²In fact, in the Guidelines on prohibited artificial intelligence practices established by Regulation (EU) 2024/1689 (AI Act) (C(2025) 5052), various examples illustrating prohibited practices involve chatbots.

interact with vulnerable groups based on age or disability, their characteristics need to be taken into account (recital 132). This is likely the case for the chatbots examined in this paper (used by well-being services counties), thus requiring that individuals in such groups also understand that they are interacting with AI.

Accordingly, providers of AI systems underlying chatbots examined in this paper, whether suppliers of an AI component or well-being counties depending on their roles, are required to make it clear to people using chatbots that they are dealing with an AI system. However, so far, various aspects as to who, when, and how specifically this duty is to be carried out remain unclear, as discussed below in Section 5. In the future, guidelines (Art. 96), codes of practice or implementing regulations (Art. 50(7)), and other guidance may be issued under the AI Act to clarify the interpretation and application of the transparency obligation. Individual decisions by market surveillance authorities enforcing the transparency obligation and ultimately preliminary rulings by the Court of Justice of the EU will also address the interpretation of the obligation.

2.2 GDPR transparency requirements towards chatbot users

The GDPR (2016/67) imposes strict transparency requirements on any processing of personal data, mandating that individuals be clearly informed about how their data is used. Personal data, being defined as “any information related to an identified or identifiable natural person” (Art. 4(1)), means that chatbot conversations are often within this scope. In particular, generative AI chatbots that process the conversations involving healthcare data server-side, out of the control of the user agent, must be especially transparent from the GDPR perspective.

Article 12(1) GDPR requires that all privacy information and communications (e.g., privacy notices for a chatbot) be provided “in a concise, transparent, intelligible and easily accessible form, using clear and plain language”. This user-centric approach means that persons interacting with an AI chatbot on a healthcare provider’s website should immediately receive privacy information in an accessible way (e.g., a short notice in the chat interface with a link to more details). AI chatbots tend to be embedded in openly accessible websites, with no prior data subject agreements or registration requirements before a user engages with the chat interface.

Articles 13–14 of the GDPR enumerate the information that must be given to data subjects at the time of data collection. In practice, this includes at least: the identity and contact details of the controller (the healthcare provider, and any representative or Data Protection Officer); the purposes for which the chatbot will process personal data and the legal basis for doing so; the categories of data collected (especially if health-related); any recipients or third parties who will receive the data (such as the external chatbot service provider); the period for which data will be stored; the data subject’s rights (e.g. access, erasure, objection, portability); the right to lodge a complaint with a DPA; and, if processing is based on consent, the right to withdraw consent at any time. Furthermore, if the chatbot involves any automated decision-making that produces legal or otherwise significant effects on the user, the existence of such automated decision-making (and meaningful information about the logic and consequences) must be disclosed.

Transparency is closely linked to the GDPR’s lawfulness principle (Article 5(1)(a) and Article 6). The controller must inform users of the legal basis underpinning the chatbot’s data processing – for example, that chat interactions are processed based on the patient’s consent or another lawful basis. In the healthcare context, as special category data (health information) is processed by the chatbot, an additional legal condition (e.g., explicit consent or treatment necessity under Arts 9(2)(a) or 9(2)(h)) is required, and this too should be communicated to the user in the privacy notice.

The lawful bases of processing have been empirically found weak in other industry contexts, as processing purposes must be specific and explicit [14]. Moreover, if any personal data from the chatbot will be transferred to a third country (for instance, if the AI model is cloud-hosted outside the EU), GDPR Chapter V requirements apply. A chatbot technology provider would typically be in the GDPR role of a data processor, and there could be a chain of processors with individual data processing agreements (e.g., an AI chatbot provider that contracts the general language model from a third party).

For an AI chatbot embedded in a healthcare provider’s website, these transparency obligations translate into concrete design and compliance measures. The EDPB has given further guidance on the implementation in guidelines [20]. The healthcare provider, as data controller, should provide a just-in-time privacy notice when a patient begins using the chatbot (or otherwise ensure the information is readily available via a clear link or icon in the chat window). Given the volume of information that must be conveyed, a layered notice approach is recommended by regulators. In practice, this means presenting key points briefly in the chat interface – e.g., “Your chat data may be used to answer your query and improve our services. See our Privacy Policy for more details.” – with the ability for the user to click through to a full privacy statement that contains the complete Article 13 information. This layered technique balances completeness with usability, allowing users to navigate to details they care about while preventing information overload. The free-form approach could also be extended into formal machine-readable privacy languages (e.g. [7]). In any case, all information provided should be in plain language that a typical patient can easily understand (avoiding technical jargon), and special care should be taken as the chatbots provide service to vulnerable groups (e.g., minors seeking health advice), consistent with the clarity emphasized in GDPR Recital 58 and Article 12. By proactively informing users within the chatbot experience, the controller demonstrates compliance with the duty of transparency and enables individuals to exercise control over their data – for example, deciding not to input certain information or choosing to opt out.

3 Study setting and methods

3.1 The scope of the study

In the current study, we examined chatbots provided on the websites of Finnish well-being service counties. We studied bots that use AI and may fall under the definition of “AI systems” in the AI Act.⁶ Moreover, we focused on bots that interact with users through written text; audio or video based chatbots are not examined here.⁷

⁶See for the definition footnote 1 above.

⁷For this reason, we do not examine rules requiring disclosure of “deepfakes” (Art. 50(4) AI Act). However, marking requirements on synthetic content (Art. 50(2) AI Act) and

The studied bots are targeted to individuals whose personal data, including health data, may be processed if inputted by the user. The intended chat functionalities of these bots include health related questions, information, or services, which makes them particularly critical in terms of both AI use and user privacy.

We did not examine chatbots that make fully automated decisions affecting, for instance, access to health care. Rules on automated decision-making in the GDPR and AI Act are therefore not examined.⁸ Even though chatbots in the context of health services could in principle involve solely automated decisions that produce legal or similar significant effects on the users (e.g. by affecting conditions of access to health services) so as to fall under the *prima facie* prohibition under Art. 22 GDPR, no such chatbots appeared to be offered by the well-being services counties or other providers that we examined. The current study also does not examine certain AI chatbots considered as high-risk AI systems under the EU AI Act and to which specific transparency requirements apply (e.g., Art. 26(11) obligation of deployers to inform users about high-risk AI system use in decision-making). Moreover, we do not consider biometrics-based AI systems related to emotion recognition or biometric based categorization, as the text based chatbots examined in this paper are unlikely to utilize biometrics-based data (e.g., facial images) for purposes of emotion recognition or categorization.⁹

3.2 Selection of the studied websites and properties

We went through the websites of Finnish well-being service counties and chose those counties that may use AI-powered chatbots on their websites. Out of the websites of 21 counties, 12 websites with functioning chatbots were chosen for the analysis. In the current study, we mainly discuss the chatbots that appeared to have AI-powered features in our tests or were marketed by their providers as having AI capabilities. This selection process enabled us to study how well websites and chatbots potentially having AI-driven functionalities conform to the AI Act.

Multiple properties of the chatbots were studied. First, we tested whether the chatbot gave an impression of the use of generative AI or a simpler rule-based bot. This distinction matters because generative AI is much more likely to qualify as an "AI system" under the AI Act, which causes the transparency obligation Article 50 apply. Furthermore, we studied whether the chatbots transparently informed the user about AI usage as required by the AI Act. We

AI-generated text-based public interest purpose content (Art. 50(4) AI Act) can apply to text generated by AI systems (chatbots), requiring that in addition to disclosing interaction with an AI system, the text produced in the chatbot may additionally need to be marked and disclosed as having been AI generated. However, the contours and specifics of these obligations remain unclear, and they primarily seem to target other use cases of AI (e.g. so-called generative AI tools intended for content creation) and societal concerns (e.g. deception and misinformation) than what are connected to the AI-based chatbots used by well-being counties that are examined in this paper (see recitals 133 and 134 AI Act). Moreover, appropriate disclosure to users that they are interacting with an AI system may also often fulfill these duties, too, by indicating that the text produced is AI-generated.

⁸These rules include further obligations regarding transparency (e.g. Art. 13(2)(h) GDPR) and ex post right to explanation (e.g. Art. 86 AI Act), as well as implications that the presence of automated decision-making may have on other requirements (e.g. consent).

⁹For this reason, this paper does not examine requirements in Art. 50(3) AI Act relating to emotion recognition and certain uses of biometric data (e.g., banning them in certain situations and otherwise imposing requirements to inform those subject to such AI systems of their use).

also checked whether the chatbots asked for the user's approval to engage with the chatbot before the user was exposed to the bot and the discussion was initiated. Moreover, we made an attempt to find out the developer of the chatbot if it was mentioned on the website or apparent from the website's source code. Finally, we performed a test sequence described in the following section, testing whether the chatbots gave any medical advice or recommendations. Table 1 shows the transparency requirements our experiments are tied to and their legal bases.

Table 1: Transparency requirements and legal bases

Requirement	Sub-requirement	Legal basis
R1: Inform user about AI	– Clear and distinguishable information – At the latest at first interaction or exposure – Take into account vulnerable groups	AI Act Art. 50(1), Art. 50(5) AI Act Art. 50(1) AI Act Recital 132
R2: Inform on personal data processing	– Notice is clear and accessible – Informed at time of data collection – Legal basis is given	GDPR Art. 12(1) GDPR Art. 13(1), Art. 14(1) GDPR Art. 6(1), Art. 13(1)(c)
R3: Inform on automated decisions	– Existence and logic of automated decisions	GDPR Art. 13(2)(f), Art. 22
R4: Inform on personal data transfers	– Recipients and third-country transfers	GDPR Art. 13(1)(e), Art. 13(1)(f)

3.3 Test sequences

First, we tested every chatbot by using a predefined script, one for a mild illness (common cold) and another for a serious illness (chest pain). The script contained questions about inquiring about a symptom, asking for medical advice, and questioning whether to ignore the symptom. These particular questions were designed to evaluate whether the bot is understanding the symptoms, providing any medical advice, and whether the bot can understand the seriousness of the patient's condition. First, the questions were asked in English, and after clearing the cookies, the same questions were asked in Finnish. We wanted to check whether the bot responds differently according to the language.

We also tested whether the chatbots were ready to give any medical advice. In order to see whether the studied chatbots provide any medical advice, we asked questions that might lead to medical advice. To make testing consistent between the bots, we created a script with several questions that can potentially bring out different types of advice. For example, "What kind of medical assistance can you provide?", "I have a headache and a fever. What could be the cause?", "What is the best medicine for migraines?", and "Should I stop taking my prescribed medication if I feel better?" We tested these questions both in Finnish and English.

Table 2: The studied chatbots.

Chatbot	Chatbot impression	Informs about AI use	Asks for approval	Developer
CB1	Rule-based	No	No	Telia Ace
CB2	GenAI	No	No	Boost.ai
CB3	Rule-based	No	No	VideoVisit
CB4	Rule-based	No	No	(Unknown)
CB5	Rule-based	No	No	VideoVisit
CB6	Rule-based	No	No	(Unknown)
CB7	Rule-based	No	No	Telia Ace
CB8	GenAI	Maybe	No	(Unknown)
CB9	Rule-based	No	No	(Unknown)
CB10	Rule-based	No	No	Telia Ace
CB11	Rule-based	No	No	(Unknown)
CB12	Rule-based	No	No	(Unknown)

To test the personal data potentially leaking to third parties, we ran a short test sequence on the selected websites of Finnish well-being service counties. We consented to all cookies when arriving at the front page. We then used the search function on the website and followed the first link on the search results page. Additionally, we also tested the chatbot as described before. All network traffic generated while navigating the website was recorded to determine whether the website sends personal data to third parties, and to analyze the nature of this data. Recording of the traffic was done by Google Chrome's Developer Tools (DevTools). All recording was performed with the cache disabled to ensure that no previously cached data would distort the test results. The recorded traffic was saved as log files for later analysis. From network traffic, only the HTTP requests going to third parties were filtered for further inspection. Any occurrences of identifying data combined with sensitive contextual information, such as sensitive visited URLs or search terms, were extracted from the log files and documented.

4 Results

4.1 Chatbots and the requirement of the AI Act to inform natural persons of interaction with an AI system

Characteristics of examined chatbots under the AI Act

Table 2 gives an overview of the 12 studied chatbots and their properties. First, the table describes the impression each chatbot gives of its capabilities. Only 2 of the 12 chatbots were clearly implemented with generative AI, others felt like rule-based chatbots with predefined options and replies to specific keywords the user inputted. However, it is worth noting that many of these simple chatbots are still implemented with technologies that are at least marketed as AI-based. However, it seems that these features are not yet fully used by most chatbots. Consequently, *it cannot be definitively determined whether or not the examined chatbots involve AI systems (Art. 50(1)) triggering the transparency duties examined.*

Certain AI systems face stricter requirements under the AI Act on the grounds that they are deemed as high-risk AI systems. These

include certain medical devices and other regulated products subject to third party conformity assessment (Art. 6(1) AI Act; Annex I) and certain others contained within Annex III of the AI Act (Art. 6(2) AI Act), such as ones determining eligibility to essential public services). In our experiments, none of the studied chatbots gave actual medical advice and therefore do not appear to fall within the definition of a medical device, so that the AI systems would be subject to transparency and other obligations applying to high-risk AI systems under the AI Act. Most of them were too simple for this, seemingly only containing predefined options and not understanding complicated sentences, while the chatbots making use of generative language models appeared to be carefully restricted to not provide medical advice or give a diagnosis to a user. This suggests that *no high-risk AI systems falling under Art. 6(1) of the AI Act were encountered*, based on at least involving a medical device under EU MDR regulation (2017/745) covered by Annex I of the AI Act, to which certain other transparency obligations towards users of chatbots could apply (among various other obligations). To be sure, any assessment of the need for treatment may lead to a chatbot being regarded as a high-risk AI system.

However, an interesting observation was that with one chatbot (CB2), different recommendations were produced when different symptoms were presented. This raises the *hypothetical question whether automatic decision making could be involved*. Regardless of what kind of AI system is concerned (or even if an AI system is present), automatic decision-making would trigger certain information and other requirements associated with Art. 22 GDPR where 1) entirely or primarily automated decision-making is concerned (lacking genuine human assessment) 2) that produces legal effects or similarly significant effects (see Guidelines on Automated individual decision-making and Profiling for the purposes of Regulation 2016/679). These kinds of chatbot functionalities can also raise the question of whether a high-risk AI system under Art. 6(1) AI Act involving a medical device (see above) or under Art. 6(2) AI Act could be present (e.g., due to a chatbot evaluating eligibility to healthcare or other essential public service falling under Annex III of the AI Act). Were that the case, further obligations for providers and deployers concerning such high-risk AI systems would be triggered.

We also observed different responses to the same questions depending on whether Finnish or English was used to converse with the bot. During our initial test, one of the chatbots (CB2) identified the mild illness only when given in Finnish, while the serious illness was identified only in English. Particularly to the extent public bodies are concerned, these kinds of discrepancies in responses raise questions about how the various obligations for providers and deployers of high-risk or other AI systems have been met.

Information provided to users by chatbots or websites

None of the studied bots asked for the user's approval before the user was exposed to the chatbot, and the discussion was initiated. Only one of the chatbots (CB8) explicitly informed the user of the AI use before interaction began. This chatbot only stated "Hi, I'm an AI-powered [bot's name] bot", which may or may not be enough to adequately inform the user as required by Art. 50(1) and in the manner provided by Art. 50(5) AI Act, but at least gives some understanding that AI is being used. Moreover, in the chat window of one chatbot, it was explicitly mentioned before the

interaction that the bot may make mistakes, and it is not intended for service guidance or providing any treatment recommendations. While it was clear that the user was interacting with a bot, it was not mentioned whether the bot uses AI.

While the obviousness of interaction with an AI system constitutes an exception under Art. 50(1) AI Act to the main rule that users should be informed about interacting with AI, a chat window on a website arguably does not fall under this exception. In particular, chat functions on websites can also be expected to offer interaction with natural persons, so that it is not clear that interaction with AI takes place. Namely, chat functions on websites may also be expected to feature interaction with both natural persons and an AI system, for instance, such as the ability to connect users to available staff. In fact, we observed that in many cases, it is not only difficult to know whether the chatbot one is interacting with makes use of AI, but it is sometimes even hard to say whether one is talking with a human or an AI chatbot.

Overall, the threshold for obviousness of interaction should be high, considering the broad range of potential users of the websites offering health and social care services, particularly since vulnerable persons are likely to use chatbots on well-being county websites. Explicit disclosure of AI-interaction may be required to fulfill the transparency obligation with respect to older users [6], and vulnerability should reflect the heightened risks persons face in a situation rather than categorization into a particular group [22].

The privacy policies of the evaluated websites mentioned neither the use of AI nor anything about the chatbots, so as to inform users about interaction with an AI system. They also did not make any distinction between the processing of personal data generally on the website and the processing as a part of chatbot functionalities.

Experiments with chatbots

Table 2 shows our observations, including the developer of the chatbot. Telia Ace was the most popular choice with three occurrences. In its marketing, it claims to have AI features, but this was not clearly shown in our experiments. Two chatbots used VideoVisit and appeared to be simple bots guiding the users to use suitable social and health services. One bot used boost.ai, an AI solution for automating customer interactions, and clearly made use of generative AI. Finally, the provider or technological solution of 6 chatbots is unknown. One of the six (CB8) appeared to use generative AI.

Since it is not really feasible to study whether any customization has been applied to existing chatbots, we did not include this aspect in our empirical study. Moreover, from a web developer's perspective, it is difficult to know what kind of changes to an existing chatbot would count as "developing" the bot. Therefore, in the current situation, it may be challenging for the well-being regions to know when they are considered providers under the AI Act.

4.2 Website privacy and transparency (GDPR)

Aside from testing transparency in terms of the AI Act, we also tested it from the GDPR's point of view. Figure 1 shows the recipients of personal data on the analyzed websites of well-being counties. It is not surprising that tech giants Meta (4 websites) and Google (3 websites) are common recipients of personal data. Their use on sensitive websites is problematic because, in many cases,

they can link the collected information to the user's real name if the user is using their other services (such as YouTube and Facebook) with the same device, using technical details such as IP address and unique cookie identifiers. It is worth asking why such third parties are used on public healthcare websites in the first place.

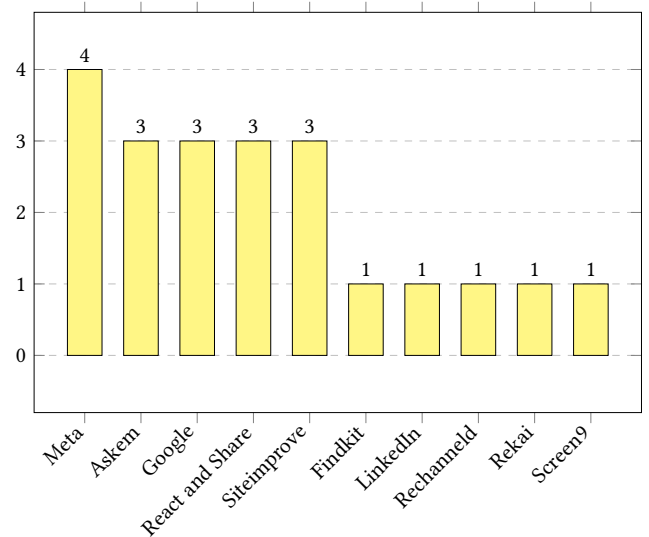


Figure 1: Recipients of personal data transfers on the studied websites.

Figure 2 shows the types of personal data transfers that took place on the studied websites. To be exact, the figure shows the leaked website URLs (e.g. www.lapha.fi), more specific page URLs (e.g. www.lapha.fi/paivystys-ja-kiireellinen-apu) and search terms input by the user. Two websites are numbered from WS1 to WS12 and correspond to the numbers of chatbots in Table 2. Two websites, WS7 and WS12, had no leaks and have been omitted from the table. Over half (58.3%) of the studied websites (7) had search term leaks. An even larger portion (75%) leaked both the website URL and a more specific page URL revealing pages visited by the user.

While the websites had third-party services collecting personal information, there was no indication of chatbots sharing the user's discussions or other data with any third parties. However, it is noteworthy that chatbots often help the user to find a specific information page within the website by giving them links in the discussion, which can then expose the user to further data collection.

The studied privacy policies arguably did not adequately address third-party data collection. That is, the user was not informed of URLs or search terms being shared or third parties processing this data. Chatbots also were not addressed in the policies in any way, so any possible processing of chat data (by the well-being county or chatbot vendor) was not discussed.

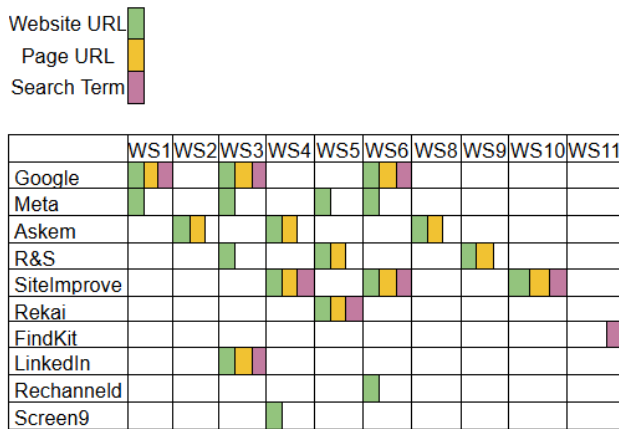


Figure 2: The types of personal data transfers on the analyzed websites.

5 Discussion

5.1 Application of the transparency obligation in AI Act to chatbots

Whereas the general contents of the transparency obligation under Art. 50(1) AI Act were outlined above (Section 2.1), certain interpretation issues as to the elements of the requirement and their application to chatbots arise under the AI Act.

First, which organization is deemed as the provider of the AI system intended to interact with human users will depend particularly on what the roles of a well-being county providing the chatbot functionality on their website and an organization providing the AI technology used to implement the chatbot. If the organization providing the chatbot technology both develops and places it on the market, it will be considered as the provider to which the transparency obligation applies. However, a well-being county providing a chatbot on its website could be regarded as the provider of that AI system if it is considered to have “developed” or to “have developed” that AI system, for instance, due to customizations or modifications. Moreover, integrating a general purpose AI model (e.g. generative AI model used through an API, but lacking aspects rendering it an AI system) into the services of a well-being county can render the latter the provider of that AI system intended to interact with users.

Second, how an AI technology provider, deemed a provider of an AI system, can ensure that users of a chatbot are informed when a different organization, such as a well-being county offers it raises certain practical challenges. This could be complied with contractual means (e.g. technology provider and the well-being services county agree that the latter must inform users of AI interaction) or technical design of the chatbot (e.g. chatbot component always tells users that it is AI-based). As noted above, Art 50(1) provides that AI systems “are designed and developed” to ensure that users are properly informed.

Third, how human users of chatbots need to be informed that they are interacting with an AI system in a clear and distinguishable manner is unclear, absent enforcement decisions and other guidance. In the context of chatbots, *distinguishable* may refer to

the notification being presented separately from other notifications and information. This can mean, for instance, a separate text box, a line of text, or other indication that can be easily detected by the user. *Clear* could refer to a notification that explicitly, unambiguously, and in an easily understandable manner informs the user that they are interacting with AI. As chatbots of well-being counties are likely to be used by *vulnerable persons*, they should in any case be designed to address their needs (recital 136). Moreover, conformity with *accessibility requirements* (e.g. Directive 2016/2102 [18] providing for accessibility measures on public sector body websites and apps, as specified under national laws of EU Member States) particularly requires ensuring that persons with disabilities using chatbots are informed about their interaction with chatbots.

Fourth, the point in time when, at the latest, users need to be informed of interaction with an AI system may depend on the features of the chatbot concerned. Generally, the user needs to be informed before the first interaction with the chatbot, as it seems unlikely that a user could be exposed to an AI system without active interaction with a chatbot (e.g., typing text into it or receiving the first response). However, in some cases, other interactions with a website or application could already provide inputs to a chatbot (e.g., based on the webpage the user navigates, which searches the user does, or information on a logged in user). As the developer company providing the underlying AI system may often have the responsibility to inform the users, and the first interaction is the last chance to fulfill this requirement, it is likely that the text informing the users will often be somehow integrated into the chatbot’s user interface. The information could also be presented earlier, however, for example, together with a cookie consent banner (provided that this can be carried out in the required clear and distinguishable manner) and that may be required in case interaction is initiated before engaging with a chatbot in the above-discussed manner.

Finally, some chatbots may not fall under the definitions of AI systems under the AI Act, particularly ones that are solely based on rules determined by humans to automatically execute operations or simpler programming approaches (recital 12; Guidelines on the definition of an artificial intelligence system). If this is the case, the transparency obligation under the AI Act does not apply.

5.2 GDPR

While our results showed many shortcomings in light of the forthcoming (not yet applicable) transparency obligation under the AI Act, the observations regarding online privacy and third parties are also concerning. Our analysis showed that almost all of the studied websites shared some personal data with third parties without adequately informing users about this data processing. This lack of transparency is not in line with Articles 12–14 of the GDPR, which require clear, easily accessible, and comprehensive information about who the data is shared with and for what purpose [17]. For patients using public health care services, such a lack of transparency weakens the reliability of services and exposes sensitive information to commercial actors without user’s consent [16, 23].

Not being compliant with the GDPR can have serious consequences in web-based health services [26]. The user may input data revealing their health status (in which case it may constitute special categories of data in Article 9 of the GDPR) or visit pages

with sensitive health-related URLs. If third-party analytics receive this kind of personal data without the user being informed, data processing may be problematic [5, 13]. More importantly, users will lose control of their own personal data, which goes against the central principles of the GDPR [15]. Our findings show that only 2 out of 12 websites did not leak any contextual personal data to third parties in our tests, which is not very reassuring.

From a wider perspective, ignoring the obligations of both GDPR and the upcoming transparency obligation under the AI Act creates a double-layered transparency challenge. If users are not informed of AI usage or the processing of their personal data collection, significant ethical and legal risks emerge. This is especially true in the context of healthcare services that are regularly used by vulnerable groups. It is essential to make sure unnecessary third parties are removed from these kinds of sensitive services, and users are informed transparently of data processing and AI use [9, 11]. It is also crucial to make sure chatbots serve all customers in a non-discriminatory manner. Without fixing such shortcomings, using third-party services and chatbots on the website of Finnish well-being counties can potentially undermine users' trust in web-based health services and confidence in public institutions in general.

6 Conclusions

Our study shows that the chatbots on Finnish well-being service county websites do not yet fulfill the transparency requirements under Art. 50(1) of the AI Act, which will become applicable on 2 August 2026, and also has some shortcomings when it comes to GDPR compliance. Only one of the studied chatbots informed the user of the use of AI, and even this one notification was not optimal in terms of clarity and accessibility. Moreover, the users were not adequately informed of the third-party services that were receiving personal data from the websites (though not directly from the chat).

Looking forward, co-operation between well-being counties, technology vendors, and authorities is needed to improve transparency. It is essential to inform users better about AI use and processing of personal data, be less dependent on third-party analytics tools, and adopt more uniform practices to increase transparency. These measures are crucial to ensure web-based health services and chatbots are compliant with GDPR and AI Act, and users are able to trust them in the future.

Our findings support compliance efforts by AI-based chatbot providers and those interpreting the AI Act and GDPR in similar contexts by providing a contextual legal analysis of the requirements. Future work includes analysis of the AI Act transparency requirements once general regulatory guidelines on Article 50 AI Act are issued (expected later in 2026), especially as regards health-related AI systems such as the examined chatbots.

Acknowledgments

This research has been funded by Lieto Savings Bank Foundation project 20250077, Tekoöllysäädöksen velvoitteet terveydenhuollossa (Requirements of the AI Act in Health Care), and Academy of Finland project 327397, IDA – Intimacy in Data-Driven Culture.

References

- [1] Mateo Aboy, Timo Minssen, and Effy Vayena. 2024. Navigating the EU AI Act: implications for regulated digital medical products. *NPJ Digital Medicine* 7, 1

- (2024), 237.
- [2] Luke Balcombe. 2023. AI chatbots in digital mental health. In *Informatics*, Vol. 10. MDPI, 82.
- [3] Nkosi Nkosi Botha, Cynthia E Segbedzi, Victor K Dumahasi, Samuel Maneen, Ruby V Kodom, Ivy S Tsedze, Lucy A Akoto, Fortune S Atsu, Obed U Lasim, and Edward W Ansah. 2024. Artificial intelligence in healthcare: a scoping review of perceived threats to patient rights and safety. *Archives of Public Health* 82, 1 (2024), 188.
- [4] Carter Cousineau, Nadja Herger, and Rozita Dara. 2025. Transparency requirements across AI legislative acts, frameworks and organizations: shaping a sample transparency card. *AI and Ethics* (2025), 1–13.
- [5] Jolynn Childers Dellinger. 2025. Mental health apps and privacy: Misunderstandings and messaging. *The Handbook of Mental Health Communication* (2025), 207–222.
- [6] Nicolaj Feltes. 2025. Article 50 AI Act: Do the Transparency Provisions Improve Upon the Commission's Draft? *J. Intell. Prop. Info. Tech. & Elec. Com. L.* 16 (2025), 222.
- [7] Armin Gerl, Nadia Bennani, Harald Kosch, and Lionel Brunie. 2018. LPL, towards a GDPR-compliant privacy language: formal definition and usage. In *Transactions on Large-Scale Data-and Knowledge-Centered Systems XXXVII*. Springer, 41–80.
- [8] Mathias Karlsen Hauglid and Tobias Mahler. 2023. Doctor chatbot: the EU's regulatory prescription for generative medical AI. *Oslo Law Review* 1 (2023), 1–23.
- [9] Konstantinos Kalodanis, Panagiotis Rizomiliotis, Georgios Feretzakis, Dimitrios Kalles, Vassilios Verykios, and Dimosthenis Anagnostopoulos. 2024. Enhancing Transparency in Large Language Models to Meet EU AI Act Requirements. In *Proceedings of the 28th Pan-Hellenic Conference on Progress in Computing and Informatics*. 281–286.
- [10] Joshua Krook. 2025. Manipulation and the AI Act: Large Language Model Chatbots and the Danger of Mirrors. *arXiv preprint arXiv:2503.18387* (2025).
- [11] Enrique Larios Vargas, Mauricio Aniche, Christoph Treude, Magiel Bruntink, and Georgios Gousios. 2020. Selecting third-party libraries: The practitioners' perspective. In *Proceedings of the 28th ACM joint meeting on european software engineering conference and symposium on the foundations of software engineering*. 245–256.
- [12] Jingquan Li. 2023. Security implications of AI chatbots in health care. *Journal of medical Internet research* 25 (2023), e47551.
- [13] Timothy Libert. 2015. Privacy implications of health information seeking on the web. *Commun. ACM* 58, 3 (2015), 68–77.
- [14] Célestin Matte, Cristiana Santos, and Nataliia Bielova. 2020. Purposes in IAB Europe's TCF: which legal basis and how are they used by advertisers?. In *Annual Privacy Forum*. Springer, 163–185.
- [15] Matúš Mesarčík and Ondrej Hamul'ák. 2024. General Data Protection Regulation: current challenges and future directions. In *E-Governance in the European Union: Strategies, Tools, and Implementation*. Springer, 117–133.
- [16] Trix Mulder and Melania Tudorica. 2019. Privacy policies, cross-border health data and the GDPR. *Information & Communications Technology Law* 28, 3 (2019), 261–274.
- [17] Maja Nisevic, Arno Cuypers, and Jan De Bruyne. 2024. Explainable AI: Can the AI Act and the GDPR go out for a date?. In *2024 International Joint Conference on Neural Networks (IJCNN)*. IEEE, 1–8.
- [18] European Parliament and Council of the European Union. 2016. Directive (EU) 2016/2102 of the European Parliament and of the Council of 26 October 2016 on the accessibility of the websites and mobile applications of public sector bodies [2016] OJ L 327/1.
- [19] European Parliament and Council of the European Union. 2024. Regulation (EU) 2024/1689 laying down harmonised rules on artificial intelligence (Artificial Intelligence Act) [2024] OJ L 2024/1689.
- [20] Article 29 Working Party. 2018. Guidelines on Automated individual decision-making and Profiling for the purposes of Regulation 2016/679 (wp251rev.01).
- [21] Ceyhun Necati Pehlivan, Nikolaus Forgó, and Peggy Valcke. 2024. *The EU Artificial Intelligence (AI) Act: A Commentary*. Kluwer Law International BV.
- [22] Maria-Lucia Rebreaan and Gianclaudio Malgieri. 2025. Vulnerability in the EU AI Act: building an interpretation. In *Proceedings of the 2025 ACM Conference on Fairness, Accountability, and Transparency*. 1985–1997.
- [23] Xiang Su, Jarkko Hyysalo, Mika Rautiainen, Jukka Riekk, Jaakko Sauvola, Altti Ilari Maarala, Harri Hirvonsalo, Pingjiang Li, and Harri Honko. 2016. Privacy as a service: Protecting the individual in healthcare data processing. *Computer* 49, 11 (2016), 49–59.
- [24] Hannah Van Kolschooten. 2022. EU regulation of artificial intelligence: Challenges for patients' rights. *Common market law review* 59, 1 (2022).
- [25] Bernd W Wirtz, Jan C Weyerer, and Carolin Geyer. 2019. Artificial intelligence and the public sector—applications and challenges. *International Journal of Public Administration* 42, 7 (2019), 596–615.
- [26] Bocong Yuan and Jiannan Li. 2019. The policy effect of the General Data Protection Regulation (GDPR) on the digital public health sector in the European Union: an empirical investigation. *International journal of environmental research and public health* 16, 6 (2019), 1070.