ANALELE ȘTIINȚIFICE ALE UNIVERSITĂȚII „ALEXANDRU IOAN CUZA” DIN IAȘI
TOM LXXI, 5, ȘTIINȚE JURIDICE, 2025

DOI: 10.47743/jss-2025-71-5-2

The Smart Home Listener: Legal and Communication Perspectives on Voice Assistants in Music Streaming

Ascultătorul din locuința inteligentă: perspective juridice și de comunicare asupra asistenților vocali în streamingul muzical

Tiberiu T. BAN[1], **Adrian CHEȚAN**[2]

Rezumat:
Asistenții vocali au devenit un punct central al modului în care utilizatorii consumă și interacționează cu platformele de streaming muzical. Prin prelucrarea bazată pe voce și analiza comportamentală, aceste sisteme creează suprapuneri complexe între tehnologia divertismentului, protecția datelor și practicile de comunicare. Deși legislația privind protecția vieții private oferă un cadru de reglementare, nivelul de conștientizare al consumatorilor și capacitatea acestora de a-și gestiona datele rămân scăzute, în special în situațiile în care sunt implicate mai multe părți, precum producătorii de dispozitive și furnizorii de servicii de streaming. Acest articol va analiza modul în care asistenții vocali colectează, prelucrează și diseminează date cu caracter personal, în special din perspectiva politicilor privind protecția vieții private, a reglementărilor juridice și a practicilor de comunicare. Analiza se va concentra pe anumite aspecte privind transparența, responsabilitatea și practicile de securitate legate de datele vocale, precum și pe dificultățile de exprimare a consimțământului. Rezultatul constă în integrarea dimensiunilor juridice, de comunicare și de securitate în serviciile de streaming muzical bazate pe voce, precum și în recomandări privind înțelegerea și exprimare consimțământului. În această lucrare, relația dintre drept și comunicare, precum și dintre acestea și securitate, este importantă pentru a preveni intruziunea și pentru a construi încrederea necesară obținerii consimțământului.

Cuvinte-cheie: asistenți vocali, streaming muzical, dreptul protecției datelor, comunicare, consimțământ, dispozitive inteligente

Abstract: Voice assistants are now a focus point of how customers consume and interact with music streaming platforms. Through voice-based processing and behavioral analysis,

[1] Doctorand în cadrul Școlii Doctorale de Drept, Universitatea Babeș-Bolyai Cluj Napoca, asistent universitar în cadrul Facultății de Drept din Universitatea Bogdan-Vodă Cluj Napoca; tiberiu.ban@gmail.com

[2] Cercetător independent, doctor în Științele Comunicării, Cluj-Napoca; adrian.chetan@ubbcluj.ro

these systems create complex overlaps of entertainment tech, data privacy, and communication practice. While privacy laws provide a regulatory framework, how much the consumer is aware and able to manage their data is low, especially where there are several parties involved, such as device manufacturers and streaming services. This paper will discuss the collection, processing, and dissemination of data by voice assistants, specifically in the areas of privacy policies, legal regulations, and communication practices. It will be focused on certain areas of transparency, accountability, and security practices related to voice data, as well as the challenges in exercising consent. The result will be the integration of the law, communication, and security aspects in voice-based music streaming services, as well as recommendations on the understanding and exercising of consent. In this work, the relationship between the law and communication, as well as security, is important so that there is no intrusion and trust is built in order to obtain consent.

Keywords: voice assistants, music streaming, privacy law, communication, consent, smart devices

1. Introduction

Voice assistants are increasingly becoming intermediaries in everyday life, including in the field of music streaming[3]. For the purposes of this article, voice assistants are understood as AI-based systems capable of processing spoken commands and enabling users to interact with digital services through natural language[4]. This increase is changing the way users interact with such services, moving from the regular screens to continuous audio interfaces that listen and process data. Since data is involved, this development has some legal implications because it involves continuous audio recording, cloud computing, and inter-service connections that reveal identity, behavior, and domestic circumstances of the users[5]. In this context, cloud computing refers to the remote processing and storage of voice data on servers operated by service providers rather than on users' local devices. The interface is transient, which makes it difficult to deliver the transparency and consent requirements that are normally fulfilled by written notices.

Therefore, voice interfaces provide users with a low-friction environment, which is fast and easy to use with shortcuts, but what happens in the background

[3] L. Uyar, M. Clement, B. Veseli, M. Kandziora, "The rise of smart speakers: A comparative analysis of music streaming service adoption and platform interdependencies", in Journal of Media Economics, vol. 37, no. 3, 2025, pp. 129–147, DOI: https://doi.org/10.1080/08997764.2025.2494994.

[4] G. Terzopoulos, M. Satratzemi, "Voice assistants and smart speakers", in Informatics in Education, vol. 19, no. 3, 2020, pp. 473–490, available online at: https://files.eric.ed.gov/fulltext/EJ1267812.pdf, accessed on 3 July 2026.

[5] J. Lau, B. Zimmerman, F. Schaub, "Alexa, are you listening?", in Proceedings of the ACM on Human-Computer Interaction, vol. 2 (CSCW), art. 102, 2018, pp. 1–31, DOI: https://doi.org/10.1145/3274371; European Data Protection Board, Guidelines 02/2021 on virtual voice assistants (Version 2.0), available online at: https://www.edpb.europa.eu/system/files/2021-07/edpb_guidelines_202102_on_vva_v2.0_adopted_en.pdf, accessed on 3 July 2026.

with the data, who and when is collecting and sharing it, is hard to see or understand. Since users may tend to be less vigilant since they may think that music streaming is a harmless service, then the transparency requirements that are specifically geared towards text are difficult to apply in audio systems, which are hard to communicate. Within the GDPR[6] framework, transparency requires that data subjects receive information about the processing of their personal data in a concise, intelligible and easily accessible form before or at the time the processing takes place[7].

From a regulatory perspective, voice-based access to music services sits at the intersection of consumer IoT, platform governance, and data protection law. It also raises questions with regard to the communication of legal bases for processing, in addition to those with regard to legal bases themselves. Although the GDPR and the EDPB Guidelines on Virtual Voice Assistants establish a general legal framework, limited legal scholarship has examined how these obligations operate specifically in voice-assisted music streaming environments, where interactions occur primarily through audio rather than graphical interfaces. From a communication perspective, the article also examines whether voice-based interfaces are capable of conveying legally required information in a manner that allows users to make informed decisions regarding the processing of their personal data. This article aims to give a concise analysis by first mapping the underlying data ecosystem, identifying relevant legal obligations under EU data protection law, and communicating legal compliance requirements relevant for voice interfaces[8].

For services offered in Romania, this EU-level framework is complemented by national implementing measures, including Law No. 190/2018[9].

Methodological note

The method adopted in this article is doctrinal and analytical and is carried out through an examination of EU data protection legislation, regulatory guidelines, and interdisciplinary research on voice assistants and the smart speakers in which they are commonly integrated. Instead of empirical

[6] European Parliament and Council of the European Union, Regulation (EU) 2016/679 (GDPR), available online at: https://eur-lex.europa.eu/eli/reg/2016/679/oj, accessed on 3 July 2026.

[7] Article 29 Data Protection Working Party, Guidelines on transparency under Regulation 2016/679 (WP260 rev.01, as last revised and adopted 11 April 2018), European Data Protection Board, available online at: https://www.edpb.europa.eu/system/files/2023-09/wp260rev01_en.pdf, accessed on 3 July 2026.

[8] J. van Mil, J. P. Quintais, "A matter of (joint) control? Virtual assistants and the general data protection regulation", in Computer Law & Security Review, vol. 45, 2022, art. 105689, DOI: https://doi.org/10.1016/j.clsr.2022.105689.

[9] Romanian Parliament, Law no. 190 of 18 July 2018 on measures for the implementation of Regulation (EU) 2016/679, available online at: https://legislatie.just.ro/Public/DetaliiDocument/203151, accessed on 3 July 2026.

quantification, the analysis is centered on the synthesis of existing results to discern patterns of legal and communicative risks pertinent to voice-assisted music streaming. This brief comment on methodology is relevant, as this article is meant to be a concise legal contribution.

2. Voice-enabled music streaming as a multi-party data ecosystem

A single voice command typically triggers device-level recording, cloud-based voice recognition, and fulfillment by a streaming service, which is typically accomplished by multiple controllers or joint controllers. Each participant may determine different elements of the processing operation, such as the collection of voice commands, their transmission, their analysis, or the provision of the requested music service. Consequently, the legal qualification of each actor depends not on the technical sequence of operations but on its actual influence over the purposes and essential means of the processing. However, despite the seamless user experience, the process is complex and involves multiple actors whose goals are partially overlapping, making it challenging to assign responsibility and accountability[10]. This fragmentation is particularly problematic from the perspective of Articles 13 and 14 GDPR[11], since data subjects may experience the processing as a single service while their personal data are in fact processed by several legally distinct entities.

Where the essential purposes and means are determined jointly, there must be a transparent arrangement between the joint controllers under Article 26 of the GDPR[12]. The obligation to establish a transparent arrangement between joint controllers serves not only to allocate responsibilities internally but also to ensure that data subjects can effectively identify the entity responsible for complying with their GDPR rights. The CJEU case law has interpreted the concept of joint controllers widely, including instances where parties have an impact on parameters of processing or enjoy the benefit of it, even if they do not access all personal data[13]. Applied to voice-assisted music streaming, this broad interpretation suggests that more than one entity involved in delivering the service may qualify as a controller,

[10] J. van Mil, J. P. Quintais, "A matter of (joint) control? Virtual assistants and the general data protection regulation", in Computer Law & Security Review, vol. 45, 2022, art. 105689, DOI: https://doi.org/10.1016/j.clsr.2022.105689.

[11] European Parliament and Council of the European Union, Regulation (EU) 2016/679 (GDPR), available online at: https://eur-lex.europa.eu/eli/reg/2016/679/oj, accessed on 3 July 2026.

[12] *Ibidem.*

[13] Court of Justice of the European Union, Judgment of 5 June 2018, Unabhängiges Landeszentrum für Datenschutz Schleswig-Holstein v. Wirtschaftsakademie Schleswig-Holstein GmbH, Case C-210/16, available online at: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex:62016CJ0210, accessed on 3 July 2026; Court of Justice of the European Union, Judgment of 29 July 2019, Fashion ID GmbH & Co. KG v. Verbraucherzentrale NRW eV, Case C-40/17, available online at: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex:62017CJ0040, accessed on 3 July 2026.

even where individual participants do not have access to all personal data processed throughout the operation. Consequently, determining controllership requires a functional legal assessment rather than a purely technical analysis of data flows[14].

Empirical research has found that voice assistants generate a large amount of metadata, which may include profiling attributes, more specifically characteristics or preferences about the user that the system deduces algorithmically from voice and listening patterns, rather than information the user provides directly. Metadata include information such as timestamps, device identifiers, interaction frequency, listening history, and other contextual information generated during the user's interaction with the service. These profiling attributes are long-term and lack user awareness and control[15]. Under Article 4(4) GDPR[16], profiling refers to automated processing used to evaluate or predict personal aspects relating to an individual, including preferences, behaviour or interests.

From a technical perspective, a single voice command initiates a sequence of distinct processing operations, ranging from recording to uploading to the cloud, analysis, execution of the command, and then storage. Further, the regulations demand that it should be clear who decides what, when, and how, but in practice, all these decisions and activities are shared by a number of actors, such as the manufacturer, the software developers, the store, and so on, so that it becomes difficult to know who is doing what. It is, of course, understandable that a simple process for using the device is required, but in this case, accountability becomes difficult to assign. This uncertainty may also hinder the effective exercise of data subject rights, since individuals may be unable to determine which controller should receive requests relating to access, erasure or objection. Accordingly, legal compliance cannot be assessed solely by examining each processing operation in isolation. Instead, the entire processing chain should be considered in order to determine whether the allocation of responsibilities remains sufficiently transparent for data subjects throughout the lifecycle of the voice command.

[14] European Data Protection Board, Guidelines 07/2020 on the concepts of controller and processor in the GDPR (Version 2.1, adopted 7 July 2021), available online at: https://www.edpb.europa.eu/system/files/2023-10/EDPB_guidelines_202007_controllerprocessor_final_en.pdf, accessed on 3 July 2026.

[15] T. Khezresmaeilzadeh, E. Zhu, K. Grieco, D. J. Dubois, K. Psounis, D. Choffnes, "Echoes of Privacy: Uncovering the Profiling Practices of Voice Assistants", in Proceedings on Privacy Enhancing Technologies, vol. 2025, no. 2, pp. 71–87, DOI: https://doi.org/10.56553/popets-2025-0050.

[16] European Parliament and Council of the European Union, Regulation (EU) 2016/679 (GDPR), available online at: https://eur-lex.europa.eu/eli/reg/2016/679/oj, accessed on 3 July 2026.

3. Legal qualification of voice data under EU data protection law

In accordance with the GDPR, voice recordings and their transcripts are considered personal data if they are linkable to a particular data subject, especially in relation to account identifiers, device identifiers, and behavioral data[17]. This qualification follows from the broad definition of personal data under Article 4(1) GDPR[18], which covers any information relating to an identified or identifiable natural person, irrespective of the format in which that information is stored or processed. In voice-enabled music streaming services, these connections are common and carry a high re-identification risk. Even where a voice recording is not directly linked to a person's name, combinations of voice characteristics, account identifiers, device identifiers and usage patterns may enable the identification of the individual concerned[19].

If the features of the voice are used for the purpose of uniquely identifying the user, then it could be considered biometric data and therefore be subject to more stringent requirements for its processing[20]. Accordingly, the decisive criterion is not the nature of the voice recording itself but the purpose for which it is processed. The same recording may therefore constitute ordinary personal data when used solely to execute a voice command and biometric data when processed for authentication or unique identification. The guidelines developed by EDPB also highlight the importance of distinguishing between data processing that is necessary for the provision of the service and data processing for secondary purposes, as well as the risks of household data and bystander data with shared living environments[21]. Unlike traditional online services, voice assistants continuously operate within domestic environments, making it more likely that personal data relating to individuals other than the primary user will also be collected.

This distinction is particularly relevant for voice assistants because a single interaction may involve several processing purposes occurring simultaneously, some necessary for providing the requested service and others intended for improving algorithms, personalisation or profiling.

Voice data is therefore context-dependent when it is regulated, so the same audio file could be treated differently under the GDPR. The legal qualification

[17] *Ibidem.*

[18] *Ibidem.*

[19] Court of Justice of the European Union, Judgment of 19 October 2016, Patrick Breyer v. Bundesrepublik Deutschland, Case C-582/14, available online at: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex:62014CJ0582, accessed on 3 July 2026.

[20] Article 29 Data Protection Working Party, Opinion 3/2012 on developments in biometric technologies (WP193, adopted 27 April 2012), available online at: https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2012/wp193_en.pdf, accessed on 3 July 2026.

[21] European Data Protection Board, Guidelines 02/2021 on virtual voice assistants (Version 2.0), available online at: https://www.edpb.europa.eu/system/files/2021-07/edpb_guidelines_202102_on_vva_v2.0_adopted_en.pdf, accessed on 3 July 2026.

therefore depends on the specific processing operation rather than on the technical characteristics of the audio file itself. As already stated, the voice that is used in the command is considered personal data, but for example, the voice that is used in recognition and authentication is considered biometric data. This distinction has practical consequences, since the processing of biometric data for the purpose of uniquely identifying an individual is subject to the stricter regime established under Article 9 GDPR[22]. Another important issue arises in shared households, where voice assistants may capture the voices or other personal data of individuals who are not the device owners or registered users, such as family members, guests, or visitors. These individuals may be unaware that the device is recording their interactions and, consequently, may neither have provided consent nor have had the opportunity to exercise their data protection rights[23]. This creates practical difficulties in complying with the GDPR transparency obligations, since these individuals may not receive the information required under Articles 13 or 14 GDPR[24] despite their personal data being processed.

The identification of the appropriate legal basis under Article 6 GDPR[25] depends on the specific processing purpose. While certain processing operations may be necessary for the performance of the requested service, additional processing activities such as profiling or service improvement require an independent legal assessment and cannot automatically rely on the same legal basis[26].

4. Transparency and consent in voice interfaces

Research on voice assistants, namely AI-based systems that enable users to interact with digital services through spoken language, has found that users tend to underestimate data processing practices and fail to make use of the privacy controls available to them, instead relying on general trust or resignation[27]. As a

[22] European Parliament and Council of the European Union, Regulation (EU) 2016/679 (GDPR), available online at: https://eur-lex.europa.eu/eli/reg/2016/679/oj, accessed on 3 July 2026.

[23] N. Malkin, J. Deatrick, A. Tong, P. Wijesekera, S. Egelman, D. Wagner, "Privacy Attitudes of Smart Speaker Users", in Proceedings on Privacy Enhancing Technologies, vol. 2019, no. 4, pp. 250–271, DOI: https://doi.org/10.2478/popets-2019-0068.

[24] European Parliament and Council of the European Union, Regulation (EU) 2016/679 (GDPR), available online at: https://eur-lex.europa.eu/eli/reg/2016/679/oj, accessed on 3 July 2026.

[25] *Ibidem.*

[26] *Ibidem.*

[27] J. Lau, B. Zimmerman, F. Schaub, "Alexa, are you listening?", in Proceedings of the ACM on Human-Computer Interaction, vol. 2 (CSCW), art. 102, 2018, pp. 1–31, DOI: https://doi.org/10.1145/3274371; G. Terzopoulos, M. Satratzemi, "Voice assistants and smart speakers", in Informatics in Education, vol. 19, no. 3, 2020, pp. 473–490, available online at: https://files.eric.ed.gov/fulltext/EJ1267812.pdf, accessed on 3 July 2026; L. Hernández Acosta, D. Reinhardt, "Alexa, how do you protect my privacy?" A quantitative study of user

result, formal compliance with transparency requirements may coexist with low levels of effective understanding.

From a legal perspective, the transparency must function across different communication modalities. This entails providing short and simple voice disclosures and simple and reversible options for any data processing beyond the voice command. At the same time, the information provided through the app should be clear and easy to understand[28].

With voice interfaces, the formal concept of transparency will not translate to actual understanding for the user, and instead, users will probably rely on convenience, habit, or trust rather than actually understanding how the data is processed. Therefore, the formal concept of notice does not become particularly important. Transparency should function for both voice and app interfaces, providing users with short and easy to understand voice explanations and easy and reversible mechanisms for any processing beyond the command. The risk with compliance in this area will not be the availability of information but how it is presented.

5. Security, retention, and enforcement

There is also a problem with voice interfaces, as it is possible for a malicious third party (an attacker) to send voice commands, including inaudible or ultrasonic voice commands, that will cause the interface to do something that was not intended. This shows the importance of higher levels of confidentiality and integrity than those provided by account security[29].

Retention practices are also equally important. Having too much recorded data creates issues of fairness and the risk of breaking the law. This can be seen in the enforcement actions in the U.S. regarding the issue of keeping children's voice

preferences and requirements about smart speaker privacy settings", in Computers & Security, vol. 151, 2025, art. 104302, DOI: https://doi.org/10.1016/j.cose.2024.104302.

[28] European Data Protection Board, Guidelines 02/2021 on virtual voice assistants (Version 2.0), available online at: https://www.edpb.europa.eu/system/files/2021-07/edpb_guidelines_202102_on_vva_v2.0_adopted_en.pdf, accessed on 3 July 2026; Article 29 Data Protection Working Party, Guidelines on transparency under Regulation 2016/679 (WP260 rev.01, as last revised and adopted 11 April 2018), European Data Protection Board, available online at: https://www.edpb.europa.eu/system/files/2023-09/wp260rev01_en.pdf, accessed on 3 July 2026.

[29] G. Zhang, C. Yan, X. Ji, T. Zhang, T. Zhang, W. Xu, "DolphinAttack: Inaudible voice commands", in Proceedings of the 2017 ACM SIGSAC Conference on Computer and Communications Security (CCS '17), 2017, DOI: https://doi.org/10.1145/3133956.3134052; S. S. Alchekov, M. A. Al-Absi, A. A. Al-Absi, H. J. Lee, "Inaudible Attack on AI Speakers", in Electronics, vol. 12, no. 8, 2023, art. 1928, DOI: https://doi.org/10.3390/electronics12081928; G. Zhang, C. Yan, X. Ji, T. Zhang, T. Zhang, W. Xu, "DolphinAttack: Inaudible voice commands", in Proceedings of the 2017 ACM SIGSAC Conference on Computer and Communications Security (CCS '17), 2017, DOI: https://doi.org/10.1145/3133956.3134052.

data in voice assistants longer than allowed[30]. Although these are not binding in the EU, they do give us an idea of what is expected in terms of minimization and deletion from a comparative law point of view.

A directly comparable precedent within the EU itself confirms that these concerns are not merely theoretical: in August 2019, the Hamburg Commissioner for Data Protection and Freedom of Information opened an urgency procedure under Article 66 GDPR against Google, provisionally prohibiting the human review and transcription of Google Assistant voice recordings across the entire EU, after leaked recordings were found to contain sensitive personal information, including medical details and recordings of individuals in distress[31].

For example, on March 19, 2025, The Associated Press wrote that Amazon would stop a function that allowed some Echo users to choose not to send voice recordings to the cloud[32].

The above topics demonstrate that security with voice-enabled systems is not just about protecting an account. The voice interface can be activated in an improper manner. The retention time is also a security issue and a legal issue. Although these regulations from outside the EU may not be binding, they reflect how seriously regulators take data minimization and deletion.

At national level, public guidance and resources made available by the Romanian supervisory authority (ANSPDCP) reinforce the practical expectation that information and user controls should be accessible and intelligible to data subjects, including in Romanian-language contexts[33].

[30] Federal Trade Commission, "FTC and DOJ Charge Amazon with Violating Children's Privacy Law by Keeping Kids' Alexa Voice Recordings Forever and Undermining Parents' Deletion Requests", 31 May 2023, available online at: https://www.ftc.gov/news-events/news/pressreleases/2023/05/ftc-doj-charge-amazon-violating-childrens-privacy-law-keeping-kids-alexa-voice-recordings-forever, accessed on 3 July 2026; Associated Press, "Amazon ends little-used privacy feature that let Echo users opt out of sending recordings to company", in AP News, 19 March 2025, available online at: https://apnews.com/article/amazon-privacy-echo-7fb3c19fa7f664bde5c5be259f8b23ee, accessed on 3 July 2026.

[31] HmbBfDI – Der Hamburgische Beauftragte für Datenschutz und Informationsfreiheit, "Sprachassistenzsysteme auf dem Prüfstand – Datenschutzbehörde eröffnet Verwaltungsverfahren gegen Google" (press release), 1 August 2019, available online at: https://datenschutz-hamburg.de/fileadmin/user_upload/HmbBfDI/Pressemitteilungen/2019/2019-08-01_Google-Assistant.pdf, accessed on 3 July 2026.

[32] Associated Press, "Amazon ends little-used privacy feature that let Echo users opt out of sending recordings to company", in AP News, 19 March 2025, available online at: https://apnews.com/article/amazon-privacy-echo-7fb3c19fa7f664bde5c5be259f8b23ee, accessed on 3 July 2026.

[33] ANSPDCP, New General Data Protection Regulation (GDPR) – resources, available online at: https://www.dataprotection.ro/?page=noua+_pagina_regulamentul_GDPR, accessed on 2 February 2026.

6. Conclusions

Voice-enabled music streaming is a high-risk area for data processing. Legal compliance is based on the similarity between the way the system is designed, the way we communicate with users, and data protection principles. The key steps that are gaining importance in this regard include separating service delivery and profiling, reducing the amount of stored data, clarifying the roles of data controllers, and making transparency a fundamental tool for compliance[34].

Generally speaking, voice interfaces undermine the classical, text-based models of consent and notice[35]. To solve this problem, we can consider our way of communication as an element of data protection compliance rather than additional information.

The problem with voice-enabled music streaming and other hands-free settings is the way that the current data protection laws are not quite suitable for the reality of the situation, in which interaction is not screen-based and not all information is written down. It is not that there are no laws or standards, but the divide is becoming wider between the system and the information provided to the end-users and the traditional methods of obtaining consent. At this point, effective communication must be considered an essential foundation of data protection laws.

References

ANSPDCP, *New General Data Protection Regulation (GDPR) – resources*, available online at: https://www.dataprotection.ro/?page=noua+_pagina_regulamentul_GDPR, accessed on 2 February 2026.

Article 29 Data Protection Working Party, *Opinion 3/2012 on developments in biometric technologies* (WP193, adopted 27 April 2012), available online at: https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2012/wp193_en.pdf, accessed on 11 July 2026.

Article 29 Data Protection Working Party, *Guidelines on transparency under Regulation (EU) 2016/679* (WP260 rev.01, as last revised and adopted 11 April 2018), European Data Protection Board, available online at: https://www.edpb.europa.eu/ system/files/ 2023-09/wp260rev01_en.pdf, accessed on 11 July 2026.

Associated Press, *Amazon ends little-used privacy feature that let Echo users opt out of sending recordings to company*, in *AP News*, 19 March 2025, available online at: https://apnews.com/article/amazon-privacy-echo-7fb3c19fa7f664bde5c5be259f8b23ee, accessed on 11 July 2026.

[34] European Parliament and Council of the European Union, Regulation (EU) 2016/679 (GDPR), available online at: https://eur-lex.europa.eu/eli/reg/2016/679/oj, accessed on 11 July 2026; European Data Protection Board, Guidelines 02/2021 on virtual voice assistants (Version 2.0), available online at: https://www.edpb.europa.eu/system/files/2021-07/edpb_guidelines_202102_on_vva_v2.0_adopted_en.pdf, accessed on 3 July 2026.

[35] L. F. Cranor, "Necessary but Not Sufficient: Standardized Mechanisms for Privacy Notice and Choice", in Journal on Telecommunications and High Technology Law, vol. 10, no. 2, 2012, pp. 273–308, available online at: https://scholar.law.colorado.edu/ctlj/vol10/iss2/7/, accessed on 3 July 2026.

Alchekov S. S., Al-Absi M. A., Al-Absi A. A., Lee H. J., *Inaudible Attack on AI Speakers*, in *Electronics*, vol. 12, no. 8, 2023, art. 1928, DOI: https://doi.org/10.3390/electronics12081928.

Court of Justice of the European Union, *Judgment of 19 October 2016, Patrick Breyer v. Bundesrepublik Deutschland*, Case C-582/14, available online at: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex:62014CJ0582, accessed on 11 July 2026.

Court of Justice of the European Union, *Judgment of 5 June 2018, Unabhängiges Landeszentrum für Datenschutz Schleswig-Holstein v. Wirtschaftsakademie Schleswig-Holstein GmbH*, Case C-210/16, available online at: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex:62016CJ0210, accessed on 11 July 2026.

Court of Justice of the European Union, *Judgment of 29 July 2019, Fashion ID GmbH & Co. KG v. Verbraucherzentrale NRW eV*, Case C-40/17, available online at: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex:62017CJ0040, accessed on 11 July 2026.

Cranor L. F., *Necessary but Not Sufficient: Standardized Mechanisms for Privacy Notice and Choice*, in *Journal on Telecommunications and High Technology Law*, vol. 10, no. 2, 2012, pp. 273–308, available online at: https://scholar.law.colorado.edu/ctlj/vol10/iss2/7/, accessed on 11 July 2026.

European Data Protection Board, *Guidelines 02/2021 on virtual voice assistants* (Version 2.0), available online at: https://www.edpb.europa.eu/system/files/2021-07/edpb_guidelines_202102_on_vva_v2.0_adopted_en.pdf, accessed on 11 July 2026.

European Data Protection Board, *Guidelines 07/2020 on the concepts of controller and processor in the GDPR* (Version 2.1, adopted 7 July 2021), available online at: https://www.edpb.europa.eu/system/files/2023-10/EDPB_guidelines_202007_controllerprocessor_final_en.pdf, accessed on 11 July 2026.

European Parliament and Council of the European Union, *Regulation (EU) 2016/679 (General Data Protection Regulation – GDPR)*, available online at: https://eur-lex.europa.eu/eli/reg/2016/679/oj, accessed on 11 July 2026.

Federal Trade Commission, *FTC and DOJ Charge Amazon with Violating Children's Privacy Law by Keeping Kids' Alexa Voice Recordings Forever and Undermining Parents' Deletion Requests*, 31 May 2023, available online at: https://www.ftc.gov/news-events/news/press-releases/2023/05/ftc-doj-charge-amazon-violating-childrens-privacy-law-keeping-kids-alexa-voice-recordings-forever, accessed on 11 July 2026.

Hernández Acosta L., Reinhardt D., *„Alexa, how do you protect my privacy?" A quantitative study of user preferences and requirements about smart speaker privacy settings*, in *Computers & Security*, vol. 151, 2025, art. 104302, DOI: https://doi.org/10.1016/j.cose.2024.104302.

HmbBfDI – Der Hamburgische Beauftragte für Datenschutz und Informationsfreiheit, *Sprachassistenzsysteme auf dem Prüfstand – Datenschutzbehörde eröffnet Verwaltungsverfahren gegen Google* (press release), 1 August 2019, available online at: https://datenschutz-hamburg.de/fileadmin/user_upload/HmbBfDI/Pressemitteilungen/2019/2019-08-01_Google-Assistant.pdf, accessed on 11 July 2026.

Khezresmaeilzadeh T., Zhu E., Grieco K., Dubois D. J., Psounis K., Choffnes D., *Echoes of Privacy: Uncovering the Profiling Practices of Voice Assistants*, in *Proceedings on Privacy Enhancing Technologies*, vol. 2025, no. 2, 2025, pp. 71–87, DOI: https://doi.org/10.56553/popets-2025-0050.

Lau J., Zimmerman B., Schaub F., *Alexa, are you listening?*, in *Proceedings of the ACM on Human-Computer Interaction*, vol. 2 (CSCW), art. 102, 2018, pp. 1–31, DOI: https://doi.org/10.1145/3274371.

Malkin N., Deatrick J., Tong A., Wijesekera P., Egelman S., Wagner D., *Privacy Attitudes of Smart Speaker Users*, in *Proceedings on Privacy Enhancing Technologies*, vol. 2019, no. 4, 2019, pp. 250–271, DOI: https://doi.org/10.2478/popets-2019-0068.

Romanian Parliament, *Law no. 190 of 18 July 2018 on measures for the implementation of Regulation (EU) 2016/679*, available online at: https://legislatie.just.ro/Public/DetaliiDocument/203151, accessed on 11 July 2026.

Terzopoulos G., Satratzemi M., *Voice assistants and smart speakers*, in *Informatics in Education*, vol. 19, no. 3, 2020, pp. 473–490, available online at: https://files.eric.ed.gov/fulltext/EJ1267812.pdf, accessed on 11 July 2026.

Uyar L., Clement M., Veseli B., Kandziora M., *The rise of smart speakers: A comparative analysis of music streaming service adoption and platform interdependencies*, in *Journal of Media Economics*, vol. 37, no. 3, 2025, pp. 129–147, DOI: https://doi.org/10.1080/08997764.2025.2494994.

van Mil J., Quintais J. P., *A matter of (joint) control? Virtual assistants and the General Data Protection Regulation*, in *Computer Law & Security Review*, vol. 45, 2022, art. 105689, DOI: https://doi.org/10.1016/j.clsr.2022.105689.

Zhang G., Yan C., Ji X., Zhang T., Zhang T., Xu W., *DolphinAttack: Inaudible voice commands*, in *Proceedings of the 2017 ACM SIGSAC Conference on Computer and Communications Security (CCS '17)*, 2017, DOI: https://doi.org/10.1145/3133956.3134052.