Access to Justice in Eastern Europe
ISSN 2663-0575 (Print)
ISSN 2663-0583 (Online)
Journal homepage http://ajee-journal.com

Research Article

# CONSENT TO PROCESSING PERSONAL DATA IN ONLINE BEHAVIOURAL ADVERTISING AS PER THE GDPR AND EXPERIENCE IN VIETNAM

***Hau Vo Trung***

## ABSTRACT

***Background:*** *The advent of computers has transformed personal information into a valuable asset. Online behavioural advertising seeks to match advertising with Internet users. However, many online behavioural advertising companies often use data collection and processing methods that violate the rights of Internet users when extracting and analysing personal data to track and profile online behavioural advertising. These risks may be related to discrimination, inequality, stereotyping, stigmatisation, and inaccuracy in decision-making. This affects the privacy of users. EU law has clear regulations on consent to process personal data in online behavioural advertising. In contrast, Vietnamese law has notable limitations, especially in recording consent to process personal data. It is necessary to improve Vietnamese law on the issue of consent to process personal data based on the provisions of EU law.*

***Methods:*** *The article uses the analytical method to clarify the concept of personal data processing and the characteristics of online behavioural advertising. The analytical method also indicates the possibility that online behavioural advertising can hurt personal information. This method is also used to analyse EU law protecting personal data in online behavioural advertising, thereby finding experiences that Vietnamese law can learn from.*

*The article also uses the comparative method. This method is mainly used to compare EU law and Vietnamese law related to the provisions on consent to process personal data in online behavioural advertising. Combined with the above analysis method, the comparative method shows the advantages of EU law compared to Vietnamese law on the issue of consent to process personal data in online behavioural advertising. From there, the article can make policy recommendations to improve Vietnamese law on this issue.*

***Results and conclusions:*** *The article concludes that Vietnam can learn from the EU on the requirement that consent to process personal data in online behavioural advertising must be given freely, with knowledge, specifically, and clearly. The article proposes policy recommendations for Vietnam on personal data consent in online behavioural advertising. First, the law must consistently define "personal data" and "personal data protection." Second, it specifies the adequate time for the data subject's consent.*

## 1 INTRODUCTION

The advent of computers has significantly transformed personal information into a valuable asset, fundamentally impacting the collection of personal information. Computers can store vast amounts of raw data relatively quickly, cheaply, and virtually indefinitely at incredible speeds. Processing often creates new information that serves as the basis for human or computer decision-making.

The development of telecommunications technology and the integration of computers with the Internet have further amplified the importance of information. With interconnected systems enabling the seamless transmission of data, the collection and use of personal information have become increasingly widespread. Personal data can now be shared across different computer users on the network, increasing accessibility but also raising significant privacy concerns.

Using computers to process personal information carries risks, including data being accessed or disclosed inaccurately, incompletely, or used for purposes beyond the original intent. A person's home, finances, mental state, physical condition, and thinking can be exposed to the most casual observer. Financial institutions, for example, collect and provide extensive information on individuals' creditworthiness, drinking habits, health, characteristics, reputation, extramarital relationships, religious beliefs, criminal records, race, and sexual preferences. As a result, they can reveal a complete profile of an individual's ability to repay a loan and personal life. In addition, direct marketing agencies leverage such data for online behavioural advertising.

## 2 METHODOLOGY AND RESEARCH METHODS

The current legal analysis focuses on the regulations governing online behavioural advertising in the European Union and Vietnam. This methodology follows a legal approach, focusing on the legislative frameworks currently in force. Specifically, the study analyses the EU and Vietnamese legislation on consent to processing personal data in online behavioural advertising, with particular attention to its negative impacts on users' privacy, information self-determination, and autonomy.

The analysis considers the current EU framework, namely the General Data Protection Regulation (GDPR), which has been effective since 25 May 2018.[1] The current legal framework of Vietnam includes the 2013 Constitution of Vietnam, the 2015 Civil Code of Vietnam, the 2016 Law on Access to Information, the 2016 Law on Children, and Decree No. 13/2023/ND-CP, issued by the Government on 17 April 2023, concerning the protection of personal data.[2]

This study hypothesises that the regulation of consent to processing personal data in online behavioural advertising under the provisions of GDPR is complete. In contrast, the provisions of Vietnamese law on this issue are sketchy. Therefore, Vietnamese law can benefit from the EU's experience regulating consent to personal data processing.

## 3 OVERVIEW OF PERSONAL DATA PROCESSING AND ONLINE BEHAVIOUR ADVERTISING

### 3.1. Overview of Personal Data Processing

According to the European Commission's classification personal data[3] is divided into: (i) contact information such as home address, place of work of the individual, email address, telephone number; (ii) technical data such as IP address, device-related data on type, international mobile equipment identity (IMEI), browser information; (iii) demographic data such as age, ethnicity, gender, education level, occupation, household income, number, gender, age of household members; (iv) location data such as mobile device, GPS data and travel history entered into satellite positioning system, radio frequency identification (RFID) sensor data; (v) interest and behavioural data such as history of websites visited and

1 Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the Protection of Natural Persons with Regard to the Processing of Personal Data and on the Free Movement of Such Data, and Repealing Directive 95/46/EC (General Data Protection Regulation) (Text with EEA relevance) [2016] OJ L 119/1.

2 Constitution of the Socialist Republic of Vietnam (adopted 28 November 2013) <https://lawnet.vn/en/vb/Constitution-dated-November-28-2013-of-the-socialist-republic-of-Vietnam-362FD.html> accessed 28 November 2024; Law no 91/2015/QH13 of 24 November 2015 'Civil Code' <https://lawnet.vn/en/vb/Law-No-91-2015-QH13-The-Civil-Code-4A07E.html> accessed 28 November 2024; Law no 102/2016/QH13 of 5 April 2016 'Children Law' <https://lawnet.vn/en/vb/Law-102-2016-QH13-children-4C457.html> accessed 28 November 2024; Law no 104/2016/QH13 of 6 April 2016 'Access to Information' <https://lawnet.vn/en/vb/Law-104-2016-QH13-access-to-information-4C458.html> accessed 28 November 2024; Decree no 13/2023/ND-CP of 17 April 2023 'On Protection of Personal Data' <https://lawnet.vn/en/vb/Decree-No-13-2023-ND-CP-dated-April-17-2023-on-protection-of-personal-data-89C77.html> accessed 28 November 2024.

3 Regulation (EU) 2016/679 (n 1); 'Data Protection: Rules for the Protection of Personal Data Inside and Outside the EU' (*European Commission*, 2024) <https://commission.europa.eu/law/law-topic/data-protection_en> accessed 28 November 2024.

number of clicks on advertisements, which may include searches on sensitive topics such as health issues or religious views, games and apps used, telecommunications data from car insurance companies, social media posts, professional websites, email exchanges; (vi) financial transaction data such as history from utility providers, service contract details, income and credit rating information, loyalty card purchase history, prices paid, income and credit rating information; (vii) social media data such as profile information and posts, connections between family members and friends, photos, videos; and (viii) public records such as birth records, death records, marriage records, land registration records.

Personal data can also be distinguished into first-party and third-party data. First-party data is collected directly by businesses from their audiences and customers—individuals who directly interact with them, such as in a commercial transaction. In contrast, third-party data can be obtained from first or third parties through purchase or exchange, as well as from public records or social media analysis. Finally, third parties may collect data directly when users visit the first-party website. Under the GDPR, personal data is further divided into ordinary and sensitive personal data. Much of the data collected for advertising purposes can reveal sensitive personal information about consumers. Therefore, personal data protection can be understood as a legal safeguard, ensuring that another individual or organisation processes individuals' data responsibly.

## 3.2. Overview of Online Behavioural Advertising

According to the European Commission, online behavioural advertising[4] encompasses (i) advertising based on the content of the website visited or the keywords entered into the search engine; (ii) advertising based on information provided by the individual when registering on a website, such as gender, age, or location; and (iii) advertising based on observing the behaviour of individuals over time through the behaviour of accessing the website repeatedly, interacting, keywords, producing online content... to develop a specific profile to provide individuals with advertisements tailored to their interests. Online behavioural advertising can be understood as using personal data to select and display digital content to introduce goods, services, or traders of goods and services to Internet users.

The online behavioural advertising market operates by matching advertising to Internet users through personal data processing procedures based on various technologies. This process involves any operation performed on personal data such as collection, recording, organisation, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination, alignment or combination, blocking, deletion, or

4 'Consumer Market Study on Online Market Segmentation Through Personalised Pricing/Offers in the European Union' (*European Commission*, 19 July 2018) <https://commission.europa.eu/publications/consumer-market-study-online-market-segmentation-through-personalized-pricingoffers-european-union_en> accessed 28 November 2024.

destruction of such data.[5] The primary goal of online behavioural advertising is to deliver more personalised, relevant, and engaging advertising content to improve the online experience of consumers.

In the past, Internet users passively consumed information from a few local media sources. Today, they can actively search for news from multiple sources that can actively align with their interests.[6] The Internet's filtering mechanisms, whether user-selected or algorithmically driven, play a crucial role in determining the content users see. Trade associations representing the advertising industry often claim that the entire Internet ecosystem is supported by online behavioural advertising.[7] After all, without the constant flow of money from online behavioural advertising, all the free services, news, videos, and apps would disappear.[8]

Online behavioural advertising publishers argue that tracking, profiling, and targeting are simply about better understanding customers, directly providing them with tailored services, and displaying more appropriate ads. However, these companies often employ data collection and processing methods that violate Internet users' rights, extracting and analysing personal data for online behavioural advertising tracking and profiling.

## 4 THE IMPACT OF ONLINE BEHAVIOURAL ADVERTISING ON HUMAN RIGHTS

### 4.1. Online Behavioural Advertising Invades Privacy

The Internet has provided an unprecedented space for new forms of advertising to flourish and for ordinary people to collect and share information at a meagre cost. While newspapers in the late 19th century were the only ones that could effectively discover and disseminate personal stories, the digital age has made personal data collection and processing accessible

5 Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the Protection of Individuals with Regard to the Processing of Personal Data and on the Free Movement of Such Data [1995] OJ L 281/31.

6 Emily Bell, CW Anderson and Clay Shirky, 'Post-Industrial Journalism: Adapting to the Present' (*Columbia Journal Review*, 27 November 2012) <https://www.cjr.org/behind_the_news/post_industrial_journalism_ada.php> accessed 28 November 2024.

7 IAB Europe, *Consumers Driving the Digital Uptake: The Economic Value of Online Advertising-Based Services for Consumers* (*EDAA*, September 2010) <https://www.youronlinechoices.com/white_paper_consumers_driving_the_digital_uptake.pdf> accessed 28 November 2024.

8 Internet Advertising Bureau UK, *The Data Deal: How Data-Driven Digital Advertising Benefits UK Citizens* (IAB UK 2014) <https://www.iabuk.com/policy/data-deal-how-data-driven-digital-advertising-benefits-uk-citizens> accessed 28 November 2024.

to almost anyone.[9] This raises a crucial question: how can privacy threats to big data, often associated with processing personal data, be compromised?

Tene and Polonetsky develop the concept of a piecemeal process through which profiles relating to individuals can become more visible as personal data accumulates. Ohm argues that if separate pieces of information from an anonymised database are entirely linked, they can be unlocked if just one of those pieces is linked to a person's real identity, ending up with a vast database.[10] Armed with a massive database of detailed personal information and data mining technologies, any organisation or individual can effortlessly uncover details about a person's employment, leisure activities, favourite supermarkets, or even highly sensitive information such as medical conditions, sexual orientation, and religious views.[11] Thus, tracking a person's online activities is like paparazzi taking photos of a celebrity's home.

The European Convention on Human Rights (ECHR) does not explicitly mention the "right to privacy"; however, Article 8 provides the right to respect private life, family, home, and correspondence.[12] Similarly, Article 7 of the Charter of Fundamental Rights of the European Union provides the right to respect private and family life, home, and communications.[13] At the national level, the constitutions of many European countries have incorporated the protection of privacy or private family life as a fundamental right.[14] While Article 7 of the Charter provides for the right to privacy, Article 8 provides the right to data protection, distinguishing but interlinking these two concepts. Similarly, Article 1(1) of the Data Protection Directive (DPD) provides for the right to privacy concerning the processing of personal data,[15] whereas Article 1(2) of the General Data Protection Regulation (GDPR) uses the term "right to personal data protection".[16]

9 Kim McNamara, 'The Paparazzi Industry and New Media: The Evolving Production and Consumption of Celebrity News and Gossip Websites' (2011) 14(5) International Journal of Cultural Studies 515, doi:10.1177/1367877910394567.

10 Paul Ohm, 'Broken Promises of Privacy: Responding to the Surprising Failure of Anonymization' (2010) 57 UCLA Law Review 1746-8.

11 Carter Jernigan and Behram FT Mistree, 'Gaydar: Facebook Friendships Exposing Sexual Orientation' (2009) 14(10) First Monday, doi:10.5210/fm.v14i10.2611.

12 Council of Europe, *European Convention on Human Rights* (Convention for the Protection of Human Rights and Fundamental Freedoms, as amended by Protocols) (ECHR 2013).

13 Charter of Fundamental Rights of the European Union (2012/C 326/02) [2012] OJ C 326/391.

14 These include the Belgian Constitution (2014), art. 22; the Bulgarian Constitution (2007), art. 32; Constitution of Croatia (2010), art. 35; Constitution of Estonia (2011), art. 26; Constitution of Finland (2011), para. 10; Constitution of Greece (2008), art. 9; Constitution of Hungary (2011), art. 6; Constitution of Latvia (2014), art. 96; Constitution of Lithuania (2006), art. 22; Constitution of the Netherlands (2008], art. 10; Constitution of Poland (2009), art. 47; Constitution of Portugal (2005), art. 26(1); Constitution of Romania (2003), art. 26; Constitution of Slovakia (2014), art. 19; Constitution of Spain (2011), para. 18. English versions of these Constitutions are available at: *CONSTITUTE* <https://www.constituteproject.org/?lang=en> accessed 28 November 2024.

15 Directive 95/46/EC (n 5).

16 Regulation (EU) 2016/679 (n 1).

In the case of online behavioural advertising, user data is almost always collected and analysed through fully automated systems. Traditionally, privacy concepts underpin the rationale for providing legal protection for personal information based on the assumption that people care about how others perceive them. These "*others*" can be just one person, such as in wiretapping cases or a broader audience, as with media disclosures. Importantly, privacy concerns arise when a human—not a machine—observes personal data. Some argue that computers themselves do not violate privacy; rather, privacy is only threatened when another person observes a person, so processing by wholly automated means should not be considered a threat to privacy. From a technical perspective, online behavioural advertisers, much like traditional media entities such as *The New York Times,* maintain vast databases but are often less focused on tracking individual customer data. Nonetheless, certain forms of automated processing of personal data are more sensitive, necessitating human oversight.

On the other hand, in addition to the websites that users intentionally visit, other third parties are involved in the tracking, profiling, and targeting process. Most of these activities are not carried out directly between services but through the user's browser. Technically, the communications are "*requested*" by the browser in response to instructions embedded in web pages. This raises important questions: Should this be considered part of a person's "*private and family life*" as defined in the ECHR or the Charter? Or do they fall within the private sphere of a person's "*leaving alone,*" as defined by Warren and Brandeis? Different perspectives yield opposing interpretations that lead to opposite perceptions of the extent to which the rights of Internet users are violated. Even if a user's interaction with a website is deemed private and confidential, third-party interference may strip away that privacy. Theoretically, the most common form of third-party tracking can only occur with permission from the web page and the browser. However, a counter-argument is that the average user, in most cases, needs to be made aware of third-party tracking, does not have the skills to turn off tracking, or is concerned about the limited functionality. Hence, their expectation remains that communications should be protected as private conversations.

With the proliferation of online behavioural advertising, digital reputations are becoming increasingly challenging to manage. User data can be merged with private and public profiles, as well as those of other individuals, effectively erasing the wall that exists between private and public life. While the digital landscape enables advertisers to build user profiles, it offers little to no tools for users to manage their online presence. If creating a technological item unfairly unbalances the current distribution of benefits, then a reformulation of the relevant legal policy is necessary. An electronic device is the property of its owner, but it serves the owner and online behavioural advertisers. Tracking, profiling, and targeting are all done in a decentralised, multi-level manner. Advertisers, publishers, and advertising service providers can all store user profiles, contributing to a situation where big data renders an individual's reputation nearly

impossible to manage. Unlike a credit score, where individuals can quickly figure out how to avoid negative factors based on their credit history, it is impossible for a person to access the scoring system based on a complex array of private activities, hidden records, external sources, and other customers.

## 4.2. Online Behavioural Advertising Violates the Right to Information Autonomy

The ability to control one's own information is a prerequisite for forming a unique "*self*" in a relatively homogeneous social context. Lynskey argues that an individual's public information can have many aspects, the combination of which can hinder their self-development.[17] Similarly, Rouvroy and Poullet have pointed out the importance of informational autonomy as an absolute element in a person's personality and the construction of personal identity.[18] Cohen views privacy as a comfortable space for individuals' personalities to form.[19] Posner argues that forced disclosure of personal information is sometimes desirable if the nature of the information will lead to external effects or if the transaction costs of voluntary information collection are too high.[20] Solove also advocates a similar approach, arguing that privacy issues should be decided based on a balance of interests from both sides.[21]

At the same time, forming personal characteristics is not just a product of individual subjectivity. Social patterns and constraints also play an essential role in maintaining a stable society. Therefore, Cohen observes that subjectivity will emerge "*gradually, in significantly constrained ways but not rigidly determined by social shaping.*"[22] In today's digital landscape, internet users have little control over data collected about them. In the era before online behavioural advertising, marketing research was conducted primarily through surveys, where consumers could decide whether to participate and provide their answers. In contrast, online behavioural data is collected automatically with only the best protections of "*opt-out*" or "*implied consent*." There is no easy way to tailor the data to an individual's wishes before sending it.

17 Orla Lynskey, 'Deconstructing Data Protection: The Added-value" of a Right to Data Protection in the EU Legal Order' (2014) 63 (3) International and Comparative Law Quarterly 569, doi:10.1017/S0020589314000244.

18 Antoinette Rouvroy and Yves Poullet, 'The Right to Informational Self-Determination and the Value of Self-Development: Reassessing the Importance of Privacy for Democracy' in Serge Gutwirth and others (eds), *Reinventing Data Protection?* (Springer 2009) 51, doi:10.1007/978-1-4020-9498-9_2.

19 Julie E Cohen, 'What Privacy is For' (2013) 126(7) Harvard Law Review 1927-32.

20 Richard A Posner, 'The Right of Privacy' (1978) 12(3) Georgia Law Review 397-401.

21 Daniel J Solove, *Understanding Privacy* (Harvard UP 2009) 50.

22 Cohen (n 19) 1910.

Individuals may be subjected to algorithmic systems where data is secretly collected and used to inform some form of decision-making, often without their explicit consent.[23] Posner, from an economic perspective, argues that making one's data public can be seen as a way to manipulate information about that person. However, manipulation is only sometimes something entirely negative. Posner believes that others can demand an individual's private information as a demand for information about an asset to inform their decision-making process.[24]

## 4.3. Online Behavioural Advertising Personal Autonomy

Online behavioural advertising can threaten a person's autonomy when data subjects cannot consciously identify themselves as being tracked online. The principle of equality can also be undermined by unfair treatment based on the use of personal data. Unfairness can arise from inaccurate information or overly general classifications on the one hand, from accurate but unverifiable information, and more apparent distinctions on the other.[25] All of these potential adverse effects can pose severe risks to data subjects. As personal data becomes more widely used, a helpful approach to maintaining autonomy is to address the issue of liberty and equality in the context of big data. It is easy to see why autonomy lies at the heart of liberty and equality. As Rawls paraphrases Kant's concept of autonomy, "*A man is acting autonomously when the principles of action he chooses are the fullest expression of his nature as a rational, accessible, and equal being.*"[26] The values of freedom and equality are inherently linked to autonomy.[27] A man who acts under external influence cannot be said to act autonomously. Benn presents a view of an autonomous man as one whose consistent life is rooted in a set of beliefs, values, and principles by which his actions are regulated. For him, choice and rational criticism are necessary conditions for autonomy, stating that "*being a chooser is not enough to be autonomous.*"[28]

With another approach, Raz presents the essence of personal autonomy as "*the vision of those who control, to some extent, the destiny of the individual himself, shaping the individual himself through successive decisions throughout his life.*"[29] To satisfy the element of autonomy, three conditions must be met: minimal mental capacity, full range of choices, and independence from coercion.[30] For Raz, "*the environment in which autonomous life can*

23 John Danaher, 'The Threat of Algocracy: Reality, Resistance and Accommodation' (2016) 29(3) Philosophy & Technology 245, doi:10.1007/s13347-015-0211-1.

24 Posner (n 20) 396.

25 Jiahong Chen, 'The Dangers of Accuracy: Exploring the Other Side of the Data Quality Principle' (2018) 4(1) European Data Protection Law Review 36, doi:10.21552/edpl/2018/1/7.

26 John Rawls, *A Theory of Justice* (Harvard UP 2009) 222.

27 Gerald Dworkin, *The Theory and Practice of Autonomy* (CUP 1988) 12-20.

28 SI Benn, 'Freedom, Autonomy and the Concept of a Person' (1976) 76(1) Proceedings of the Aristotelian Society 123.

29 Joseph Raz, *The Morality of Freedom* (OUP 1988) 369.

30 ibid 369-78.

*develop*" is essential for achieving autonomy.[31] Accordingly, a desirable model of freedom must be one that "*protects those pursuing different lifestyles from intolerance and calls for the provision of conditions of autonomy without which autonomous living is impossible.*"[32]

Between these two approaches lies Dworkin's theory of autonomy, which focuses heavily on the individual's ability to reflect on life decisions. He sees autonomy as an intermediary between a person's particular preferences and the general, principled values that the person possesses. For him, autonomy is conceived as a second-order human capacity to critically reflect on preferences and desires and accept or attempt to change these by higher-order preferences. By exercising such a capacity, humans define their nature, give meaning and coherence to their lives, and take responsibility for who they are. Dworkin points out that "*a state may be required to recognise the autonomy of its citizens. That is, it may only restrict the freedom of individuals if it can justify such restrictions by arguments that the individual himself can consider accurate.*"[33]

Raz's theory may be intrinsically relevant to data protection because it views autonomy as a matter of lifestyle rather than specific decisions. The emphasis on the role and limitations of law in promoting autonomy fits well with the ongoing debate about the model of data protection law. Much of Raz's work on legal theories concerns the seemingly conflicting normative requirements of human reason and authority. In short, his question is if the nature of law requires that organisations and individuals in society obey it without questioning its rationale, how can this be compatible with human autonomy? In everyday life, it is not uncommon for us to give up our final decision-making power or limit future choices by, for example, committing to a contract or setting a speed limit. The point is that there are many other ways to achieve the fundamental value of being able to act on our judgment by reason. For Raz, obedience to authority "*is not a denial of people's ability to act rationally, but simply a means if the authority allows the subject to confirm better reasons.*"[34]

## 5 EU LEGAL REGULATION ON CONSENT TO PROCESSING PERSONAL DATA IN ONLINE BEHAVIOURAL ADVERTISING

Information about EU law relating to personal data protection and the authorities ensures this law is applied consistently. It includes separate regulations in each specific aspect related to e-commerce. Specifically, (i) Directive 2002/58/EC of the European Parliament and of the Council of 12 July 2002 concerning processing personal data and protecting privacy in the electronic communications sector (Directive on privacy and electronic communications).

31 ibid 391.
32 ibid 425.
33 Dworkin (n 27) 40.
34 Joseph Raz, *Between Authority and Interpretation: On the Theory of Law and Practical Reason* (OUP 2009) 140, doi:10.1093/acprof:oso/9780199562688.001.0001.

(ii) Directive (EU) 2019/770 of the European Parliament and of the Council of 20 May 2019 on certain aspects concerning contracts for the supply of digital content and digital services. (iii) Regulation (EU) 2022/1925 of the European Parliament and of the Council of 14 September 2022 on contestable and fair markets in the digital sector and amending Directives (EU) 2019/1937 and (EU) 2020/1828 (Digital Markets Act). (iv) Regulation (EU) 2022/2065 of the European Parliament and of the Council of 19 October 2022 on a Single Market for Digital Services and amending Directive 2000/31/EC (Digital Services Act).

However, direct regulation of personal data consent in online behavioural advertising is detailed in the General Data Protection Regulation (GDPR). EU data protection law applies when a company processes "personal data," information relating to an identified or identifiable data subject.[35] The definition of "processing" is comprehensive, and almost anything that can be done with personal data falls within its scope. Online behavioural advertising requires the processing of personal data. Pseudonymised data attached to cookies are personal because they "*allow data subjects to be identified, even when their real names are* unknown."[36] This is consistent with the case law of the Court of Justice of the European Union. European data protection law applies when a company is established in the European Union. The law also applies if a company is not based in Europe but uses European-based equipment to process data.[37] Alternatively, it uses cookies to track EU citizens.[38] Consent is the sole legal basis for processing personal data collected by cookies;[39] it is also the sole legal basis for processing data during the tracking period.

Under Clause 11, Article 4, according to the GDPR, consent is "*any freely given, specific, informed and unambiguous indication of the data subject's wishes which, by a statement or by a clear affirmative action, signifies agreement to the processing of personal data relating to the data subject*."[40] The GDPR also establishes stricter requirements for legal consent regarding children's data, sensitive data, and data used in automated decision-making. The GDPR requires that consent be a freely given, specific, informed, and unambiguous indication, by a statement or by an explicit affirmative action, by the data subject. Consent must be specific,

35 Regulation (EU) 2016/679 (n 1) art 80(2).

36 European Commission Opinion 2/2010 on Online Behavioural Advertising (adopted on 22 June 2010) <https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/index_en.htm> accessed 28 November 2024.

37 Lokke Moerel, *Binding Corporate Rules: Corporate Self-Regulation of Global Data Transfers* (OUP 2012) 72, doi:10.1093/acprof:oso/9780199662913.001.0001.

38 European Commission Opinion 1/2008 on Data Protection Issues Related to Search Engines (adopted 4 April 2008) <https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/index_en.htm> accessed 28 November 2024.

39 Directive 2002/58/EC of the European Parliament and of the Council of 12 July 2002 Concerning the Processing of Personal Data and the Protection of Privacy in the Electronic Communications Sector (Directive on Privacy and Electronic Communications) [2002] OJ L 201/37, para (25).

40 Regulation (EU) 2016/679 (n 1) art 4, s 11.

comprehensive, based on clear and specific requirements, and be demonstrable by the controller. Specifically, consent must be freely given, consent must be specific, consent must be informed, and consent must be unambiguous.

## 5.1. Consent Must Be Freely Given

First of all, consent must be "*freely given*."[41] Previously, the DPD did not provide criteria for what constitutes or does not constitute "*freely given*" consent. However, the GDPR has clarified that "*consent is not considered to be freely given if the data subject does not have a genuine or free choice or is unable to refuse or withdraw consent without detriment.*"[42] The Taskforce considers that "*if the data subject does not have a genuine choice, feels obliged to give consent or would suffer negative consequences if they do not give consent, then the consent is invalid.*" [43]

Consent requirements must include (i) the availability of appropriate options and (ii) withholding consent does not result in detriment. Statements of consent prepared in advance by data controllers must be provided in an easily accessible, understandable form using clear, easy-to-understand language.[44] If the data subject's refusal to consent would put them at a disadvantage, then the consent cannot be considered freely given. The Working Group considers that "*if withdrawing the consent would result in a downgrade of the performance of the service to the detriment of the user, then consent was never lawfully given.*"[45]

Article 7.4 of the GDPR states: "*When assessing whether consent has been freely given, due regard shall be paid to whether, among other things, the performance of the contract is conditioned on consent to the processing of personal data.*"[46] In other words, if the processing of personal data is not necessary for providing a service but the provider still requests it as a condition, the consent will be considered invalid because the situation will be subject to "*due regard*." The draft GDPR proposed that "*the performance of a contract or the provision of a service shall not be conditioned on consent to the processing of data*

41 Noor Ashikin Basarudin and Ridwan Adetunji Raji, 'Implication of Personalized Advertising on Personal Data: A Legal Analysis of the EU General Data Protection Regulation' (2022) 7(22) Environment-Behaviour Proceedings Journal 109, doi:10.21834/ebpj.v7i22.4160.

42 Regulation (EU) 2016/679 (n 1) art 7.

43 European Commission, *Guidelines on Automated Individual Decision-Making and Profiling for the Purposes of Regulation 2016/679 (wp251rev.01)* (adopted 3 October 2017, last revised and adopted 6 February 2018) 10 <https://ec.europa.eu/newsroom/article29/items/612053> accessed 28 November 2024.

44 Eroupean Data Protection Board, *Guidelines 1/2024 on processing of personal data based on Article 6(1)(f) GDPR Version 1.0* (adopted 8 October 2024) <https://www.edpb.europa.eu/our-work-tools/documents/public-consultations/2024/guidelines-12024-processing-personal-data-based_en> accessed 28 November 2024.

45 European Commission Guidelines on Automated Individual Decision-Making (n 47) 10.

46 Regulation (EU) 2016/679 (n 1) art 7, s 4.

*which is not necessary for the performance of the contract or the provision of the service*."[47] This proposal was rejected but reintroduced with softer wording and reworded into the current GDPR.[48] That is, consent to processing personal data for the performance of a contract is only sometimes valid, and the data controller will need to demonstrate a legitimate reason for the data processing request.[49] Therefore, for the consent to be valid, the online behavioural advertising company must demonstrate that if the Internet user expresses a refusal to consent to data processing, the online behavioural advertising company will not deny the service; otherwise, it will lead to the conclusion that this case is not "*freely given consent*."

The Task Force suggests that when determining the validity of consent, the requirements set out by other laws should be considered.[50] It states, "*Article 7.4 of the GDPR seeks to ensure that the purpose of processing personal data is not disguised nor is it accompanied by the provision of a service contract for which the personal data are not necessary*."[51] Online behavioural advertising is a separable purpose and is not necessary for the provision of online services.[52] In other words, requiring Internet users to consent to the use of their personal data for advertising as a condition for accessing a service would likely violate the provisions of the GDPR.[53]

However, users often have to click on links and read in-depth documents to understand how their data is used for online behavioural advertising. For example, Facebook requires users to click on its cookie policy to learn how they may be tracked online. The only alternative is

47 Draft European Parliament Legislative Resolution on the Proposal for a Regulation of the European Parliament and of the Council on the Protection of Individuals with Regard to the Processing of Personal Data and on the Free Movement of Such Data (General Data Protection Regulation) (21 November 2013) amendment 82 <https://www.europarl.europa.eu/doceo/document/A-7-2013-0402_EN.html> accessed 28 November 2024.

48 Council of the EU, *Proposal for a Regulation of the European Parliament and of the Council on the Protection of Individuals with Regard to the Processing of Personal Data and on the Free Movement of Such Data (General Data Protection Regulation) - Preparation for Trilogue* (27 November 2015) 2 <https://www.eumonitor.eu/9353000/1/j9vvik7m1c3gyxp/vjzebx068vy6> accessed 28 November 2024.

49 Information Commissioner's Office, *Consultation: GDPR Consent Guidance* (ICO 2017) 19-21 <https://ico.org.uk/media/about-the-ico/consultations/2013610/gdpr-consent-guidance-consultation-form-word-201703.docx> accessed 28 November 2024; Philipp Hacker, 'Personal Data, Exploitative Contracts, and Algorithmic Fairness: Autonomous Vehicles Meet the Internet of Things' (2017) 7(4) International Data Privacy Law 266, doi:10.1093/idpl/ipx014.

50 European Commission Opinion 15/2011 on the Definition of Consent (adopted 13 July 2011) <https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/index_en.htm> accessed 28 November 2024.

51 Frederik J Zuiderveen Borgesius and others, 'Tracking Walls, Take-It-Or-Leave-It Choices, the GDPR, and the ePrivacy Regulation' (2017) 3(3) European Data Protection Law Review 360-1.

52 European Commission Opinion 06/2014 on the Notion of Legitimate Interests of the Data Controller under Article 7 of Directive 95/46/EC (adopted 9 April 2014) <https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/index_en.htm> accessed 28 November 2024.

53 Zuiderveen Borgesius (n 51) 360-1.

to click the "*manage data settings*" button to navigate through a more complex interface that makes it easier for users to opt out of specific cookies. Data subjects often need to be allowed to give separate consent for their data to be processed by different parties for online behavioural advertising purposes.[54]

In summary, consent is not considered to be freely given in the following cases:

(i) There is an imbalance between data subjects and data controllers. Unbalanced situations arise when one party has a dominant market position, as with online behavioural advertising companies.[55] In all these cases, the online behavioural advertising company must demonstrate no risk of "*deception, intimidation, coercion or significant negative consequences if the data subject does not consent*."
(ii) The consent given is not sufficiently specific. That is, the personal data subject does not have the opportunity to give separate consent for different personal data processing activities.
(iii) Consent to processing personal data is considered a condition of the contract's performance. That is, the performance of the contract, including the provision of services, is entirely dependent on consent, even if such consent is not necessary for the performance of the contract. The control that EU agencies exercise over national authorities in the matter of consent is also clearly reflected in the judgment of the General Court dated 29 January 2025.[56]

On 7 March 2024, the European Court of Justice issued a critical decision on the scope of the definition of "personal data" under EU data protection law. Case C-604/22 aimed at a more objective approach to the concept of personal data. The case primarily addressed the issue of whether the European IAB, which provides its members with a framework to enable them to comply with the GDPR, could be considered a (joint) controller. The Court decided that the TCF string, a combination of letters and characters, could be regarded as personal data. The Court also assessed that combining the TCF string with additional data, such as an IP address, could help with re-identification. The Court's decision opened the door to a more "objective" approach to personal data. This "protective" approach is realiSed by considering that regardless of who holds the additional data, if the data can be re-identified through additional information, then the

54 Centre for Information Policy Leadership, *The Limitations of Consent as a Legal Basic for Data Processing in the Digital Society* (CIPL 2024) <https://thelivinglib.org/the-limitations-of-consent-as-a-legal-basis-for-data-processing-in-the-digital-society/> accessed 28 November 2024.

55 Eroupean Data Protection Board, *Guidelines 05/2020 on Consent under Regulation 2016/679* (adopted 4 May 2020) <https://www.edpb.europa.eu/our-work-tools/our-documents/guidelines/guidelines-052020-consent-under-regulation-2016679_en> accessed 28 November 2024.

56 Case T-70/23 (Joined Cases T-70/23, T-84/23, T-111/23) *Data Protection Commission v European Data Protection Board* (General Court (EU), 29 January 2025) <https://curia.europa.eu/juris/document/document.jsf?text=&docid=294757&pageIndex=0&doclang=en&mode=lst&dir=&occ=first&part=1&cid=1971675> accessed 28 November 2024.

data must be regarded as personal data.[57] In addition, consent can be withdrawn, according to the Court's judgment of 4 October 2024, Case C-200/23.[58]

## 5.2. Consent Must be Explicitly Given

The requirement that consent must be given through a specific act was addressed by the ECJ in Case C-673/17(57-58).[59] In it, the Court stated that consent is invalid if information storage or access to information already stored in the website user's terminal is permitted by a checkbox pre-checked by the service provider, which the user must uncheck to refuse. In this decision, the Court linked affirmative action to specificity, stating that consent must relate specifically to the processing of the data in question and cannot be inferred from the data subject's indication of his or her wishes for other purposes. Consent that is freely given, specific, informed, and unambiguous can only be the user's explicit consent, given with full knowledge of the facts and after providing complete information about the use of their data. In Case C40/17,[60] the ECJ dealt with a third-party social add-on (a Facebook-like button) included in a website. The add-on caused the visitor's browser to request content from the owner of the add-on (Facebook) and transmit personal data about the visitor to that owner.

The Court affirmed that the website operator should only request consent to transmit the add-on to the owner. This requires the owner of the add-on to specify the legal basis for any further processing. Another relevant case was recently decided by the French Council of State, which heard Google's appeal against a fine imposed by the French National Data Protection Commission (CNIL). The judges upheld the fine, stating that Google violated the requirement that consent must be informed, specific, unambiguous, and based on affirmative action as provided in Article 4 of the GDPR. Users are provided with a pre-ticked box allowing advertising personalisation, contrary to affirmative action; they cannot easily access the information for processing, contrary to the requirement of freedom of expression, and the information is not specific and too vague. Therefore, the processing of user data, especially in the case of online behavioural advertising, lacks a legal basis according to Article 6, GDPR provisions.

57 Case C-604/22 *IAB Europe v Gegevensbeschermingsautoriteit* (CJEU (Fourth Chamber), 7 March 2024) <https://curia.europa.eu/juris/document/document.jsf?text=&docid=283529&pageIndex=0&doclang=EN&mode=lst&dir=&occ=first&part=1&cid=1971675> accessed 28 November 2024.

58 Case C-200/23 *Agentsia po Vpisvaniyata* (CJEU (First Chamber), 4 October 2024) <https://curia.europa.eu/juris/document/document.jsf?text=&docid=290701&pageIndex=0&doclang=en&mode=lst&dir=&occ=first&part=1&cid=1971675> accessed 28 November 2024.

59 T Van Canneyt and others, 'Data Protection: CJEU Case Law Review – 1995-2020' (2021) 56 Computerrecht 78.

60 Case C-40/17 *Fashion ID GmbH & Co KG v Verbraucherzentrale NRW eV* (CJEU (Second Chamber), 29 July 2019) <https://curia.europa.eu/juris/document/document.jsf?text=&docid=216555&pageIndex=0&doclang=en&mode=lst&dir=&occ=first&part=1&cid=1971675> accessed 28 November 2024.

## 5.3. Consent Must Be Given in an Informed Manner

The third criterion for the validity of consent is whether the consent is given "*informed*"? The Task Force explains that "*for consent to be informed, it is necessary to inform the data subject of certain elements that are important for making a choice and that such information is clear, distinguishable from other matters and provided in an understandable and accessible form.*"[61] There is a close connection and even overlap between the "specific" and "*informed*" requirements.[62] The GDPR stipulates that "*for consent to be informed, the data subject must at least know the controller's identity and the intended purpose of processing personal data.*"[63]

On the other hand, the information that the data controller is obliged to provide is broader in scope than what the "*specific*" element requires. According to Article 13 and Article 14 of the GDPR, the data controller must provide details such as: "*information about the data controller; the purposes and legal basis for the processing; the categories of personal data concerned; the identity or categories of data recipients; the period for which the personal data is stored; the right of the data subject to withdraw consent; the existence of automated decision-making and the potential for influence on the data subject.*"[64]

All of these elements must be mentioned in the privacy policy for online behavioural advertising. The collection of personal data in online behavioural advertising often occurs not only on the intended website of the user but also on the advertiser's server. Information about the advertiser, the publisher, the advertising service provider, and other relevant parties must be made clear to the data subject, including the scope of the data processed and how the personal data is processed. To express consent, at a minimum, the data subject must know the controller's identity and the purposes for which the personal data are being processed. The GDPR states that "*consent shall cover all processing operations carried out for the same or more purposes. Where processing has multiple purposes, consent shall be required for all processing operations for the same or more purposes*". Informed consent is also linked to the idea of transparency since data subjects can be said to be informed only when a person has a real opportunity to know the processing features, i.e., when the information provided is detailed but also specific and understandable.

A company may process personal data for online behavioural advertising when the data subject has given "*explicit consent.*"[65] Explicit consent is interpreted as meaning that the condition that an authorised entity, to be able to bring a representative action under that provision, must assert that it considers the rights of a data subject provided for in that

61 Eroupean Data Protection Board, *Guidelines 05/2020* (n 55) para 67.
62 Information Commissioner's Office (n 49) 21-2.
63 Regulation (EU) 2016/679 (n 1) para 42.
64 ibid, art 13.
65 Regulation (EU) 2016/679 (n 1) art 80(2).

regulation to have been infringed "as a result of the processing", within the meaning of that provision, is satisfied where that entity asserts that the infringement of the data subject's rights occurs in the course of the processing of personal data and results from the controller's infringement of its obligation, under the first sentence of Article 12(1) and Article 13(1)(c) and (e) of that regulation, to provide the data subject, in a concise, transparent, intelligible and easily accessible form, in clear and plain language, with information relating to the purposes of that data processing and the recipients of such data, at the latest when they are collected. This was made clear in the court judgment of 11 July 2024, dispute C-757/22.[66]

Transparency is a prerequisite for data subjects to have some control over how online behavioural advertising companies use their data. Articles 10 and 11 of the GDPR require online behavioural advertising companies to provide at least information regarding their identity and processing purposes and provide additional information to ensure fair processing. Companies must always be transparent about processing personal data, regardless of whether they rely on consent. Internet users must be provided with additional information that is easy to read, and they must act affirmatively to give consent. These regulations have a significant impact on the way stakeholders present information online and ask for user consent.

## 6 VIETNAM CONTEXT OF ONLINE BEHAVIOURAL ADVERTISING

According to the 2023 E-commerce White Book, the size of Vietnam's retail e-commerce market will reach 20.5 billion USD, an increase of 4 billion USD (equivalent to 25%) compared to 2022, and Vietnam's e-commerce growth rate is among the top 10 countries with the fastest trade growth rate in the world.[67] Many major e-commerce sites in Vietnam have been hacked, and their data has been stolen.[68] The shortage of specialised human resources and security technology makes dealing with cyber security threats difficult.[69] Sometimes, businesses intentionally share customer

66 Case C-757/22 *Meta Platforms Ireland (Action représentative)* (CJEU (Fourth Chamber), 11 July 2024) <https://curia.europa.eu/juris/document/document.jsf?text=&docid=288148&pageIndex=0&doclang=EN&mode=lst&dir=&occ=first&part=1&cid=143131> accessed 28 November 2024.

67 Minitry of Industry and Trade of the Socialist Republic of Vietnam, *E-commerce White Book 2023* (Department of E-commerce and Digital Economy 2024) 40.

68 Bui Thi Nguyet Thu, 'Some Solutions to Contribute to Improving Personal Data Protection in Vietnam' (2024) 26 Vietnam Integration Journal 339.

69 Manh Chung, 'Consecutive Attacks on Vietnamese Businesses: "Just the Tip of the Iceberg"' *VnEconomy* (Hanoi, 6 April 2024) <https://vneconomy.vn/lien-tiep-cac-vu-tan-cong-mang-vao-doanh-nghiep-viet-chi-la-phan-noi-cua-tang-bang.htm> accessed 28 November 2024.

information with third parties without their consent.[70] In addition, information disclosure also occurs due to subjective reasons from consumers.[71]

When participating in activities on the Internet platform, the right to ensure the safety and confidentiality of consumers' information is stipulated in Article 6 of the Law on Protection of Consumer Rights 2010. However, these regulations only acknowledge the legal protection of Internet users' information—a small part of the concept of privacy. The lack of clear rules on the specific responsibilities of related parties, such as publishers and advertising networks, in users' activities on the Internet platform leads to a lack of legal tools to force associated entities to comply. Because advertising activities on the Internet platform today still have a huge gap compared to traditional advertising methods. Online advertising has many loopholes, such as difficulty in control, the lack of legal basis for organisations providing this activity, and specific responsibilities or conditions for online advertising activities. This form is gradually becoming a tool for illegal advertising, as well as advertising in forms that do not meet the conditions prescribed by law, to appear more and more and cause significant harm to consumers.

Vietnam's data protection law must ensure that data owners have a complete choice about whether to consent to the use of their data. This is important because, currently, in Vietnam, online behavioural advertising systems lack three technical elements that affect the consent of personal data owners, as described below.

*First, there is a need for alternative services*. In key online sectors such as search engines and video streaming, a few service providers control the market. In effect, Internet users often have no viable alternatives, as the most essential features are available only through these platforms.

*Second, there is a lack of alternative data processing models.* While some "pay-as-you-go" or "freemium" (free + premium) business models are gaining popularity in some sectors,[72] "free" services supported by online behavioural advertising continue to dominate the Internet environment. For example, in the social media sector, major service providers are still primarily funded by online behavioural advertising revenue.[73]

70 Phong Linh, 'Panicking about Personal Information Disclosure: 80% of the Causes Come from this Reason…' *Thanh Nien* (Hanoi, 18 August 2023) <https://thanhnien.vn/phat-hoang-vi-lo-thong-tin-ca-nhan-80-nguyen-nhan-xuat-phat-tu-ly-do-nay-185230817164650831.htm> accessed 28 November 2024.

71 Thu Huong, 'Be Careful to Avoid Being Scammed When Buying Online' *Quảng Ngãi* (Quang Ngai, 14 March 2024) <https://baoquangngai.vn/phap-luat/202403/canh-giac-tranh-bi-lua-dao-khi-mua-hang-online-06d1722/> accessed 28 November 2024.

72 Mark Sweney, 'Online Paid-content Market Poses Threat to Traditional Advertising' *The Guardian* (London UK, 1 November 2012) <https://www.theguardian.com/media/2012/nov/01/online-paid-contect-rise-8-billion-pounds> accessed 28 November 2024.

73 Kurt Wagner, 'Pinterest Expects to Make More than $500 Million in Revenue this Year' (*CNBC*, 21 March 2017) <https://www.cnbc.com/2017/03/21/pinterest-revenue-projected-at-500-million-this-year.html > accessed 28 November 2024.

*Third, there is a need for alternative data networks.* When a data subject withdraws consent, the data controller is obliged to delete the relevant data immediately[74] unless another legal basis for processing applies or an exception is in place.[75] At the same time, if the data has been shared with third parties and the data subject requests its deletion, the data controller must "*take reasonable steps, including technical measures,*" to notify them of the request.[76] Notably, the data controller must ensure that withdrawing consent is as easy as giving consent.[77]

## 7 CONCLUSIONS

Online behavioural advertising has been shown to negatively impact consent for processing personal data. The article's analysis shows that this can lead to privacy violations, information self-determination violations, and user autonomy violations. EU law has addressed these concerns through regulations that govern consent for personal data processing, requiring that consent be freely given, explicit, and informed. Vietnam can learn some lessons from these regulations.

Online behavioural advertising has been shown to be negligent in obtaining consent to process personal data. The article's analysis shows that this can lead to privacy violations, information self-determination violations, and user autonomy violations. EU law has controlled these issues through regulations that prescribe the appropriate obtaining of consent for processing personal data. Consent must be given freely, explicitly, and informedly. Vietnam can learn some lessons from these regulations.

Vietnam has 69 legal documents related to personal data protection. First, the 2013 Constitution of Vietnam stipulates the right to protect information about private life, family secrets, and personal secrets. Then, the 2015 Civil Code, the 2016 Law on Access to Information, and the 2016 Law on Children also use "information about private life, personal secrets, and family secrets" but do not define these terms. Decree No. 13/2023/ND-CP, dated 17 April 2023, defines "personal data" and "personal data protection," but its scope does not cover all areas of society.[78]

74 Regulation (EU) 2016/679 (n 1) art 17, para 1.

75 ibid, art 17, para 1, (b).

76 ibid, art 17, s 2.

77 ibid, art 17, s 3.

78 Law on Cyber Security 2015; Law on Denunciation 2013, Decree No. 146/2018/ND-CP dated October 17, 2018, detailing and guiding measures to implement several articles of the Law on Health Insurance; Decree No. 85/2016/ND-CP on ensuring information system security at different levels; Decree No. 72/2013/ND-CP dated July 15, 2013, on management, provision and use of internet services and information on the network; Decree No. 52/2013/ND-CP dated May 16, 2013, on e-commerce; Decree No. 64/2007/ND-CP on the application of information technology in the activities of government agencies.

Legal documents are not unified in terms of personal data protection, and many different terms are used to express this issue. The lack of uniformity in terminology has caused difficulties in application. Therefore, Vietnamese law needs to unify the use of the term "personal data" to ensure compatibility in content, scope, method, and specific application cases. Vietnam should refer to the provisions of the GDPR to develop a definition for the term "personal data."

In addition, the provisions of Vietnamese law are also unclear on the consent of the personal data subject. Article 11 of Decree 13/2023/ND-CP, dated 17 April 2023, stipulates the data subject's consent in a list-based manner. Specifically, the consent of the data subject is only valid when: (i) the data subject voluntarily and knows the content of the data type, the purpose of processing personal data, and the person who will receive the data; (ii) the data subject's consent must be clearly and specifically expressed in writing or by voice; (iii) the consent must be given for the same purpose; (iv) consent is expressed in a verifiable format; and (v) the data subject's silence or non-response is not considered consent.

However, these provisions are insufficient to fully protect the data owner's rights. Therefore, Vietnamese law could strengthen consent regulations by adopting clearer and more specific provisions on voluntary consent, drawing inspiration from the GDPR.

Besides, Vietnamese law needs to be more specific on the following issues:

First, telecommunications service providers should be required to strictly censor and ensure the accuracy of information, humane content, and conformity with cultural traditions before coordinating with service users to post advertisements on electronic media.

Second, it is necessary to quickly complete and supplement more specific qualitative and quantitative regulations and directly mention advertising on electronic media.

Third, relevant parties must ensure that systems running in browsers can more accurately identify the current user interacting with the system. One option is to use keystroke dynamics, which can be changed depending on each user. Another option is to identify the current user based on the last few pages viewed immediately. That is, if a user visits several websites related to children in a short period, the current user is likely a child rather than an adult, so timely solutions can be taken to prevent and limit online behavioural advertising at that time. This is also the social responsibility of businesses towards consumers, especially children.

## REFERENCES

1. Basarudin NA and Raji RA, 'Implication of Personalized Advertising on Personal Data: A Legal Analysis of the EU General Data Protection Regulation' (2022) 7(22) Environment-Behaviour Proceedings Journal 109, doi:10.21834/ebpj.v7i22.4160.
2. Bell E, Anderson CW and Shirky C, 'Post-Industrial Journalism: Adapting to the Present' (*Columbia Journal Review*, 27 November 2012) <https://www.cjr.org/behind_the_news/post_industrial_journalism_ada.php> accessed 28 November 2024.
3. Benn SI, 'Freedom, Autonomy and the Concept of a Person' (1976) 76(1) Proceedings of the Aristotelian Society 109.
4. Chen J, 'The Dangers of Accuracy: Exploring the Other Side of the Data Quality Principle' (2018) 4(1) European Data Protection Law Review 36, doi:10.21552/edpl/2018/1/7.
5. Cohen JE, 'What Privacy is For' (2013) 126(7) Harvard Law Review 1904.
6. Danaher J, 'The Threat of Algocracy: Reality, Resistance and Accommodation' (2016) 29(3) Philosophy & Technology 245, doi:10.1007/s13347-015-0211-1.
7. Dworkin G, *The Theory and Practice of Autonomy* (CUP 1988).
8. Hacker P, 'Personal Data, Exploitative Contracts, and Algorithmic Fairness: Autonomous Vehicles Meet the Internet of Things' (2017) 7(4) International Data Privacy Law 266, doi:10.1093/idpl/ipx014.
9. Jernigan C and Mistree BFT, 'Gaydar: Facebook Friendships Exposing Sexual Orientation' (2009) 14(10) First Monday, doi:10.5210/fm.v14i10.2611.
10. Lynskey O, 'Deconstructing Data Protection: The Added-value" of a Right to Data Protection in the EU Legal Order' (2014) 63 (3) International and Comparative Law Quarterly 569, doi:10.1017/S0020589314000244.
11. McNamara K, 'The Paparazzi Industry and New Media: The Evolving Production and Consumption of Celebrity News and Gossip Websites' (2011) 14(5) International Journal of Cultural Studies 515, doi:10.1177/1367877910394567.
12. Moerel L, *Binding Corporate Rules: Corporate Self-Regulation of Global Data Transfers* (OUP 2012) doi:10.1093/acprof:oso/9780199662913.001.0001.
13. Nguyet Thu BT, 'Some Solutions to Contribute to Improving Personal Data Protection in Vietnam' (2024) 26 Vietnam Integration Journal 339.
14. Ohm P, 'Broken Promises of Privacy: Responding to the Surprising Failure of Anonymization' (2010) 57 UCLA Law Review 1701.
15. Posner RA, 'The Right of Privacy' (1978) 12(3) Georgia Law Review 393.
16. Rawls J, *A Theory of Justice* (Harvard UP 2009).

17. Raz J, *Between Authority and Interpretation: On the Theory of Law and Practical Reason* (OUP 2009) doi:10.1093/acprof:oso/9780199562688.001.0001.

18. Raz J, *The Morality of Freedom* (OUP 1988).

19. Rouvroy A and Poullet Y, 'The Right to Informational Self-Determination and the Value of Self-Development: Reassessing the Importance of Privacy for Democracy' in Gutwirth S and others (eds), *Reinventing Data Protection?* (Springer 2009) 45, doi:10.1007/978-1-4020-9498-9_2.

20. Solove DJ, *Understanding Privacy* (Harvard UP 2009).

21. Van Canneyt T and others, 'Data Protection: CJEU Case Law Review – 1995-2020' (2021) 56 Computerrecht 78.

22. Zuiderveen Borgesius FJ and others, 'Tracking Walls, Take-It-Or-Leave-It Choices, the GDPR, and the ePrivacy Regulation' (2017) 3(3) European Data Protection Law Review 353.

## AUTHORS INFORMATION

**Hau Vo Trung**
Ph.D. (Law), Lecturer, Law Department, Binh Duong University, Binh Duong, Vietnam
hauvotrung1819@gmail.com
https://orcid.org/0009-0006-3560-4359
**Corresponding author**, responsible for conceptualization, methodology, data curation, resources, investigation, formal analysis and writing – original draft.

**Competing interests**: No competing interests were disclosed.

**Disclaimer**: The author declare that his opinion and views expressed in this manuscript are free of any impact of any organizations.

## ABOUT THIS ARTICLE

**Cite this article**
Vo Trung H, 'Consent to Processing Personal Data in Online Behavioural Advertising as Per the GPDR and Experience in Vietnam' (2025) 8(2) Access to Justice in Eastern Europe 179-202 <https://doi.org/10.33327/AJEE-18-8.2-a000101>

**DOI** https://doi.org/10.33327/AJEE-18-8.2-a000101

**Managing editor** – Mag. Yuliia Hartman. **English Editor** – Julie Bold.

***Keywords:*** *online behavioural advertising, consent reason data, personal information.*

## DETAILS FOR PUBLICATION

Date of submission: 06 Dec 2024
Date of acceptance: 10 Feb 2024
Date of Online First publication: 17 Mar 2025
Last Publication: 14 May 2025
Whether the manuscript was fast tracked? - No
Number of reviewer report submitted: 2 reports
Number of revision rounds: 1 round, revised version submitted 08 Feb 2025

**Technical tools were used in the editorial process:**
Plagiarism checks - Turnitin from iThenticate https://www.turnitin.com/products/ithenticate/
Scholastica for Peer Review https://scholasticahq.com/law-reviews

## RIGHTS AND PERMISSIONS

## АНОТАЦІЯ УКРАЇНСЬКОЮ МОВОЮ

Дослідницька стаття

# ЗГОДА НА ОБРОБКУ ПЕРСОНАЛЬНИХ ДАНИХ У ПОВЕДІНКОВІЙ ОНЛАЙН-РЕКЛАМІ ВІДПОВІДНО ДО GDPR ТА ДОСВІД В'ЄТНАМУ

***Хау Во Трунг***

АНОТАЦІЯ

***Вступ.*** *Поява комп'ютерів перетворила особисту інформацію на цінний актив. Поведінкова онлайн-реклама прагне адаптувати рекламу до користувачів Інтернету. Однак багато компаній, що займаються цим питанням, часто використовують методи збору та обробки даних для відстеження та профілювання поведінкової онлайн-реклами, які порушують права користувачів Інтернету. Ці ризики можуть бути пов'язані з дискримінацією, нерівністю, стереотипами, стигматизацією та неточністю у прийнятті рішень. Це впливає на конфіденційність користувачів. Законодавство ЄС чітко регламентує згоду на обробку персональних даних у поведінковій онлайн-рекламі. Натомість в'єтнамське законодавство має значні обмеження, особливо щодо питань згоди на обробку персональних даних, тож це необхідно вдосконалити, взявши за основу положення законодавства ЄС.*

***Методи.*** *У статті використовується аналітичний метод для з'ясування поняття обробки персональних даних та характеристик поведінкової онлайн-реклами. Цей метод вказує на можливість того, що поведінкова онлайн-реклама може завдати шкоди персональним даним. Аналітичний метод також використовується для аналізу законодавства ЄС щодо захисту персональних даних у поведінковій онлайн-рекламі, що дає змогу дізнатись про досвід, який може бути використаний у в'єтнамському законодавстві.*

*У дослідженні було застосовано також порівняльний метод. Цей метод в основному використовується для порівняння законодавства ЄС і законодавства В'єтнаму щодо положень про згоду на обробку персональних даних у поведінковій онлайн-рекламі. У поєднанні з наведеним вище методом аналізу порівняльний метод показує переваги законодавства ЄС над законодавством В'єтнаму щодо питання згоди на обробку персональних даних у поведінковій онлайн-рекламі. На основі цього в статті можна сформулювати рекомендації щодо політики для покращення в'єтнамського законодавства з цього питання.*

***Результати та висновки.*** *У статті було зроблено висновок, що В'єтнам, з огляду на досвід ЄС, може повчитися ставити вимоги стосовно того, що згода на обробку персональних даних у поведінковій онлайн-рекламі повинна надаватися вільно, зі знанням справи, конкретно та чітко. У дослідженні пропонуються рекомендації щодо політики В'єтнаму стосовно надання згоди на персональні дані в поведінковій онлайн-рекламі. По-перше, закон має узгодити визначення понять «персональні дані» та «захист персональних даних». По-друге, має бути визначенно відповідний час для отримання згоди суб'єкта даних.*

***Ключові слова:*** *поведінкова онлайн-реклама, підстави для згоди, персональні дані.*