Eksplorium *p*-ISSN 0854-1418
Volume 46 No. 1, May 2025: 683–697 *e*-ISSN 2503-426X

Right to be Informed: GDPR Research and Policy Implications for Vietnam

Dr. Le Thi Minh
Thu Dau Mot University, Vietnam
minhlt@tdmu.edu.vn
ORCID: 0000-0003-0156-4046

Article Received: 20 Feb 2025, Revised: 22 April 2025, Accepted:05 May 2025

Abstract: The right to be informed is considered to have high practical value among the rights of data subjects. The General Data Protection Regulation (GDPR) on the right to be informed is rooted in some fundamental values such as privacy, autonomy, transparency and fairness. The article presents the provisions of the GDPR on the right to be informed, including Content of notification information, Provision of InformationInformation on automated decisions, and Information on privacy policies. Vietnamese laws on personal data protection must thoroughly impact the right to be informed. Legal regulations need to ensure the right to be informed not only for data subjects but also establish transparency for the entire digital economy, including competitors, civil society and state management agencies. Vietnamese laws on personal data protection need to specifically regulate acts of providing inappropriate information. The right to be informed is not a separate right but part of a broader and comprehensive data protection regime under Vietnamese law. This regime must ensure that it provides an individual with meaningful control over their data. It must be one of the most detailed and comprehensive data protection regimes suitable for the digital economy.

Keywords: Right to be informed, data transparency, data protection

1. INTRODUCTION

The right to be informed is considered to have the highest practical value among the rights of data subjects. Formally, all rights are considered equal, but in practice, the right to be informed stands out as an illustration of the principle of transparency and represents the heart of all other rights of data subjects. Without the necessary information, data subjects cannot participate meaningfully in the digital economy, nor can they exercise their other control rights. The General Data Protection Regulation (GDPR) right to be informed is rooted in several fundamental values such as privacy, autonomy, transparency and fairness. The right to be informed is closely linked to transparency as a fundamental value. The right to be informed is the cornerstone of the system of rights of control over personal data under the General Data Protection Regulation (GDPR).

Previously, the right to be informed was not included in the provisions relating to the rights of data subjects under the European Union (EU) Data Protection Directive (DPD). However, the General Data Protection Regulation (GDPR) changed the structure of the Directive by making the right to be informed a part of Chapter 3 on the rights of data subjects. Schrems, who became famous after suing Facebook, used the right to be informed and access to fight the social media giant. [1]. Schrems argued that if he had not known about the quantity and quality of data that Facebook was processing, he would have had difficulty consenting to Facebook's data processing activities in the first place. In the Bara case, the European Court of Justice (CJEU) also agreed with this view, stating that: "*The right to be informed is a prerequisite for other rights since the requirement to inform the data subject about the processing of his or her data is all the more important when it affects the data subject's exercise of his or her right to access and to rectify the data being processed and his or her right to object to the processing of such*

[1] Cyrus Farivar (2012). How one law student is making Facebook get serious about privacy, https://arstechnica.com/tech-policy/2012/11/how-one-law-student-is-making-facebook-get-serious-about-privacy/2/

data"[2]. The need to ensure that individuals are informed when they exercise their right to control their data was recognized by the law's drafters and included in several provisions of the General Data Protection Regulation (GDPR).

2. GDPR PROVISIONS ON THE RIGHT TO BE INFORMED

2.1. Content of information notification to personal data subjects

2.1.1. List of InformationInformation that must be communicated to the personal data subject

Articles 13 and 14 of the General Data Protection Regulation (GDPR) represent the core of the right to be informed. These two provisions provide a detailed list of information that must be disclosed to the data subject as part of the individual's right to be informed and are divided into two cases: (i) when the data is obtained directly from the data subject; (ii) when the data is obtained from a third party. A typical example of the first case is collecting information from social media users. When the user registers for a service and the user's data is about to be processed, the data controller must provide the user with all the information listed in Article 13 of the General Data Protection Regulation (GDPR). To illustrate the second case, one can think of a recruitment manager in a large enterprise who tries to identify suitable candidates using information available on social media. In this second case, the applicant must also be informed about data processing – for example, in a job advertisement.

When the data is not collected directly from the data subject, both parties may be responsible for ensuring that the information reaches the recipient. The scope of information must be provided to the data subject differs between these two cases. Most obviously, only when the data is not collected from the data subject is there an obligation to describe data types such as address, gender, and behavioural data under Article 14.1(d) of the General Data Protection Regulation (GDPR). This is probably because, in such cases, the data subject does not have an overview of the control over the shared data. Describing the data types helps the data subject understand the nature and scope of the data processing; otherwise, the data may remain hidden. Furthermore, where data is not collected from the data subject but is instead collected from other sources, the data controller must provide information about the source of this data. And, if possible, whether the data comes from publicly accessible sources.

The original proposal for the General Data Protection Regulation (GDPR) drafted by the Commission did not distinguish between the two cases as Articles 13 and 14 of the General Data Protection Regulation (GDPR) do in the current version. Instead, it combined them into a single provision. While there are still some differences depending on whether the data is obtained from an individual or not [3], the idea behind this integrated provision is that the two cases are comparable and that the obligation to provide information should be considered comprehensively. The GDPR's information categories are so broad that this has two consequences. On the one hand, transmitting a lot of Information burdens individuals who have to navigate lengthy and confusing policies. On the other hand, data subjects should be able to access detailed and comprehensive information. This may be particularly important in the context of the digital economy, where people often have very limited knowledge of what actually happens to their data.

The categories of information under the General Data Protection Regulation (GDPR) are of particular interest because they have implications for protecting individuals in the digital economy. The selected elements relate to information on the legal basis for processing personal data, the storage of personal data, recipients of personal data and third parties, and the

[2]Case C-201/14 Bara.

[3] Commission (2012), Proposal for a Regulation of the European Parliament and of the Council on the protection of individuals about the processing of personal data and the free movement of such data (General Data Protection Regulation), page 25.

processing of personal data for other purposes. The provisions under Article 13 (2) (f) and Article 14 (2) (g) of the GDPR on InformationInformation relating to automated decision-making deserve special attention. They are analyzed in more detail under the section on automated decision-making.

2.1.2. InformationInformation on the legal basis for processing personal data

The General Data Protection Regulation (GDPR) ensures that the data subject is fully aware of the legal basis for data processing. In the GDPR, the communication of information about the legal basis is a mandatory provision under Article 13(1) (c) and Article 14(1) (c) of the General Data Protection Regulation (GDPR). The data controller must inform the data subject of any legal basis it uses, such as the data subject's consent, public interest or a contract between the controller and the data subject. Suppose the processing is based on the legitimate interests of the data controller. In that case, these interests must also be detailed and communicated to the data subject under Article 13(1) (d) and Article 14(2) (b) of the General Data Protection Regulation (GDPR). By receiving information about legitimate interests, data subjects are better informed about the controller's intentions and can more easily assess what is happening with their data. The InformationInformation provided under Article 13(1) (c) and Article 14(1) (c) of the General Data Protection Regulation (GDPR) must also reflect the results of the balancing test that controllers are obliged to carry out whenever legitimate interests are used as the basis for data processing. It must be demonstrated that controllers have balanced their commercial interests with the fundamental rights and interests of data subjects, ensuring that the protection of the fundamental rights of individuals is not put at risk. This is important because controllers often pursue commercial interests only in the case of secondary data use.

2.1.3. InformationInformation on personal data storage period

As a new category of Information, the General Data Protection Regulation (GDPR) requires data controllers to provide information on the period for which personal data is stored or, if this is not possible, the criteria used to determine that period by Article 13.2(a) and Article 14.2(a) of the General Data Protection Regulation (GDPR). This new category is consistent with the storage limitation principle set out in the GDPR[4]. In the digital economy, storing data locally on external hard drives is almost no longer feasible. Due to cost constraints, companies are increasingly using cloud storage solutions. This leads to the involvement of third parties in the data processing of this new type of data. Dropbox and Amazon Web Services are two cloud service providers widely known to many businesses. The processing of personal data must be adequate, relevant and limited to what is necessary for the purposes for which the data is processed[5]. In particular, this requires ensuring that the storage period of personal data is limited to a strict minimum[6]. This will reduce the risk of misuse or overuse because less data is likely to be misused in a shorter period. This requirement is particularly relevant because the illegal retention of Personal Information is one of the most contested online information practices[7]. Cloud storage providers do not leave users' data idle on their servers but often share it with third parties. Dropbox's privacy policy informs users that the company will not sell their data to advertisers or other third parties[8]. However, the policy also provides a long list of exceptions about competent state agencies, other users, trusted parties and other applications[9].

[4]Point e, paragraph 1, Article 5 of the General Data Protection Regulation (GDPR).
[5] Point e, Clause 1, Article 5 of the General Data Protection Regulation (GDPR).
[6]Paragraph 39 of the General Data Protection Regulation (GDPR)
[7] Joel Reidenberg and others (2015), Disagreeable Privacy Policies: Mismatches Between Meaning and Users' Understanding, Berkeley Technology Law Journal, page 56.
[8] Dropbox Privacy Policy https://www.dropbox.com/privacy
[9] Dropbox Privacy Policy https://www.dropbox.com/privacy

2.1.4. InformationInformation about the recipient of personal data

The disclosure and sharing of data to combine and reuse third-party data sources has become an inherent part of the digital economy. This leaves individuals often unaware of the data flow, and the reuse of data does not meet privacy expectations. Article 13(1) e and Article 14(1) e of the General Data Protection Regulation (GDPR) require controllers to provide InformationInformation on the categories of recipients of personal data. A recipient of personal data is a natural or legal person, a competent public authority to whom the personal data is disclosed, whether or not it is a third party. Competent public authorities that may receive personal data in the context of a specific investigation under European Union (EU) or Member State law shall not be recipients under Article 4(9) of the General Data Protection Regulation (GDPR). This means that user data has been shared with competent state agencies not provided under the right to be informed.

The obligation to inform data subjects that their personal data has been shared with competent state authorities does not apply. The safeguard clause is a statement on the public website that the service provider does not accept any requests for confidential data from competent state authorities. Once such a request has been made, the notice will be removed from the website[10]. Sometimes, the protection of public interest and national security requires absolute confidentiality, but greater transparency regarding data flows between competent state authorities and personal data subjects seems increasingly necessary. These data flows are everywhere, but they are often completely hidden. The proposal of the European Parliament's Committee on Civil Liberties, Justice and Home Affairs (LIBE) on the General Data Protection Regulation (GDPR) would require data subjects to be informed whether personal data has been provided to competent state authorities in the most recent 12-month period[11].

In contrast, the General Provisions of the General Data Protection Regulation (GDPR) can be a useful tool to achieve greater transparency in data flows without hindering law enforcement activities[12]. The requirement that information about the recipient is always provided to the data subject is a welcome improvement. However, in principle, the General Data Protection Regulation (GDPR) ceases to apply once data has been anonymized[13]. Therefore, when sharing anonymized data, the recipient is not disclosed[14].

2.1.5. InformationInformation on other purposes of processing personal data

Where the controller intends to further process personal data for a purpose other than that for which the data were collected, the controller must provide the data subject with information about that other purpose and any other relevant information prior to further processing[15]. In practice, this obligation means that if the controller subsequently processes personal data for a new purpose not stated in the initial notification, it must provide an updated notification of this new processing. This reflects the changes that have taken place in the digital economy in recent years. Data reuse and sharing are two of the main business strategies of data controllers. A

[10] What is a warrant canary? http://www.bbc.com/news/technology-35969735 .

[11] European Parliament, Committee on Civil Liberties, Justice and Home Affairs (LIBE)(2013), European Parliament, Report on the proposal for a regulation of the European Parliament and of the Council on the protection of individuals about the processing of personal data and the free movement of such data (General Data Protection Regulation)(COM(2012)0011 – C7-0025/2012 – 2012/0011(COD)), http://www.europarl.europa.eu/cmsdata/59696/att_20140306ATT80606-4492192886392847893.pdf

[12]See Facebook's privacy policy and their transparency report: https://transparency.facebook.com/government-data-requests

[13]Tene O and Polonetsky J (2013), Big Data for All: Privacy and User Control in the Age of Analytics, Northwestern Journal of Technology and Intellectual Property, pp. 5 7.

[14]Amanda Hess (2017). How Privacy Became a Commodity for the Rich and Powerful, https://www.nytimes.com/2017/05/09/magazine/how-privacy-became-a-commodity-for-the-rich-and-powerful.html

[15] Article 13.3 of the General Data Protection Regulation (GDPR).

typical example is social media platforms where user-provided data is exchanged with third parties, such as data brokers, for reuse for their specific purposes. Furthermore, user behaviour analytics can convert information about a person's shopping habits into information information about that person's health status.

Changes in the purpose of data processing often occur as part of a business process. Employers use social media data to pre-screen suitable candidates. This challenges the privacy expectations of social media users. Most people who share personal data on social media expect the data to be processed for the purpose of enabling online communications and are surprised when it is processed as part of a recruitment strategy. Without preliminary information about the intended purpose, it is difficult for any individual to determine what purpose-specific data is used. Communication of purpose is even more important as data reuse is increasingly done in the background. Purpose limitation is one of the core restrictions in the General Data Protection Regulation (GDPR). According to the purpose limitation principle, data cannot be reused unless the controller ensures a valid legal basis for such reuse, such as obtaining additional consent from the data subject. This is, of course, in contrast to big data businesses, which seek to profit from data reuse. Furthermore, the process can become lengthy and inefficient if the data controller has to notify the data subject each time the data is used for a new purpose.

2.1.6. InformationInformation about third-party data sources

Where data is obtained from a third party, the controller has an additional obligation to provide information about the sources of that third party and, where applicable, whether the data comes from publicly available sources under Article 14.2(f) of the General Data Protection Regulation (GDPR). In the digital economy, this provision seems appropriate as data collection is rarely limited to one source. For example, real-world data in the pharmaceutical industry is used to improve clinical trials with data collected from sources outside the traditional clinical setting. These sources may include large-scale simplex trials, pragmatic clinical trials, prospective observational or registries, retrospective database studies, case reports, administrative and health care claims, electronic health records, data collected as part of public health surveys or public health surveillance, and device, procedure or disease registries[16]. The unique combination of sources can contribute to better results in clinical trials and allow for more accurate analysis of drug effects.

Combining someone's social media profile with their clinical trial report can be much more in-depth and invasive of privacy. Combining data sources is also a trend in a number of other data-driven marketplaces. Facebook has admitted to regularly combining and enriching its own data with databases purchased from Acxiom[17]. Merging an individual’s social media profile data with information about that person’s health or ethnicity can be a valuable source of information for advertising companies that are Facebook's customers[18]. That’s why knowing the data sources is important to understanding the scope of data processing. However, section 61 of the General Data Protection Regulation (GDPR) stipulates that if it is not possible to provide the source of personal data to a data subject because of the use of multiple data sources, then only

[16] Food and Drug Administration (2017), Use of Real-World Evidence to Support Regulatory Decision-Making for Medical Devices Guidance for Industry and Food and Drug Administration Staff Document https://www.fda.gov/downloads/medicaldevices/deviceregulationandguidance/guidancedocuments/ucm513027.pdf

[17] Drew Harwell (2018). “ Facebook, a longtime friend of data brokers, becomes their stiffest competition ”, The Washington Post, https://www.washingtonpost.com/news/the-switch/wp/2018/03/29/facebook-longtime-friend-of-data-brokers-becomes-their-stiffest-competition/.

[18] Jim Edwards (2013). Facebook's Big Data Partner Knows Who You Are Even When You Use A Different Name On The Web, Business Insider, https://www.businessinsider.com/facebook-and-acxioms-big-data-partnership-2013-9

general information should be provided. Data provenance is understood as the data's history or description of where the data comes from, how the data is obtained, and how the data is updated over time[19]. One important reason to care about data provenance is to find the source of error. Therefore, controlling the integrity of the data is at the core of data provenance. The General Data Protection Regulation (GDPR) requirements for data provenance convey a similar idea. By transparently presenting the sources, there is a greater possibility of full control over the use of the data and the results of data analysis.

2.2 . Providing InformationInformation about automated decisions

According to Article 13, paragraph 2, point f and Article 14, paragraph 2, point g of the General Data Protection Regulation (GDPR), individuals have the right to be informed about automated decision-making. Where a data controller engages in automated decision-making, including profiling, which is based solely on automated processing and produces legal effects concerning the data subject or similarly significantly affects the data subject[20]. The data subject must be provided with appropriate information about the decision's logic, significance, and intended results. According to Article 12 of the Data Protection Directive (DPD), Information about the logic behind automated decisions is only provided if the data subject himself requests it through the right of access. The General Data Protection Regulation (GDPR) has preserved this provision and added information about automated decision-making to the standard information list. This new obligation to provide information is sometimes referred to as the right to explanation and can, therefore, function as a right to clarify complex algorithms and decisions derived from them[21].

In the context of the digital economy, the right to an explanation can indeed play an important role. Data-driven decisions are often hidden from public view, based on complex algorithms that are difficult to understand and have consequences that are not easily predictable[22]. Therefore, explanations tailored to the needs of data subjects seem to be desirable. The obligation to provide information about automated decisions is not limited to cases where notification to data subjects is mandatory; given the risks of automated decision-making, the obligation to provide information is broader. Automated decision-making, such as profiling, often leads to discrimination and bias due to deficiencies in the quality and quantity of data available to train and test algorithms, as well as issues with data sourcing and classification[23].

According to Article 13, paragraph 2, point f and Article 14, paragraph 2, point g of the General Data Protection Regulation (GDPR), the data subject will receive the following three types of InformationInformation: (i) Meaningful InformationInformation about the logic involved in the automated decision-making; (ii) Meaningful InformationInformation about the processing; (iii) Meaningful InformationInformation about the intended results of the processing. It will be difficult for software users to provide detailed answers as to why an individual has been selected to receive different treatment by an automated decision-making system. Therefore, it

[19] Sven Abels et al. (2017). WP4 Finalizing the model D4.4 Report on technological requirements and barriers, https://ec.europa.eu/research/participants/documents/downloadPublic?documentIds=080166e5b56d75c1&appId=PPGMS

[20] Article 13, Article 14, Article 22 of the General Data Protection Regulation (GDPR).

[21] Bryce Goodman & Seth Flaxman (2016). European Union Regulations on Algorithmic Decision-Making and A "right to
Explanation" http://arxiv.org/abs/1606.08813

[22]Cathy O'Neil (2016). Weapons of Math Destruction: How Big Data Increases Inequality and Threatens Democracy, Crown, page 102.

[23]Dimitra Kamarinou and others (2016), Machine Learning with Personal Data, Queen Mary School of Law Legal Studies Research, page 20.

is argued that: "*only unique algorithmic approaches among all methods encountered a lack of explanation.*"[24]

Edwards and Veale examined the computer science literature to determine what it means to explain an algorithm in a meaningful way by focusing on the subject and focusing on the system[25]. Focusing on the subject is limited to the space around a series of data, which is considered more meaningful mainly because it allows users to develop more effective and appropriate thinking methods[26]. Other solutions that can help communicate the logic of a system to individuals without going into technical details are the use of hypotheses and simple statements that indicate how external events can vary to reach the desired result[27]; and case-based approaches that provide explanations by retrieving the most similar cases from the computer's memory [28]. Finally, a useful explanation of the logic used to make a decision should also include an explanation of the type of data used to make the decision[29]. The second piece of information is meaning. The decision has objective and subjective implications. Subjective significance refers to individuals' perceptions of the impact of automated decisions[30].

In principle, data controllers tend to ignore the risks that are particularly relevant. Hildebrandt believes that this provision should be interpreted broadly[31]. According to Hildebrandt, unintended but conceivable effects due to the complete nature of the profiling process must also be approached and communicated[32]. In this regard, Hildebrandt points out the important connection between this requirement and the principle of determination of purpose: "*The principle of determination of purpose is restored as an important legal rule because the prediction of effects requires the prior identification of the intended effects*"[33]. Articles 13 and 14 of the General Data Protection Regulation (GDPR) seem to warrant a prior explanation but do not include an explanation of a specific, separate decision that will be provided after data processing[34]. This interpretation may affect the right of access in Article 15 and the right to object to a decision in Article 22 of the General Data Protection Regulation (GDPR)[35]. However, the right to be informed about automated decision-making is considered an important new feature of the General Data Protection Regulation (GDPR). First, the provision has become an integral part of the information category, which increases the likelihood that data subjects will be confronted with it. Second, if interpreted positively, the provision could help establish a more responsible and transparent system of data processing by data controllers.

---

[24]PJG Lisboa (2013). Fuzzy Logic and Applications, Springer International Publishing, page 132.

[25]Lilian Edwards & Michael Veale (2017). Slave to the Algorithm? Why a "right to an Explanation" Is Probably Not the Remedy You Are Looking for, Duke Law and Technology Review, page 30.

[26]Lilian Edwards & Michael Veale (2017). Slave to the Algorithm? Why a "right to an Explanation" Is Probably Not the Remedy You Are Looking for, Duke Law and Technology Review, page 30.

[27]Sandra Wachter, Brent Mittelstadt & Chris Russell (2018). Counterfactual Explanations Without Opening the Black Box:
Automated Decisions and the GDPR, Harvard Journal of Law & Technology, page 44.

[28]Dónal Doyle, Alexey Tsymbal, Pádraig Cunningham, A Review of Explanation and Explanation in CaseBased Reasoning,
https://scss.tcd.ie/publications/tech-reports/reports.03/TCD-CS-2003-41.pdf

[29]Edwards L and Veale M (2017), Slave to the Algorithm? Why a "right to an Explanation" Is Probably Not the Remedy You Are Looking for, Duke Law and Technology Review, page 42.

[30]Lee A Bygrave (2001). Minding the Machine: Article 15 of the EC Data Protection Directive and Automated Profiling, Computer Law & Security Report, page 25.

[31]Mireille Hildebrandt (2012). Digital Enlightenment Yearbook (2012). IOS Press, page 51

[32] Mireille Hildebrandt (2012). Digital Enlightenment Yearbook (2012). IOS Press, page 53

[33]Mireille Hildebrandt (2012). Digital Enlightenment Yearbook (2012). IOS Press, page 53

[34] Wachter S, Mittelstadt B and Floridi L (2017). Why a Right to Explanation of Automated Decision-Making Does Not Exist in the General Data Protection Regulation, International Data Privacy Law, page 5

[35]Edwards L & Veale M (2017). Slave to the Algorithm? Why a "right to an Explanation" Is Probably Not the Remedy You Are Looking for, Duke Law and Technology Review, page 35.

2.2.1. Information should be concise, transparent, understandable and accessible, using clear and easy-to-understand language.

Article 12 of the General Data Protection Regulation (GDPR) sets out requirements relating to transparency and means of facilitating the rights of individuals. Article 12(1) of the General Data Protection Regulation (GDPR) sets out a number of distinct attributes of the information communicated by requiring the data controller to provide such information "*in a concise, transparent, understandable and accessible form, using clear and easy-to-understand language, in particular for any information specifically addressed to children".* Compared to the Data Protection Directive (DPD), this provision of the General Data Protection Regulation (GDPR) explicitly requires the data controller to adopt a more transparent, user-friendly and open approach. Two requirements stem from the first paragraph of Article 12 of the General Data Protection Regulation (GDPR). The first requirement concerns the quality of the information provided in the form. Information must be concise, clear, understandable and accessible. The second requirement concerns language that must be clear and understandable. Concise means that information is presented clearly and in a few short but complete words, conveying information concisely, without unnecessary words and with the right level of detail[36]. The end result is clearer and more engaging text for readers[37]. For example, after being scrutinized by European data protection authorities, Google's privacy policy was expanded. However, the information is no longer provided in a single paragraph but is structured into multiple paragraphs and bullet points for ease of reading. By using this hierarchical format, the information information has become more concise.

Exercising the right to be informed of quality information Sometimes, we need to consider what format the information will be most easily understood by a particular group of people. There are two distinct situations where appropriate provision of information is important: (i) where the proliferation of subjects and the technological complexity of practices make it difficult for data subjects to know and understand whether personal data relating to them are being collected, by whom and for what purposes, such as in the case of online behavioural advertising; (ii) where the processing of data concerns children under paragraph 58 of the General Data Protection Regulation (GDPR)[38]. In the digital economy, explaining algorithmic decision-making requires a different level of detail and simplification than providing contact information for a data protection officer[39].

Article 12 of the General Data Protection Regulation (GDPR) stipulates that information should be provided electronically where appropriate. An example of such information provision is through websites and mobile applications. The application of a technology can work to the advantage or disadvantage of the user requesting to be informed. On the one hand, application developers are often in the best position to provide notice and disclosure due to their proximity to the end user[40]. On the other hand, a lack of understanding of privacy rules, the inherent limitations of current mobile architectures, and the reliance on third parties can

[36] Mark Osbeck (2012). What is "Good Legal Writing" and Why Does It Matter?, Drexel Law Review, p. 38.
[37] Mark Osbeck (2012), What is "Good Legal Writing" and Why Does It Matter?, Drexel Law Review, p. 38.
[38]Paragraph 58 of the General Data Protection Regulation (GDPR).
[39] Point b, Clause 1, Article 13 of the General Data Protection Regulation (GDPR).
[40]Future of Privacy Forum and The Center for Democracy & Technology (2011), Best Practices for Mobile Application Developers https://www.cdt.org/wp-content/uploads/pdfs/Best-Practices-Mobile-App-Developers.pdf

undermine these good hopes[41]. An uncontrollable system is a system that should not be used. Therefore, accessible information is as important as the information itself[42].

The General Data Protection Regulation (GDPR) recognizes the interest of companies in keeping information about their internal decision-making processes confidential if disclosure adversely affects trade secrets, patents or copyrights[43]. The reason for this provision is that forcing companies to disclose algorithms may conflict with trade secrets[44]. Furthermore, controllers are not transparent about whom they share information with. It is clear that Facebook users' data is shared with third-party applications every day, but only a small number of users are aware that their information is being transferred around the world[45]. Second, transparency can be threatened by the structure of modern data processing systems, which sometimes do not allow for meaningful explanations of their functionality. For example, some types of analytics, such as machine learning, can yield novel, unexpected results that cannot be explained to data subjects in advance because they evolve gradually, learning from past decisions and thus becoming largely unpredictable[46].

2.2.2. Information must be provided in writing or other electronic means.

Regarding the form used to communicate information requested by data subjects, the General Data Protection Regulation (GDPR) provides only minimal suggestions. Form means the way something is organized, presented and structured. In terms of format, the General Data Protection Regulation (GDPR) mentions a number of options, such as information being provided in writing or by other means and by electronic means where appropriate[47]. With an increasing amount of data being processed online, electronic forms should be preferred. An example of an electronic form that the GDPR explicitly mentions is via a website under Section 58 of the GDPR. An alternative is to provide information via a mobile application. In terms of format, information information is usually communicated as a privacy policy or as part of the general terms and conditions[48].

2.3.Information about the privacy policy

Privacy policies are internally focused tools that outline a company's policy regarding the use of personal data and how the company intends to achieve compliance with privacy principles[49]. Today, the majority of companies in Europe have privacy policies[50]. Although there is no explicit legal obligation for a company website to publish a policy, having a policy is often the only viable way to meet a company's information obligations to website users[51]. This increased transparency is also required under industry self-regulation as companies increasingly

[41]Future of Privacy Forum and The Center for Democracy & Technology (2011), Best Practices for Mobile Application Developers https://www.cdt.org/wp-content/uploads/pdfs/Best-Practices-Mobile-App-Developers.pdf

[42] Matt Kusner et al. (2017). Counterfactual Fairness, NIPS, p. 17.

[43]Section 63 of the General Data Protection Regulation (GDPR).

[44]Katja De Vries, Sari Depreeuw and Mireille Hildebrandt (2015), D3.2 Profile Transparency, Trade Secrets and Intellectual
Property Rights in OSNs – v1, USEMP, page 9.

[45]Transcript of Mark Zuckerberg's testimony before the US Congress on April 10, 2018
https://www.washingtonpost.com/news/the-switch/wp/2018/04/10/transcript-of-mark-zuckerbergs-senate-hearing/

[46]J.A. Kroll et al. (2016). Accountable Algorithms, University of Pennsylvania Law Review, p. 38.

[47] Article 12.1 General Data Protection Regulation (GDPR)

[48]Kosta E (2013). Consent in European Data Protection Law, Nijhoff, page 10.

[49]Neil Robinson and others (2009), Review of the European Data Protection Directive, https://www.rand.org/pubs/technical_reports/TR710.html.

[50]ARA Bouguettaya and MY Eltoweissy (2003), Privacy on the Web: Facts, Challenges, and Solutions, IEEE Security and Privacy Magazine, page 40.

[51] Kuner C (2012). European Data Protection Law: Corporate Compliance and Regulation, Oxford University Press, page 83.

acknowledge consumers' need for information information[52]. In the wake of the General Data Protection Regulation (GDPR), many data-centric companies have made a notable move to update the language and format of their privacy policies. Policies are a key source of information for data subjects, particularly in helping them decide whether to consent to data processing[53].

If consent no longer makes sense for the data subject's right to control, then so does the right to be informed associated with consent. It is, therefore, not surprising that privacy policies as a form of communication have received criticism[54]. Several solutions have been considered to address these shortcomings, and one of them has been implemented in the General Data Protection Regulation (GDPR). These solutions do not set a new standard but rather provide an alternative to traditional privacy policies. The first is the use of information symbols and titles as a means to more effectively communicate privacy policies. In Article 12 of the GDPR, controllers are given the option to use information symbols as an alternative to written policies. The second solution is the use of standard contracts in the relationship between companies and consumers. These policies were part of some previous versions of the General Data Protection Regulation (GDPR) but do not appear in the final text of the General Data Protection Regulation (GDPR).

2.3.1. Other symbols and images

Icons are symbolic or graphic representations of privacy policies that convey information quickly. They can, therefore, be a viable solution to the drawbacks of privacy policies in the digital economy, which are often too long and too complex to provide meaningful information. Icons can be beneficial because they simplify the understanding of InformationInformation and save time for readers. Article 12, paragraph 7 of the General Data Protection Regulation (GDPR) provides for the option of using standardized icons. Paragraph 58 of the General Data Protection Regulation (GDPR) adds that visualizations should be used where appropriate. Symbols provide an alternative approach aimed at making the privacy policy more accessible to users. The information required by articles 13 and 14 of the GDPR may be provided in conjunction with standardized symbols to provide a meaningful overview of the intended processing in a visible, understandable and legible manner; the symbols may be presented in electronic form, which must be machine-readable.

European Union (EU) legislation is not the only source that companies can use to make their policies more user-friendly. Visualization has also been proposed as a possible way to incorporate information about automated decision-making into privacy policies[55]. A similar approach is to embed privacy policies in videos[56]. Finally, data protection information can also be provided in more creative ways. For example, presenting the policy as a kind of key information label in a standardized table format to let users know where to find the information in a consistent location and facilitate comparison between policies[57]. Or using a policy compressed into a graphical representation of a data flow built on AI text analysis. Visualization can help some consumers better understand complex data flows. Cranor's study found that in

[52] Kuner C (2012). European Data Protection Law: Corporate Compliance and Regulation, Oxford University Press, page 83.

[53]Kosta E (2013). Consent in European Data Protection Law, Nijhoff, page 15.

[54] Lilian Edwards and Wiebke Abel (2014). The Use of Privacy Icons and Standard Contract Terms for Generating Consumer Trust and Confidence in Digital Services Authors https://zenodo.org/record/12506/files/CREATe-Working-Paper-2014-15.pdf

[55]Edwards L and Veale M (2017), Slave to the Algorithm? Why a "right to an Explanation" Is Probably Not the Remedy You Are Looking for, Duke Law and Technology Review, page 21.

[56]The Guardian Privacy Policy https://www.theguardian.com/info/video/2014/sep/08/guardian-privacy-policy

[57]Lorrie Faith Cranor (2011), Necessary but Not Sufficient: Standardized Mechanisms for Privacy Notice and Choice, Journal on Telecommunication & High Technology Law, page 88.

conditions without a privacy information symbol, most participants purchased from the least expensive websites. However, in the condition with the privacy instructions, a large number of participants paid more to purchase items from more privacy-protecting websites[58].

In addressing the problems of information overload, lack of time and attention for privacy-related information, and lack of digital literacy, information icons and similar simplification methods can play an important role. Information icons are beneficial for two reasons. First, they significantly reduce the information overload that consumers face in the online environment. Closely related to this, they reduce the complexity of information. Therefore, consumers need less time and attention to grasp the implications of the disclosure of their personal data. The downside is that information icons do not provide comprehensive knowledge about data collection activities but rather provide information in a highly generalized and simplified way. By using trustworthy standardized language, consumers can be less affected by the fact that they only receive partial information. However, in the digital economy, it is the hidden and invisible information that is more meaningful than some general information[59].

2.3.2. Standardized security policy

A standardized managed privacy policy has been recommended as an effective means of ensuring that consumers are adequately protected against unfair supplier terms in the industry[60]. The management of standard contracts is an approach that has similar results to the information symbol in reducing policy complexity, shortening the time required to review terms and giving consumers control. Cranor believes that the digital environment can be a good enabler for standardization as machine-readable policies allow for greater standardization and better comparability[61]. In fact, open-source software already exists to support the comparison and evaluation of privacy policies[62].

However, it cannot be ruled out that envisioned or standardized security policies may suffer from the same disadvantages as non-standardized policies since they may become too general and leave out some important details[63], or they may become too detailed and impossible to follow [64]. More importantly, to be effective, standardized notices need to have fairly stringent requirements so that their elements are directly comparable[65]. Ideally, it is standardized by international treaty or standards-setting bodies such as ISO[66].

2.3.3. InformationInformation is summarized in the standard terms and conditions

A privacy policy is the most common approach to informing data subjects but is not required under the General Data Protection Regulation (GDPR). Instead of a privacy policy, some companies may choose to provide information about the processing of personal data under their standardized terms and conditions. Standardized terms and conditions are contracts between

[58]Lorrie Faith Cranor (2011). Necessary but Not Sufficient: Standardized Mechanisms for Privacy Notice and Choice, Journal on Telecommunication & High Technology Law, page 92.

[59]Helen Nissenbaum (2011). A Contextual Approach to Privacy Online, Daedalus, the Journal of the American Academy of Arts & Sciences, page 36

[60]Edwards L & Abel W (2014). The Use of Privacy Icons and Standard Contract Terms for Generating Consumer Trust and Confidence in Digital Services Authors, CREATe Working Paper 2014/15, page 21.

[61]Lorrie Faith Cranor (2011). Necessary but Not Sufficient: Standardized Mechanisms for Privacy Notice and Choice, Journal on Telecommunication & High Technology Law, page 93.

[62] Privacy Policy Comparison Sites https://tosdr.org

[63] Hintze M (2015). In Defense of the Long Privacy Statement, Maryland Law Review, page 51.

[64]Omri Ben-Shahar and Carl Schneider (2014), More than You Wanted to Know: The Failure of Mandated Disclosure, Princeton University Press, p. 17.

[65] Lorrie Faith Cranor (2011). Necessary but Not Sufficient: Standardized Mechanisms for Privacy Notice and Choice, Journal on Telecommunication & High Technology Law, page 30.

[66]Edwards L & Abel W (2014). The Use of Privacy Icons and Standard Contract Terms for Generating Consumer Trust and Confidence in Digital Services Authors, CREATe Working Paper 2014/15, page 4.

two parties, where the terms and conditions of that contract are set by one party, and the other party has little or no ability to negotiate more favourable terms and is therefore placed in a position to accept or reject them. In principle, a privacy policy is provided as part of a contract and should, therefore, not be considered uncommon. Where consent is the basis for fair and lawful processing, it is easy to incorporate any data protection practices into the contract and legitimize them through acceptance of the contract[67].

However, even in the presence of a privacy policy, contractual terms can still be an important source of information for data subjects because they may indirectly relate to the subject's privacy. For example, X's Application Programming Interface (API)[68] allows developers to use X's data streams[69]. Data subjects can only fully understand the risks of processing personal data by receiving information about the developer's possible reuse of the data. In some cases, such as deleting short posts on X containing personal data, this is not absolute because the data has been shared with developers[70]. By combining the privacy policy and contractual terms, data subjects can see a more complete picture.

3. POLICY RECOMMENDATIONS FOR VIETNAM

Factors such as psychology, technology, and economics undermine the effectiveness of the rights of personal data subjects, increasing the possibility that data subjects will not be able to control the flow of information. These factors also have an impact on the right to be informed. Barriers to effective information provision stem from individual psychological patterns, the specific characteristics of data-based technologies and the digital economic environment. Westin argues that effective control includes mechanisms that help individuals understand where their personal information may flow and in what context it may flow[71]. Vietnamese personal data protection legislation related to the right to be informed should pursue both goals. To understand where data is going, the controller must communicate detailed information about the recipients of the data, international transfers of data, and storage of data. To understand the context in which data flows, Vietnamese data protection law must provide Internet users with the legal basis and purpose of data processing. In the past, understanding data flows may have been sufficient to achieve effective control. However, in today's complex and mysterious digital economy, control will also be more difficult. To address this issue, the Vietnamese data protection law needs to introduce a number of new provisions to strengthen the control of data subjects in the digital economy. These new mechanisms include the right to an explanation and information symbols. According to the experience of the European Union (EU), the right to an explanation seems to have been included in the General Data Protection Regulation (GDPR) to address the problem of incomprehensibility of data-based decisions. The technical complexity of algorithmic decisions often makes it impossible to explain exactly how data is used. In the General Data Protection Regulation (GDPR), the new right to explanation is reinforced by a number of other relatively new overarching provisions on accountability, fairness and transparency, and privacy impact assessment requirements. Liisa Jaakonsaari suggests that " *a common framework for algorithmic accountability and transparency"* could be the next step in achieving these goals without raising unrealistic

[67]Edwards L & Abel W (2014). The Use of Privacy Icons and Standard Contract Terms for Generating Consumer Trust and Confidence in Digital Services Authors, CREATe Working Paper 2014/15, page 6.
[68] API stands for programming interface application.
[69]X Developer Agreement https://developer.x.com/en/developer-terms/agreement
[70] Helena Ursic (2016), The Right to Be Forgotten or the Duty to Be Remembered? Twitter Data Reuse and Implications for Users Privacy, https://bdes.datasociety.net/wp-content/uploads/2016/10/Ursic-politiwoops.pdf
[71]Westin AF (2015). Privacy and Freedom, Ig Publishing, page 50.

expectations about the right to be informed in the General Data Protection Regulation (GDPR)[72].

Infomarks can be seen as another enabler in the sense that they provide an additional option for consumers who prefer visual representations, and they replace complex privacy policies with a series of simple images. The inclusion of info marks and some related mechanisms in the General Data Protection Regulation (GDPR) suggests a closer connection between data protection and consumer protection. Indeed, the convergence of personal data law and consumer law is increasingly discussed as a benefit to data subjects. After all, the failure of a controller to fulfil its information obligations may have adverse legal consequences arising from both contractual and consumer law[73]. Information about the legal basis for data processing, third parties involved in the data processing, sources of personal data and information about the purposes of data processing are the most relevant information provided to the data subject regarding the data processing.

Vietnamese laws on personal data protection need to expand the scope of information categories available to data subjects and pay more attention to the user-friendly design of the information presentation. In particular, the right to explanation and information symbols seem to offer a new, promising option for greater control over modern data flows. In the digital economy, psychological, technological and economic factors seem to have a negative impact on the ability of data subjects to control the flow of information.

Therefore, Vietnamese law on personal data protection needs to have a thorough impact on the right to be informed. Legal provisions need to ensure the right to be informed not only for data subjects but also establish transparency for the entire digital economy, including competitors, civil society and state management agencies. Vietnamese law on personal data protection needs to have specific provisions for acts of providing inappropriate information. Finally, the right to be informed is not a separate right but part of a broader and comprehensive data protection mechanism under Vietnamese law. This mechanism must ensure that it creates conditions for meaningful control of an individual's data and must be one of the most detailed and comprehensive data protection mechanisms to suit the digital economy.

REFERENCES

[1] Amanda Hess (2017). How Privacy Became a Commodity for the Rich and Powerful, https://www.nytimes.com/2017/05/09/magazine/how-privacy-became-a-commodity-for-the-rich-and-powerful.html

[2] ARA Bouguettaya and MY Eltoweissy (2003), Privacy on the Web: Facts, Challenges, and Solutions, IEEE Security and Privacy Magazine, page 40.

[3] Bryce Goodman & Seth Flaxman (2016). European Union Regulations on Algorithmic Decision-Making and A "right to Explanation" http://arxiv.org/abs/1606.08813

[4] Cathy O'Neil (2016). Weapons of Math Destruction: How Big Data Increases Inequality and Threatens Democracy, Crown, page 102.

[5] Cyrus Farivar (2012). How one law student is making Facebook get serious about privacy, https://arstechnica.com/tech-policy/2012/11/how-one-law-student-is-making-facebook-get-serious-about-privacy/2/

[6] Commission (2012), Proposal for a Regulation of the European Parliament and of the Council on the protection of individuals about the processing of personal data and the free movement of such data (General Data Protection Regulation), page 25.

[72]Lisa Jaakonsaari (2016). Who sets the agenda on algorithmic accountability? https://www.euractiv.com/section/digital/opinion/who-sets-the-agenda-on-algorithmic-accountability/ .

[73] Kuner (2012), European Data Protection Law: Corporate Compliance and Regulation, Oxford University Press, page 86.

[7] Drew Harwell (2018). " Facebook, a longtime friend of data brokers, becomes their stiffest competition ", The Washington Post, https://www.washingtonpost.com/news/the-switch/wp/2018/03/29/facebook-longtime-friend-of-data-brokers-becomes-their-stiffest-competition/.
[8] Dimitra Kamarinou and others (2016), Machine Learning with Personal Data, Queen Mary School of Law Legal Studies Research, page 20.
[9] Dónal Doyle, Alexey Tsymbal, Pádraig Cunningham, A Review of Explanation and Explanation in CaseBased Reasoning, https://scss.tcd.ie/publications/tech-reports/reports.03/TCD-CS-2003-41.pdf
[10] European Parliament, Committee on Civil Liberties, Justice and Home Affairs (LIBE)(2013), European Parliament, Report on the proposal for a regulation of the European Parliament and of the Council on the protection of individuals about the processing of personal data and the free movement of such data (General Data Protection Regulation)(COM(2012)0011 – C7-0025/2012 – 2012/0011(COD)), http://www.europarl.europa.eu/cmsdata/59696/att_20140306ATT80606-4492192886392847893.pdf
[11] Edwards L and Veale M (2017), Slave to the Algorithm? Why a "right to an Explanation" Is Probably Not the Remedy You Are Looking for, Duke Law and Technology Review, page 42.
[12] Food and Drug Administration (2017), Use of Real-World Evidence to Support Regulatory Decision-Making for Medical Devices Guidance for Industry and Food and Drug Administration Staff Document https://www.fda.gov/downloads/medicaldevices/deviceregulationandguidance/guidancedocuments/ucm513027.pdf
[13] Future of Privacy Forum and The Center for Democracy & Technology (2011), Best Practices for Mobile Application Developers https://www.cdt.org/wp-content/uploads/pdfs/Best-Practices-Mobile-App-Developers.pdf
[14] Helen Nissenbaum (2011). A Contextual Approach to Privacy Online, Daedalus, the Journal of the American Academy of Arts & Sciences, page 36.
[15] Helena Ursic (2016), The Right to Be Forgotten or the Duty to Be Remembered? Twitter Data Reuse and Implications for Users Privacy, https://bdes.datasociety.net/wp-content/uploads/2016/10/Ursic-politiwoops.pdf.
[16] Hintze M (2015). In Defense of the Long Privacy Statement, Maryland Law Review, page 51.
[17] J.A. Kroll et al. (2016). Accountable Algorithms, University of Pennsylvania Law Review, p. 38.
[18] Joel Reidenberg and others (2015), Disagreeable Privacy Policies: Mismatches Between Meaning and Users' Understanding, Berkeley Technology Law Journal, page 56.
[19] Jim Edwards (2013). Facebook's Big Data Partner Knows Who You Are Even When You Use A Different Name On The Web, Business Insider, https://www.businessinsider.com/facebook-and-acxioms-big-data-partnership-2013-9
[20] Katja De Vries, Sari Depreeuw and Mireille Hildebrandt (2015), D3.2 Profile Transparency, Trade Secrets and Intellectual Property Rights in OSNs – v1, USEMP.
[21] Kuner C (2012). European Data Protection Law: Corporate Compliance and Regulation, Oxford University Press, page 83.
[22] Kosta E (2013). Consent in European Data Protection Law, Nijhoff, page 10.
[23] Lilian Edwards & Michael Veale (2017). Slave to the Algorithm? Why a "right to an Explanation" Is Probably Not the Remedy You Are Looking for, Duke Law and Technology Review, page 30.

[24] Lilian Edwards and Wiebke Abel (2014). The Use of Privacy Icons and Standard Contract Terms for Generating Consumer Trust and Confidence in Digital Services Authors https://zenodo.org/record/12506/files/CREATe-Working-Paper-2014-15.pdf
[25] Lorrie Faith Cranor (2011), Necessary but Not Sufficient: Standardized Mechanisms for Privacy Notice and Choice, Journal on Telecommunication & High Technology Law, page 88.
[26] Lisa Jaakonsaari (2016). Who sets the agenda on algorithmic accountability?
[27] https://www.euractiv.com/section/digital/opinion/who-sets-the-agenda-on-algorithmic-accountability/ .
[28] Lee A Bygrave (2001). Minding the Machine: Article 15 of the EC Data Protection Directive and Automated Profiling, Computer Law & Security Report, page 25.
[29] Mireille Hildebrandt (2012). Digital Enlightenment Yearbook (2012). IOS Press, page 51
[30] Mark Osbeck (2012), What is "Good Legal Writing" and Why Does It Matter?, Drexel Law Review, p. 38.
[31] Matt Kusner et al. (2017). Counterfactual Fairness, NIPS, p. 17.
[32] Neil Robinson and others (2009), Review of the European Data Protection Directive, https://www.rand.org/pubs/technical_reports/TR710.html.
[33] Omri Ben-Shahar and Carl Schneider (2014), More than You Wanted to Know: The Failure of Mandated Disclosure, Princeton University Press, p. 17.
[34] PJG Lisboa (2013). Fuzzy Logic and Applications, Springer International Publishing, page 132.
[35] Tene O and Polonetsky J (2013), Big Data for All: Privacy and User Control in the Age of Analytics, Northwestern Journal of Technology and Intellectual Property, pp. 5 7.
[36] Sandra Wachter, Brent Mittelstadt & Chris Russell (2018). Counterfactual Explanations Without Opening the Black Box.
[37] Sven Abels et al. (2017). WP4 Finalizing the model D4.4 Report on technological requirements and barriers, https://ec.europa.eu/research/participants/documents/downloadPublic?documentIds=080166e5b56d75c1&appId=PPGMS
[38] Westin AF (2015). Privacy and Freedom, Ig Publishing, page 50.
[39] Wachter S, Mittelstadt B and Floridi L (2017). Why a Right to Explanation of Automated Decision-Making Does Not Exist in the General Data Protection Regulation, International Data Privacy Law,.