FROM AWARENESS TO LITERACY: KNOWLEDGE ORIENTATION IN THE REGULATORY ENVIRONMENT OF THE GDPR AND THE AI ACT

Dr. Tamás Sándor Török
Doctorate student, Doctoral Shool of Law, University of Pécs (Hungary)
Corresponding address: tamas.drtorok@gmail.com
ORCID: 0009-0006-1065-1730

DOI: 10.47272/KIKPhD.2025.3.1

ABSTRACT

The comparative analysis of the General Data Protection Regulation and the Artificial Intelligence Act has become one of the most prominent topics in contemporary legal scholarship. This is due to several reasons, one of the most important being that the impact of both instruments extends far beyond the European Union, allowing them to function as de facto global standards. At the same time, both legislative texts are products of the digital age, and consequently their interpretation and the demonstration of compliant behaviour require specific competencies and prior knowledge.

This study analyses the concept of "AI literacy" as defined in the Artificial Intelligence Act, drawing on the notion of "data protection awareness" under the General Data Protection Regulation and on empirical findings from available research data, with a view to mapping potential risks and challenges. Digital literacy, awareness, and literacy more broadly are concepts without which compliant behaviour in the field of technology regulation cannot realistically be expected. Accordingly, experience gained under the GDPR provides important lessons for the development of AI literacy as well.

KEYWORDS

GDPR awareness, AI literacy, AI Act, GDPR, digital literacy, data subject

ARTICLE HISTORY

SUBMITTED 14 Nov 2025 | REVISED 21 Nov 2025 | ACCEPTED 1 Dec 2025

I. Introduction and Working Hypothesis

It is characteristic of technology regulation that it seeks to govern an environment which is subject to constant and dynamic change and which, at the same time, demands a high level of prior knowledge from both legal practitioners and other legal and natural persons. In order to anticipate the expected impact and effectiveness of such regulation, it is therefore necessary to understand and assess the relevant competencies of those persons subject to it, as their knowledge and skills directly influence regulatory effectiveness.

In the case of more recent European Union regulatory instruments, a knowledge-oriented approach can be observed alongside the now familiar risk-based approach, at least as regards data protection law and the emerging regulation of artificial intelligence.

The present study seeks to answer how the concepts of data protection awareness and artificial intelligence literacy relate to one another, how and from which perspectives they can be interpreted, and, in light of their different temporalities, which conclusions and lessons can be drawn from the practical experiences with data protection awareness for the regulation of artificial intelligence and, by extension, for future technology regulation more generally.

Regulation (EU) 2024/1689 of the European Parliament and of the Council of 13 June 2024 on artificial intelligence (hereinafter: Artificial Intelligence Act or AIA) aims to provide relevant responses to several key risks brought to the fore by AI technologies.[1] A central element of this regulatory strategy is the introduction of the concept of AI literacy and its elaboration as a normative category.

It is important to note, however, that the interpretation of "literacy" ipso facto extends beyond the boundaries of legal scholarship. Its definition necessarily involves, in addition to the analysis of the addressees of the regulation, questions of measurability and evaluability of outputs. This in turn requires drawing on other social sciences and, where appropriate, on pedagogical research in order to arrive at adequate conclusions.

The examination of AI literacy inevitably presupposes an analysis of the practical experiences accumulated in relation to "data protection awareness" under the General Data Protection Regulation. Data protection awareness, similarly to AI literacy, seeks to promote the preparedness of the "receiving side", and the research results generated in the seven years following the applicability of 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, repealing Directive 95/46/EC (hereinafter: GDPR

[1] Regulation (EU) 2024/1689 of the European Parliament and of the Council of 13 June 2024 on artificial intelligence, OJ L 2024/1689.

or General Data Protection Regulation), may thus provide relevant initial lessons for the AIA.[2]

The study therefore addresses the following central questions: what is the precise normative content of the concepts of data protection awareness and AI literacy, and which addressee groups do they burden with what types of responsibilities? The working hypothesis is that the foundations of data protection awareness and AI literacy can be aligned conceptually, and that legislative and practical experiences generated under the GDPR are consequently worth considering and, where appropriate, adapting in the context of the AIA as well.

II. Framework of Data Protection Awareness

1. Complexity of Data Protection Awareness

The General Data Protection Regulation has undoubtedly brought about far-reaching changes in the protection of personal data worldwide. In adopting the GDPR, the European Commission sought to achieve several declarative objectives, including increasing transparency for data subjects regarding the processing of their personal data, enhancing individuals' control over their own data, and promoting data protection awareness.[3]

In its Communication entitled "Data protection rules as a trust-enabler in the EU and beyond -- taking stock", the Commission characterised the EU data protection legal framework as "a cornerstone of the European, human-centric approach to innovation".[4] In the same document, the Commission acknowledged that, although individuals are increasingly aware of their rights and are exercising them more frequently, additional efforts are required in order to further raise awareness.

It is important to emphasise, however, that data protection awareness is a highly complex concept which is not defined in the normative text of the GDPR. As a result, several possible approaches exist for understanding its meaning. The GDPR explicitly assigns obligations related to data protection awareness to two actors: the data protection officer and the supervisory authorities.

The tasks of the data protection officer include ensuring "awareness-raising and training of staff involved in processing operations".[5] As regards supervisory authorities, the legislative text is more detailed. Recital 132 already states

[2] 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, repealing Directive 95/46/EC, OJ L 2016/679.

[3] European Commission, *Communication from the Commission to the European Parliament and the Council: Data protection rules as a trust-enabler in the EU and beyond -- taking stock* (2019) https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:52019DC0374.

[4] Ibid.

[5] Regulation (EU) 2016/679, art 39(1)(b).

that "[a]wareness-raising activities by supervisory authorities addressed to the public should include specific measures directed at controllers and processors, including micro, small and medium-sized enterprises, as well as natural persons, in particular in the educational context".[6] In addition, the GDPR entrusts supervisory authorities with the task of educating the public by requiring them, in the framework of promoting "public awareness and understanding of the risks, rules, safeguards and rights in relation to processing", to inform not only controllers and processors but also natural persons.[7] Furthermore, supervisory authorities are obliged to draw the attention of controllers and processors to their obligations under the Regulation.

It is equally striking that the GDPR does not formulate explicit expectations with regard to awareness on the part of data subjects, nor does it set out any behavioural expectations in respect of data processing. Only Recital 47 refers to "the reasonable expectations of data subjects" as a benchmark in the context of legitimate interest.[8]

Data protection awareness is multi-component. One of its cornerstones is the concept of privacy itself, for which there is no single, universally accepted definition. From the perspective of the present study, only two approaches will be highlighted here. Paul A. Pavlou defines privacy as an individual's right to determine what personal information to share with others and under which circumstances.[9] Data or information confidentiality forms an integral part of privacy protection and, according to Luciano Floridi, "functions as a shield of personal identity".[10]

Understanding the position of natural persons -- or data subjects, in the terminology of the GDPR -- is a prerequisite for answering the research questions. While Article 8 of the Charter of Fundamental Rights of the European Union provides fundamental rights protection for personal data, there is no comparable, clearly articulated fundamental rights framework underpinning the AIA.[11]

Despite this difference in fundamental rights orientation, or precisely because of it, the protection of natural persons remains of crucial importance, as it provides the basis for the practical implementation of all subsequent provisions.

As a starting point, it is worth accepting that every individual is vulnerable. However, the degree and nature of individual vulnerability differ and depend on social contexts and relational structures.[12] According to Florencia Luna, the intensity

[6] Ibid, Recital 132.
[7] Ibid, art 57(1).
[8] Ibid, Recital 47.
[9] Paul A Pavlou, 'Consumer Acceptance of Electronic Commerce: Integrating Trust and Risk with the Technology Acceptance Model' (2003) 7(3) *International Journal of Electronic Commerce* 101. https://doi.org/10.1080/10864415.2003.11044275
[10] Luciano Floridi, 'The Ontological Interpretation of Informational Privacy' (2005) 7(4) *Ethics and Information Technology* 129. https://doi.org/10.1007/s10676-006-0001-7
[11] See Regulation (EU) 2024/1689, Preamble (recitals 1-79) and arts 1-71, which do not contain an explicit fundamental rights framework comparable to that in the GDPR.
[12] Gianclaudio Malgieri and Jedrzej Niklas, 'Vulnerable data subjects' (2020) 37(1) *Computer Law & Security Review* 105482. https://doi.org/10.1016/j.clsr.2020.105415

of legal protection afforded to vulnerable persons must be proportionate to the quantity and quality of so-called layers of vulnerability. The identification and assessment of these layers must be based on multiple criteria, in particular on the analysis of the origin and effects of vulnerability.[13] Luna concludes that the obligations arising from the assessment of layers of vulnerability must extend to preventing their deterioration, eliminating them where possible, and minimising them through different strategies.[14]

Transposed into the context of data protection law, this raises the question of whether an individual or a universal approach to vulnerability should be preferred. According to the universal approach, data protection law protects all individuals equally in the digital sphere, as all natural persons are equally exposed to potential infringements.[15] The individual approach, by contrast, offers a more accurate picture of risks affecting specific persons, yet it is doubtful to what extent it can be effectively implemented in practice.

Closely related to this distinction is the observation that, due to the rigidity of the concept of "data subject",[16] the assessment of individual vulnerability may easily become generalised, with the result that protective measures adopted for data subjects risk becoming schematic and ineffective.

The GDPR itself supports this concern by distinguishing between "general" data subjects and, for example, children as a group requiring special protection. In this latter case, increased protection is justified, as children, due to their age, are less able to understand the circumstances and effects of specific processing operations, and their level of data protection awareness can therefore only be expected to be relatively low. Reference should also be made to the provisions on data protection impact assessments and the handling of data breaches, where the GDPR places the consideration of individual interests and preferences at the centre of the analysis. However, this recognition must lead to the conclusion that other social groups, due to their life circumstances, are likewise limited in their ability to exercise their rights. One only needs to think of illiteracy.[17]

The determination of vulnerability and of those groups that require special protection is particularly complex and urgent in the context of digital citizenship.

[13] Florencia Luna, 'Elucidating the Concept of Vulnerability: Layers not Labels' (2009) 2(1) *International Journal of Feminist Approaches to Bioethics* https://doi.org/10.3138/ijfab.2.1.121

[14] Florencia Luna, 'Identifying and evaluating layers of vulnerability – a way forward' (2019) 19(2) *Developing World Bioethics* https://doi.org/10.1111/dewb.12206

[15] Malgieri and Niklas (n 12).

[16] Peter Blume, 'The Data Subject' (2015) 1(4) *European Data Protection Law Review* https://doi.org/10.21552/EDPL/2015/4/4

[17] Ibid.

Digital citizenship can be defined as the totality of social and technological arrangements that enable individuals to use digital tools to participate in society.[18] Digital citizenship is grounded in digital literacy, that is, the skills needed to navigate the online world and handle digital technologies. It goes beyond individual abilities by encompassing the relationships between individuals and other actors in the digital sphere. The concept of digital citizenship builds on the digital participation of members of society, which presupposes the active interpretation of information flows and the formation of digital identities.[19]

A prerequisite for digital citizenship is thus the digital literacy of citizens. In its absence, those who lack such competencies are excluded not only from social discourse, but also from significant decision-making processes. As a result, social groups that are unable, or only with great difficulty able, to acquire adequate levels of digital literacy qualify as data subjects requiring enhanced protection also from a data protection law perspective. This is because digital literacy affects not only the protection of personal data in the digital environment, but also the prospects for social participation and the exercise of civil rights. If this is accepted, it follows directly that, in the context of society's digital transformation, data protection no longer safeguards only individual but also collective rights. It can moreover be understood as a boundary condition for the formation of digital citizenship, operating as a gatekeeper of individual and collective interactions.

2. Data Protection Awareness in the Mirror of Data

The definition of data subjects, or more precisely the determination of data subject status, is therefore a key issue, as the applicable level of protection is aligned with it. Against this background, it is necessary to examine what empirical data exist on data protection awareness and GDPR knowledge, in particular with regard to individually distinguishable groups of data subjects.

In 2019, at the request of the European Commission, a Special Eurobarometer survey was conducted with the aim of mapping awareness of the GDPR as well as more general attitudes and behaviours regarding data sharing and data protection.[20]

One of the most important findings of this survey, from the perspective of the present study, is that a majority of respondents (67%) had heard of the

[18] Razvan Rughiniş and others, 'From social netizens to data citizens: Variations of GDPR awareness in 28 European countries' (2021) *Computer Law and Security Review*. 42, 1-15. https://doi.org/10.1016/j.clsr.2021.105585

[19] Luci Pangrazio and Julian Sefton-Green, 'Digital Rights, Digital Citizenship and Digital Literacy: What's the Difference?'(2021) 10, *Journal of New Approaches in Educational Research* https://doi.org/10.7821/naer.2021.1.616

[20] European Commission. (2019b). Special Eurobarometer 487a: The General Data Protection Regulation. Publications Office of the European Union. Online: https://doi.org/10.2838/579882

GDPR. Of these, 36% had both heard of it and knew what it was, while 31% had heard of it but did not know precisely what it regulated.[21]

On the basis of these results, further interpretative possibilities emerge. Using indicators of GDPR awareness, respondents from the EU-27 and the United Kingdom can be divided into four groups: offline citizens (22%), social netizens (32%), web citizens (17%), and data citizens (29%). Offline citizens show the lowest levels of internet use and GDPR awareness. Web citizens are located around the average values. Data citizens exhibit the highest levels both in terms of digital experience and in terms of GDPR knowledge and usage. The fourth group, social netizens, display a more contradictory profile: their use of social networks is extremely high, their experience with online shopping is below average, and their level of GDPR awareness is likewise below average.[22]

Since 2019, no new comprehensive Eurobarometer survey has been conducted that focuses exclusively and specifically on GDPR awareness. This does not mean, however, that there are no further data on GDPR awareness embedded in other research.

In 2021 and again in 2024, the Eurobarometer carried out comprehensive surveys entitled "Justice, Rights and Values" in the Member States. As a contextual background, it should be noted that, as part of the European Union's 2021--2027 long-term budget, the "Citizens, Equality, Rights and Values" programme and the Justice programme were adopted on 28 April 2021, with a combined budget of 1.8 billion euros. These surveys sought to capture EU citizens' views on the values promoted by these programmes and their knowledge of the various instruments used to promote and protect rights and values.[23] In what follows, the present study analyses the data series generated by the Eurobarometer with regard to the GDPR.

2.1 Numbers and Tendencies

The 2019 survey explicitly placed knowledge of the GDPR at the centre of the research. The 2021 and 2024 surveys, although more limited in this regard, nevertheless contain questions that allow for comparison and analysis over time. In the following, the available data series are compared along four main dimensions: (1) the proportion of respondents who had heard of the GDPR in the relevant period; and (2) how awareness is structured according to age; (3) employment status; and (4) financial status. The examination of these three clearly delineated data subject groups provides a suitable empirical foundation for the previously outlined discussion on the concept of the data subject.

[21] Ibid.

[22] Rughiniş and others (n 18).

[23] European Commission. (2021). Special Eurobarometer 514: Justice, Rights and Values. Publications Office of the European Union. https://doi.org/10.2838/3

In 2019, as noted, a majority of respondents (67%) had heard of the GDPR; 36% had heard of it and knew what it was, while 31% had heard of it but did not know exactly what it was. By age group, the highest level of awareness was found among respondents aged 25--54 (75%), followed by respondents younger than this age group (66%), and the lowest level among those older than 54 (58%).[24]

With respect to employment status, managers displayed the highest level of awareness regarding the GDPR (86%), while retired respondents recorded the lowest figure (55%). The Eurobarometer survey also addressed the dimension of financial difficulties. The fewer financial problems respondents faced, the more likely they were to be aware of the Regulation. Among respondents who reported no difficulty in paying their bills, GDPR awareness stood at 71%, while among those for whom paying bills posed serious difficulties, this figure was only 49%.[25]

By the time of the 2021 data collection, a visible improvement could be observed across these indicators.

More than 77% of respondents indicated that they had heard of the GDPR, and 47% reported that they had both heard of and understood the Regulation. Almost one third of respondents in the EU (30%) had heard of the GDPR but did not know exactly what it was, while more than one fifth (21%) stated that they had never heard of it.[26]

In terms of age distribution, 83% of respondents aged 25--39 reported awareness of the GDPR in 2021. This group was followed by respondents aged 40--54 (81%), then by those aged 15--24 (77%), while the least aware group remained respondents aged 55 and over (71%). By employment status, managers again reported the highest level of awareness (90%), followed by other office workers (86%) and the self-employed (84%). Among household employees (63%), retirees (68%), and the unemployed (72%), it was less likely that respondents were aware of the GDPR.

A similar pattern can be observed for financial status. EU citizens who had never experienced difficulties in paying their bills were more likely (80%) to report that they knew the GDPR than those who most often struggled with financial difficulties (69%).[27]

Compared to the positive trends identified in 2021, the 2024 data reveal a certain deterioration in awareness of the GDPR. In summary, more than seventy per cent (72%) of respondents across the EU indicated that they had heard of the GDPR, of whom 40% knew exactly what type of instrument it was. Nearly 32%

[24] Ibid (2019 data).
[25] Ibid.
[26] Ibid (2021 data).
[27] Ibid.

had heard of it but did not have precise knowledge, while 26% stated that they had never heard of the GDPR.[28]

For the individual groups examined, the distribution shows that the 25--39 age group continues to demonstrate the highest level of awareness (79%), followed by those aged 40--54 (76%), those aged 15--24 (71%), and finally those aged 55 and over (65%). The 2024 data also confirm the earlier ranking of employment-based groups. Managers again occupy the first place (85%), followed by office workers and the self-employed (both 80%). Household employees (54%), retirees and the unemployed (both 63%) remain the least aware groups.

In terms of financial status, respondents who never or almost never encountered payment difficulties are more familiar with the GDPR (74%) than those who frequently face financial problems (61%).

Overall, the data series show that, in the EU and the United Kingdom, knowledge of the GDPR increased by an average of ten percentage points between 2019 and 2021. In 2019, there were still 13 countries in which less than 70% of respondents were aware of the GDPR. In contrast, by 2021, 16 countries had more than 80% awareness among respondents. In 2024, however, the average familiarity with the GDPR across the Union decreased by five percentage points compared to 2021. While in 2021 more than 70% of respondents were aware of the GDPR in 24 countries, this was the case in only 19 countries in 2024.[29]

2.2 Common Directions and Different Risks

A decrease in GDPR familiarity can be observed across all examined groups between 2021 and 2024. This trend is particularly worrying in relation to those groups that are most vulnerable, such as young people (15--24 years), retirees, the unemployed, and those facing financial difficulties.

The present study does not provide the framework for an in-depth exploration of the reasons underlying these developments. Nonetheless, it is clear that substantial changes are needed in the field of data protection awareness if the groups most in need of protection are to be adequately safeguarded.

Recital 75 of the GDPR explicitly highlights the processing of personal data of vulnerable natural persons -- in particular children -- in connection with risks of varying likelihood and severity to the rights and freedoms of natural persons. It is important to note, however, that children are mentioned in this context merely by way of example ("in particular"). Taken as a whole, the GDPR accords children a quasi-privileged position, whereas other vulnerable groups are not explicitly identified as such. This leads in practice to controllers applying particularly strict safeguards to the processing of children's data, without necessarily enforcing higher levels of protection in relation to other, similarly vulnerable groups.

[28] Ibid (2024 data).
[29] Ibid.

In this respect, it can be concluded that an absolute understanding of the category of data subjects is not tenable, and that the universal application of the vulnerability concept cannot ensure risk-proportionate protection for natural persons.

3. Whose Responsibility Is It to Promote Data Protection Awareness?

The GDPR identifies two addressees in connection with raising awareness: the data protection officer and the supervisory authority.

Pursuant to Article 39(1)(b) GDPR, the data protection officer is to monitor compliance with the GDPR, with other Union or Member State data protection provisions, and with the controller's or processor's internal policies relating to the protection of personal data, including the assignment of responsibilities, awareness-raising and training of staff involved in processing operations, and the related audits. It is important to note that neither the GDPR nor established case law elaborates in detail on the obligation of the data protection officer to raise awareness. This is a serious gap, as the DPO is, in principle, the actor best positioned to contribute effectively to awareness-raising and education within the organisation of the controller or processor.

As regards supervisory authorities, Article 57(1) GDPR provides that, without prejudice to their other tasks under the Regulation, they shall, on their respective territories, promote public awareness and understanding of the risks, rules, safeguards and rights in relation to the processing of personal data, with specific attention to activities addressed to children.[30]

Article 57 GDPR thus expressly establishes the promotion of public awareness and knowledge regarding the processing of personal data as a dedicated task of supervisory authorities.

When this obligation is juxtaposed with the demonstrable decrease in data protection knowledge among EU citizens between 2021 and 2024, several questions arise.

The first and most important question is to what extent supervisory authorities in individual Member States can be held responsible for the observed decline in awareness.

Exclusive responsibility clearly cannot be established, as the GDPR merely requires supervisory authorities to "promote" the dissemination of data protection knowledge -- a rather open-ended formulation. Nevertheless, the wording of the GDPR undoubtedly implies a requirement to undertake concrete awareness-raising actions.

It also remains an open question which specific types of action can reasonably be expected of supervisory authorities and which results may be

[30] Regulation (EU) 2016/679, art 57(1).

realistically anticipated from such measures. The present study does not allow for a comprehensive and in-depth analysis of these issues. However, some aspects deserve attention, both from a retrospective and from a forward-looking perspective.

In their analysis of the Polish supervisory authority and the challenges of reflexive regulation in its practice, Pichlak and Gaczol identified five key factors that, in the author's view, merit consideration in assessing the operation and enforcement methodologies of supervisory authorities in all EU Member States: resources, capture, capacities, characteristics of controllers, and inconsistencies of the GDPR.[31]

Among these, the first -- resources -- is of particular relevance. Following the logic of Pichlak and Gaczol's study, resources encompass both material means and human capacity. The issue is illustrated here by reference to three Member State supervisory authorities selected on the basis of GDP per capita: France, which roughly corresponds to the EU average (38,000 euros, EU average 37,600 euros), the Netherlands, which exceeds the Union average (48,900 euros), and Hungary, which is below the average (28,700 euros).[32]

In 2025, the French Data Protection Authority operated with a budget of 28.2 million euros and a staff of 298 persons. Between 2019 and 2024, its staff numbers increased by 62%.[33] In the same year, the Dutch Data Protection Authority disposed of 49 million euros and employed 320 persons, an 89% increase compared to 2021.[34] The Hungarian supervisory authority, the National Authority for Data Protection and Freedom of Information, had a budget of 5.8 million euros in 2025 and 129 employees in the first quarter of 2025, which represents an increase of only 19% between 2021 and 2025.[35]

The absolute size of the budget and the growth in staff numbers cannot, in themselves, serve as the basis for comprehensive conclusions. Nevertheless, it can be stated that, despite the expansion of resources, there is no detectable increase in the effectiveness of national authorities as regards data protection awareness. If resources are not the decisive factor, then, according to Pichlak and Gaczol's interpretation, the combination of the other four elements (with varying weight in each Member State) may be responsible for the unfavourable trends.

[31] Maciej Pichlak and Klaudia Gaczol, 'Simple and advanced reflexivity in GDPR enforcement: empirical evidence from DPA activity' (2023) *International Data Privacy Law* 13(4) https://doi.org/10.1093/idpl/ipad018

[32] European Union, EU countries – Facts and figures https://european-union.europa.eu/principles-countries-history/eu-countries_hu

[33] CNIL, *Status & Composition* (2025) https://www.cnil.fr/en/cnil/status-composition

[34] Autoriteit Persoonsgegevens, *Facts and figures about the AP. Autoriteit Persoonsgegevens* (2025) https://www.autoriteitpersoonsgegevens.nl/en/over-de-autoriteit-persoonsgegevens/feiten-en-cijfers

[35] Nemzeti Adatvédelmi és Információszabadság Hatóság, *2025. I. negyedév személyi juttatások: Bér- és létszámadatok* (2025) https://www.naih.hu/files/3_2_2025_I_negyedev_szemelyi_juttatasok.pdf

As regards capture, generalisations are difficult. The extent to which national supervisory authorities are genuinely independent of political or economic power in their respective countries must be assessed on a case-by-case basis; yet, in many instances, empirical substantiation is hardly possible. The concept of capacities, as used by Pichlak and Gaczol, points to deficits in expertise and cultural competence, which may help explain why certain authorities devote relatively little attention to awareness-raising even when resources would permit more proactive engagement. Finally, regulatory inconsistency and the structure of data controllers in the Member State concerned may also significantly influence the practice of supervisory authorities. In particular, adaptation to specific social and economic realities requires different strategies in different Member States.[36]

Looking back, it should be emphasised once again that the role of data protection officers cannot be overlooked when discussing awareness-raising. While supervisory authorities can exert influence at Member State level, it is the DPO who is best placed to promote the dissemination of knowledge within individual controller organisations. Ideally, this would allow for complementary top-down and bottom-up awareness-raising campaigns.

III. Artificial Intelligence Literacy

1. AI Literacy and Digital Literacy

The social integration of artificial intelligence (AI) is marked by significant concerns. Research communities, governmental bodies, and non-profit organisations alike have emphasised that AI is far more than a mere technological innovation.[37] Due to its novelty and complexity, it is frequently described as a revolutionary, "next wave" technology.[38] Given its general, horizontal and pioneering nature, AI brings with it not only considerable opportunities, but also risks for individuals and society as a whole, including negative effects that are difficult to foresee and to measure.[39]

Risk perception and, consequently, expectations regarding regulation differ considerably across cultures. A community's perception of threats associated with the unknown, and thus its degree of uncertainty avoidance, has a decisive influence on the chosen regulatory approach to technologies that are perceived as

[36] Pichlak and Gaczol (n 38).
[37] Francesca Foffano, Teresa Scantamburlo and Atia Cortés, 'Investing in AI for social good: an analysis of European national strategies' (2022) 38. *AI and Society* https://doi.org/10.1007/s00146-022-01445-8
[38] Mustafa Suleyman and Michael Bhaskar, *A következő hullám: Mesterséges intelligencia, technológia, hatalom és a 21. század legnagyobb kihívása* (Magnólia 2023).
[39] High-Level Expert Group on AI, *Ethics Guidelines for Trustworthy AI* (European Commission 2019).

risky. Previous studies have shown that societies with a high level of uncertainty avoidance tend to adopt a more critical stance towards new technologies.[40]
In addition to differences in risk perception, there are also significant divergences between countries regarding the normative orientation of AI regulation.[41]
With regard to emerging technologies, the pace of technological development inevitably outstrips the speed of regulatory responses. In the case of AI, widespread public uncertainty is more pronounced than ever, and governmental responses alone are no longer sufficient to address questions relating to the benefits, risks and future potential of this technology.[42] This, in itself, is likely to increase uncertainty and shift risk perception in a more negative direction.

Research nonetheless suggests that there are global patterns in AI regulation and in public perception of AI. These include shared assumptions about the economic consequences and impacts of AI, i.e. the recognition of the challenges and opportunities associated with AI and their incorporation into public policy thinking in many countries. At the same time, it is noteworthy that the "European" conception of restrictions on individual AI systems has not found broad support in global public opinion.[43]

One of the most important determinants of the risks and impact of artificial intelligence is the way in which the technology is used. Usage, in turn, directly depends on users' knowledge and understanding and thus on their AI literacy.

At first glance, the concepts of data protection awareness and AI literacy appear to differ. However, both are grounded in similar regulatory logics and expectations. Unlike the GDPR, which relies on the notion of "awareness", the AIA relies on the concept of "literacy".

There is, and is unlikely to be, a uniform, globally accepted general definition of AI literacy. It is therefore useful to begin by delineating the main elements of literacy as they appear in the AIA, before turning to concepts developed in scholarly literature.
Article 3(56) AIA defines "AI literacy" as:[44] "skills, knowledge and understanding that allow providers, deployers and affected persons, taking into account their

[40] Bartosz Wilczek, Sina Thäsler-Kordonouri and Maximilian Eder, Government regulation or industry self-regulation of AI? Investigating the relationships between uncertainty avoidance, people's AI risk perceptions, and their regulatory preferences in Europe' (2025) 40(5) *AI & Society* https://doi.org/10.1007/s00146-024-02138-0

[41] Soenke Ehret, 'Public preferences for governing AI technology: comparative evidence' (2022) *Journal of European Public Policy* https://doi.org/10.1080/13501763.2022.2094988

[42] Wendell Wallach and Gary Marchant, 'Toward the Agile and Comprehensive International Governance of AI and Robotics' *Proceedings of the IEEE*, 107(3), 505–508 https://doi.org/10.1109/JPROC.2019.2899422

[43] Ehret (n 48).

[44] Regulation (EU) 2024/1689, art 3(56).

respective rights and obligations in the context of this Regulation, to make an informed deployment of AI systems, as well as to gain awareness about the opportunities and risks of AI and possible harm it can cause."

Recital 20 supports and refines this definition. It states that the aim of AI literacy is to provide "providers, deployers and affected persons with the necessary notions to make informed decisions regarding AI systems", to enable them to appropriately interpret the output of AI systems, and to ensure that they are aware of the impact of such systems' decisions on them.[45]

In its "Discussion Paper on Draft Recommendation on AI literacy" published in February 2025, the Council of Europe identified three main dimensions of AI literacy: technological, practical and human. The technological dimension concerns understanding how AI systems work and how they can be further developed. The practical dimension focuses on the ability to use AI effectively. The human dimension relates to the impact of AI on people, human rights, democracy and the rule of law.[46]

As this already indicates, the AIA does not provide an exhaustive definition of AI literacy, but only outlines its main aspects. This is confirmed by Recital 20, which specifies that the required level of understanding may vary depending on the context.[47]

In general terms, AI literacy can be described as the set of competencies that enable individuals to interact effectively with AI technologies. This includes an understanding of basic AI concepts, the ability to critically evaluate AI systems and their outputs, and the ethical use of AI tools in different contexts.[48]

The challenge of defining AI literacy is well known in the scholarly literature, and numerous concepts have been proposed in recent years. Kandlhofer and co-authors, for instance, define AI literacy as the capacity to understand the basic techniques and concepts underlying AI, particularly as they are applied in specific products and services.[49] Ng and co-authors conceptualise AI literacy as a complex body of knowledge that encompasses understanding basic AI functions and applications, the ability to use and apply AI, to evaluate and create AI systems,

[45] Ibid, Recital 20

[46] Council of Europe, *Discussion Paper on Draft Recommendation on AI Literacy* (2025) https://www.coe.int

[47] Regulation (EU) 2024/1689, Recital 20

[48] Yueqiao Jin , Roberto Martinez-Maldonado, Dragan Gašević, Lixiang Yan, 'GLAT: The generative AI literacy assessment test' (2025) *Computers and Education: Artificial Intelligence* https://doi.org/10.1016/j.caeai.2025.100436

[49] Martin Kandlhofer, Gerald Steinbauer, Sabine Hirschmugl-Gaisch and Petra Huber, 'Artificial intelligence and computer science in education: From kindergarten to university' (2016) in *IEEE Frontiers in Education Conference (FIE)* https://doi.org/10.1109/FIE.2016.7757570

and to understand AI ethics and human-centric considerations.[50] Other approaches emphasise technical understanding, practical application, critical ability, efficiency, and the quality of AI-generated outputs.[51]

The definition of AI literacy also depends significantly on the target group of the assessment. Here, it is useful to distinguish between experts and non-experts, i.e. laypersons. For the latter, Laupichler and co-authors propose an assessment framework comprising three components: technical understanding of AI, critical evaluation, and practical application.[52]

All of the above concepts share a similar conceptual lineage with digital literacy. In contemporary knowledge-based societies, digital literacy denotes the basic digital competencies that all citizens must possess in order to enjoy equal opportunities in the labour market.[53]

The origins of digital literacy can be traced back to the 1960s. However, its definition has evolved continuously alongside technological developments and the changing environments to which it refers.[54] Initially, digital literacy was associated primarily with the visual processing of information, a notion captured in John Debes' concept of "visual literacy".[55]

With technological advancement, the semantic content of digital literacy has changed, and there is still no widely accepted, fully standardised definition. Different authors define digital literacy in different ways, as the evolution of the technological environment and the pace of innovation significantly influence how people use digital tools. At the same time, there is broad agreement that digital literacy is a multidimensional construct encompassing technical and cognitive skills, metacognitive processes, civic engagement, and ethical awareness.[56]

[50] Davy Tsz Kit Ng, Jac Ka Lok Leung, Samuel Kai Wah Chu and Maggie Shen Qiao, Conceptualizing AI literacy: An exploratory review' (2021) *Computers and Education: Artificial Intelligence* https://doi.org/10.1016/j.caeai.2021.100041

[51] Senad Bećirović , Edda Polz1 and Isabella Tinkel, 'Exploring students' AI literacy and its effects on their AI output quality, self-efficacy, and academic performance ' (2025) 12(29) *Smart Learning Environments* https://doi.org/10.1186/s40561-025-00384-3

[52] Matthias Carl Laupichler, Alexandra Aster, Nicolas Haverkamp and Tobias Raupach, Development of the "Scale for the assessment of non-experts' AI literacy" – An exploratory factor analysis' (2023) *Computers in Human Behavior Reports* https://doi.org/10.1016/j.chbr.2023.100338

[53] David Bawden, 'The distractions of documentation' (2008) *Journal of Documentation* https://doi.org/10.1108/jd.2008.27864faa.001

[54] Nikitas Kastis and Roberto Carneiro,' Digital Literacy—The Evolution of the 21st Century Literacies' (2009) https://www.openeducationeuropa.eu/en/paper/digital-literacy-%E2%80%93-evolution-21st-century-literacies

[55] Colin Lankshear and Michele Knobel, 'Digital Literacies: Concepts, Policies and Practices' (2008) *Peter Lang Publishing*

[56] Pritika Reddy, Bibhya Sharma and Kaylash Chaudhary , 'Digital Literacy: A Review of Literature' (2020) 11(2) *International Journal of Technoethics (IJT)* https://doi.org/10.4018/IJT.20200701.oa1

Balázs Hohmann considers digital literacy the foundation of all meaningful platform regulation, as it enables individuals to find, understand and critically evaluate the services they use.[57]

The measurement of AI literacy raises additional methodological challenges. While knowledge of the GDPR can be probed through relatively clear and measurable questions, the assessment of AI literacy requires more differentiated instruments.

Existing measurement tools largely rely on self-assessment, while performance-based instruments are used much less frequently. This raises questions about the reliability of survey data. Although performance-based tests exist for general AI literacy -- for example, the Hornberger test -- there is, as yet, no suitable methodology for assessing knowledge of generative AI (GenAI). Without performance-based instruments, self-reporting biases cannot be adequately controlled, particularly in relation to new technologies such as AI and GenAI tools.[58]

IV. Conclusion

The working hypothesis of this research was that the foundations of data protection awareness and AI literacy can be aligned and that experiences gained following the entry into force of the GDPR could usefully inform the implementation of the AIA. Comparing the concepts and legal content of data protection awareness and AI literacy is far from straightforward. Nevertheless, the assertion that both are prerequisites for digital literacy -- that is, for the capacity of users to know and understand the nature of their use of digital tools -- appears well founded.

The GDPR does not define data protection awareness. However, on the basis of the literature and the tasks assigned to data protection officers and supervisory authorities, it can be interpreted as a special form of legal awareness that extends to the rights deriving from the GDPR, to their content, and, where appropriate, to the obligations flowing from the Regulation.

AI literacy, particularly as conceptualised in the AIA, has a more technology-focused semantic content, emphasising concrete use of AI systems, their results and their evaluation. The two normative concepts also relate to partially different personal scopes. As regards data subjects, the GDPR places the obligation to promote data protection awareness on data protection officers and supervisory authorities. By contrast, the AIA assigns responsibility for ensuring AI literacy to providers and deployers of AI systems. In this context, neither fundamental rights authorities under Article 77 AIA nor market surveillance authorities have a direct

[57] Balázs Hohmann, 'The Interplay Between User Awareness And Transparency Requirements In The Context Of European Platform Regulation' (2025) *Journal Of Humanities and Social Science* (IOSR-JHSS) 30 (8) https://doi.org/10.9790/0837-3008052433

[58] Jin and others (n 55).

role. Only in relation to the European Artificial Intelligence Board (hereinafter: Board) does the legislator refer to awareness-raising, providing in Article 66(f) that the Board may support the Commission's "public awareness-raising activities on AI literacy and the use of AI systems".

Ultimately, both normative concepts aim to enhance the protection, awareness and knowledge of "end users". A further commonality is that both build on digital literacy and can be regarded as its specific manifestations.

Unlike the GDPR, however, the AIA does not require public authorities to develop literacy. It essentially treats literacy as an obligation incumbent solely upon providers and deployers. Consequently, it can be concluded that, while the AIA defines the concept of literacy, it does not render it enforceable through the instruments of public authorities.

In light of the empirical findings presented in this study, it is doubtful that this legislative approach will lead to satisfactory outcomes. A decrease in data protection awareness -- particularly among vulnerable groups -- can be demonstrated despite the fact that, over the same period, data protection authorities performed their tasks with increasing budgets and staff numbers. If this is recognised as a broader trend, even in a regulatory environment in which the allocation of responsibility is more clearly defined and is shared between two main addressee groups (supervisory authorities and controllers through data protection officers), it is not immediately apparent why one should expect better results in a regime in which only one of these groups has been designated (providers and deployers).

Based on the research presented, the social environment from which the persons "protected" by these normative concepts originate cannot be ignored. In the context of the GDPR, Eurobarometer data show that the social and sociocultural background of data subjects is relevant. When the same question is posed in relation to the AIA, however, attention must be paid not only to individuals' prior education, but also to the broader attitudes prevailing in the social environments in which they live.

Continuing this line of thought, it must also be noted that the concept of AI literacy as employed in the AIA is overly restrictive, as it fully excludes those who do not use or deploy a given AI system, yet are nonetheless affected by it. This gap cannot be filled by reference to the seven principles laid down in the AIA either. Against this background, it is particularly problematic that the AIA does not establish a uniform supervisory authority system comparable to that of the GDPR, thereby preventing the emergence of corrective mechanisms that could potentially arise from authority involvement.

In light of the experiences and data accumulated under the GDPR and considering the horizontal risk exposure of AI systems, it remains an open question which control mechanisms will ultimately be applicable in practice.

STATEMENTS

Disclosure statement
No potential conflict of interest was reported by the author.

Funding
The author received no financial support for the research, authorship, or publication of this article.

Data deposition and availability
There is no data set associated with the study. No data deposition was required for this study.

Use of Artificial Intelligence
The author acknowledges the use of Perplexity AI for translation assistance. The author has reviewed and edited the AI-generated translation to ensure accuracy, clarity and appropriate legal terminology, and assumes full responsibility for the final content of this article.

Author contributions (CRediT)
Conceptualization; Methodology; Investigation; Formal analysis; Resources; Data curation; Writing – Original Draft; Writing – Review & Editing.