Andrés Chomczyk Penedo

A duty of assistance to make sense of privacy notices

Lessons from financial services regulation

Abstract

The average length of a privacy notice has constantly increased in the last few years. If data controllers are putting out there longer and longer privacy notices, should not they also be helping data subjects in making sense of them? With data-intensive activities getting more and more complex, we can only expect this to impact negatively on these documents. At this stage, we can compare them to complex financial documents such as a prospectus of a publicly-traded company or a mortgage application.

While GDPR asks for concise and easy-to-read language, it is possible that the complexity of the operations cannot be simplified, which calls for researching alternatives. For this, we can draw inspiration from the financial services industry to address this ever-growing complexity. In this sense, the financial services industry has developed a duty of assistance to help clients in certain scenarios when complex documents, such as prospectus or credit sheets, are involved.

Therefore, the purpose of this contribution is to explore how this duty could be grounded in current European data protection regulations, particularly GDPR, and how it should be implemented to ensure that data subjects are assisted in their choices. As part of this discussion, the article shall address the notion of nudging and compare it with the notion of assisting to argue why an assisted consent would still meet the GDPR requirements for valid consent.

If such a duty can be grounded under GDPR, it can be addressed one of the most criticized topics in data protection: the notice and consent model. By doing so, the relationship between data subjects and data controllers could change dramatically towards a more engaged interaction between the two to accommodate the more data-intensive activities. In this respect, it is foreseeable a more participatory model for governing personal data.

Keywords

Data economy, duty of assistance, financial regulation, GDPR, notice-and-consent, transparency.

About the Author

PhD Researcher at the Law, Science, Technology and Society Research Group, Vrije Universiteit Brussel (Belgium) and Visiting Researcher at the Dublin City University Law and Tech Research Cluster (Ireland). Marie Skłodowska-Curie fellow at the PROTECT ITN.

Email: andres.chomczyk.penedo@vub.be

The Author has received funding from the European Union's Horizon 2020 research and innovation programme under the Marie Skłodowska-Curie grant agreement No 813497.

How to cite

Andrés Chomczyk Penedo, 'A duty of assistance to make sense of privacy notice: Lessons from financial services regulation', DCU Law & Tech Working Paper Series, 2022-1, DOI: 10.5281/zenodo.7305219

1. Introduction

Data subjects have to deal with a considerable number of digital interactions in their daily lives,[1] and they can only expect them to expand more as we move towards a more digitalized economy and society. Information, particularly personal data, is used to fuel a wide-range of technological developments for the benefit of society at large. Authors, such as Zuboff,[2] have highlighted the abusive downsides that this approach to information entail, from the extractive practices that see individuals as a resource to generate data rather than as human beings up to manipulative interactions to further consolidate the model and its extractive nature. Despite these critics, existing policy strategies around the digital economy are inclined to preserve it albeit with some changes to ensure the respect of fundamental rights, such as the right to personal data protection.

These activities involve processes and steps that might seem enigmatic, almost undecipherable, for a layman. Laws have long been structured around the idea of a rational and thinking individual that makes carefully thought and planned decisions. From contract law to consumer protection law, its very core remains and was picked up by other legal regimes, including data protection law. However, this idea is getting everyday far and far behind, particularly in those areas where is a clear power imbalance between the involved parties.[3] In this respect, data protection is also structured around this very idea from its inception and,[4] despite its shortcomings,[5] remains to this day across jurisdictions as a core tenet for data protection regimes.

Choices made by individuals involve understanding close and short-term effects, something that the individual should be able to grasp, but also the consequences that are into the future or that they might carry for the rest of society.[6] For example, personal data of one individual might have a small price in data markets but when aggregated alongside other people the value of the dataset as a whole changes considerably given what can be done with that information. In this sense, this resembles the characteristic of 'emergence' found in complex systems, i.e., that the aggregate of certain elements is more than its mere summation and has something that makes it unique.[7] Applying complexity theory in law is not something new,[8] but has received very little attention from scholars in the field of data protection regulation.[9]

Each level of decisions is accompanied by its own set of information related to the concrete situation, usually required by sector specific regulations. As such, each layer presents its own challenges to ensure that it is understood. However, and relying on complexity theory, each level would also influence each other - known as 'top-down' and 'bottom-up' effects-[10] in a manner beyond merely adding up the information available about the system. For example, a data subject in an online marketplace might have to pay attention not only to the privacy notice provided by the platform to understand how his/her

[1] Aleecia M Mcdonald and Lorrie Faith Cranor, 'The Cost of Reading Privacy Policies' (2008) 4 I/S: A Journal of Law and Policy for the Information Society 543.

[2] Shoshana Zuboff, *The Age of Surveillance Capitalism: The Fight for a Human Future at the New Frontier of Power* (Profile Books 2019).

[3] Natali Helberger and others, 'EU Consumer Protection 2.0 Structural Asymmetries in Digital Consumer Markets, A Joint Report from Research Conducted under the EUCP2.0 Project' (BEUC - The European Consumer Organization 2021) <https://pure.uva.nl/ws/files/62051712/beuc_x_2021_018_eu_consumer_protection.0_0.pdf> accessed 16 December 2021.

[4] Eleni Kosta, *Consent in European Data Protection Law* (Martinus Nijhoff Publishers 2013); Daniel J Solove, 'Privacy Self-Management and the Consent Dilemma' (2013) 126 Harvard Law Review 1880.

[5] Bart W Schermer, Bart Custers and Simone van der Hof, 'The Crisis of Consent: How Stronger Legal Protection May Lead to Weaker Consent in Data Protection' (2014) 16 Ethics and Information Technology 12.

[6] Nicolas Petit and Thibault Schrepel, 'Complexity-Minded Antitrust' (2022) Working Paper 4 <http://dx.doi.org/10.2139/ssrn.4050536>.

[7] John H Holland, *Complexity: A Very Short Introduction* (OUP Oxford 2014).

[8] JB Ruhl, 'Fitness of Law: Using Complexity Theory to Describe the Evolution of Law and Society and Its Practical Meaning for Democracy, The' (1996) 49 Vanderbilt Law Review 1406.

[9] Kunbei Zhang and Aernout HJ Schmidt, 'Thinking of Data Protection Law's Subject Matter as a Complex Adaptive System: A Heuristic Display' (2015) 31 Computer Law & Security Review 201.

[10] Holland (n 7) 35.

personal data is processed but also to the terms and conditions between the platform and the online merchant to spot further details about his/her personal data being processed between the other two parties as well as between the data subject and the merchant.

But how exactly can an individual grasp all this complexity? Information about these activities is typically provided in a privacy notice; but these have constantly increased in size during the last years, as has been demonstrated by other researchers,[11] to provide the mandated information required by, generally, data protection rules. Not only that but also the amount of different services running at the same time makes reality more complex as for a given situation an individual might have to read more than one notice. As such, if data controllers are putting out there more and longer privacy notices, they should also be helping data subjects in making sense of them.

This article proposes the development of a duty of assistance, inspired by financial services regulation, from data controllers to data subjects to collaborate in understanding the consequences that providing personal data has on a particular situation. At this stage, it is relevant to indicate that the study will be conducted within the context of EU regulation. In this respect, this article is structured as follows. Section 2 provides an overview of the complex reality caused by existing data usage strategies within the context of the European Union. Section 3 focuses on the role of transparency in the data/platform economy, particularly from a European perspective, and reflects on how complexity affects data flows. Section 4 reflects on the role of transparency within EU data protection regulations. Section 5 is devoted to challenges currently present in data protection transparency. Section 6 introduces the duty of assistance drawing inspiration from the regulation of the financial services. Section 7 discusses the possibility of introducing a duty of assistance within the context of GDPR. Section 8 overviews the potential consequences of such a duty in relation to its intended objective. Finally, Section 9 addresses some possible future research paths.

2. Living in a complex datafied world: the ‘data/platform’ economy and its implications

Data already plays a key role in the European economy and this trend is expected only to increase and consolidate, as described in the European Union’s policy document titled ‘A European Strategy for Data’ (the ‘EU Data Strategy’).[12] While there are 'smaller' objectives, such as developing cross-sectoral governance frameworks like the Data Act or empowering individuals through educating in digital skills, the ultimate purpose is to '(…) create a single European data space – a genuine single market for data, open to data from across the world – (…)'.[13] This particular appetite for consolidating data in a common and shared environment is not new but it was already present in previous policy documents from the EU.[14] In this respect, the EU Data Strategy seeks to put in practice years of thinking into how data should be regulated and used for society’s benefit through the use of data spaces.

The primary reason behind this policy and regulatory agenda is that an integrated data economy requires common standards to facilitate, from a technical point of view, data sharing between mostly disconnected datasets. On top of this, a common data-sharing regulatory framework would tackle the fragmented and sectorial regulation that limits how information can flow between different industries

[11] Isabel Wagner, ‘Privacy Policies Across the Ages: Content and Readability of Privacy Policies 1996--2021’ [2022] arXiv:2201.08739 [cs] <http://arxiv.org/abs/2201.08739> accessed 1 February 2022.

[12] ‘Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions: A European Strategy for Data’ (European Commission 2020) COM(2020) 66 final.

[13] ibid 4–5.

[14] ‘Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions - A Digital Single Market Strategy for Europe’ (2015) COM(2015) 192 final s 4.1. ‘Communication from the Commission to the European Parliament, the Council, The European Economic and Social Committtee and the Committee of the Regions “Towards a Thriving Data-Driven Economy”’ (European Commission 2014) COM(2014) 442 final.

and stakeholders. With both elements in place, it is expected that businesses would be interested in developing digital economy products and services in Europe by choice given the substantial benefits in place, i.e., easy interoperability and legal clarity over the authorization to do so.

This economic and societal model seeks to directly challenge the current corporate practices, particularly of big tech companies, that tend to accumulate, and profit, from owning massive sets of information and are not in the obligation to disclose them to competitors. For example, Meta operates a considerable number of databases fueled by its different 'businesses' -from Facebook to WhatsApp including Instagram or others- but the degree to which such datasets are available to outside parties is limited to very few venues, such as developers' APIs, and constrained by tight and restrictive terms of use. Just like Meta produces further value from that information, the EU Data Strategy seeks to break such closeness and benefit all interested parties from it. Therefore, and as mentioned above, the EU has been pushing for the development of data spaces, even before the adoption of the EU Data Strategy itself,[15] to foster the flow of data from individuals to businesses and governments, between businesses themselves as well as with public authorities.[16]

However, alongside the adoption of data space, the EU is also pushing for the consolidation of the platform business model through several upcoming regulations,[17] such as the Digital Services Act (DSA)[18] or the Digital Markets Act (DMA)[19]. This acknowledges the role that platforms have in allowing the development of such data-driven environments by enabling larger pools of individuals and companies to find each other relatively easily beyond borders. Following up with the previous example on Meta and data sharing, these large big tech companies have also taken the role of a key economic actor to attract businesses, as well as users, and provide a fertile ground for operation at a price, be it their data or a fee. In addition, data collected by these platforms is extremely valuable because of the technical and organizational infrastructure put in place by the platform itself and that, probably, could not have been generated in any other manner whatsoever to adjust quickly to economic trends. For example, YouTubers use the platform's data to adjust their content and vice versa or Amazon can leverage the data generated by sellers operating on its platform and offer demanded products at a lower price.

When read in tandem, it is possible to assess that the EU has two objectives in mind: (i) make more data available to as such stakeholders as possible; and (ii) concentrate regulatory compliance in the head of platform operators to ensure that access to it is made available and data is adequately protected. In this sense, the EU would be pushing forward a model based around these two pillars, which can be called the 'data/platform' economy.

As mentioned above, this 'data/platform' economy would have at its very core the free flow of all available information. However, and as noted in different policy documents, this is not expected to be

[15] 'Communication from the Commission to the European Parliament, the Council, The European Economic and Social Committtee and the Committee of the Regions "Towards a Common European Data Space"' (European Commission 2018) COM/2018/232 final.

[16] The exact notion of what is a data space is still a very vague concept scattered across much different policy and regulatory instruments. For more on this concept, see Boris Otto, 'A Federated Infrastructure for European Data Spaces' (2022) 65 Communications of the ACM 44. Some legal scholars have tried to untangle the legal definition but focused on the legal consequences of an unknown thing (see Anastasiya Kiseleva and Paul de Hert, 'Creating a European Health Data Space: Obstacles in Four Key Legal Area' (2021) 5 European Pharmaceutical Law Review (EPLR) 21; Giovanni Comandè and Giulia Schneider, 'It's Time. Leveraging The GDPR to Shift the Balance Towards Research-Friendly EU Data Spaces' [2022] Common Market Law Review 34.)

[17] In this respect, the Digital Single Market strategy had also grounded the future development of the EU digital economy around these intermediaries (see 'Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions - A Digital Single Market Strategy for Europe' (n 14) s 3.3.) As with data spaces, the notion of platform remains elusive and varies from legal instrument to legal instrument without a comprehensive and unique definition; for example, the final text for the DMA contains the definition of 'core platform services', which includes services such as online intermediation, search engines, social networking, among others.

[18] Proposal for a REGULATION OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL on a Single Market For Digital Services (Digital Services Act) and amending Directive 2000/31/EC.

[19] Proposal for a REGULATION OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL on contestable and fair markets in the digital sector (Digital Markets Act)

done in an unrestrictive manner without regard to other existing and upcoming rules. In this respect, data sharing still needs to be done in compliance with substantial rules, particularly around personal data due to the GDPR as well as in the Data Governance Act(DGA),[20] or upcoming regulation as the Data Act.[21] While there is no (general) prohibition for sharing (as a form of processing) personal data, with the notable of sensitive data under Article 9.1 GDPR, stored across many datasets and any available legal basis would be available, consent is expected to play a key role to enable data sharing across different actors,[22] particularly in sensitive fields such as healthcare or financial services.[23] The emergence of novel data intermediaries, such as data cooperatives under the DGA, also provides for the reliance on consent to enable data sharing with third parties by helping cooperatives members in assessing their choices.

Recurring to other legal bases could avoid having to deal with the challenges that consent pose.[24] However, consent can be regarded as the prime legal basis given its ample possibilities for data processing as the individual itself is involved in the process, particularly when there is no other legal basis to enable it.[25] The downside of this approach is that data subjects would be further overloaded with more digital interactions about their data. Consequently, this would be increasing the already existing consent fatigue, as described by Custers, van der Hof and Schermer.[26] While other legal bases can enable certain data sharing within a defined context, such as in the case of transferring information to public bodies for a reason defined in a law, the current interpretations from authoritative bodies place a considerable limitation on the further processing and sharing upon the initial circulation of data. Consequently, this reinforces the need to use consent as a legal basis given its modularity and 'case-by-case' possibilities. However, consent has a considerable high standard to meet to achieve legal compliance with the involved regulations.[27]

In this respect, where can we start addressing the challenges that the 'data/platform' economy presents for individuals and their data? One of the preconditions for any data processing activity is having a legal basis to do so, as discussed in the previous paragraphs. The other main precondition for processing data is to disclose to data subjects how their data will be used. This leads us to analyze how transparency is provided to disclose these data flows, in an era of dark patterns.[28] Besides the obvious regulatory requirements, transparency can be seen as a necessary step towards addressing the complexity posed by this mixed economic model where one field influences the other and vice versa, leading to its emergence. The following section will review how data flows are made transparent in the 'data/platform' economy.

3. The role of transparency in EU data economy regulation

[20] Regulation (EU) 2022/868 of the European Parliament and of the Council of 30 May 2022 on European data governance and amending Regulation (EU) 2018/1724 (Data Governance Act) (Text with EEA relevance) PE/85/2021/REV/1 OJ L 152, 3.6.2022, p. 1–44

[21] Proposal for a REGULATION OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL on harmonized rules on fair access to and use of data (Data Act), COM(2022) 68 final

[22] Andrés Chomczyk Penedo, 'Towards a technologically assisted consent in the upcoming new EU data laws?' [2022] PinG Privacy in Germany 5.

[23] For example, see 'Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions: A European Strategy for Data' (n 12) 10, 29.

[24] 'Guidelines on Consent under Regulation 2016/679' (European Data Protection Board 2020) Guidelines 05/2020.

[25] Waltraut Kotschy, 'Article 6. Lawfulness of Processing' in Christopher Kuner, Lee A Bygrave and Christopher Docksey (eds), *The EU General Data Protection Regulation (GDPR) A Commentary* (1st edn, Oxford University Press 2020).

[26] Bart Custers, Simone van der Hof and Bart Schermer, 'Privacy Expectations of Social Media Users: The Role of Informed Consent in Privacy Policies: Privacy Expectations of Social Media Users' (2014) 6 Policy & Internet 268.

[27] 'Guidelines on Consent under Regulation 2016/679' (n 25).

[28] 'Shaping Choices in the Digital World: From Dark Patterns to Data Protection: The Influence of UX/UI Design on User Empowerment' (Commission Nationale de L'informatique et des Libertés 2019) 6 <https://linc.cnil.fr/sites/default/files/atoms/files/cnil_ip_report_06_shaping_choices_in_the_digital_world.pdf> accessed 10 February 2022.

Transparency plays a role in many different aspects of the data/platform economy. For example, we can address the transparency needed between social media platforms and online users on how content gets moderated,[29] the conditions that an app store would require developers for an app to get uploaded and distributed as well the privacy standards,[30] or between online marketplaces and businesses regarding which products get ranked first and the reasons, i.e. the data involved, for such decisions.[31] All of these examples, as we discussed above, deal with the complex 'data/platform' economic model where a core entity -the platform- makes considerable decisions on how to use certain parameters -the data- to define, primarily, economic conditions. However, the reasons for making those decisions remain, at best, obscure for the involved parties at each stage.[32]

As a response, slowly but steadily, at a European level, the European Commission started to proposed regulatory frameworks. In this respect, existing rules such as the Platform-to-Business Regulation,[33] or upcoming regulations, like the DSA or the DMA proposals have taken transparency as a core principle to bring disclosure into some of these areas. For example, the Platform-to-Business Regulation has improved the transparency provided by operators of both online intermediation services, such as Amazon or Facebook, as well as online search engines, such as Google, with regards to the 'professional' users of such platforms on how data is used or not for making decisions with an economic impact in their course of operation.[34] While the extent of the DSA is significant, one of its core pillars is improving the transparency due by platforms, particularly social media, to its users and which data can influence their content gets taken down.[35]

A common trend among the reviewed regulations is that transparency is, primarily, provided through terms of use. Building on Celeste's analysis of their (digital) constitutional role in setting rights, principles, and duties,[36] platforms are already compelled, because of this role, to be as clear as possible when indicating how digital life takes place within their boundaries. Being obscure, unclear, or in any other way not transparent about what happens in the platform, particularly when using personal data, already sets up the stage in the wrong manner and, potentially, can cause significant harm to fundamental rights.

Besides this, we can also explore how transparency has been conceived for the data aspect of this economic and social model. In this respect, the EU Data Strategy places a considerable amount of attention on transparency. For example, a great deal of importance is placed upon novel technical

[29] Paul De Hert and Andrés Chomczyk Penedo, 'A Democratic Alternative to the Digital Services Act's Handshake between States and Online Platforms to Tackle Disinformation' (*EU Law Analysis*, 11 January 2022) <http://eulawanalysis.blogspot.com/2022/01/a-democratic-alternative-to-digital.html> accessed 21 February 2022.

[30] Joris van Hoboken and RÓ Fathaigh, 'Smartphone Platforms as Privacy Regulators' (2021) 41 Computer Law & Security Review 105557.

[31] *Google Search (Shopping)* [2017] European Commission AT.39740; *Google Shopping* [2021] General Court (Ninth Chamber, Extended Composition) T-612/17.

[32] This taps into the larger discussion on how to govern the 'data/platform' economy, an exchange that has far larger connotations and effects than those that analyzed here (for example see José van Dijck, Thomas Poell and Martijn de Waal, *The Platform Society* (Oxford University Press 2018). Nevertheless, the discussion around transparency, following our complexity theory approach, can have a considerable impact on how transparency is addressed at lower levels/compartments of this societal model. Without going into the latter arguments, the digital constitutionalism approach might provide tools to address this and ensure that certain values are safeguarded at all levels of this new societal scheme.

[33] Regulation (EU) 2019/1150 of the European Parliament and of the Council of 20 June 2019 on promoting fairness and transparency for business users of online intermediation services (Text with EEA relevance), OJ L 186.

[34] While there are many provisions in this respect, it is particularly relevant Article 9.1 Platform-to-Business Regulation: 'Providers of online intermediation services shall include in their terms and conditions a description of the technical and contractual access, or absence thereof, of business users to any personal data or other data, or both, which business users or consumers provide for the use of the online intermediation services concerned or which are generated through the provision of those services.'

[35] Turning to the DSA, Article 12.1 can be highlighted: 'Providers of intermediary services shall include information on any restrictions that they impose in relation to the use of their service in respect of information provided by the recipients of the service, in their terms and conditions. That information shall include information on any policies, procedures, measures, and tools used for the purpose of content moderation, including algorithmic decision-making and human review. It shall be set out in clear and unambiguous language and shall be publicly available in an easily accessible format.'

[36] Edoardo Celeste, 'Terms of Service and Bills of Rights: New Mechanisms of Constitutionalisation in the Social Media Environment?' (2019) 33 International Review of Law, Computers & Technology 122.

implementations around personal information management systems to further allow data subjects to control, and understand how, their data can be used. [37] This is reasonable considering the previously mentioned emphasis around consent as a legal basis for allowing these further data processing activities.[38] Considering this, and to keep on disentangling the complex 'data/platform' economy to address how to make informed choices, we need to go down another level. This leads us to the sphere of data protection regulation and how transparency is approached in it.

4. Transparency in EU personal data protection rules

When turning specifically to data protection rules, such as the GDPR, transparency is a fundamental part of these regulations both as a principle and as part of many obligations. Enshrined in Article 5.1.a, transparency can be seen as one of the building blocks of the GDPR. While transparency is present in many different obligations, both in *ex-ante* and as *ex-post* modality,[39] its main related provisions can be identified in Arts. 12 through 14.[40]

While many scholars are currently focusing on the *ex-post* aspect of transparency, [41] particularly due to the regulatory and policy focus on AI for explaining automated decisions,[42] *ex-ante* still constitutes a substantial portion of the obligations provided in GDPR and many other jurisdictions. The basic premise upon which most data protection rules are built is that the data subject should be notified before any processing activity takes place or, if that was not possible, at the very first opportunity that occurs unless a reasonable and legally authorized reason allows for not disclosing the situation to the data subject.[43]

Traditionally, data controllers have complied with these obligations through privacy notices, also known as privacy policies. Despite their relevance as the main informative instrument on a particular data

[37] When it comes to personal data, the EU Data Strategy suggests that technological tools can help in making data flows more transparent. In this respect, and while still underdeveloped, the strategy aims at personal information management systems to help data subjects in understanding how their information is used ('In response to this, there are calls to give individuals the tools and means to decide at a granular level what is done with their data (by the MyData movement and others). This promises significant benefits to individuals, including to their health and wellness, better personal finances, reduced environmental footprint, hassle-free access to public and private services and greater oversight and transparency over their personal data. Those tools and means include consent management tools, personal information management apps, including fully decentralized solutions building on blockchain, as well as personal data cooperatives or trusts acting as novel neutral intermediaries in the personal data economy. Currently such tools are still in their infancy, although they have significant potential and need a supportive environment', see 'Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions: A European Strategy for Data' (n 12) 31–32.)

[38] This particular emphasis around consent can also be appreciated in the different regulatory instruments that emerged after the EU Data Strategy, such as the DMA and its Article 5 around consent and data aggregation/combination, the DGA and the role of data cooperatives to help data subjects in making informed decisions, or the Data Act and its own Article 5 when it comes to sharing data with third parties.

[39] Heike Felzmann and others, 'Transparency You Can Trust: Transparency Requirements for Artificial Intelligence between Legal Norms and Contextual Concerns' (2019) 6 Big Data & Society 2053951719860542.

[40] Radim Polčák, 'Article 12 Transparent Information, Communication and Modalities for the Exercise of the Rights of the Data Subject' in Christopher Kuner, Lee A Bygrave and Christopher Docksey (eds), *The EU General Data Protection Regulation (GDPR) A Commentary* (1st edn, Oxford University Press 2020); Gabriela Zanfir-Fortuna, 'Article 13 Information to Be Provided Where Personal Data Are Collected from the Data Subject' in Christopher Kuner, Lee A Bygrave and Christopher Docksey (eds), *The EU General Data Protection Regulation (GDPR) A Commentary* (1st edn, Oxford University Press 2020); Gabriela Zanfir-Fortuna, 'Article 14 Information to Be Provided Where Personal Data Have Not Been Obtained from the Data Subject' in Christopher Kuner, Lee A Bygrave and Christopher Docksey (eds), *The EU General Data Protection Regulation (GDPR) A Commentary* (1st edn, Oxford University Press 2020).

[41] Felzmann and others (n 43).

[42] See for example, Lilian Edwards and Michael Veale, 'Slave to the Algorithm? Why a "Right to an Explanation" Is Probably Not the Remedy You Are Looking for International' (2017) 16 Duke Law & Technology Review 18; Margot E Kaminski, 'The Right to Explanation, Explained' (2019) 34 Berkeley Technology Law Journal 189; Alexander J Wulf and Ognyan Seizov, '"Please Understand We Cannot Provide Further Information": Evaluating Content and Transparency of GDPR-Mandated AI Disclosures' [2022] AI & SOCIETY <https://doi.org/10.1007/s00146-022-01424-z> accessed 20 September 2022.

[43] For example, Arts. 13 and 14 provide for certain exemptions to the provision of the information but these should be applied in a restrictive manner not to compromise the data subjects' rights, particularly for those situations where the data subject's data has not been collected directly from it but rather from other sources.

processing activity,[44] their actual effectiveness is highly questionable. In their current form, this crucial and fundamental document for any personal data-related activity has been taken by lawyers as a compliance exercise to tick off the list of the information required by GDPR, mainly, Articles 13 and 14, or other applicable and relevant data protection regulation.

Despite being the first contributors to this, data controllers alone are not the sole culprits of this approach to privacy notices. National data protection agencies are on the frontline to ensure that these privacy notices are useful for data subjects. In this sense, a considerable number of decisions issued by them across Europe have mainly focused on whether the notice containing the information required by Articles 13 or 14, as applicable. While having the minimum information is a legal requirement, the disclosed details need to be fit for purpose. Also, the same authorities have not contributed in providing an innovative approach when putting out their privacy notices templates that incur the same defects as those developed by data controllers themselves. Nevertheless, some guidance and decisions from both data protection authorities and European authoritative bodies have tackled the flaws of this approach, namely the difficulty for data subjects to approach privacy notices, by suggesting alternative strategies to tackle how they present information to data subjects.[45]

However, the effective implementation of these approaches and tools remains the exception rather than the rule when it comes to drafting privacy notices. This has given rise to considerable criticism from both academia and data protection authorities. Among the most common critiques are:

- that they are far too long to be read by data subjects,[46]
- that they employ a too complex language,[47] and
- that the real meaningful information is too scattered across many documents to make any sense out of them,[48] among others.

Landmark decisions from national supervisory authorities, such as that involving WhatsApp Ireland,[49] have questioned the approach of merely providing more and more information to data subjects, as GDPR asks for concise information in an easy-to-read language, but also how such information is placed in the online environment. In other words, an abundance of information does not necessarily lead to a more well-informed data subject but rather it might lead to the quite opposite due to confusion on how to interpret that information if he/she is not already exhausted before trying to read the information and just clicking 'accept' to get through. On top of this, if the data protection-related information is located within a large set of information, for example, some terms of use or the signup contract for a service, this might affect the data subject's willingness to engage with that information.

5. Improving transparency with legal design: a dead-end road?

Despite these critics, these documents are here to stay unless this obligation is deleted from current and future data protection rules. And even before doing so, it is necessary to research alternatives that

[44] Joel R Reidenberg and others, 'Disagreeable Privacy Policies Mismatches between Meaning and Use' 30 Berkeley Technology Law Journal 39.

[45] 'Guidelines on Transparency under Regulation 2016/679' (Article 29 Working Party 2018) WP260 rev.01.

[46] Mcdonald and Cranor (n 1).

[47] For example, it is possible to mention the case of the social media application, Instagram, as a key example of an everyday application that incurs in this kind of behavior. See *Instagram Ireland* [2022] Data Protection Commission DPC Inquiry Reference: IN-20-7-4.

[48] On this point, we can mention the case of the communication application, WhatsApp, as a key example of an everyday application that incurs in this kind of behavior. See *WhatsApp Ireland Limited* [2021] Data Protection Commission DPC Inquiry Reference: IN-18-12-2.

[49] *WhatsApp Ireland Limited* (n 53). It is important to highlight that this decision from the Irish Data Protection Commissioner is currently being challenged before the CJEU. For further information on this, please see the following link: https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:62021TN0709&from=EN.

can provide the relevant information to decide whether this approach is necessary at all.[50] As of now, most of the research conducted has been focused on improving the notices to facilitate understanding of the data subject. In this respect, many solutions have been proposed. From privacy icons[51] to the use of labels[52] or privacy seals,[53] all these recipes are inspired by the application of legal design methods,[54] still put a considerable amount of effort on data subjects to understand what the privacy notice is saying without active involvement from the controller beyond the design and upload of the information.

While it is expected that the application of these different tools would facilitate the understanding of the notice, there are two critiques: on the one hand, trying to simplify complexity is not appropriate as, due to the emergence characteristic mentioned in the introduction, the aggregate aspects of the system poses properties that the mere summation does not,[55] i.e. data subjects would be missing crucial information to fully grasp how their data is used if just focused on a single data point or only taking into consideration a very circumscribed aspect. Also, lacking information on the potential consequences might influence the decision to be taken by the data subject. On the other hand, data subjects need to have sufficient knowledge to translate icons or labels into more rich information.

Layers, icons, and legal design techniques can help enormously in improving the current understanding of data protection situations, but it can be said of any 'obvious' situation where potential harm is at stake. For example, a radioactive sign (icon) in a powerplant can inform both technical -workers- and non-technical -visitors or administrative personnel- about potential risky areas, it does the job because the harm at hand is clear and understandable as well as the sign has seen widespread adoption. Turning to data protection, an icon that discloses a data transfer to the US might be quite clear as to the extent of the potential harms -for example, US intelligence agencies possibly getting access to the data- for the general population given the influence of the Snowden revelations but more intricated harms can be harder to grasp using icons. There is only so much that the data subjects can do with their limited resources -time and knowledge- in contrast to data controllers.

To top the situation, this framing assumes a fully capable and rational data subject, which is usually not the case. Using Malgieri's and Niklas's framework on data subjects' vulnerability, it is possible to argue that it comes in different shapes and sizes, being heavily context-dependent.[56] As such, these measures have a general design with an average data subject in mind, which is usually the case when engaging with data controllers for massive online services but reality might show that data subject are far from average. While data controllers can provide for more adjusted measures to the actual data subjects using their services, an individualized approach might not be possible without, at first, profile -by processing personal data- the individual into the relevant category.

In this sense, it is possible to wonder if these approaches are a continuation of existing defects when providing transparency on data processing activities rather than novel solutions. By no means does this intends to discredit those efforts as they are sufficiently grounded in both theoretical as well as empirical research. However, it would be reasonable to explore new paths to overcome the current issues around this principle/obligation more creatively, but also in a manner that does not further put pressure on data subjects.

---

[50] Ryan Calo, 'Against Notice Skepticism in Privacy (and Elsewhere)' (2011) 87 Notre Dame Law Review 1027.

[51] Arianna Rossi and Gabriele Lenzini, 'Which Properties Has an Icon? A Critical Discussion on Data Protection Iconography' in Thomas Groß and Theo Tryfonas (eds), *Socio-Technical Aspects in Security and Trust*, vol 11739 (Springer International Publishing 2021) <https://link.springer.com/10.1007/978-3-030-55958-8_12> accessed 16 June 2021.

[52] Joel R Reidenberg and others, 'Trustworthy Privacy Indicators: Grades, Labels, Certifications, and Dashboards' (2018) 96 Washington University Law Review 1409.

[53] Rowena Rodrigues and others, *EU Privacy Seals Project: Inventory and Analysis of Privacy Certification Schemes.* (Publications Office 2013) <http://dx.publications.europa.eu/10.2788/29861> accessed 20 December 2019.

[54] Ari Ezra Waldman, 'Privacy, Notice and Design' (2018) 21 Stanford Technology Law Review 74.

[55] Holland (n 7) 34.

[56] Gianclaudio Malgieri and Jędrzej Niklas, 'Vulnerable Data Subjects' (2020) 37 Computer Law & Security Review 105415.

Since the data subject is currently already overloaded with information and its capacity to decide could be compromised, the focus should be placed on what data controllers can do to help data subjects more proactively. Once data controllers set them up to their data disclosures, either a privacy notice, icons, etc., they do not make a single additional effort to inform the data subject as no further obligations are required from them. While it is true that their attention and efforts move towards other issues, such as ensuring that data subjects' rights are complied with, new users can be expected as well as questions over certain data processing activities might emerge in the future; this last issue is particularly relevant when consent is being used as legal basis due to the possibility of withdrawing it. Even more so as these data controllers, usually platforms or in a joint control scenario with platforms,[57] can have a complete and broader picture of the whole complex system rather than focusing on a single data operation.

As part of our theoretical framework, the aggregate parts of the 'data/platform' economy have a reciprocal influence on each other and, as such, it is reasonable to see how other regulatory frameworks influence data protection. Even without relying on this particular approach, authoritative bodies such as the EDPB have identified that different fields can influence the other; for example, regarding the particular issue of consent, when analyzing the interplay between different rules such as the GDPR and the Payment Services Directive 2, the EDPB has mentioned that consent from a contractual point of view is not the same as consent as a legal basis but the first can determine the aspect of the latter.[58] Picking up this example, from other available, is no coincidence. In the following sections it will be address how the (digital) financial services sector might have some alternatives to contemplate regarding novel manners in which we can seek to help data subjects in understanding the information on data processing activities.

6. Looking for inspiration elsewhere: the duty of assistance in financial services regulation

This particular field has long held a risk-based approach for its regulation while balancing market integrity, innovation, and rule simplicity.[59] On the other hand, GDPR is also moving towards a risk-based approach, particularly with the introduction of mechanisms such as data protection impact assessments.[60] Other authors have also looked into this sector for inspiration to tackle data-related challenges; in this sense, while Benthall and Viljoen seem to have given up on the notice and consent model and borrow categories from financial services regulation to tackle data markets just like their financial equivalents, [61] this particular set of rules can also help us to give a second chance to consent as a legal basis and, as a consequence, to improve transparency.

The criticism around privacy notices revolves around a common idea: complexity in the scope, in the language, or, even, in the location of the information. If data-intensive activities are getting more and more complex, then it is possible to expect that the size of these privacy notices would just keep on expanding accordingly. If we analyze how information is provided in this industry, we will find similar practices to data protection and, consequently, similar problems, as shown by recent research on digital

[57] *Fashion ID GmbH & CoKG v Verbraucherzentrale NRW eV* [2019] Court of Justice of the European Union (Second Chamber) C-40/17, ECLI:EU:C:2019:629.

[58] 'Guidelines on the Interplay of the Second Payment Services Directive and the GDPR' (European Data Protection Board 2020) Guidelines 6/2020.

[59] Chris Brummer and Yesha Yadav, 'Fintech and the Innovation Trilemma' (2019) 107 Georgetown Law Journal 235.

[60] Claudia Quelle, 'Enhancing Compliance under the General Data Protection Regulation: The Risky Upshot of the Accountability- and Risk-Based Approach' (2018) 9 European Journal of Risk Regulation 502.

[61] Sebastian Benthall and Salome Viljoen, 'Data Market Discipline: From Financial Regulation to Data Governance' (2021) 8 Journal of International and Comparative Law 459.

financial services.[62] In this regard, we can compare them to complex financial documents such as a prospectus of a publicly-traded company or even the credit sheet information when applying for a loan.

Certain rules have provided an alternative path to bridge this issue of understanding complex documents. In this sense, the financial services industry has developed an 'assist-your-customer' obligation to safeguard clients in certain scenarios when complex documents, such as prospectus or credit sheets, are involved in a decision-making process. This obligation is not equal across such a diverse and wide industry, as researched by legal scholars.[63] In this respect, rules such as MiFID II[64], the Crowdfunding Regulation,[65] the Consumer Credit Directive,[66] and the Mortgage Credit Directive,[67] just to name a few, have their version of it, as shown in Table 1 below.[68] Despite their differences, they share certain common objectives: preventing the exposure of a vulnerable individual to risk and, if the person can be exposed to such risk, help in making a decision based on complex information.

Table 1 – Summary of 'assist-your-customer' obligations in the EU financial services sector

Regulation	Assist-your-customer obligation	Beneficiary	Obliged entities and products covered	Assessed facts/materials
MIFID II	Suitability assessment	Clients	firms providing investment advice or portfolio management services on financial instruments and structured deposits	Knowledge and experience, financial situation, and investment objectives
	Appropriateness assessment		firms that provide 'execution-only services'	Knowledge and experience relevant to the specific type of product or service offered or demanded
IDD[69]	Suitability assessment	Customer (both retail and professional)	insurance undertakings and insurance intermediaries on insurance-based investment products	Knowledge and experience, financial situation, and investment objectives
	Appropriateness assessment		insurance undertakings and insurance intermediaries for non-advised sales of	Knowledge and experience relevant to the specific type of product or service offered or demanded

[62] James Suter and others, 'Behavioural Study on the Digitalisation of the Marketing and Distance Selling of Retail Financial Services' (European Commission 2019) <https://ec.europa.eu/info/sites/info/files/live_work_travel_in_the_eu/consumers/digitalisation_of_financial_services_-_main_report.pdf> accessed 6 May 2020.

[63] Danny Busch, Veerle Colaert and Geneviève Helleringer, 'An "assist-Your-Customer Obligation" for the Financial Sector?', *European Financial Regulation: Levelling the Cross-Sectoral Playing Field* (Bloomsbury Publishing 2019).

[64] Directive 2014/65/EU of the European Parliament and of the Council of 15 May 2014 on markets in financial instruments and amending Directive 2002/92/EC and Directive 2011/61/EU Text with EEA relevance, OJ L 173.

[65] Regulation (EU) 2020/1503 of the European Parliament and of the Council of 7 October 2020 on European crowdfunding service providers for business, and amending Regulation (EU) 2017/1129 and Directive (EU) 2019/1937 (Text with EEA relevance), OJ L 347.

[66] Directive 2008/48/EC of the European Parliament and of the Council of 23 April 2008 on credit agreements for consumers and repealing Council Directive 87/102/EEC, OJ L 133.

[67] Directive 2014/17/EU of the European Parliament and of the Council of 4 February 2014 on credit agreements for consumers relating to residential immovable property and amending Directives 2008/48/EC and 2013/36/EU and Regulation (EU) No 1093/2010 Text with EEA relevance, OJ L 60.

[68] The table is based on the work of Busch, Colaert and Helleringer mentioned in footnote 63 but updated with in force regulation as of the date hereof.

[69] Directive (EU) 2016/97 of the European Parliament and of the Council of 20 January 2016 on insurance distribution (recast)Text with EEA relevance OJ L 26, 2.2.2016, p. 19–59

Regulation	Assist-your-customer obligation	Beneficiary	Obliged entities and products covered	Assessed facts/materials
			insurance-based investment products	
	Demands and needs analysis		Insurance distributor for all insurance products	Customer's concrete demands and needs
PEPP Regulation[70]	Suitability assessment	PEPP savers	financial undertakings that advise PEPP savers on pan-European personal pension products	Knowledge and experience, financial situation, and investment objectives
	Demands and needs analysis			Customer's concrete demands and needs
Crowdfunding Regulation	Entry knowledge test	Non-sophisticated investor	crowdfunding services providers on admitted instruments for crowdfunding purposes	basic knowledge and understanding of risk in investing in general and in the types of investments offered on the crowdfunding platform
Consumer Credit Directive	Duty of assistance	Customer	Creditors and credit intermediaries	Customer's concrete needs and financial situation
	Responsible lending			Customer creditworthiness
Mortgage Credit Directive	Duty of assistance	Customer	Creditors and credit intermediaries	Customer's concrete needs, financial and personal situation, and preferences and objectives
	Responsible lending			Customer creditworthiness

From these rules, those related to loans from banks are particularly relevant for our analysis. As Busch, Colaert, and Helleringer mention, the purpose of the duty of assistance in this situation is to provide '(…) adequate explanations to the consumer in order to place the consumer in a position enabling him to assess whether (…) is adapted to his needs and to his financial situation'.[71] These explanations should be adapted to each customer as no situation is equal to another regarding both the person and its context.

What does this duty mean in practice? Because of a complex reality, a customer might suffer harm that it was made aware of but could not properly understand, such as exposure to overindebtedness or securities that have a higher level of default, particularly when the financial services have been digitalized.[72] As such, the entity that is putting the customer in front of such risk should help it out to assess the options, and their consequences, on the table and make a decision.

This duty is tailored to the category that is receiving the assistance. To do so, each instrument relies on different criteria to classify the client, from their knowledge and experience in the field to their financial situation or economic objectives, and even their risk profile or their ESG preferences, just to name a few. The whole purpose is to provide fit-for-purpose assistance when making sensible choices for that

[70] Regulation (EU) 2019/1238 of the European Parliament and of the Council of 20 June 2019 on a pan-European Personal Pension Product (PEPP) (Text with EEA relevance) PE/24/2019/REV/1 OJ L 198, 25.7.2019, p. 1–63

[71] Busch, Colaert and Helleringer (n 72).

[72] 'Consumer Risks in Fintech New Manifestations of Consumer Risks and Emerging Regulatory Approaches' (World Bank Group - Ministry of Foreign Affairs of the Netherlands 2021) Policy research paper <https://documents1.worldbank.org/curated/en/515771621921739154/pdf/Consumer-Risks-in-Fintech-New-Manifestations-of-Consumer-Risks-and-Emerging-Regulatory-Approaches-Policy-Research-Paper.pdf> accessed 2 June 2021.

person, or at least the category to which said person belongs. This can be done on an automated basis, as provided by each specific piece of regulation. If we make a comparison with the data economy, this would mean that data controllers should be able to guide data subjects in the choices imposed by this economic model: with whom, what, and how data should be shared.

7. Can the GDPR provide for a duty of assistance?

The duty of assistance in the financial service industry, particularly for the banking sector, has an interesting end objective embedded into it: fostering prudential lending and the avoidance of overindebtedness by clients.[73] Through this, it is acknowledged that banks play a fundamental role in managing both micro and macro risk levels: securing consumer protection and protecting the financial system. With its particularities from legal system to legal system, both these objectives can be associated with constitutionally protected objects. For example, dealing with this at a European level, consumer protection is enshrined in Article 38 of the Charter of Fundamental Rights of the European Union and the stability of the financial system is pursue in many provisions of the Treaty of the Functioning of the European Union.

If we have a look at GDPR, we can see that controllers, and to a lesser extent processors, have a duty to process personal data complying with it but also in due respect for fundamental rights, as noted by Celeste and De Gregorio.[74] Building on their understanding of GDPR's purpose, all of its provisions should, to a variable degree in each scenario, aim at securing a constitutionally protected object, i.e., fundamental rights. Using this lens, it is possible to argue that the transparency duties, particularly those related to ex-ante obligations, aim at preventing that poorly informed choices cause harm to constitutionally protected rights. In contrast to financial services where harm is more tangible as, for example, the person will lose money or have to pay more because of a bad decision and their right to property might be compromised, data-related harms might not be as clear as aforethought before accepting certain processing conditions. For example, a person might be willing to provide personal data to access a freemium streaming service,[75] and while it can be expected to receive marketing material as a general practice in this kind of business model, it can have not expected that the data would be used to predict and influence political opinion, as it has happened before with personal data protection scandals as Cambridge Analytica.

In this respect, and returning to the broader issue of transparency, we can argue that current practices can be seen as ‘compliant’ with GDPR, but it can be argued that these are not ‘compliant’ with the underlying constitutional principles that GDPR is called to safeguard. The whole purpose of GDPR is to guide processing activities in a manner that minimizes or prevents harm to fundamental rights, regardless of if it is the dignity of the data subject, their right to free assembly or its rights as a consumer. As such, 'throwing' a privacy notice to data subjects' faces cannot be considered a measure effective enough for this purpose, as demonstrated by research from scholars and decisions from supervisory authorities.

While Articles 13 and 14 of the GDPR indicate what information must be provided, it is not indicated how such information should be given beyond some very general rules stipulated in Article 12, i.e., '(…) the information shall be provided in writing, or by other means, including, where appropriate, by electronic means’. While the status quo has been for quite some time a privacy notice, and despite that

[73] Busch, Colaert and Helleringer (n 72).

[74] Edoardo Celeste and Giovanni De Gregorio, ‘Digital Humanism: The Constitutional Message of the GDPR’ (2022) 3 Global Privacy Law Review <https://kluwerlawonline.com/journalarticle/Global+Privacy+Law+Review/3.1/GPLR2022002> accessed 14 April 2022.

[75] While this is legally ‘correct’ under the Directive (EU) 2019/770 of the European Parliament and of The Council of 20 May 2019 on certain aspects concerning contracts for the supply of digital content and digital services (Text with EEA relevance), OJ L 136, the matter remains controversial (see for example Václav Janeček and Gianclaudio Malgieri, ‘Commerce in Data and the Dynamically Limited Alienability Rule’ (2020) 21 German Law Journal 924.).

both supervisory authorities[76] and legal scholars[77] take privacy notices for granted, this does not preclude the possibility of giving more personalized and specific information to the data subject. On the contrary, current practices on data protection transparency constitute a *de minimis* approach to transparency in general. As such, there is plenty of room for improvement in the way information on data processing is delivered to data subjects. Building up on Calo's work on notices, a more 'visceral' approach might be preferred to effectively convey information to the data subject;[78] in this respect, what more significant that the data controller breaking the so-called 'consent flow' and 'advising' the data subject on the actual risk?

Going back to Article 12, it should be used as guidance to provide grounding to this duty of assistance. If a privacy notice provides the information indicated in Articles 13 or 14, as appropriate, but fails to meet the criteria in Article 12 (concise, transparent, intelligible, and easily accessible form, using clear and plain language), then an appropriate measure to supply such deficiencies could be introducing a duty of assistance from the data controller.

Explanations are not unknown strangers to GDPR, particularly thanks to Article 22.[79] While the provision lacks any reference to an explanation, Recital 71 indicates that potential suitable measures to mitigate automated decisions would provide the data subject with an explanation. *An ex-post* explanation would not contain the same information as an ex-ante one, but the questions are open when it comes to how effective an ex-ante explanation can be to mitigate data subjects' hunger for understanding what is happening with their information.

8. Potential shortcomings and ways to address them

This approach is not free of potential shortcomings. In this respect, we can identify certain issues that could jeopardize its effective implementation, such as: (i) compromising the 'free' requirement of consent; (ii) the further stress placed on data controllers; and (iii) the actual commitment by data controllers.

Regarding the first issue at hand, if such a duty can be grounded in the GDPR as proposed, it is possible to address one of the most criticized topics in data protection: the use of consent as a legal basis.[80] By doing so, the relationship between data subjects and data controllers could change dramatically towards a more engaged interaction between the two to accommodate more data-intensive activities. In this respect, it is possible to envisage a more democratic and participatory model for governing personal data, without having to introduce radical changes as suggested.[81]

However, as data controllers engage in a more 'influential' manner over data subjects by helping them in making decisions, this begs the question of whether such consent, while properly informed, is truly free. This is related to the issue of nudges and whether a 'nudged' consent is a valid consent,[82] as the same can be said about the proposed 'assisted' consent. Transparency, again, might prove to be the

[76] 'Guidelines on Transparency under Regulation 2016/679' (n 50) para 3.

[77] Eleni Kosta, Ronald Leenes and Irene Kamara (eds), *Research Handbook on EU Data Protection Law* (Edward Elgar Publishing 2022) ch 20 <https://www.elgaronline.com/view/edcoll/9781800371675/9781800371675.xml> accessed 2 June 2022.

[78] Calo (n 57).

[79] Lee A Bygrave, 'Article 22. Automated Individual Decision-Making, Including Profiling' in Christopher Kuner, Lee A Bygrave and Christopher Docksey (eds), *The EU General Data Protection Regulation (GDPR) A Commentary* (1st edn, Oxford University Press 2020).

[80] Solove (n 4); Schermer, Custers and van der Hof (n 5); Custers, van der Hof and Schermer (n 27); Masooda Bashir and others, 'Online Privacy and Informed Consent: The Dilemma of Information Asymmetry' (2015) 52 Proceedings of the Association for Information Science and Technology 1.

[81] Salomé Viljoen, 'A Relational Theory of Data Governance' (2021) 131 The Yale Law Journal 573.

[82] Sheng Yin Soh, 'Privacy Nudges: An Alternative Regulatory Mechanism to Informed Consent for Online Data Protection Behaviour' (2019) 5 European Data Protection Law Review (EDPL) 65.

key distinguishing element between these two as data subjects are made aware of the assistance provided.

Moving on to the second potential critique, the widespread adoption of this duty would entail more 'compliance' work for data controllers. However, this argument can be countered with the following. When designing a data processing operation and how information should flow through the system, data controllers are bound by the principles outlined in GDPR. Among those, the data minimization becomes highly relevant. The only way to reduce the complexity is, simply put, to use fewer data. If less data is used or involved, the subsequent privacy notice should be more concise as fewer data processing activities would be taking place. Only when data is necessary, it should be sought out and used, therefore triggering at that stage the information obligation. This should be sufficient to knock off a considerable number of potential situations. For example, just like the duty of assistance does not apply to a single cash withdrawal from an ATM where the involved personal data points are not further used, this duty would not be extended to the underlying privacy notice for such data processing activity.

Building on the work of De Filippi, Mannan and Reijers,[83] the notions of trust and confidence play a crucial role to support the adoption of measures to improve the failings and shortcomings of one another. Picking up with our example, data subjects are confident that a simple cash withdrawal would not carry alongside its further data protection concerns that could result in potential harm. In this scenario, the simple privacy notice provided should be sufficient and we can sleep soundly under the blanket of the 'fallacy of understanding' the law at hand. However, lack of confidence in a system, particularly due to lack of understanding, makes data subjects reliant on their trust in data controllers. To boost such trust, the duty of assistance can bridge when confidence is not sufficient. Even if the data subjects' perception regarding the data controller's trustworthiness is low, the existence of the accountability principle can foster confidence in what the data controller will explain is relevant to reality.

The issue of trust and confidence is also relevant as it could influence whether data subjects would trust the advice provided by data controllers. In this respect, for example, the DGA has a provision aligned with my proposed duty of assistance but extremely limited to the so-called 'data cooperatives'.[84] Cooperatives have long held a close relationship with their members and it's reasonable for this kind of advice to them. However, the scope is limited, and, on the other hand, it requires data subjects to be part or delegate power to a cooperative, which again puts more stress on them to manage their data preferences. So, if such trust is lacking, then confidence -through regulation- could be an alternative to ensure that this proposed duty does not fall short.

To sum up the potential future reply to this comment, the duty of assistance should be used as a last resort effort when actual complex data processing operations are at hand that could have considerable harm to the data subjects. A misassignment of this duty can cause data controllers whose processing activities are straightforward to add another 'compliance' cost to their legal budget but also dilute its importance for data controllers engaged in risky activities, such as those subject to a data protection impact assessment. A proportionate approach would be much appreciated for this.

Finally, and related to the previous potential critique, data controllers can easily disregard this novel approach as there is no legal obligation to do so. However, the current decisions from European data protection agencies are highly critical of current transparency approaches,[85] as sanctions are steadily

[83] Primavera De Filippi, Morshed Mannan and Wessel Reijers, 'Blockchain as a Confidence Machine: The Problem of Trust & Challenges of Governance' (2020) 62 Technology in Society 101284.

[84] Article 2 Definitions For the purposes of this Regulation, the following definitions apply: (15) 'services of data cooperatives' means data intermediation services offered by an organisational structure constituted by data subjects, one-person undertakings or SMEs who are members of that structure, having as its main objectives to support its members in the exercise of their rights with respect to certain data, including with regard to making informed choices before they consent to data processing, to exchange views on data processing purposes and conditions that would best represent the interests of its members in relation to their data, and to negotiate terms and conditions for data processing on behalf of its members before giving permission to the processing of non-personal data or before they consent to the processing of personal data;

[85] Since the enter into force of GDPR, a substantial amount of decisions from supervisory authorities have been issued on this regard: *22bet.com - EDPBI:CY:OSS D:2019:72* [2019] Office of the Commissioner for Personal Data Protection

emerging and increasing. Data controllers would welcome this approach given the flexibility they have to implement given the accountability principle. Something as simple as a chatbot that explains privacy notice conditions could contribute enormously to improving current transparency practices.[86]

9. Conclusions and further work

This article has explored the possibility of developing a duty of assistance for data subjects within the context of European data protection regulations in a particular field, financial services, by expanding the scope of such a duty to also cover personal data protection issues. However, given that the expansion of this right is grounded in the GDPR, rather than in specific financial services rules, it is expected that this duty is further 'exported' into other areas and industries where GDPR is applicable. Considering that notice is a key component of other personal data protection regimes, it would be possible to applied it there, without even taking into consideration the direct consequences from the Brussels effect regarding GDPR to other jurisdictions [87]

As for the next steps in the research agenda for this right, it is necessary to further analyze the implications of this duty when it comes to consent. This is particularly relevant since if the assistance negates the consent's 'free' requirement, then it would make little sense for its implementation to overcome the shortcomings around consent. Nevertheless, it could prove to be effective when processing is based on another legal basis. However, given the central role that the EU digital strategy for the upcoming years has around consent, this path demands further exploration.

11.17.001.006.019; *Ajuntament de Tiana* [2021] Autoritat Catalana de Protecció de Dades PS 28/2021; *Allergie-Tagesklinik GmbH* [2018] Datenschutzbehörde DSB-D213.692/0001-DSB/2018; *Ayuntamento de ***localidad1* [2021] Agencia Española de Protección de Datos PS/00128/2020; *BBB* [2021] Agencia Española de Protección de Datos PS/00279/2020; *Banco Bilbao Vizcaya Argentaria, SA* Agencia Española de Protección de Datos Personales PS/00070/2019; *Caixabank, SA* Agencia Española de Protección de Datos PS/00477/2019; *Cerrajería Verín, SL* Agencia Española de Protección de Datos Personales PS/00265/2019; *Cerrajero Online, SL* Agencia Española de Protección de Datos Personales PS/00266/2019; *Deliberation of the Restricted Committee SAN-2019-001 of 21 January 2019 pronouncing a financial sanction against GOOGLE LLC* [2019] Commission nationale de l'informatique et des libertés SAN-2019-001 29; *Deliveroo Italy* Garante per la protezione dei dati personali 9685994; *EDPBI:FR:OSS D:2019:73* (Commission nationale de l'informatique et des libertés); *EDPBI:LV:OSS D:2019:79* [2019] Data State Inspectorate L-2-4.3/4627; *Federación de balonmano del Principado de Asturias* [2021] Agencia Española de Protección de Datos PS/00285/2020; *Fine against a natural person* (Autoritatea Națională de Supraveghere a Prelucrării Datelor cu Caracter Personal); *Furnishconcept* Agencia Española de Protección de Datos PS/00462/2019; *Jubel* [2019] Autorité de Protection des Données DOS-2019-01356; *Monsanto* [2021] Commission Nationale de l'Informatique et des Libertés SAN-2021-012; *Mymoviles Europa 2000, SL* Agencia Española de Protección de Datos Personales PS/00423/2019; *NAIH/2019/769/* (Nemzeti Adatvédelmi és Információszabadság Hatóság); *Plus Real Advertisment* [2021] Hellenic Data Protection Authority (Αρχή προστασίας δεδομένων προσωπικού χαρακτήρα) 57/2021; *Solo Embrague, SL* Agencia Española de Protección de Datos Personales PS/00469/2019; *Todotecnicos24H, SL* Agencia Española de Protección de Datos Personales PS/00268/2019; *WhatsApp Ireland Limited* (n 53).

[86] Sergio Guida, 'Privacy Policies between Perception and Learning through Legal Design: Ideas for an Educational Chatbot Combining Rights'awareness, Optimized User Experience and Training Efficacy.' (2021).

[87] Anu Bradford, *The Brussels Effect: How the European Union Rules the World* (Oxford University Press 2020).