

DOI: 10.47743/jss-2021-67-4-22

## Data Protection and Digital Services – European Union Perspectives

### Protecția datelor cu caracter personal și serviciile digitale – perspective ale Uniunii Europene

Andreea Șerban<sup>1</sup>, Cláudio Barbosa Teixeira<sup>2</sup>

**Abstract:** The EU is taking further steps towards the regulation of the digital space. Following on the adoption of the General Data Protection Regulation (GDPR), the European Commission now proposes two new regulation proposals aimed at regulating online markets and create a safer online environment, where the fundamental rights of users are protected: the Digital Services Act and the Digital Markets Act. However, it is still up for discussion how these proposals will articulate with GDPR provisions. In this study, we shall discuss the potential impact on data protection rules of the latest EU legislative push and how it intends to balance the new horizontal regulation for digital markets with already existing legislation, in particular on data protection.

**Keywords:** data protection; digital services; digital markets; online platforms; content moderation; GDPR; DSA; DMA

**Rezumat:** Uniunea Europeană face noi pași pentru reglementarea spațiului digital. În urma adoptării Regulamentului general privind protecția datelor (GDPR), Comisia Europeană lansează două noi propuneri de regulament care vizează reglementarea mediului online, Actul legislativ privind serviciile digitale și Actul legislativ privind piețele digitale, cu scopul de a crea un mediu online mai sigur, în care drepturile fundamentale ale utilizatorilor să fie protejate. Cu toate acestea, există în continuare dezbateri privind modul în care prevederile acestor regulamente vor fi coroborate cu GDPR. În prezentul studiu, vom urmări potențialul impact al noilor propuneri legislative europene asupra normelor privind protecția datelor cu caracter personal.

**Cuvinte-cheie:** protecția datelor; servicii digitale; platforme online; moderarea conținutului; GDPR; DSA; DMA

---

<sup>1</sup> PhD candidate, Faculty of Law, “Alexandru Ioan Cuza” University of Iași, Romania, e-mail: andreeaserban20@yahoo.com.

<sup>2</sup> Master in European Law (LL.M.), College of Europe (Bruges, Belgium), Master of Public International Law and European Law, Universidade de Coimbra (Coimbra, Portugal), e-mail: claudio.teixeira@coleurope.eu.

## 1. General considerations

The General Data Protection Regulation<sup>3</sup> (hereinafter, the GDPR) is a landmark in the evolution of the European privacy framework<sup>4</sup>, with a resounding global impact. The GDPR has definitely raised the bar for data protection legislations around the globe<sup>5</sup>, effectively setting the European Union (EU) legislation and the case-law of the Court of Justice of the European Union (CJEU) as a “global gold-standard”<sup>6</sup> for other jurisdictions<sup>7</sup>, with several international legislators, as well as private companies, following its lead<sup>8</sup>.

Nonetheless, the technological and digital revolution which is currently is taking place at an ever-accelerating rate is putting into evidence that the broad scope of the GDPR is starting to grow too broad to fully cover all potential situations where personal data is processed. As Purtova<sup>9</sup> puts it, as the material scope of the GDPR is “bound to expand even further and, as a result, to apply to an exponentially growing range of situations”, EU data protection law faces a real risk of becoming “the law of everything”, which is “meant to deliver the highest legal protection under all circumstances, but in practice impossible to comply”.

The GDPR guarantees the protection of personal data whenever the data is being processed, regardless of the format of the data. According to the regulation, data protection is about the rights and interests of individuals – data subjects – and

---

<sup>3</sup> Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation), [Online] at <https://eur-lex.europa.eu/eli/reg/2016/679/oj>, accessed at 10.11.2021.

<sup>4</sup> M. Goddard, *The EU General Data Protection Regulation (GDPR): European regulation that has a global impact*, in International Journal of Market Research Vol. 59, Issue 6, p.703, DOI: <https://doi.org/10.2501/IJMR-2017-050>.

<sup>5</sup> G. Buttarelli, *The EU GDPR as a clarion call for a new global digital gold standard*, 2016, p. 77-78.

<sup>6</sup> J.P. Albrecht, *How the GDPR will change the world*, in European Data Protection Law Review. 2, 2016, p. 287; W. Veil, *The GDPR: The Emperor's New Clothes-On the Structural Shortcomings of Both the Old and the New Data Protection Law*, in Neue Zeitschrift für Verwaltungsrecht 10.2018, pp. 686-696.

<sup>7</sup> J. Kessler, *Data Protection in the Wake of the GDPR: California's Solution for Protecting the World's Most Valuable Resource*, in Southern California Law Review, vol. 93:99, 2019, p. 99.

<sup>8</sup> This “domino-effect” showcases the “Brussels Effect”, how European standards become global standards not only due to mimicked legislation, but also the interest of private companies to comply with EU standards in order to access the Single Market, A. Bradford, *The Brussels Effect. How the European Union rules the world*. Oxford University Press, 2020.

<sup>9</sup> N. Purtova, *The law of everything. Broad concept of personal data and future of EU data protection law*, in Law, Innovation and Technology, 10:1, 40-81, p. 41. DOI: <https://doi.org/10.1080/17579961.2018.1452176>.

not about the data relating to them<sup>10</sup>. Article 4 para. (1) provides us with our definition for ‘*personal data*’: *any information relating to an identified or identifiable natural person*, while Article 4 para. (2) defines ‘*processing*’: *any operation or set of operations which is performed on personal data or on sets of personal data, whether or not by automated means, such as collection, recording, organisation, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction*. Therefore, any information can be considered personal data, provided that the processing of such data may refer to an identified or identifiable person. The European legislator distinguishes between personal data and non-personal data, the latter being the subject of *Regulation (EU) 2018/1807 on a framework for the free flow of non-personal data*<sup>11</sup> and defined, according to its article 3, para. (1) as “*data other than personal data as defined*” in the GDPR. Although the non-personal data regulation provides obligations which are mostly directed to the Member States, these are of relevance for the private sector as well, a reminder that data should not be perceived and observed through a tunnel-vision perspective.

Overall, the purpose of the GDPR is to establish the adequate legal framework for the processing of personal data and protecting the rights of individuals, by placing a burden of responsibility and accountability on the data processors while, simultaneously, ensuring the protection of the rights of data subjects under any circumstance, including potential situations which are not yet provided for by the GDPR, a future-proofing element given the continuous technological advancements and the absence of immediate legislative responses.

Just how sufficient is the GDPR and how successful has it been so far? In the GDPR third anniversary communication, the European Data Protection Supervisor (hereinafter, the EDPS) acknowledged that “the GDPR has been a sensational achievement for Europe and its citizens, acting as a lighthouse for the entire global policy-making scene and illuminating long-held privacy and data protection values enshrined across the horizon of the European legislative landscape. It has acted as a catalyst for many jurisdictions around the world to draft and implement their own privacy and data protection legislation”<sup>12</sup>.

The GDPR granted data protection authorities with extended competences to curb the unlawful data power and enforce privacy rules and the rule of law.

---

<sup>10</sup> P. Hustinx, *EU Data Protection Law: the Review of Directive 95/46/EC and the Proposed General Data Protection Regulation*, p. 1, [Online] at [https://edps.europa.eu/sites/default/files/publication/14-09-15\\_article\\_eui\\_en.pdf](https://edps.europa.eu/sites/default/files/publication/14-09-15_article_eui_en.pdf), accessed at 10.11.2021.

<sup>11</sup> Regulation (EU) 2018/1807 of the European Parliament and of the Council of 14 November 2018 on a framework for the free flow of non-personal data in the European Union, [Online] at <https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A32018R1807>, accessed at 10.11.2021.

<sup>12</sup> W. Wiewiorowski, *GDPR: a three-year old who must still learn to walk before it runs*, [Online] GDPR: a three-year-old who must still learn to walk before it runs | European Data Protection Supervisor (europa.eu), accessed at 10.11.2021.

Though, it is rather questionable just how far do the extended powers of national authorities go in enforcing GDPR. Such fears can be illustrated by the latest track record of Ireland, the Member State that hosts some of the biggest actors that process personal data in the EU<sup>13</sup>. The Irish Data Protection Commission (hereinafter, DPC) catches the attention of other GDPR enforcers, as the decisions by the DPC have the potential to set relevant precedents of practice and legal interpretation in this still-young field of practice. However, the most recent (leaked) draft decision on Facebook<sup>14</sup>, the DPC has set a questionable precedent, for several reasons: on the one side, at first sight, this decision that was shared with other EU data protection authorities potentially provides cover for a Facebook legal trick aimed at, essentially, *bypassing the GDPR*<sup>15</sup>. In the view of the DPC in its draft decision, “there is no obligation on Facebook to seek to rely solely on consent for the purposes of legitimizing personal data processing where it is offering a contract to a user which some users might assess as one that primarily concerns the processing of personal data”. Facebook can therefore simply choose to include the agreement on data processing in a contract which would make the GDPR requirements for consent not apply anymore. Yet, the authority suggests (only) a penalty of 28 to 36 million EUR as “Facebook ought to have been more transparent on this bypass”<sup>16</sup>.

Has the GDPR achieved its purpose? Should we consider the protection of the rights of the data subject in relation to the processing of their personal data, then indeed it has. The above-mentioned general framework ensures said protection in any potential situation of data processing. Given the direct effect of a EU regulation, directly and immediately enforceable in Member States, GDPR has achieved the quite visible purpose of setting standardized data protection rules across the EU and even realizing a secondary purpose of triggering an awareness movement that made inroads in educating the general population on their privacy and data rights. Indeed, when it comes to its impact on the private sector, the GDPR provided for considerable changes to the privacy protection by fostering compliance by private companies, from the necessity to review their strategy to reassessing their information systems and documentation in order to ensure compliance with the new provisions in order to freely trade with and within the Single Market<sup>17</sup>.

---

<sup>13</sup> For example, Twitter International Company, Facebook, Google and so on.

<sup>14</sup> See the draft decision published [Online] at [www.noyb.eu: https://noyb.eu/sites/default/files/2021-10/IN%2018-5-5%20Draft%20Decision%20of%20the%20IE%20SA.pdf](https://noyb.eu/sites/default/files/2021-10/IN%2018-5-5%20Draft%20Decision%20of%20the%20IE%20SA.pdf), accessed at 14.10.2021.

<sup>15</sup> Irish DPC greenlights Facebook's "GDPR bypass". *Irish DPC greenlights Facebook's "GDPR bypass". Schrems: "Decision undermines key element o GDPR"*, [Online] at <https://noyb.eu/en/irish-dpc-greenlights-facebooks-gdpr-bypass>, accessed at 14.10.2021.

<sup>16</sup> *Ibidem*.

<sup>17</sup> C. Tikkinen-Piri, A. Rohunen, J. Markkula, *EU General Data Protection Regulation: Changes and implications for personal data collecting companies*, in *Computer Law & Security Review*, Vol. 34, Issue, 1, February 2018, p. 134-153.

Yet is the GDPR the only go-to piece of legislation when it comes to the continuously improving technologies and their impact on the processes related to personal data? Definitely not. Just as the Directive 95/46<sup>18</sup>, the precursor of the GDPR, eventually ceased to adequately respond to the regulatory needs of a rapidly changing and evolving technological reality of constant technological developments, it is curious to observe that, almost two decades later, the GDPR starts to find itself in a similar situation. While the first act is a Directive, therefore leaving room for implementation by Member States, in its turn the GDPR is calling for additional legislative acts which will complement and provide a more in-depth framework, depending on the legislative needs correlated to the emerging technologies. For example, its broadened material scope and generalized – or rather stand-alone – provisions have raised more questions than provided answers; questions which have eventually been brought before the CJEU for further clarifications – one of the latest examples in this regard, the Schrems II decision<sup>19</sup>, indeed invalidated the European Commission’s Privacy Shield Decision<sup>20</sup>, determining a period of legislative gap in terms of transfers of personal data between the EU and the United States of America, and, later, the adoption of new sets of standard contractual clauses<sup>21</sup>.

We can therefore conclude thus far that the GDPR stands as a comprehensive legal framework, which covers multiple situations where personal data is processed. Nonetheless, it is not a catch-all legislation, with several shortcomings having been identified over its tenure in force. However, one of the most pressing concerns has become the challenge of online platform economy and processing and monetisation of data.

---

<sup>18</sup> Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data, [Online] at <https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex%3A31995L0046>, accessed at 14.10.2021.

<sup>19</sup> Judgement of the Court of 16 July 2020, in Case C-311/18, *Data Protection Commissioner v Facebook Ireland Ltd, Maximillian Schrems*.

<sup>20</sup> Commission Implementing Decision (EU) 2016/1250 of 12 July 2016 pursuant to Directive 95/46/EC of the European Parliament and of the Council on the adequacy of the protection provided by the EU-U.S. Privacy Shield, [Online] at [https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=uriserv%3AOJ.L\\_.2016.207.01.0001.01.ENG](https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=uriserv%3AOJ.L_.2016.207.01.0001.01.ENG), accessed at 14.10.2021.

<sup>21</sup> Commission Implementing Decision (EU) 2021/915 of 4 June 2021 on standard contractual clauses between controllers and processors under Article 28(7) of Regulation (EU) 2016/679 of the European Parliament and of the Council and Article 29(7) of Regulation (EU) 2018/1725 of the European Parliament and of the Council, [Online] at [https://eur-lex.europa.eu/eli/dec\\_impl/2021/915/oj](https://eur-lex.europa.eu/eli/dec_impl/2021/915/oj), accessed at 14.10.2021. Commission Implementing Decision (EU) 2021/914 of 4 June 2021 on standard contractual clauses for the transfer of personal data to third countries pursuant to Regulation (EU) 2016/679 of the European Parliament and of the Council, [Online] at [https://eur-lex.europa.eu/eli/dec\\_impl/2021/914/oj](https://eur-lex.europa.eu/eli/dec_impl/2021/914/oj), accessed at 14.10.2021.

## ***2. The challenge of online platform economy: data collection and monetization***

The GDPR was adopted at a time when it became more and more clear that personal data has become over the past decades “a critical source of innovation and value”, and the business boundaries<sup>22</sup> keep being redrawn. Personal data has become an extremely valuable commodity, as the online platform economy took off based on an advertised-based business model. Data provides relevant information to companies about people’s interests and activities, and thus offering a relevant basis for personalized advertising, but not only. The companies that provide services on the Internet are built on the economics of personal data<sup>23</sup>.

Personal data is now an economic asset – the identities and online behaviours of data subjects is traded in exchange for services and products of higher quality<sup>24</sup>. The monetization of personal data is a reality, and it has been identified as a relevant aspect of the new market for consumer’s data, given the fact that individuals have a broad access to digital services<sup>25</sup>. It provides an “advantage” to the consumers of the digital services, usually found in at least three forms: (1) “free” or discounted provision of online services – such as wifi access in public spaces by accepting the cookies and trackers and providing an email address in exchange of free Internet navigation; (2) “free” or discounted provision of (valuable) online content – such as access to music platforms that provide all kind of songs and music content, even if protected by copyright, for free, in exchange of the creation of a profile which contains personal data such as email address and, in certain cases, the profile used on other social media platforms; (3) “free” or discounted provision of an “offline” service – such as insurance<sup>26</sup>.

---

<sup>22</sup> World Economic Forum, *Personal Data: the emergence of a new asset class*, January 2011, [Online] at [https://www3.weforum.org/docs/WEF\\_ITTC\\_PersonalDataNewAsset\\_Report\\_2011.pdf](https://www3.weforum.org/docs/WEF_ITTC_PersonalDataNewAsset_Report_2011.pdf), accessed at 20.11.2021.

<sup>23</sup> A. Esteve, *The business of personal data: Google, Facebook, and privacy issues in the EU and the USA*, in *International Data Privacy Law*, 2017, Vol. 7, no. 1, p. 36.

<sup>24</sup> C. Liem, G. Petropoulos, *The economic value of personal data for online platforms, firms and consumers*, blog post, January 2016, [Online] *The economic value of personal data for online platforms, firms and consumers* | Bruegel, accessed at 20.11.2021.

<sup>25</sup> “Different platforms collect and monetize data in various ways: either through a direct subscription model (e.g. Spotify)—by using collected data to tailor products directly to users (e.g. Amazon)—or by selling targeted ads (e.g. Facebook and Google Search). Most zero-price ad-based platforms use the latter business model, enabling them to establish market power in the complementary positive-price digital advertising market.” B. Kira, V. Sinha, S. Srinivasan, *Regulating digital ecosystems: bridging the gap between competition policy and data protection*, *Industrial and Corporate Change*, in *Industrial and Corporate Changes*, 2021, 00, 1-24, DOI: <https://doi.org/10.1093/icc/dtab053>.

<sup>26</sup> G. Malgieri, B. Custers, *Pricing privacy: the right to know the value of your personal data*, in *Computer Law & Security Review*, 2017, p. 5-6.

*Directive (EU) 2019/770 on contracts for the supply of digital content and digital services*<sup>27</sup> acknowledged that, in the modern digital economy, personal data can be used as payment for digital content, instead of money. Its recital 24 states that “digital content or digital services are often supplied also where the consumer does not pay a price but provides personal data to the trader. Such business models are used in different forms in a considerable part of the market”. It further stipulates that “while fully recognizing that the protection of personal data is a fundamental right and that therefore personal data cannot be considered as a commodity, this Directive should ensure that consumers are, in the context of such business models, entitled to contractual remedies”. In its article 3 para. (1), the Directive states that it applies “to any contract where the trader supplies or undertakes to supply digital content or a digital service to the consumer and the consumer pays or undertakes to pay a price”, including when “the trader supplies or undertakes to supply digital content or a digital service to the consumer, and the consumer provides or undertakes to provide personal data to the trader”, with the exception where “the personal data provided by the consumer are exclusively processed by the trader for the purpose of supplying the digital content or digital service in accordance with this Directive or for allowing the trader to comply with legal requirements to which the trader is subject, and the trader does not process those data for any other purpose”. Although the price, for the purposes of this Directive, is defined in art. 1 (7) as “money or a digital representation of value that is due in exchange for the supply of digital content or a digital service” and personal data is understood as it is defined by the GDPR, the conclusion is that the equation of personal data in exchange for “free” digital content has the same result as the one regarding money in exchange for paid digital content, which is the provision of digital services to consumer, such as provision of access to the consumer of digital content.

The discussion on privacy and data protection has opened a veritable *Pandora’s Box*. The GDPR is a legislative instrument that protects personal data, although it remains insufficient to cover all aspects of the processing of data, given this being an on-going learning process, constantly adapting to the development of technologies and digital realities. Any type of data, either personal or non-personal, is tradable<sup>28</sup> and the data market is ever growing. The digital space provides the environment for experimenting with situations and outcomes of data processing which must be addressed by the legislator to provide a legal basis to the upcoming realities.

From the identified GDPR shortcomings, given the rapidly evolving technological landscape, the most pressing for EU legislators at this moment seems to be the need to provide adequate protection of the data subject in relation to their

---

<sup>27</sup> 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, [Online] at [https://eur-lex.europa.eu/legal-content/en/ALL/?uri=CELEX: 32019L0770/](https://eur-lex.europa.eu/legal-content/en/ALL/?uri=CELEX:32019L0770), accessed at 20.11.2021.

<sup>28</sup> For further detailing of the trade with data, see C.T Ungureanu, *Drept international privat european in raporturi de comert international*, Hamangiu, 2021, pp. 117-125.

personal data on the Internet, where any information relates to a person in the sense of EU data protection law. At a time when the online platform economy processes and monetises data in exchange of providing digital services, which are highly optimised to benefit advertising-driven business models relying, in turn, on advanced data analytics and data-driven decision-making systems, the challenge of the increase of targeted profiling and automated decision-making techniques which depend on the processing of personal data, mostly obtained via applications of extremely intrusive nature<sup>29</sup>, requires an adequate and complementary response from the European legislator. The response of the current European legislative agenda so far? The Digital Services Act package.

### ***3. The Digital Services Act package***

In December 2020, as a part of the Digital Services legislative package, the European Commission presented two new legislative proposals<sup>30</sup>, the Digital Services Act (DSA) and the Digital Markets Act (DMA), new *ex ante* horizontal legislation to govern digital services “applicable across the whole EU to create a safer and more open digital space”. The legislative procedure on these proposals is still ongoing therefore our analysis will naturally focus on the original proposal<sup>31</sup>.

In general terms, the proposals bear a strong influence from the GDPR and share elements in common<sup>32</sup>. While the GDPR has laid down the main principles of transparency, fairness and lawfulness, which apply to all kinds of personal data processing activities - including online platforms – the DSA and DMA proposals bring their added value to the table by elaborating on these principles while introducing a specific regulatory framework for digital platforms. Therefore, the interplay between GDPR, on the one hand, and the DSA and DMA proposals, on the other hand, is of extreme importance to ensure effective complementarity of the data protection rules.

---

<sup>29</sup> S. Hännö, *Profiling and Automated Decision-Making: Legal Implications and Shortcomings*, in M. Corrales, M. Fenwick, N. Forgó, (eds) *Robotics, AI and the Future of Law in Perspectives in Law, Business and Innovation*, Springer, Singapore, [https://doi.org/10.1007/978-981-13-2874-9\\_6](https://doi.org/10.1007/978-981-13-2874-9_6).

<sup>30</sup> The DSA and DMA are still draft proposals by the European Commission which, at the time of this article, are still under discussion by the EU co-legislators, the European Parliament and the Council of the EU, whose position is awaited until the end of year of 2021, with interinstitutional negotiations aimed at achieving a final agreement expected to take place in early 2022.

<sup>31</sup> See European Commission, *The Digital Services Act package*, [Online] at <https://digital-strategy.ec.europa.eu/en/policies/digital-services-act-package>, accessed at 15.11.2021.

<sup>32</sup> A. Gascón Macén, *El Reglamento General de Protección de Datos como modelo de las recientes propuestas de legislación digital europea*, Cuadernos de Derecho Transnacional, 13(2), 209-232, <https://doi.org/10.20318/cdt.2021.6256>.



The Commission clarified on both proposals that the future regulations will complement of data protection rules “without prejudice of their application”<sup>33</sup>, namely GDPR and the E-Privacy Directive (Directive 2002/58/EC)<sup>34</sup>. The fact that the proposal seeks to complement, rather than to replace the GDPR, was welcomed by the European Data Protection Supervisor (EDPS), having considered that, in the context of the online platform economy, “competition, consumer protection and data protection law are three inextricably linked policy areas”<sup>35</sup>, that should have a relationship of complementarity and not of overlapping, “where one area replaces or enters into friction with another”<sup>36</sup>.

#### ***4. Brief considerations on the Digital Services Act proposal***

##### **4.1. Context**

The DSA proposal lays down rules and obligations for intermediary service providers, including platforms and hosting services<sup>37</sup> (i.e., online marketplaces, social networks, app stores, content-sharing, travel, and accommodation platforms), having a special focus on protecting users from illegal activities online and increase transparency for online platforms. More importantly, “very large online platforms” (VLOPs)<sup>38</sup>, will have additional obligations: thresholds for designation as a VLOP and falling under such additional obligations is currently estimated as serving more than 45 million service recipients within the EU. This threshold should be adjusted by the Commission so that it consistently corresponds to 10% of the EU population<sup>39</sup>.

---

<sup>33</sup> Article 1 (5), recitals 9 to 11, of the DSA proposal; recital 11 of the DMA proposal.

<sup>34</sup> Directive 2002/58/EC of the European Parliament and of the Council of 12 July 2002 concerning the processing of personal data and the protection of privacy in the electronic communications sector (Directive on privacy and electronic communications), [Online] at <https://eur-lex.europa.eu/legal-content/EN/ALL/?uri=CELEX%3A32002L0058>, accessed at 15.11.2021.

<sup>35</sup> *Preliminary Opinion of the European Data Protection Supervisor Privacy and competitiveness in the age of big data: The interplay between data protection, competition law and consumer protection in the Digital Economy*, March 2014, [Online] at [https://edps.europa.eu/sites/edp/files/publication/14-03-26\\_competition\\_law\\_big\\_data\\_en.pdf](https://edps.europa.eu/sites/edp/files/publication/14-03-26_competition_law_big_data_en.pdf), accessed at 15.11.2021.

<sup>36</sup> European Data Protection Supervisor, Opinion 1/2021, on the Proposal for a Digital Services Act, p. 3, [Online] at [https://edps.europa.eu/system/files/2021-02/21-02-10-opinion\\_on\\_digital\\_markets\\_act\\_en.pdf](https://edps.europa.eu/system/files/2021-02/21-02-10-opinion_on_digital_markets_act_en.pdf), accessed at 15.11.2021.

<sup>37</sup> Proposal of the European Parliament and of the Council on a Single Market for Digital Services (Digital Services Act) and amending Directive 2000/31/EC, [Online] at <https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:52020PC0825&from=en>, accessed at 15.11.2021.

<sup>38</sup> Such as the commonly known “Big Four” or GAFA: Google, Apple, Facebook, Amazon.

<sup>39</sup> Proposal of the European Parliament and of the Council on a Single Market for Digital Services (Digital Services Act) and amending Directive 2000/31/EC, [Online] at <https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:52020PC0825&from=en>, accessed at 15.11.2021.

In its Opinion 1/2021, the EDPS confirmed that the DSA proposal “will clearly have an impact on processing of personal data”, considering it “necessary to ensure complementarity in the supervision and oversight” of platforms and other providers. Moreover, given the “already endemic monitoring of individuals’ behavior, in particular on online platforms”<sup>40</sup>, the supervisor recognised that “certain activities in the context of online platforms present increasing risks not only for the rights of individuals, but for society as a whole”<sup>41</sup>.

#### 4.2. Online advertising, recommender systems

And what are said risks? In the context of “surveillance capitalism”<sup>42</sup>, the advertising industry provides the major incentive towards the collection and selling of personal data. The increase of profiling and automated decision-making techniques which depend on the processing of personal data can lead to the uncontrolled spread of illegal content, harmful content (such as disinformation), discrimination and privacy violations<sup>43</sup>. Regulators are starting to catch-up to the need to address the issue: recently, the United Kingdom’s Competition and Markets Authority (CMA) has called for a “right not to be profiled”, or the “choice requirement”<sup>44</sup>.

The EDPS has equally revealed its concern on its Opinion on the DSA proposal, where it concluded that, in order to ensure complementarity with the GDPR, the proposal requires additional safeguards, making specific recommendations against profiling and tracking on content moderation, online targeted advertising (articles 24 and 30) and recommender systems (article 29)<sup>45</sup>.

Regarding online advertising, the supervisor comes out in support a future ban on targeted tracking-based advertising, asking for a “phase-out leading to a prohibition of targeted advertising on the basis of pervasive tracking” and for stricter regulation “in favour of less intrusive forms of advertising that do not

---

[lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:52020PC0825&from=en](https://lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:52020PC0825&from=en), accessed at 15.11.2021.

<sup>40</sup> European Data Protection Supervisor, Opinion 1/2021, on the Proposal for a Digital Services Act, p. 13

<sup>41</sup> *Idem*, p. 3.

<sup>42</sup> S. Zuboff, *The Age of Surveillance Capitalism: The Fight for a Human Future at the New Frontier of Power*, 2019.

<sup>43</sup> S. Hänold, *Profiling and Automated Decision-Making: Legal Implications and Shortcomings*, in M. Corrales, M. Fenwick, N. Forgó, (eds) *Robotics, AI and the Future of Law in Perspectives in Law, Business and Innovation*. Springer, Singapore, [https://doi.org/10.1007/978-981-13-2874-9\\_6](https://doi.org/10.1007/978-981-13-2874-9_6).

<sup>44</sup> Competition and Markets Authority (CMA), United Kingdom, *Online platforms and digital advertising*, July 2020, 8.90, p. 379, [Online] at [https://assets.publishing.service.gov.uk/media/5efc57ed3a6f4023d242ed56/Final\\_report\\_1\\_July\\_2020\\_.pdf](https://assets.publishing.service.gov.uk/media/5efc57ed3a6f4023d242ed56/Final_report_1_July_2020_.pdf), accessed at 15.11.2021.

<sup>45</sup> European Data Protection Supervisor, Opinion 1/2021, on the Proposal for a Digital Services Act, p. 3.

require any tracking of user interaction with content”<sup>46</sup>. In addition, it recalled the risks of profiling and micro-targeting in the context of recommender systems<sup>47</sup>, noting that article 29 para. (1) of the DSA proposal should comply with the requirements of data protection by design and by default set out in Article 25, GDPR: recommender systems should by default not be based on “profiling”, as defined in Article 4 para. (4) GDPR. Article 29 para. (1) of the DSA proposal should therefore provide for an opt-in, instead of an opt-out on profiling.

In summary, the EDPS has stated that transparency measures alone will not sufficiently address the risks posed by targeted tracking-based advertising; non-profiling by default should therefore be the default option for legislators, by prohibiting surveillance advertising and profiling-based recommender systems.

### 4.3. Supervision and enforcement

One of the main identified shortcomings of the application of EU data protection rules is their enforcement. The experience of GDPR enforcement has put into questioning the efficiency of the one-stop-shop approach and the “country-of-origin principle”, where supervision and enforcement powers first rely with national regulatory authorities of Member States where the companies are established. Given that most of the major technological companies covered by the scope of this legislation finds its headquarters in only a limited number of Member States, such as Ireland or Luxembourg, cross-border enforcement bottlenecks remain a significant challenge: in Ireland, the Irish Civil Liberties Council (ICCL) has revealed that about 98% of major GDPR cases referred to the Irish Data Protection Commission (DPC) remain unresolved<sup>48</sup>.

Justice delayed is justice denied<sup>49</sup>. Should the new legislation aim to adequately complement GDPR, it would go a long way in addressing enforcement bottlenecks. However, the DSA proposal maintains the preference for the “country-

---

<sup>46</sup> European Parliament resolution of 20 October 2020 with recommendations to the Commission on the Digital Services Act: Improving the functioning of the Single Market, P9\_TA(2020)0272, [Online] at [https://www.europarl.europa.eu/doceo/document/TA-9-2020-0272\\_EN.pdf](https://www.europarl.europa.eu/doceo/document/TA-9-2020-0272_EN.pdf), accessed at 15.11.2021.

<sup>47</sup> See European Data Protection Supervisor, “Opinion 3/2018 EDPS Opinion on online manipulation and personal data”, 19 March 2018, p. 9, [https://edps.europa.eu/sites/edp/files/publication/18-03-19\\_online\\_manipulation\\_en.pdf](https://edps.europa.eu/sites/edp/files/publication/18-03-19_online_manipulation_en.pdf) (“Manipulation also takes the form of microtargeted, managed content display which is presented as being most ‘relevant’ for the individual but which is determined in order to maximize revenue for the platform. This is akin to the ‘secret menus’ used to steer users of ecommerce sites and the ‘dark patterns’ used to dissuade decisions less desirable from the platform’s perspective (such as declining to add additional items, like insurance, to a shopping cart”).

<sup>48</sup> Irish Civil Liberties Council, 2021 report on the enforcement capacity of data protection authorities, [Online] at <https://www.iccl.ie/news/2021-gdpr-report/>, accessed at 15.11.2021..

<sup>49</sup> N. Burstyn, T. Sourdin, *Justice Delayed is Justice Denied*, in Victoria University Law and Justice Journal, 4(1), October 2014, DOI: <https://doi.org/10.15209/vulj.v4i1.61>.

of-origin principle”<sup>50</sup>, thus sharing a similar enforcement model with GDPR and raising pertinent questions whether enforcement issues will remain.

### **5. Brief considerations on the Digital Markets Act proposal**

Personal data is a source of market power: this data-driven advantage of large platforms derives from their access, collection and monetisation of users’ personal data on an industrial scale, from all kinds of sources and backgrounds<sup>51</sup>. Moreover, this advantage amounts to market entry barriers for entry-level competitors, as large online platforms that play a systemic role in the market become entrenched.

To ensure digital markets are fairer and more contestable, the DMA proposal sets out *ex ante* horizontal rules, creating obligations for the designated “gatekeepers”<sup>52</sup>: a new definition which applies to large online platforms, with a strong economic position with significant market impact, a strong intermediation position or an entrenched and durable position in the market<sup>53</sup>. The DMA in the proposed form sets out provisions concerning the designation of gatekeepers of the service provider while providing the core platform services as well as other digital services.

In its current form, the DMA may affect the following eight categories of core platform service: (1) social media networks, (2) search engines, (3) video platforms, (4) communication services, (5) intermediation services, (6) cloud computing services, (7) operating systems, and (8) advertising networks that operate alongside any of the above. To qualify as gatekeeper, the following criteria is considered: (1) 45 million monthly users (around 10% of the EU population), (2) global turnover of or exceeding 6,5 billion EUR, and (3) operations in at least 3 of the 27 EU Member States, according to Article 3 of the DMA proposal. The criteria for designation of these “gatekeepers” has been called out<sup>54</sup> for their legal certainty and accountability, as well as proportionality issues that are raising in their current form.

While the GDPR has met shortcomings when addressing the importance of data for competition, the proposal on DMA attempts to respond to this issue: gatekeepers may not combine personal data from different sources, and the DMA

---

<sup>50</sup> Article 40, Proposal on Digital Services Act (DSA)

<sup>51</sup> B. Kira, V. Sinha, S. Srinivasan, *Regulating digital ecosystems: bridging the gap between competition policy and data protection, Industrial and Corporate Change*, in *Industrial and Corporate Changes*, 2021, 00, 1-24, <https://doi.org/10.1093/icc/dtab053>.

<sup>52</sup> Proposal for a Regulation of the European Parliament and of the Council on contestable and fair markets in the digital sector (Digital Markets Act) (DMA), Article 5, [Online] at <https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:52020PC0842&from=en>, accessed at 15.11.2021.

<sup>53</sup> DMA proposal, Explanatory Memorandum, p. 1, [Online] at <https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:52020PC0842&from=en>, accessed at 15.11.2021.

<sup>54</sup> Digital Europe, *Digital Markets Act position paper*, [Online] at <https://www.digitaleurope.org/resources/digital-markets-act-position-paper/>, accessed at 29.11.2021.

may offer real-time data portability to both business and individuals-users of the platforms, real-time data access to business users, and personalized search engine data<sup>55</sup>. The DMA thus reinforces the GDPR and complements it at competition level.

In its Opinion 2/2021<sup>56</sup>, the EDPS also provided specific recommendations for the DMA proposal to effectively complements the GDPR. For example, it recommended specifying in Article 5(a) of the DMA proposal that the “gatekeeper shall provide end-users with a solution of easy and prompt accessibility for consent management”; clarifying the scope of the data portability envisaged in the DMA proposal.

### ***Final considerations***

The DMA and DSA have met a generally welcoming view from the EU Member States so far, as well as, for example, the European Data Protection Supervisor as mentioned above, though, being still in the draft form, it raises some questionable provisions that could be considered either too vague or in need of rewriting and amending.

Given the fact that they are still subject to discussions at the EU institutions level and the civil society organizations are advocating for clearer provisions, it is to be expected that the final form of the two proposals, if adopted, to be modified at least partially. Nonetheless, the discussion provided by the DMA and DSA proposals is welcome as it complements the privacy and data protection activity undertaken at the European level and beyond.

The GDPR alone, as shown, has blind spots that only specifically tailored legislation could clarify the situations raised in practice. The final agreed versions of the above-discussed legislative proposals should either provide these answers or raise even more questions.

### **Reference list**

- Albrecht J. P., *How the GDPR will change the world*, in European Data Protection Law Review. 2, 2016, DOI: <https://doi.org/10.21552/EDPL%2F2016%2F3%2F4>
- Blankerts A., Jaurisch J., *What the European DSA and DMA proposals mean for online platforms*, January 2021
- Bradford A., *The Brussels Effect. How the European Union rules the world*, Oxford University Press, 2020
- Burstyner N., Sourdin T., *Justice Delayed is Justice Denied*, in Victoria University Law and Justice Journal, 4(1), October 2014, DOI: <https://doi.org/10.15209/vulj.v4i1.61>
- Buttarelli G., *The EU GDPR as a clarion call for a new global digital gold standard*, 2016

---

<sup>55</sup> A. Blankerts, J. Jaurisch, *What the European DSA and DMA proposals mean for online platforms*, January 2021, [Online] at <https://www.brookings.edu/techstream/what-the-european-dsa-and-dma-proposals-mean-for-online-platforms/>, accessed at 29.11.2021.

<sup>56</sup> European Data Protection Supervisor, Opinion 2/2021 on the Proposal for a Digital Markets Act, [Online] at [https://edps.europa.eu/system/files/2021-02/21-02-10-opinion\\_on\\_digital\\_markets\\_act\\_en.pdf](https://edps.europa.eu/system/files/2021-02/21-02-10-opinion_on_digital_markets_act_en.pdf), accessed at 29.11.2021.

- Esteve A., *The business of personal data: Google, Facebook, and privacy issues in the EU and the USA*, in *International Data Privacy Law*, 2017, Vol. 7, no. 1, DOI: <https://doi.org/10.1093/IDPL%2FIPW026>
- Gascón Macén A., *El Reglamento General de Protección de Datos como modelo de las recientes propuestas de legislación digital europea*, *Cuadernos de Derecho Transnacional*, 13(2), DOI: <https://doi.org/10.20318/cdt.2021.6256>
- Goddard M., *The EU General Data Protection Regulation (GDPR): European regulation that has a global impact*, in *International Journal of Market Research* Vol. 59, Issue 6, DOI: <https://doi.org/10.2501%2FIJMR-2017-050>
- Hånold S., *Profiling and Automated Decision-Making: Legal Implications and Shortcomings*, in M. Corrales, M. Fenwick, N. Forgó, (eds) *Robotics, AI and the Future of Law in Perspectives in Law, Business and Innovation*, Springer, Singapore
- Hustinx P., *EU Data Protection Law: the Review of Directive 95/46/EC and the Proposed General Data Protection Regulation*
- Kessler J., *Data Protection in the Wake of the GDPR: California's Solution for Protecting the World's Most Valuable Resource*, in *Southern California Law Review*, vol. 93:99, 2019
- Kira B., Sinha V., Srinivasan S., *Regulating digital ecosystems: bridging the gap between competition policy and data protection*, *Industrial and Corporate Change*, in *Industrial and Corporate Changes*, 2021, 00, 1-24
- Liem C., Petropoulos G., *The economic value of personal data for online platforms, firms and consumers*, blog post, January 2016
- Malgieri G., Custers B., *Pricing privacy: the right to know the value of your personal data*, in *Computer Law & Security Review*, 2017
- Purtova N., *The law of everything. Broad concept of personal data and future of EU data protection law*, in *Law, Innovation and Technology*, 10:1, 40-81, DOI: <https://doi.org/10.1080/17579961.2018.1452176>
- Tikkinen-Piri C., Rohunen A., Markkula J., *EU General Data Protection Regulation: Changes and implications for personal data collecting companies*, in *Computer Law & Security Review*, Vol. 34, Issue, 1, February 2018, DOI: <https://doi.org/10.1016/J.CLSR.2017.05.015>
- Ungureanu C.T., *Drept international privat european in raporturi de comert international*, Hamangiu, 2021
- Veil W., *The GDPR: The Emperor's New Clothes-On the Structural Shortcomings of Both the Old and the New Data Protection Law*, in *Neue Zeitschrift für Verwaltungsrecht* 10.2018
- Wiewiorowski W., *GDPR: a three-year old who must still learn to walk before it runs*
- Zuboff S., *The Age of Surveillance Capitalism: The Fight for a Human Future at the New Frontier of Power*, 2019