The CDSL Working Paper Series

WP8/2024

CYBER & DATA SECURITY LAB

Five years after 2018, the annus mirabilis for EU data protection: Where we stand and the outlook ahead

Vagelis Papakonstantinou

Abstract

The law has an ambivalent relationship with the future. It is not only that it is hard to make predictions, especially about the future, but also that a single word (in the future) by the lawmaker can quickly make years of law implementation (and relevant case law and legal theory) obsolete. Notwithstanding incertitude, however, path dependence ("the tendency of institutions or technologies to become committed to develop in certain ways as a result of their structural properties or their beliefs and values") perhaps helps make predictions a bit less hopeless. It is around these thoughts, and concerns, that the analysis that follows unfolds. Five years have passed after 2018, the annus mirabilis for EU data protection when both the GDPR and the LED became effective, and this anniversary invites a retrospective assessment and a, modest, attempt to look into the future.

Table of Contents

1.Introduction

The law has an ambivalent relationship with the future. It is not only that it is hard to make predictions, especially about the future,[1] but also that a single word (in the future) by the lawmaker can quickly make years of law implementation (and relevant case law and legal theory) obsolete. Notwithstanding incertitude, however, path dependence ("the tendency of institutions or technologies to become committed to develop in certain ways as a result of their structural properties or their beliefs and values")[2] perhaps helps make predictions a bit less hopeless.

On the other hand, if beauty is in the eyes of the beholder, same is frequently the case with public interest. Particularly experts suffer often from tunnel vision, whereby they imagine that whatever they themselves find interesting and relevant each time must also interest other experts in their field or, even, the wider public. When expectations, as is often the case, fail in practice, these same experts become exasperated and put the blame on others instead of their own lack of helicopter view.

It is around these thoughts, and concerns, that the analysis that follows unfolds. Five years have passed after 2018, the *annus mirabilis* for EU data protection when both the GDPR[3] and the LED[4] became effective,[5] and this anniversary

[1] Niels Bohr, Bulletin of the Atomic Scientists, Vol. 27, 1971.
[2] Ian Greener, Path Dependence, Encyclopedia Britannica, 9 January 2019, available at https://www.britannica.com/topic/path-dependence, accessed 21 December 2023.
[3] 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), OJ L 119, 4.5.2016.
[4] Directive (EU) 2016/680 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 by competent authorities for the purposes of the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, and on the free movement of such data, and repealing Council Framework Decision 2008/977/JHA, OJ L 119, 4.5.2016.
[5] See articles 99 par. 2 of the GDPR and 63 par. 1 of the LED. The annus mirabilis characterization for 2018 becomes a European milestone, if one adds to the picture the Council of Europe's Convention 108+ (Modernised Convention for the Protection of Individuals with Regard to the Processing of Personal Data, 17-18 May 2018).

invites a retrospective assessment and a, modest, attempt to look into the future. However, a "where we stand" analysis is unavoidably prejudiced by interests, previous research work, and opinions, of the author, particularly in view of the extremely wide scope of implementation for personal data protection in Europe today. Similarly, predictions on future developments may prove not to be worth the paper they are printed on if, for example, a political, financial or social development dictates a specific regulatory response – one must after all always keep in mind that both the GDPR and the LED are largely the result of the Snowden revelations back in 2016.[6] At any event, section 1 of the analysis that follows will attempt to present the major issues that personal data protection law has to deal with today in Europe, while section 2 will attempt, on the basis of path dependence and assuming no major event taking place (in spite of recent history repeatedly overturning the latter assumption and Europe currently being in the middle of war), to present a possible outlook ahead for this relatively new and promising field of EU law.

[6] See, for example, Agustin Rossi, How the Snowden Revelations Saved the EU General Data Protection Regulation, The International Spectator, Vol. 53, 2018.

2. Major issues facing personal data protection law in the EU

The fifth anniversary of the coming into effect of what started out many years ago as the EU Data Protection Reform Package[7] invites a retrospective assessment – not the least due to the anyway mandatory re-evaluation of their implementation self-imposed by the GDPR and the LED themselves. In line with better-regulation guidelines, each one of these legal acts mandates its periodic re-evaluation.[8] At the point in time when this paper is drafted (in late 2023) we have at hand, as regards the GDPR, the European Commission's first report on its application that was published in 2020[9] (henceforth, the "Commission's 2020 GDPR Report") and the European Data Protection Board (EDPB)'s views on the next European Commission's evaluation report that is due in the summer of 2024 (henceforth, the "EDPB GDPR 2024 Report").[10] As regards the LED, we only have one European Commission report, that was published in 2022 (the "Commission's 2022 LED report").[11] These will form the basis of reference of the analysis that follows.[12]

Even however within these strictly circumscribed terms of reference, an assessment of the overall condition of data protection today in the EU is impossible. This is due to data protection's extremely wide scope, especially when combined with any expert's unavoidable tunnel vision described in Section 1. In practice, data protection, particularly

[7] See European Commission, A comprehensive approach on personal data protection in the European Union, COM(2010) 609 final.
[8] The GDPR in art. 97 and the LED in art. 62.
[9] European Commission, Communication from the Commission to the European Parliament and the Council: Data protection as a pillar of citizens' empowerment and the EU's approach to the digital transition - two years of application of the General Data Protection Regulation, COM/2020/264 final.
[10] European Data Protection Board, Contribution of the EDPB to the report on the applicationof the GDPR under Article 97, adopted on 12 December 2023.
[11] European Commission, Communication from the Commission to the European Parliament and the Council: First report on application and functioning of the Data Protection Law Enforcement Directive (EU) 2016/680 ('LED'), COM/2022/364 final.
[12] A necessary clarification refers to the fact that, although interest in this paper is focused only on the GDPR and the LED, these are by no means the only important EU data protection legal instruments. Regulation 1725… or the agency-specific (Europol, Eurojust etc.) data protection regimes certainly compete for attention and complement the EU data protection law picture. The selection here is therefore arbitrary, in line with the assumptions made in Section 1. Having said that, however, a deliberate attempt has been made to make the findings of this paper also applicable outside the GDPR and LED regulatory environment as well.

taking the GDPR into account, applies on each and every moment of any European's daily life, both personal and professional. Data protection in the EU today applies on all fields of human activity, all technologies regardless whether emerging or mature, all business models regardless whether off-line or on-line, all scientific or research or even artistic fields. Within such ubiquitusness, how could anyone formulate a "where we stand" picture without arbitrarily prioritising one topic over another? How could anyone have helicopter view?

It is in view of these difficulties that the approach in this Section will focus on principles instead of concrete topics. This choice is not only due to the fact that the list of topics has been already constructed authoritatively by the bodies competent to do so (specifically, by the EDPB, in its GDPR 2024 report). Data protection in the EU is a principles-driven system anyway.[13] The whole EU data protection architecture is based on a number of principles that run through it and shape it. All of them (accountability, transparency, proportionality) are readily identifiable in the texts of the GDPR and the LED, and are immediately recognisable by all practitioners in the field. The assumption is therefore that, if one focused on these principles, the major issues facing data protection law in the EU will make themselves more clearly viewed and understood. It is in this context that a principles-driven analysis is considered suitable to convey whatever state-of-the-art can be drawn in EU's data protection today.

[13] See Paul De Hert / Vagelis Papakonstantinou / David Wright / Serge Gutwirth, The proposed Regulation and the construction of a principles-driven system for individual data protection, Innovation: The European Journal of Social Science Research, Volume 26, 2013.

2.1. Accountability

The principle of accountability is of paramount importance in the EU data protection system. Formally, it is included in par. 2 of art. 5 of the GDPR, [14] however in practice it runs through all of the EU data protection architecture. This update of the 1995 Data Protection Directive approach,[15] although precipitated by technological developments and data protection ubiquitusness (see also Section 2.3), has been no small feat: essentially, it affects controllers (who need not only to comply but also be able to demonstrate it), data subjects (who may focus on protection of their rights, rather than compile a complete file each time), and DPAs (who are afforded with wider monitoring and enforcement powers) alike.

Taking these into account the principle of accountability is examined here both as data protection implementation and enforcement. Although at first sight these may seem two different topics that merit separate attention and analysis, because the principle of accountability runs through them and affects them gravely, they are interconnected and, as such, paralleled. After all, even in practice implementation needs to be followed by enforcement.

Implementation itself is a major topic within data protection in Europe today. Expectations run high with the GDPR and LED release and it is contested whether practice has justified them. The rate of success, if any, is of course subjective: to some what has been achieved in the past five years may seem enough, to others inadequate. The opinions therefore of representative organisations matter. The EDPB, speaking on behalf of all DPAs in the EU, has declared itself satisfied[16] – not of course without identifying points for improvement. The market may sound less satisfied, with complaints ranging from the compliance costs to persistent lack of harmonisation across the EU in spite of this being the primary target of the GDPR.[17] As regards the LED, the Commission seemed satisfied back in 2020,

[14] "The controller shall be responsible for, and be able to demonstrate compliance with, paragraph 1 ('accountability')."; see also par. 4 of art. 4 of the LED.
[15] Compare art. 6, par. 2 of the 1995 Data Protection Directive.
[16] "The application of the GDPR in the first 5 and a half years has been successful.", EDPB GDPR 2024 Report, p. 3.
[17] See, for example, FEDMA's (Federation of European Data and Marketing) views in "GDPR 5 years on – Key areas of improvement needed in the the Data and Marketing Industry", 24 May 2023, available at https://www.fedma.org/2023/05/24/gdpr-5-years-on-key-areas-of-improvement-needed-in-the-the-data-and-marketing-industry accessed on 20 December 2023.

however not without addressing individual requests to Member States for improvements in their national implementing laws.[18]

Enforcement reveals a similarly overall positive picture. Fines (by no means the only or even preferred tool for enforcement, but still the one that attracts most of the general public's attention) may have had a slow start[19] but have apparently peaked during the past five years.[20] Expectedly, record-setting fines were imposed by those DPAs where the large personal information processing companies of today are seated in Europe, meaning in Ireland and Luxembourg.[21] Also expectedly, this has raised concerns by other DPAs – and incited a regulatory intervention by the European Commission.[22] At any event, one must not lose the forest for the trees: back in 2016 the discussion was whether the cross-border enforcement models of EU data protection law would work at all. Today nobody is questioning it.

In view of a mostly positive assessment, what are the major issues facing personal data protection law in the EU today from a principle of accountability point of view? A comprehensive list can be found in the EDPB GDPR 2024 Report.[23] Technological advances pose an obvious challenge. Personal data protection has developed into the go-to piece of legislation for any new technology developed by humankind, regardless whether in information technology, biology, the automotive industry or warfare. Whether this is ultimately a good thing will be examined in section 2.3. Here it is enough to be noted that the provisions of the GDPR and the LED will have to remain agile enough to continue accommodating whatever the human intellect (and digital economy) is testing against them while protecting individual human rights.

In the same vein, the cohort of new EU laws aimed at regulating digital technologies that have recently come into effect or are in the process of finalisation are expected to pose significant challenges on EU data protection provisions and put significant strain on its enforcement mechanism. No matter whether regulating large online platforms (the

[18] See the Commission's 2022 LED report, in p.34 and pp.8-16, respectively.
[19] See Commission's 2020 GDPR Report, p.5.
[20] See Martin Armstrong, EU Data Protection Fines Hit Record High in 2023, statista.com, 8 January 2024, available at https://www.statista.com/chart/30053/gdpr-data-protection-fines-timeline/ accessed on 8 January 2024.
[21] Ibid.
[22] See European Commission, Data protection: Commission adopts new rules to ensure stronger enforcement of the GDPR in cross-border cases, Press Release, 4 July 2023, available at https://ec.europa.eu/commission/presscorner/detail/en/ip_23_3609, accessed on 21 December 2023.
[23] See its pages 4-6.

Digital Markets Act)[24] or online commerce (the Digital Services Act)[25] or data use (the Data Governance Act[26] and the Data Act[27]) or artificial intelligence (the Artificial Intelligence Act[28]), all of them relate to, and have specific provisions on, personal data protection. The way they will coordinate with ongoing data protection mechanisms in Europe once they become fully effective will most likely occupy the attention of regulators, practitioners and the public in the next few years.

Enforcement continues to be a major issue facing EU data protection today, and this is true both at the level of large international corporations and small businesses and SMEs. Each case poses its own challenges: the former, cross-border personal data processing and complex business structures and models, and the latter, limited resources and a need to remain competitive. DPAs, from their part, are faced with high expectations from all of the EU data protection recipients (controllers and data subjects alike) without however frequently been afforded with the necessary resources to satisfy them.[29]

While the above describe a more or less state-of-the-art as regards the principle of accountability that is also viewable in the EDPB's GDPR 2024 Report, a personal preference refers to the relationship between data protection and (cyber)security. Cybersecurity threats and incidents being on the rise and security being a basic principle enshrined also in EU data protection, the perennial question of balancing security with individual rights poses itself time and again also in the personal data protection field. This has been the case in the past, with the basic EU cybersecurity legislation carefully avoiding to tread on data protection territory, as well as currently, when major cybersecurity incidents also include personal data breaches. Striking the correct balance each time is a difficult task that not only attracts much attention but also reflects our broader approach on European societies.

[24] Regulation (EU) 2022/1925 of the European Parliament and of the Council of 14 September 2022 on contestable and fair markets in the digital sector and amending Directives (EU) 2019/1937 and (EU) 2020/1828 (Digital Markets Act), OJ L 265, 12.10.2022.
[25] Regulation (EU) 2022/2065 of the European Parliament and of the Council of 19 October 2022 on a Single Market For Digital Services and amending Directive 2000/31/EC (Digital Services Act), OJ L 277, 27.10.2022.
[26] 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), OJ L 152, 3.6.2022.
[27] Proposal for a Regulation of the European Parliament and of the Council on harmonised rules on fair access to and use of data (Data Act), COM/2022/68 final.
[28] Proposal for a Regulation of the European Parliament and of the Council laying down harmonized rules on artificial intelligence (Artificial Intelligence Act) and amending certain Union legislative acts, COM/2021/206 final.
[29] See the EDPB GDPR 2024 Report, p.6.

2.2. Transparency

The principle of transparency is another principle that runs through EU data protection law. Although its formal inclusion in the text of the GDPR is found in only one article,[30] as was also the case with the principle of accountability, it applies as well in terms of compliance, data protection-specific individual rights (rights to information, access, deletion, rectification etc.), joint controllership, codes of conduct, certification, as well as the work of DPAs themselves. In spite of the fact that a principle of transparency is not listed among the fundamental principles of EU law, the European Commission has granted it increased importance particularly when regulating digital technologies: it is a centrepiece principle in practically all recent relevant initiatives listed above (in Section 2.1).

This being the case, how well have these requirements worked in practice? Practice seems to have adopted a twofold approach, as regards transparency in EU data protection: a sector-specific approach, and introduction of transparency-enhancing tools. Each one of these approaches is not exclusive, in fact they complement each other. Specifically, a number of sectors (healthcare, scientific research, artificial intelligence) have introduced methodologies and examined solutions in order to increase transparency as regards personal data processing.[31] In addition, new transparency-enhancing tools have been recommended that could assist implementation of this principle horizontally in EU data protection.[32]

Transparency, however, does not refer exclusively to controllers and other data protection recipients; it is also addressed to supervisory authorities. In this regard, concrete transparency-enhancing steps have been taken by DPAs

[30] "Personal data shall be processed lawfully, fairly and in a transparent manner in relation to the data subject ('lawfulness, fairness and transparency');", par. 1(a), art. 5 of the GDPR; see also Recital 26 of the LED.
[31] See, for example, Miranda Mourby / Katharina Ó Cathaoir / Catherine Bjerre Collin, Transparency of machine-learning in healthcare: The GDPR & European health law, Computer Law & Security Review, Volume 42 November 2021; Sandra Wachter, The GDPR and the Internet of Things: a three-step transparency model, Law, Innovation and Technology, Volume 10, Issue 2, 2018;
[32] See, for example, Elias Grünewald / Paul Wille / Frank Pallas / Maria C. Borges / Max-R. Ulbricht, TIRA: An OpenAPI Extension and Toolbox for GDPR Transparency in RESTful Architectures, 2021 IEEE European Symposium on Security and Privacy Workshops (EuroS&PW), Vienna, Austria, 2021, pp. 312-319; Rossi, Arianna / Monica Palmirani, DaPIS: A data protection icon set to improve information transparency under the GDPR, *Knowledge of the Law in the Big Data Age*, 2019.

themselves, among which placing all their decisions and other interventions on-line (often translated in more than one EU languages), publishing all fine-relevant details, or producing detailed and comprehensive annual reports. This

bore fruit: the press and NGOs picked up,[33] and by now there are cross-EU measurements and infographics on the activities of DPAs – which will in turn incite DPAs to improve their practices within a virtuous cycle.

Notwithstanding the above assessments, it could be argued that transparency is an objective that cannot be measured. While, for example, the principle of accountability can be measured in terms of compliance and enforcement, how could one measure transparency? Complete transparency, even if it was ever considered desirable, would most likely be impractical, both as regards controllers and processors and as regards the enforcement mechanism. Administrative and technical obstacles make it impossible to achieve. This being the case, achieving lesser degrees of transparency each time is bound to leave some dissatisfied. The ultimate arbitrator being an ad hoc decision either by a DPA or by a court, the principle of transparency is by definition elusive and subjective.

Having said that, transparency remains a major issue facing EU data protection today. Requests come from all parts of the data protection spectrum: data subjects ask for transparency from controllers on their processing; controllers ask for transparency from DPAs on their monitoring and enforcement; DPAs ask for transparency from controllers, on their compliance. Whatever steps have been made so far are certainly in the right direction, particularly taking into consideration that transparency was not a basic data protection requirement under the previous (1995 Data Protection Directive) regime.[34]

If this author was to add a personal preference on the issues facing EU data protection today as regards the principle of transparency (same as was done in Section 2.1), this would have to be artificial intelligence. While by no means wishing to downplay the importance of transparency in such sectors as the Internet of Things or big data processing, I would prioritise transparency in artificial intelligence for two reasons: first, because of its importance, being an ubiquitous (instead of a sector-specific) digital technology, and, second, on account of the fact that, even under its

[33] See, for example, Giovanna Coi / Clothilde Goujard / Laurens Cerulus, Europe's privacy regime: 5 years in 5 charts, 25 May 2023, Politico.eu, available at https://www.politico.eu/article/meta-online-safety-europe-privacy-gdpr-big-tech-regime-5-years-in-5-charts/ , accessed on 20 December 2023.

[34] In spite of Recital 63 of 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, OJ L 281, 23.11.1995.

manufacturers' best intentions, transparency is not certain to be achieved. In other words, while in cases of other personal data processing (e.g. IoT or Big Data) algorithms and categories of processing can be more or less explained, it is not certain that this is the case in future advanced machine-learning environments.

2.3. Proportionality

Proportionality is the last, but certainly not least, of the three principles discussed in this paper as running through the EU data protection system and setting the agenda facing data protection today. In general, the principle asks for 'some articulate relationship between means and ends',[35] and it is in this context that it holds its place among the fundamental principles of EU law.[36] In the EU data protection system the principle of proportionality is of central importance. Its piecemeal inclusion in the GDPR provisions (either explicit[37] or tacit[38]) barely does it justice: in fact, it is ever-present in the EU data protection system no matter from which angle anybody is viewing it: from the point of view of controllers, as regards the level of effort they need to put in their compliance; from the point of view of data subjects, as regards what level of protection they must expect each time; from the point of view of DPAs as a threshold in their enforcement practices (including any administrative fines' imposition).

The principle of proportionality affects, therefore, both implementation and enforcement of EU data protection law. However, it is not within this context that it is examined here. As an agenda-setting principle for data protection today, proportionality is called upon to address a much more basic question: is EU data protection law a proportionate response for protection of the individual right to data protection, as enshrined in art. 16 TFEU?

This at first may sound as a counter-intuitive question. After all, the basics of secondary legislation (unlike any other fundamental human rights) are included in the wording of art. 8 CFREU itself.[39] How can it be then that such secondary legislation is questioned?

[35] See Eric Engle, 'The history of the general principle of proportionality: An overview', Dartmouth Law Journal, Issue 10, 2012.
[36] See, for example, Koen Lenaerts, Proportionality as a matrix principle promoting the effectiveness of EU law and the legitimacy of EU action, ECB Legal Conference 2021; Paul Craig / G. De Búrca, EU law: Text, cases, and materials, Oxford University Press, 2020 (7th edn.), p.585.
[37] For example, in the cases of further processing (art. 6, par. 4) or in the cases of art. 23.
[38] For example, in art. 5, par. 1(c) or art. 5, par. 1(f).
[39] "Such data must be processed fairly for specified purposes and on the basis of the consent of the person concerned or some other legitimate basis laid down by law. Everyone has the right of access to data which has been collected concerning him or her, and the right to have it rectified.", art. 8, par. 2 of the Charter of Fundamental Rights of the European Union.

The opposing (or, correctly phrased, questioning) view is best summarized by Attorney General Bobek's remarks: "Humans are social creatures. Most of our interactions involve the sharing of some sort of information, often at times

with other humans. Should any and virtually every exchange of such information be subject to the GDPR?",[40] concluding that "in my view, I suspect that either the Court, or for that matter the EU legislature, might be obliged to revisit the scope of the GDPR one day. The current approach is gradually transforming the GDPR into one of the most de facto disregarded legislative frameworks under EU law. That state of affairs is not necessarily intentional. It is rather the natural by-product of the GDPR's application overreach, which in turn leads to a number of individuals being simply in blissful ignorance of the fact that their activities are also subject to the GDPR."[41]

It is therefore data protection ubiquitusness that attracted the AG's criticism, a finding confirmed in legal theory as well.[42] Data protection ubiquitusness (or, depending on the perspective, scope overreach) is not an issue to be discarded light-heartedly, because it gives birth to a number of issues facing EU data protection today: Can the GDPR effectively deal with any new technology or new business model modern human life may throw at it? Can the GDPR and the LED co-exist with traditional fields of law (civil law, business law, penal law), whose basic assumptions they sometimes challenge? Can the two survive well-established legal systems' procedures (such as court proceedings or criminal investigations), without affecting the careful internal balance that these systems have already achieved? These questions not only raise important issues facing EU data protection today, but threaten its very core.

Perhaps, then, new approaches and new regulatory tools will need to be devised. The theory behind the individual right to data protection may need to be seen under new light, as for example within the, recently proposed, context of so-called "interface rights", meaning rights "whose primary function, in relation to a given social phenomenon, is to ensure a productive reflexive relationship between substantive constitutional rights and social context".[43] In this case, data protection would constitute the interface, particularizing other, substantive constitutional rights into new technological, market or social developments, warranting the continued relevance of both.[44]

[40] CJEU, Opinion of Advocate General Bobek, delivered on 6 October 2021, on Case C-245/20 (X, Z v Autoriteit Persoonsgegevens), par. 55.
[41] Ibid, par. 65.
[42] See Nadezhda Purtova, The law of everything; Broad concept of personal data and future of EU data protection law, Law, Innovation and Technology, Issue 10, no. 1 (2018), with further references.
[43] Dara Hallinan, A Theory of EU Data Protection Law, European Data Protection Law Review, 9 (2023), p.314.
[44] In the same context, that of explaining the origins and continued necessity for EU data protection ubiquitusness, see also Vagelis Papakonstantinou, States as Information Platforms: a Political Theory of Information, The CDSL Working Paper Series WP6/2023, November 2023, available at https://ssrn.com/abstract=4642499 or http://dx.doi.org/10.2139/ssrn.4642499, accessed on 23 December 2023.

The principle of proportionality is therefore brought forward here not (as is usually the case) as a tool for implementation and enforcement but as a tool to identify the continued relevance of EU data protection's *raison d'être*. Within an environment of constant change and ceaseless challenges the wide scope of both the GDPR and the LED threatens their basic core. Their continued necessity as fundamental rights' protective mechanisms needs to be continuously confirmed and, whenever needed, updated and reinvigorated in legal theory.

3. The outlook ahead

As explained in the introduction, in view of broader uncertainty to make any predictions for the future, path dependence may serve as a useful tool. If this is the case, then a widening and deepening of EU data protection scope and implementation are to be expected. The widening of its scope will come as a result both of its own nature (which is expansive by definition) and on account of forthcoming legislative developments. As far as the former is concerned, because data protection in the EU involves any and all of automated personal data processing,[45] unavoidably any new consumer-oriented technology or business model will fall within its remit. EU data protection, by opting to be technology-neutral,[46] is neither industry nor sector-specific. (Having said that, developments are to be expected also in the e-Privacy front, through finalisation of work on the, still in draft, e-Privacy Regulation.[47]) In addition, as far as the deepening of the EU data protection implementation is concerned, this is expected to soon take the form of an implementing regulation on procedural rules,[48] that is being issued on the aftermath of huge fines imposed on certain international technology corporations.[49] Once this has been accomplished, one sees no reason for the European

Commission to stop: in view of an already identified "wish list" by the EDPB,[50] focused regulatory interventions will most likely be the preferred regulatory tool to strike items out of it.

[45] See art. 2, par. 1 of the GDPR.
[46] See Recital 15 of the GDPR, as well as, the Commission's 2020 GDPR Report, p.10.
[47] Proposal for a Regulation of the European Parliament and of the Council concerning the respect for private life and the protection of personal data in electronic communications and repealing Directive 2002/58/EC (Regulation on Privacy and Electronic Communications), COM(2017) 10 final.
[48] European Commission, Proposal for a Regulation of the European Parliament and of the Council laying down additional procedural rules relating to the enforcement of Regulation (EU) 2016/679, COM/2023/348 final.
[49] See above, ftn. nr. 22.
[50] EDPB GDPR 2024 Report, p.11.

Is the future, then, expected to be a bed of roses for EU data protection? Although expectations may be high, the very same reasons that give cause to celebrate today, in the fifth anniversary since the *annus mirabilis* of 2018, and make us feel optimistic about the future may also prove disastrous, if not enough attention is paid by legislators and practitioners alike. As seen, the extremely wide scope of EU data protection has raised quite a few eyebrows – a trend that is not expected to subside any time soon, particularly in view of the fact that all new regulatory initiatives by the EU for digital technologies develop around (if not mimic)[51] data protection. Compliance fatigue may lead to irrelevance of the laws concerned. In the same vein, a deepening within the data protection field of law may mean that further specialisation will become necessary – if, for example, the GDPR and the LED are separated enough to make it impossible for the same practitioners to be experts in both. Although this may in principle be a welcome development (in the sense that it demonstrates legislative maturity), in practice compliance may be hindered by controllers who may be unwilling to hire ever-more experts and engage in ever-more complex compliance requirements.

Having said that, a relatively safe prediction is that, until the next five-year anniversary at least, it is unlikely that either the GDPR or the LED will have been replaced. Not only are they relatively young (their predecessors exceeding 25 and 10 years respectively) and their law-making procedure cumbersome (this one lasting for more than five years, same as was, after all, the case also with the 1995 Data Protection Directive, thus setting a precedent), but, most importantly, no stakeholder seems to be unsatisfied with them. Most notably, both the European Commission and the EDPB, for the moment at least, view them in a positive light.

[51] See Vagelis Papakonstantinou / Paul de Hert, The Regulation of Digital Technologies in the EU:
The law-making phenomena of "act-ification", "GDPR mimesis" and "EU law brutality", Technology and Regulation, 2022.

4. Conclusions

A five-year anniversary, particularly if the assessment is overall positive as is the case here, invites not only celebratory feelings but also a certain melancholy: will there ever be another *annus mirabilis* in EU data protection? Is 2018 ever to be repeated, in view of the very high bar it set? Will there ever be worthy successors to the GDPR and the LED? Such feelings are inevitable amid celebrations, however they should not blur the general picture of both success and robustness. Notwithstanding their being the result of political circumstances and in spite of a shaky start, both the GDPR and the LED have entrenched their position within the EU regulatory edifice by now, not only embedding themselves in it but also, particularly in the case of the GDPR, setting the example *par excellence* against which all other technology-oriented regulatory instruments are to be compared in the future. This is no small feat, and congratulations are in order. Regardless what the future holds, EU data protection is in a position to face it confidently - after all, perhaps another *annus mirabilis* may not be needed anyway.