Editorial

Once again, the EU Court of Justice (CJEU) has placed a bomb under the open data and re-use of information regimes adopted by the European Union. Back in 2021, the Court handed down a far-reaching ruling on Latvian legislation in which governmental data could be obtained by anyone who so requested. The authorities did not assess what purpose the requesting party was pursuing and therefore also not whether that purpose was in line with the original purpose for processing personal data: the prevention of traffic offences and road safety. Among other things, because it had not been demonstrated that the new processing operations served that original purpose, the CJEU found a violation of the General Data Protection Regulation, in particular in relation to purpose specification and the limitation principle.

A long standing problem is that the EU broadly adopts two types of laws that are difficult to reconcile: privacy and data protection legislation on the one hand and legislation on open data and the re-use of information on the other. The legal instruments falling in the latter category usually include a provision stating that they do not affect privacy and data protection instruments; moreover, Articles 7 and 8 EU Charter of Fundamental Rights override secondary legislation on open data and re-use of data. Consequently, if there are personal data included in a dataset or they can be derived from it, the privacy and data protection principles must be respected in full. Needless to say that almost all datasets contain personal data, that even highly anonymised datasets can often still be re-identified and that personal data might be obtained through linking two or more datasets that in themselves do not contain identifiable data. This poses a problem, as data disclosure for re-use is counter to most data protection principles. For example, the GDPR requires data to be kept confidentially and securely so that third parties cannot access them, data may only be reused for purposes compatible with the original purpose for acquiring the data and data processing must be limited to only those data that are necessary for the purpose pursued and data must be deleted as soon as they are no longer needed for that purpose.

Although experts have pointed out at least since 2003 that these two legal concepts are fundamentally incompatible and that therefore, their relationship needs to be clarified, the EU has not done so. To the contrary, it has pushed for stricter privacy and data protection laws and, at the same time, for legal instruments that mandate parties to actively make data public for reuse by third parties. One consequence of this constellation is that both national governments and data-processing organisations are faced with two different EU frameworks; they generally feel the need to 'balance' them. This usually means that they do disclose data, but filtered out, for example, the most directly identifying or sensitive personal data from the datasets. This is problematic because it is perfectly clear that these are not two equivalent legal regimes; data may on-

DOI: 10.21552/edpl/2022/4/3

ly be disclosed if such fully meets all the requirements that follow from Articles 7 and 8 CFREU, the GDPR and other privacy and data protection legislation. In the 2021 case, the Court explicitly confirmed this.[1] Although that case concerned passive disclosure (disclosure of data upon request), the most logical interpretation seemed to be to extend the ruling to active disclosure (the disclosure of datasets on a party's own initiative, often on the internet, usually accessible to anyone without conditions). Despite this ruling being widely circulated among organisations that disclose data, most continued with business as usual. Perhaps the Court's new ruling from late 2022 will change this.[2]

A certain degree of disclosure has always been common in market transactions; for example, companies are registered, with the names of the board members and any vicissitudes, so that the reliability of parties can be checked. A research company Veritas sounds promising, but if it turns out that Liz Truss is its director, a party may hesitate to acquire its services. Two things have changed with respect to this longstanding tradition.[3] First, the EU has encouraged that existing data on market participants be actively made public, preferably on the internet. This means that not only market participants can inquire about the background of a company they might want to do business with, but that anyone can access the data. One consequence of this has been the availability of private individuals' names and addresses of sole traders, which has led to unsolicited advertisements and spam sent to their home address, among other things. Secondly, the EU has required more data to be made available, including for other purposes. An example is the Money Laundering and Terrorist Financing Directive,[4] which requires that information on corporate beneficiaries must be disclosed. The Luxembourg Implementation Law required that the following information about the beneficial owners of registered entities must be entered and kept in the beneficial owners' register: name, nationality/ies, day of birth, month of birth, year of birth, place of birth, state of residence, full private or business address, for individuals registered in the National Register of Individuals: the identification number, for individuals not residing in Luxembourg and not registered in the National Register of Individuals: a foreign identification number, the nature of the beneficial interest held and the size of the beneficial interest held.

Both the EU Directive and Luxembourg law contained an exception in case there were disproportionate disadvantages for the beneficiary in disclosing these data. The case

1 ECLI:EU:C:2021:504, Case C-439/19, 22 June 2021.

2 ECLI:EU:C:2022:912, Joined Cases C-37/20 and C-601/20, 22 November 2022.

3 Similarly, there was a tradition of open government, a tradition in which critical citizens and investigative journalists could have access to specific government documents, but this has been changed by the EU by requiring that governmental information be actively disclosed, accessible to all, made suitable for re-use, and that this re-use should not have the goal to critically assess the use of power, but to re-use data for commercial purposes.

4 Directive (EU) 2015/849 Of The European Parliament And Of The Council of 20 May 2015 on the prevention of the use of the financial system for the purposes of money laundering or terrorist financing, amending Regulation (EU) No 648/2012 of the European Parliament and of the Council, and repealing Directive 2005/60/EC of the European Parliament and of the Council and Commission Directive 2006/70/EC. Directive (EU) 2018/843 Of The European Parliament And Of The Council of 30 May 2018 amending Directive (EU) 2015/849 on the prevention of the use of the financial system for the purposes of money laundering or terrorist financing, and amending Directives 2009/138/EC and 2013/36/EU.

before the CJEU is a conflation of two cases at the Luxembourg level, with respect to which the Luxembourg court asked preliminary questions. In both cases, a request for an exception was rejected. The Luxembourg court asked a rather diverse set of questions, all of which the Court puts under the heading of privacy and data protection. It takes two steps to that end.

First, it looks at whether there is an interference with the right to privacy and/or data protection. This is evidently so, as the case involves the processing of personal data. According to the Court, it is a 'serious interference', inter alia because the information is freely accessible to everyone and because the reuse of this information for other purposes cannot be excluded, especially since the data has been published on the internet and can be downloaded and further disseminated. It will be highly difficult or even illusory for data subjects to defend themselves effectively against misuse in the case of successive sharing and re-use of their data.

Second, the CJEU looks at whether such interference is justified. The EU Directive and its implementation on a national level in Luxembourg provide a legal basis for the processing of personal data, the CJEU makes clear, and the disclosure of the data does not violate the essence of Articles 7 and 8 CFREU. Regarding the public interest, it notes that by providing for access to information on beneficial owners, the EU aims to prevent money laundering and terrorist financing by creating, through increased transparency, an environment that is less likely to be used for that purpose. This objective constitutes a public interest objective which, according to the Court, can justify even serious interferences with the fundamental rights guaranteed by Articles 7 and 8 CFREU.

With regard to the legitimate interest, the Court notes something essential. 'In so far as the Council of the European Union also refers, in that context, expressly to the principle of transparency, as follows from Articles 1 and 10 TEU and from Article 15 TFEU, it should be noted that that principle, as the Council itself states, enables citizens to participate more closely in the decision-making process and guarantees that the administration enjoys greater legitimacy and is more effective and more accountable to the citizen in a democratic system. While, in that respect, the principle of transparency is given concrete expression primarily in the requirements of institutional and procedural transparency covering activities of a public nature, including the use of public funds, such a link with public institutions is lacking where, as in the present case, the measure at issue is intended to make available to the general public data concerning the identity of private beneficial owners and the nature and extent of their beneficial interests held in companies or other legal entities. Accordingly, the principle of transparency, as it results from Articles 1 and 10 TEU and from Article 15 TFEU, cannot be considered, as such, an objective of general interest capable of justifying the interference with the fundamental rights guaranteed in Articles 7 and 8 of the Charter, which results from the general public's access to information on beneficial ownership.'[5]

5 Joined Cases C-37/20 and C-601/20, 22 November 2022, § 60-62.

It then comes to the essential point of the ruling, namely the question of the necessity, proportionality and subsidiarity of the interference. On this point, the Commission had indicated that it would be difficult to limit access to the data only to individuals or organisations with a legitimate interest, because that legitimate interest is difficult to define and could therefore lead both to great diversity between Member States and to very restrictive decisions concerning access to the data. It was therefore decided to simply provide that everyone should have access to the data. The Court rejects this reasoning by stating 'that the fact that it may be difficult to provide a detailed definition of the circumstances and conditions under which the public may access information on beneficial ownership is no reason for the EU legislature to provide for the general public to access that information'.[6]

It continues by noting that there are certainly parties who have a legitimate interest in accessing the information, such as organisations seeking to do business with the companies in question and journalists and civil society organisations investigating money laundering and terrorist financing. But there is no need to give everyone access to the information, the CJEU emphasises. Indeed, the Court states that in principle, it is primarily for governmental organisations to investigate money laundering and terrorist financing. It notes that 'the fact remains that, first, combating money laundering and terrorist financing is as a priority a matter for the public authorities and for entities such as credit or financial institutions which, by reason of their activities, are subject to specific obligations in that regard. Indeed, it is for that reason that points (a) and (b) of the first subparagraph of Article 30(5) of Directive 2015/849 as amended provide that information on beneficial ownership must be accessible, in all cases, to competent authorities and Financial Intelligence Units, without any restriction, as well as to obliged entities, within the framework of customer due diligence.'[7]

Finally, it zooms in on the possibility for specific parties to request an exception regarding the disclosure of their data. In doing so, the Court is critical of two provisions that give Member States substantial room for interpretation: first, they are allowed to determine whether information other than that mentioned in the EU Directive must also be disclosed and, second, they can determine the conditions under which an exception applies. This means that the legislation on this point is not sufficiently clear and unambiguous, especially given the serious interference with citizens' fundamental rights.[8]

This judgment has caused great commotion among Member States' Chamber of Commerce, registers and other public entities that actively disclose data. And rightly so. The Court emphasises once again that Articles 7 and 8 of the Charter take precedence

6 Joined Cases C-37/20 and C-601/20, 22 November 2022, § 72.

7 Joined Cases C-37/20 and C-601/20, 22 November 2022, § 83-84.

8 It is interesting that the Court does not discuss this shortcoming under the question of whether there is a sufficient legal basis for the interference, because both the Court of Justice and the European Court of Human Rights increasingly assume that under this requirement, there should not only be a legal basis, but that it also means that the law should also meet several quality of law requirements, such as that the law should be sufficiently accessible, clear and specific.

over secondary legislation on public access to information and the re-use of data. It is important to note that these parties have oftentimes made the claim that if they make data publicly available, no misuse of the data has to take place, data does not have to be used for purposes incompatible with the original purposes. If Party A discloses data and Party B gains access and then processes the data for another, incompatible purpose, this is not Party A's fault, so it was suggested, but Party B's, as Party B does not comply with the GDPR and Articles 7 and 8 of the Charter. The CJEU rejects this line of argumentation: if data is published on the internet that is freely accessible for everyone, it is highly likely that there will be some person or another that will use the data for incompatible purposes. Consequently, party A has a duty of care to do everything reasonably possible to prevent misuse of the data it has made available.

An important consequence of this ruling is also that another argument is taken off the table. It was often argued that there were three purposes for processing when disclosing data: (1) the original purpose for processing by Party A, (2) the purpose of disclosing the data by Party A and (3) the purpose for processing by Party B. In this line of argument, (2), the disclosure of data, serves a purpose in its own right; as such, data disclosure is a public interest, it was suggested, as it contributes to an open society, transparency and an accountable government and the accountability of commercial enterprises. Experts have long argued that this argument does not hold water, because 'transparency' or similar purposes are not specific enough to satisfy the purpose-specification principle (requiring well-defined, explicit and legitimate purposes). The Court accordingly dismisses this argument, leaving only purposes (1) and (3) and leaving open both the question to what extent the disclosure of data (2) amounts to purpose (1) and to what extent the purpose for processing data by the party having obtained the data (3) contributes to purpose (1). It follows that public and active disclosure is almost by definition problematic; this ruling could therefore have very far-reaching consequences.

This issue of EDPL opens with two great forewords. Kevin Guyan, the author of the book *Queer Data*, shows the complexities involved with inclusion, representation and bias in datasets. There are no easy answers, while there are many tensions and problems to solve. Catherine D'Ignazio, first author of the book *Data Feminism,* argues that it is not possible to evaluate algorithms using purely statistical or technical methods. Rather, we must consider the context and history of their deployment environments and evaluate risks accordingly. Both books are highly recommended to readers of EDPL who are interested in fairness, algorithmic decision making and statistical representation in datasets.

Our articles sections has three excellent articles, all revolving in some way or another around the notion of individuality, autonomy and control, or collectivity, as an alternative to the focus on the subjective rights of data subjects to protect their personal interests. Diana Dimitrova has penned an analysis of the data subject's right to control over her personal data, which she rightly points out is legally not well-defined. She develops a coherent approach to this concept in her article. Stephen Mulders discusses the doctrine of collective damages for data protection breaches, arguing that

the feasibility of mass claims ultimately depends on whether a GDPR breach actually leads to substantial collective damages. Maximilian Gartner, analyses the notion of individual autonomy in the Data Act.

The reports section, led by Mark Cole and Christina Etteldorf, as always, is packed with highly valuable contributions. There are two reports on European developments. Dominika Kuźnicka-Błaszkowska provides a more general evaluation of the potential role of the data protection framework in preventing sexual abuse and Sandra Schmitz-Berndt discusses the EDPB guidelines on Data Breach Notifications. There are two national reports as well. Joao Pereira, Aida Cepa, Pedro Carneiro, Antonio Pinto and Pedro Pinto analyse the position of the Portuguese Data Protection Officer, while Hubert Bekisz and Dominik Dworniczak present the first insights on how Polish courts have interpreted Article 82 GDPR, concerning liability and the right to compensation. Finally, in the Practicioner's Corner, Friederike Knoke and Iheanyi Nwankwo discuss the use of maturity models for compliance purposes.

Both the case note section, led by Maria Tzanou, and the book review section, led by Gloria Gonzalez Fuster, contain one contribution. David Erdos delves into a recent CJEU case in which the purpose and storage limitation principles are explicated. Finally, Max von Grafenstein shares his thoughts on Felix Bieker's book on the right to data protection.

For those interested in submitting an article, report, case note or book review, please e-mail our Executive Editor Jakob McKernan (mckernan@lexxion.eu) and keep in mind the following deadlines:

– Issue 1/2023: 15 January 2023;

– Issue 2/2023: 30 April 2023;

– Issue 3/2023: 15 July 2023;

– Issue 4/2023: 15 October 2023.

Bart van der Sloot
Tilburg Institute for Law, Technology, and Society (TILT) Tilburg University, Netherlands