Editorial

As several Regulations have already been adopted and the Commission proposes even more Acts for the data-driven environment, the EU hopes to lay down a detailed and comprehensive legislative package for the 21st century. The extensive corpus now on the table should make Europe fit for the digital age, allow enterprises to flourish and governmental organisations to operate more effectively, while at the same time providing a high level of protection to EU citizens. Each of these instruments contains valuable provisions, prohibitions, and rights, meaning that taken separately, their introduction should be welcomed. One thing the EU has invested in little, however, is the consistency between these and other legal instruments and the consistency between the laws applicable to the data-driven environment. There are at least three relevant examples.

First, ever since the EU started to adopt laws that moved away from the socio-economic realm and entered the field of human rights law, little effort went to harmonising these with the more established European Convention on Human Rights of the Council of Europe and the jurisprudence by the European Court of Human Rights. Often, EU law simply mentions that account should be had of the case law of the ECtHR on, for example, the concepts of necessity and proportionality, while leaving open what that exactly means for the interpretation of EU laws and legal principles. This is important because the EU's legal corpus, including the ECJ judgments, is not on all points consistent with the approach taken within the Council of Europe. Examples include, but are not limited to:

– The difference between the protection of privacy under Article 8 of the European Convention on Human Rights and the EU's data protection regime under the General Data Protection Regulation and the Police Directive.

– The differences between the prevention of discrimination under Article 14 ECHR and the EU laws on specific forms of discrimination, such as on grounds of race and ethnic origin (Directive 2000/43/EC), discrimination at work on grounds of religion or belief, disability, age or sexual orientation (Directive 2000/78/EC), equal treatment for men and women in matters of employment and occupation (Directive 2006/54/EC), equal treatment for men and women in the access to and supply of goods and services (Directive 2004/113/EC) and discrimination based on age, disability, sexual orientation and religion or belief beyond the workplace (Directive Proposal (COM(2008)462)).

– The difference between the EU's approach to liability of internet intermediaries, focussing on safe harbours and a notice and takedown or notice and action regime,

DOI: 10.21552/edpl/2022/1/3

and the ECtHR's focus on the freedom of expression and the obligations of publishers.

Because of the discrepancy between both legislative corpuses, it matters for the outcome of a legal dispute whether it is treated under EU law or the European Convention on Human Rights, whether it is judged by the ECJ or the ECtHR.

Second, the EU adopts so much legislation, in such broad terms, that it will be almost impossible for national legislators to bring their full legislative corpus in compliance with EU national law. At least two points should be underlined here:

– One is the scope of EU laws, such as the GDPR (the GDPR obviously only being one example among many). The GDPR, being an EU regulation, will prevail over national law of Member States. National laws of Member States need to be brought in conformity with the GDPR. But quasi every law will entail some form of data processing, e.g. when referring to the requirement to keep or produce 'documents', 'files', 'registers' or 'information', and virtually all of the specific documents, files, registers or information will or may contain personal data. No Member State has assessed its entire legislative corpus and revised it in full to bring it in conformity with the GDPR; rather they have chosen to update a handful of laws central to data processing practices and stressed that all other laws must be interpreted 'in light of the GDPR'.

– This leads to the second point, and that is that the EU often takes a similar approach when it comes to determining the relationship between various EU laws. It does not provide clarity on how various EU laws should be interpreted in light of each other. Instead, the GDPR is 'without prejudice to the application of Directive 2000/31/EC', while the e-Commerce Directive shall not apply to 'questions relating to information society services covered by' the e-Privacy Directive and the GDPR. In similar vein, the Open Data Directive finds: 'This Directive is without prejudice to Union and national law on the protection of personal data, in particular Regulation (EU) 2016/679 and Directive 2002/58/EC and the corresponding provisions of national law.' These types of formulations leave it to Member States to harmonize the various legal regimes, which will often entail complicated legal interpretations. For example, the Open Data Directive requires Member States to make publicly available for re-use public sector information, which will often contain personal data, while the GDPR in principle prohibits re-use of personal data for different purposes than for which they were initially processed, emphasises confidentiality rather than openness and obliges the data controller to inform the data subject who had access to her data, while such may often be unknown to the data controller in open data environments. The fact that Member States, having to decide on the right interpretation of these seemingly conflicting requirements, make choices that are sometimes explicitly condemned by the European Court of Justice, makes things even more complicated.[1]

1 ECLI:EU:C:2021:504Latvijas Republikas Saeima (HvJ EU, C-439/19).

Third, the EU itself is often not consistent or harmonious in its approach and terminology. Not only are these inconsistencies left intact and smoothened out by magic formulas such as that one instrument is 'without prejudice' to another, but different instruments often also take different regulatory approaches, engage with different actors and distinguish between different types of data.

– For example, while the GDPR applies different levels of protection to personal data, sensitive data, anonymous and aggregated data, places pseudonymous data somewhere in between anonymous and personal data, and recognises several types of sensitive data, such as genetic data, biometric data and data concerning health, many of the proposed Acts now on the table use different terminologies. The e-Privacy Regulation distinguishes between metadata, including location and traffic data, electronic communications data, electronic communications content, electronic communications metadata and also makes reference to publicly available directories with data about end-users. The AI Act defines and regulates still different types of data, such as training data, validation data, testing data and input data. The DMA yet again emphasises the difference between aggregated and non-aggregated and between personal and anonymised data, but also refers to data, both in contrast to the definition of personal data, for which reference is made to the GDPR, and to that of non-personal data, for which reference is made to the Regulation on the transfer of non-personal data. Interestingly, the Regulation on the transfer of non-personal data itself does not give a definition of non-personal data but of data, which is seen as encompassing all data but personal data. The DSA refers to illegal content as a special category of data, the Data Governance, like the DMA distinguishes between three types of data, though not between data, personal data and non-personal data, but between data, non-personal data and metadata, the Data Act only refers to data and the Open Data Directive refers to dynamic data, research data and high-value datasets as categories of data that are specifically regulated. How these various categories of data and the partial overlaps and contrasts that exist between them will have to be interpreted is left open.

– If these different and sometimes conflicting categorisations of data and the various regimes for protection that are connected to them is not already difficult enough from a compliance perspective, parties that want to abide by the various regimes that may be applicable to them are themselves categorised differently in each legal regime, with different roles and responsibilities being connected to these categories. The GDPR differentiates between the data subject, the data processor and the data controller, the Regulation on the transfer of non-personal data speaks of service providers, users and professional users, the DSA refers to information society services, recipients of services, consumers, traders, intermediary services and online platforms, the DMA at its turn differentiates between gatekeepers, core platform services, cloud computing services, software application stores, online intermediation services, online search engines, ancillary services, online social networking services, identification services, video-sharing platform services, number-independent interpersonal communication services, operating systems, end users, business users and

undertakings, the Data governance Act makes reference to data holders and data users, the Data Act to users, data holders, data recipients and data processing services and the AI Act, to give a final example, has rules for providers, small-scale providers, users, importers, distributors and operators.

This means that the same entity may be qualified differently under one legislative regime than under another, the same data may be categorised differently under one act than under another and consequently, the types of rules, prohibitions and obligations applicable to data processing activities may vary significantly, if not conflict on certain points.

Although the EU stresses time and again the comprehensiveness of the interrelated data regimes and the fact that the one complements the other, in reality, very little effort seems to be put in making the regimes compatible and coherent. Interestingly, the EU first began regulating the data-driven environment through the Data Protection Directive 1995 because it feared that the inconsistencies between the various data regimes in place at that time in the various Member States, with conflicting rules and obligations for data controllers, would hamper the data market and the free flow of personal data across borders. The Data Protection Directive laid down a minimal framework for data processing to be implemented by all Member States equally. In a way, the EU, by adopting so many regulatory regimes that have not been streamlined, runs the risk of duplicating the incoherent legal landscape that existed before the Data Protection Directive and transcending that that landscape from a Member State to an EU level. Perhaps, before adopting the various Acts that are now on the table, it would be worthwhile to invest in the consistency of the various terminologies for the types of data, the actors involved and their responsibilities.

For this issue, we are proud to have two forewords, this time on the protection of children's data. The GDPR does refer specifically to children in relation to online services and consent for those services, but according to many, these rules are not in and by themselves sufficient to adequately protect the online privacy of children. Sara Grimes, author of, inter alia, *Digital Playgrounds: The Hidden Politics of Children's Online Play Spaces, Virtual Worlds, and Connected Games*, that came out several months ago, argues that children's digital technology use is always political as it is shaped by the politics of the technologists who design the software and hardware children engage with, by the politics of the legislators who enact (or refuse to enact) laws that support and limit children's access, and by the hopes and fears of the parents, educators, and other adults trying to guide children through the technologization of their everyday lives. In addition, the Irish Data Protection Commission provides us with an introduction to their comprehensive *Fundamentals to a Child-Oriented Approach to Data Processing*. Just a few of the many relevant principles that are laid down in those fundamentals are that children should always be heard, that consent by children, or their parents, should not be treated as a legitimation for treating them as adults and that children cannot simply be restricted in their access to services so as to circumvent obligations under the GDPR.

In the articles section, we have five important scientific contributions. Tuulia Karjalainen stresses that although accountability does not radically change the European data protection paradigm, the principle does contribute to increasing controllers' responsibility and facilitating enforcement. Paul de Hert and Guillermo Lazcoz explain that accountability is the relationship between an agent and a principal, where the first needs to explain and to justify his or her conduct, under the judgment of the latter, and to bear the consequences of infringing the rules given for such a relationship. Larisa-Mădălina Munteanu and Mark Povey explain how data protection is ensured for the employees, in the relationship between employers and trade unions, and how the global regulatory framework answers to these new challenges. Daniela Copetti Cravo sets out to identify the gaps existing in the implementation of data portability, to propose some roadmaps that could be adopted by authorities or by the private sector and doing so, focuses on data portability as an individual right within the context of data protection. Finally, Simone van der Hof and Sanne Ouburg have studied whether apps popular among children have implemented adequate methods to meet both verification obligations by analysing the registration process of these apps. No, is their conclusion.

The reports section led by Mark Cole, assisted by Christina Etteldorf, as always, is packed with many outstanding reports, giving the reader an almost full overview of all the legislative, judicial, and administrative initiatives on EU and Member State level. Natalija Bitiukova introduces the reader to a case in Lithuania on the journalistic exemption in the GDPR, the question of legitimate interest and the privacy of public persons. Lorna Woods deals with the legality of a new exemption in the UK, namely the so called immigration exception which disapplies certain data protection rights in relation to the processing of personal data for effective immigration control. Alina Wolski deals with a topic that is controversial in Germany, namely compulsory vaccination, and the extent to which registration is allowed in light of the GDPR. Kristin Benedikt sheds light on a decision that gained much national and international attention, namely the Belgian DPA's critical ruling on online advertising, according to some questioning the basic assumptions of the current revenue model on the internet. Florence D'Ath reports that Luxembourg, acknowledging the crucial role of DPOs, has set out to assess their functioning and has issued several recommendations. Stephan Winklbauer and Robert Horner discuss the continued role of Austria as a lab for crucial role data protection cases, especially with respect to international data transfers. This time, the DPA issued a critical ruling with respect to Google Analytics. Finally, there are three reports on developments in the European Union. Teresa Quintel discusses the exertion of corrective powers by the EDPS against Europol, demanding that the organisation delete all data about persons with no link to a criminal activity. Pier Giorgio Chiara discusses a relevant Commission Delegated Regulation that had escaped my attention and perhaps that of others, among others dealing with privacy and security concerns with respect to IoT devices. Angelica Fernandez, finally, discusses the Data Act, the newest legislative initiative by the European Commission.

In the case note section led by Maria Tzanou, there are two case notes, one on a judgement by the European Court of Human Rights and the other on several judgements by

the EU Court of justice. Rowin Jansen sheds light on the ECtHR's case of Ekimdzhiev and others v. Bulgaria, which in many respects can be seen as the follow up of the Centrum för rättvisa and Big Brother Watch and others cases. Interestingly, the Court takes a strict stance. Sarah Eskens discusses the three joined cases of La Quadrature du Net and others in addition to the case of Privacy International, both on the legitimacy of data retention regimes. In a detailed analysis, she walks the reader through all relevant aspects of those cases.

In the book review section led by Gloria Gonzalez Fuster, Tatiana Duarte discusses an edited volume on AI, data and private law, with many interesting contributions. For example, the very first chapter deals with a topic that should be of interest to the European reader, namely the concepts of personal data, de-identification and pseudonymisation in South Korean legislation.

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 2/2022: 30 April 2022;
- Issue 3/2022: 15 July 2022;
- Issue 4/2022: 15 October 2022.
- Issue 1/2023: 15 January 2023;

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