Editorial

In the Netherlands, a new rule was introduced some time ago. The Dutch railway service had noticed that a lot of people taking the trains were commuting and that many wanted to rest in the train or work. In both cases, what they desired was silence. That is way the 'silent compartments' were introduced; parts of the train were now officially determined noise-free zones. A good idea, many thought; no longer having to ask people to keep their voice or music down, no arguments over how loud the music can be played or having to put up with excuses such as that the person would get off at the next stop anyway. The plan worked out quite to the contrary; it had two main effects. First, in the non-silent compartment, to the kind request to keep the volume down a bit, the most common response became: 'why, this is not a silent compartment'. Second, in the silent compartment, the problem is that many people are unaware of the concept of the silent compartment, such as tourists, or simply forget about the rule while randomly taking a seat. Although when asked, some people are willing to tone down their volume, most of the time you get into a discussion: what does silence really mean, can you whisper, can you play music softly, can you sit silently in a silent couch with a crying baby on your lap, what about dogs, etc? Consequently, many believe that the policy has failed. Before the introduction of the new policy, people would normally limit their behaviour, wanting to show socially desirable conduct, and would be quite receptive to requests made by others. Due to the introduction of rules, this has changed; people feel they have the right to play loud music in the non-silent compartments and will discuss with you the correct interpretation of the rules applicable to the silent compartments.

Some senior colleagues often tell a similar story about the introduction of data protection rules in the Netherlands, through *de Wet persoonsregistratie* from 1989. When there were no explicit rules on data processing, it was left up to the responsibility of citizens, companies and governmental institutions to determine whether and if so, in which manner they would engage with data processing. Although obviously there were parties that behaved in a clearly irresponsible or undesirable manner, most of them actually did undertake a genuine effort to act appropriately, and when confronted with a critical comment or request, they would take those seriously. The open norms forced parties to rely on their and each others' ethical assessment of data processing initiatives. What happened, they say, when the data protection rules were formalised, was exactly the same as what happened with the introduction of the silent compartments. On the one hand, if the rules do not explicitly prohibit data processing, parties usually feel they are justified in processing personal data, without relying on their own ethical evaluation; when they are confronted with requests or comments by others, they will usually point to the rules to explain that they have every right to process those data. On the other hand, when the rules do imply a restriction on the data collection process, parties will often enter into a discussion about the correct interpretation of the rules in the specific circumstances of the case: how precisely should the purpose be outlined, what is an incompatible purpose for the re-use of data, how

updated do data have to be, how much should be invested in technological security, etc.

The same discussion is now applied to the General Data Protection Regulation (GDPR). Some say that the instrument is simply too big, with too many rules and obligations and too many details about the correct interpretation and application of the rules. Some fear that parties will either treat the GDPR as a check-list, without reflexively thinking about the rules and their own behaviour, or will start a discussion about the correct interpretation of the detailed rules in a specific context, as there will always be one principle about which a valid discussion can be had. Some have consequently proposed to move away from the detailed rules and principles and instead go back to the more limited rules of the earlier data protection instruments; or even to incorporate all the data protection rules and obligations in one open norm, in which all relevant principles, potential harms and benefits of a data processing initiative are weighed and balanced against each other.

I've myself struggled a bit with determining my position in this debate. For a long time, I was quite sceptical about regulating data protection through an almost 100-articles-long instrument that has direct effect in the entire European Union (EU). I preferred the original data protection instruments, for example those issued in the 1970s by the Council of Europe. Those were literally one-pagers and contained all of the most important data protection principles, such as the data minimalisation, transparency and security principle. However, this was before I spoke to a number of representatives from data companies and actually became a bit more optimistic. The fact that high sanctions are introduced means that these parties are now taking the rules seriously. In fact, many data protection officers are now being trained by larger accountancy and consultancy firms, who will be contracted to data companies in order to help them comply with the rules. Maybe this will be a check-box exercise, maybe some initiatives that we feel must be limited aren't under the legalistic interpretation of the GDPR, while others we feel are quite innocent, do fall under the scope. But in general, it might be a good start to create awareness with companies and institutions that they have to take data protection seriously; if the Regulation actually succeeds in getting the American companies to take the data protection principles seriously, I would say this alone would be quite significant. And a number of the bigger companies have actually said that they will apply the GDPR not only to their EU-based activities, but as a global standard (whether this is true only time will tell). Maybe after a decade or so, when most companies have adopted the data protection rules and have internalised the meaning and importance of the principles, it is time to relax the ties a bit and take a less legalistic stance.

Data processing organisations already had decades to rely on their own interpretation and ethical assessments, because the rules on the data protection instruments were pretty open and enforced only to a limited extent. But so far, this has not worked; many parties have in fact not limited their activities in relation to gathering and processing data in reference to what is ethically or socially desirable. In this light, it might be con-

sidered logical to adopt a new, more legalistic stance. It is also important to point out that although the Regulation contains almost 100 articles, the basic rules and principles have actually stayed the same: data minimisation, data quality, transparency, safety and confidentiality, purpose and purpose limitation, extra protection for sensitive data, the right to access and rectification, etc. Some additional rights have been introduced, such as the right to data portability and the right to be forgotten, but this is not the reason why the Regulation is so much bigger than the current Directive. The reason is the introduction of many rules on the applicability, accountability and enforcement of the data protection principles. The problem of data protection rules was obvious - that although the principles sounded nice, they were often ignored in practice. Now, the EU legislator has decided to close the gap between law and practice by investing strongly in rules on enforcement, fines and sanctions.

This has incited another critique directed at the Regulation, to which I was also receptive at first, but now think is not entirely convincing, namely that the rules are outdated and should be changed. Given the gap between the law and practice in the data protection realm, many have said that the rules should change - the law should be adapted to the practice and not the practice to the law, as the EU legislator is trying to do. Proponents of this argument stress that in the age of Big Data, it is simply unrealistic to maintain the 'ancient' data protection principles. Big Data is about gathering as much as data as possible, not about data minimalisation; Big Data analytics can work with messy data, quantity over quality, and so the data quality principle is outdated; there is often no specific purpose for which data are gathered, rather they are gathered and only afterwards it is determined what use they might have; the purpose limitation principle is no longer of use, because the exact idea of Big Data is that data can always be given a second life, by combining them with other data or by aggregating them in new groups or profiles; the transparency principle no longer works, because data controllers often do not know about whom they process data and if they do, they often do not know how to reach the data subjects, etc. That is why some have argued that the law should be changed, not the practice; the legal principles are simply outdated, are no longer realistic, are too complex and muffle innovation. It's an appealing argument, but I've grown ever more sceptical about its strength. Let me discuss and try to rebut some of the arguments that have been put forward against the Regulation and in favour of fewer rules and more open norms,[1] perhaps even one open norm in which all interests are balanced and weighed.[2]

The first argument suggests that the current rules are interpreted too strictly in practice, while the rules themselves actually leave room for many of the new data processing initiatives that are being developed. Although many data controllers think they have to obtain informed consent from the data subject, there are other grounds they can rely on, such as the ground which requires them to balance their own interests against

1 The risk based approach is often used to develop similar arguments; I mostly disagree with those arguments.

2 The most prolific on this point are two colleagues of mine: EML Moerel and JEJ Prins, 'Privacy voor de homo digitalis' (2016) <http://njv.nl/wp-content/uploads/2011/04/Preadviezen-NJV-2016.pdf>.

those of those of the data subject. The data quality principle does not require that all data are absolutely correct and kept up to date constantly; rather, the data controller must undertake a reasonable effort to ensure their quality. Similarly, the requirement to store data securely and confidentially requires data controllers to implement reasonable levels of protection, taking into account the state of the art, the costs of implementation and the nature, scope, context and purposes of processing as well as the risk of varying likelihood and severity for the rights and freedoms of natural persons. A similar argument can be made with respect to the purpose limitation principle. It does not prohibit the re-use of personal data; it only stresses that data may not be re-used for purposes incompatible with the original purpose. Among others, the British Data Protection Authority (DPA) has issued the following statement: 'The DPA does not say that processing for a new purpose is not permissible, nor does it say that the new purpose must be the same as the original purpose, nor even that it must be compatible with the original purpose: it says that it must not be incompatible with it.'[3] Consequently, the argument goes, the current rules themselves already allow for many of the new data initiatives; they are only interpreted and applied too strictly in practice. This argument seems plausible, but it means in fact that the rules contained in the Directive and the Regulation are in fact adequate and do leave sufficient room for new data initiatives. It is not the rules that should change, but their interpretation.

The second argument is that there are simply too many rules and they are too complex for companies and institutions to adequately understand and follow. Rather than relying on the detailed rules and obligations, only a few minimal rules or even one open norm should be adopted instead. This argument seems false for several reasons. First, as stressed above, there is actually only a small set of rules and obligations included the Regulation. The most important ones can be summed up as: have a legitimate purpose, don't re-use data for different purposes, store data safe and confidentially, keep them correct and up to date, be transparent, keep documentation on the processing activity, assess what impact the data processing programme might have, report when data leaks have occurred, stop data processing when the data subject sends a legitimate request and give the data subject the data when requested. This does not seem like an unreasonably long list for data controllers to take into account. Second, these rules are not complex, they seem rather intuitive. To keep data safe, to ensure that they are correct, gather no more data than really needed, etcetera, all seem common sense principles. Third, even if these rules would be considered complex, the company or institution should hire an expert to help it, just like companies hire accountants, competition law experts, lawyers in the field of intellectual property, etc. Data protection is just like many of the other legal norms companies have to abide by; if they do not want to invest in it, they should face the consequences. Fourth, what might make the applicability of the data protection rules a bit complex is that they are rather open-ended. What precisely does it mean to keep data correct and up to date, to store data safely and to abstain from re-using personal data for purposes that are in-

3 United Kingdom's Information Commissioner's Office, 'Big Data and data protection' (2014) <https://ico.org.uk/media/for-organisations/documents/1541/big-data-and-data-protection.pdf> 21.

compatible with the original purpose? It is difficult for data controllers to know exactly what to do in specific situations, because the precise interpretation and applicability of the rules in specific circumstances does not follow from the Regulation. If this argument is true, however, it would point in the direction of more and more detailed rules, instead of less; it would mean a shift towards a more 'check-box' approach and away from relying on the reflexive understanding of the rules by data processors themselves.

The third argument is that the EU regulator is simply ignorant and out of touch with reality. It does not see what is happening in the 'real' world and sticks to the current approach because it does not realize that it no longer works. This is perhaps the weakest argument of all; it echoes the populist opinion that 'Brussels' is out of touch with reality, that the EU-mandarins are unaware of what the common man thinks and that the EU only produces rules that are clearly ridiculous, like specifying the shape of bananas, like the current data protection rules. It also echoes the popular sentiment that law is always lagging behind the rapidly changing technological environment. Of course, at least in this instance, the critique is misplaced; the EU politicians are very well aware of Big Data and other new phenomena and understand perfectly how they relate to the data protection rules. The Article 29 Working Party, the European Data Protection Supervisor and many national DPAs have issued reports on the relationship between data protection and Big Data, the European Commission has discussed this issue multiple times and EU parliamentarians like Jan-Phillip Albrecht are among the most knowledgeable persons in the field. The point is not that they do not know about this new phenomenon, but that they take an approach different from what some data controllers hoped for. It is not the law that is brought into uniformity with the practice, but the practice that will be brought in line with the data protection rules.

The fourth argument is that the rules simply don't work anymore: it is just unrealistic to think that the rules will change the practice, because data collection is so easy, data storage is so cheap and data analytics has developed so quickly that even the high sanctions will not turn the tide. First, a lot depends on one's views on the new data processing techniques. Some think that they are primarily positive and that data processing is an inherent and important part of this progress. Others compare data processing to the environmental pollution following from the Industrial Revolution; they think data processing is the pollution the data revolution is producing. It is difficult to take a stance in this debate. On the one hand, it might be argued that with respect to environmental pollution, we have waited too long, until real, severe and perhaps partially irrevocable damage had occurred, to really try and mitigate the negative effects of the Industrial Revolution. On the other hand, it might be argued that the value and meaning of privacy have changed ever since they were conceived. Perhaps, in 20 years' time, we will find the mass surveillance and Big Data practices a normal part of our lives; just like most citizens are generally okay with many of the data collections that are ongoing right now, which would have shocked and perhaps terrified people 20 years ago. On a final thought, however, I think that until now, all societies that have ever existed have protected some form of privacy and have reserved certain

practices, such as defecation and sex, for the private domain. Although it is not unconceivable that a future society will have no, or very limited, respect for the right to privacy, perhaps it's better to be safe than sorry. Second, the question is whether the Regulation is the right type of instrument to ensure that privacy and data protection are adequately protected. Maybe it is true that these rules will be unable to turn the tide, but maybe the additional obligations for data controllers, the harmonization of the rules in a Regulation having direct effect throughout the EU, the close cooperation between the national Data Protection Authorities, the wide task and capacities of the DPAs, the authority of the Commission to develop further rules on specific points and of course the sanctions which may run up to €20 million or 4% of the worldwide revenue of a company, will be able to turn the tide. I think it is rather cynical to give up before having tried this approach. Third, if it would be argued that it is not the Regulation, but the underlying principles as such that no longer work, and even if this argument would be true, then the most logical stance would be to develop new and better rules, not to throw them away and integrate them into one big balancing exercise.

Fifth and final, and perhaps most prominent argument, is that the current principles muffle innovation. If the rules in the Regulation would be strictly enforced, many companies would have to close shop, many people would lose their jobs and perhaps most importantly, many of the positive aspects of Big Data, such as innovation to the benefit of society, would be unutilised. The strongest reaction I have come across was given by a chair of a DPA I spoke to recently, who said: 'so what, we have had these rules for decades. They have worked well for decades. And they are important conditions and safeguards against the abuse of power by governments and companies.' Sometimes, legal rules prohibit certain innovation, so the counter argument goes, because not all innovation is desirable. To require of a governmental agency to have a legal ground, as established by the democratic legislator, for the gathering of data about citizens seems to be a minimum condition for the legitimacy and legality of governments; the requirement for Google to ensure that the Gmail system is secured against data leaks, seems to be a minimum condition for consumer products, just like there is a prohibition on selling drugs that are ineffective and dangerous, or cars that are clearly unsafe. If a new technology undermines these very basic principles, then alas for this new technology.

In conclusion, I think the Regulation might actually have a chance of changing the data processing environment, but I'm not sure whether it will; I think the rules and principles are still relevant, but it may also be the case that in 20 years' time our interest in privacy and data protection will have lowered drastically; and I think that the Regulation may be the right instrument to close the gap between law and practice, but there may also be other instruments that could prove valuable. Consequently, I think we are at a crossroad now. Will American companies accept the European rules, will citizens become more aware of the dangers of privacy violations and will states curtail their mass surveillance programs, or are these all hopes of times past? I don't know, but I'm very existed to see what happens.

To give a better perspective on the questions that lie ahead of us, we have invited both the old and the new generation of privacy scholars to shed their light on some of the most important developments. We have asked the two sensei of privacy and data protection, Lee Bygrave and Paul De Hert, to reflect on the future of privacy and privacy scholarships in their respective forewords. And we are honoured by the papers of the five young academics, who were selected by a jury of three, from dozens of papers we received for the call for papers to the European Data Protection Law Review's Young Scholars Award. The best five papers are published in this journal and the best three authors will be offered the opportunity to present their research at the Computer, Privacy and Data Protection Conference in Brussels, on 26 January 2017. During this conference, we will also select the very first winner of the EDPL Young Scholars Award. The winner will get the price every privacy scholar longs for: a free subscription for the best privacy and data protection journal … the European Data Protection Law Review. In alphabetical order of the authors' names, the five selected papers are:

István Böröcz: *Risk to the right to the protection of personal data – an analysis through the lenses of Hermagoras*. István has written about the risk-based approach of the GDPR. He believes a unified perception of risk to a right is the necessary as it is the core element of the risk-based approach. A varying perception of risk to a right would undermine the endeavours of the GDPR to harmonize data protection law. His paper proposes a general understanding of risk to a right and risk to the right to the protection of personal data. To understand the concept of risk, more specifically risk to a right, his paper divides the concept of risk into its 'seven circumstances'. The role of circumstances was pivotal in ancient Greek rhetoric. It helped to define the specific attributes of a case. A Greek rhetorician from the second century BC, Hermagoras of Temnos, recognized both thesis and hypothesis as rhetorical controversies. István takes from this seven attributes - *quis* (who), *quid* (what), *quando* (when), *ubi* (where), *cur* (why), *quem ad modum* (in what way), *quibus adminiculis* (by what means) – and uses it to develop an approach to risk in data protection law.

Raphaël Gellert: *We have always managed risks in data protection law: Understanding the similarities and differences between the rights-based and the risk-based approaches to data protection*. Raphaël also discusses the notion of risk in the GDPR. He stresses that the risk-based approach to data protection meant to address the purported shortcomings of the traditional data protection principles, with regard to evolving data processing practices such as Big Data. It does so by replacing these principles with risk analysis tools, the goal of which is to assess the benefits and harms of each processing operation, and on this basis to manage the risk, that is, to take a decision whether or not to undertake the processing at stake. Such risk-based approach has been hailed as diametrically opposed to the legal, rights-based nature of data protection. Raphaël's contribution investigates this opposition and finds that the two approaches (risk-based and rights-based) are actually much more similar than is currently acknowledged. Both aim at managing the risks stemming from data processing operations, he controversially claims. This is epitomised by the fact that they have the exact modus operandi namely, two balancing tests, with risk reduction measures (known

as safeguards in the legal context) associated to the second balancing. Yet, if both approaches manage data processing risks, they nonetheless do so differently. Whereas the risk-based approach manages risks in a contextual, tailor-made manner, the rights-based approach manages risks from the outset once and for all. The contribution concludes with a discussion and possible policy recommendations highlighting the benefits and drawbacks of each approach.

Bryce Goodman: *Big Data's Crooked Timbers: Algorithmic Discrimination and the European Union General Data Protection Regulation*. Bryce's contribution asks whether and to what extent the GDPR effectively addresses algorithmic discrimination. He provides a review of the literature on algorithmic discrimination, highlighting tensions between research on technical v ethical, social and legal aspects, and the need for a robust theory that is sensitive to both areas. He uses mathematical modelling to develop a theory of algorithmic discrimination that has its roots in economic literature on discrimination. He evaluates the GDPR's explicit provisions on algorithmic discrimination and concludes that they are at best an incomplete solution and potentially worsen the problem. Bryce also suggests that the GDPR implicitly supports a more promising solution, algorithm auditing. He analyses potential auditing schemes and argues for an inferential, application-centric and tiered approach, noting a number of open questions along the way. The conclusion of this paper is that the greatest contribution of the GDPR is creating an incentive for private and public organisations to invest in understanding and combating algorithmic discrimination. The GDPR's true value is not the answers it gives, but the questions it raises.

Christopher F Mondschein: *Some iconoclastic thoughts on the effectiveness of simplified notices and icons for informing individuals as proposed in Article 12(1) and (7) GDPR*. Christopher's article discusses the notices and icons used to inform data subjects about the data processes that are affecting them. The article proceeds by first illustrating the information that must be presented to data subjects as well as the way in which it must be presented, along with the measures suggested in the GDPR – ie simplified language notices and standardised icons. Subsequently, the notions of individual and systemic issues faced by individuals are discussed. Christopher draws on findings from empirical research and behavioural economics to illustrate the problems faced by individuals. He discusses the benefits and drawbacks of simplified language and standardised icons with regard to the aforementioned individual and systemic issues and concludes that the Commission may develop standardised icons and an approach to simplified notices that improve the provision of information to data subjects. However, Christopher argues, such an improvement is likely to address only individual issues and neglects to tackle systemic issues with informed consent.

Worku Gedefa Urgessa: *The Protective Capacity of the Criterion of 'Identifiability' under EU Data Protection Law*. Worku's paper addresses the notion of identifiability in the concept of 'personal data'. Data protection laws operate under the assumption that if 'identifiable data' is covered under their protective rules, fundamental rights to privacy and data protection are properly protected. The article aims to challenge this and

other established assumptions underlying the 'identifiability' criterion which serves as one of the essential building blocks of the definition of personal data in the EU data protection law. Worku also analyses the problems associated with the application of the criterion assuming that it serves as a fairly good mechanism of protection. He focuses on legislative sources at the EU level, though national laws are also relied on when pertinent.

The reports section edited by Mark Cole contains four reports. The first is by EDPL Board Member Indra Spiecker and many colleagues. It gives a comparative analysis of the regulation of commercial profiling in Germany, France, UK, US, Brazil and Australia. The second is written by Charles Raab and Roger Clarke and discusses the inadequacies in the UK's Data Science Ethical Framework. The third is by Kristin Benedikt, who provides insights about investigations of smart TV users' security by the German Data Protection Authorities. The final one is written by Jan Tomíšek and covers the relationship between Electronic Healthcare and Data Protection in the Czech Republic. We are also hosting a small section under the Reports section, called 'The Practitioners Corner'. We invite politicians, DPAs, practicing lawyers and others to share in small contributions descriptions or opinions on topical developments in their field. This issue contains one contribution by our new Board Member Axel Freiherr von dem Bussche (Head of the Technology, Media & Telecoms Practice Area at Taylor Wessing), cowritten with Anna Zeiter from eBay. The two data protection experts provide a business perspective on the implementation of the General Data Protection Regulation. We invite others to share their opinions and thoughts for the upcoming issues.

We also have four case notes. Gabriela Zanfir Fortuna has written about the *Amazon* case by the Court of Justice, that almost turned data subjects into consumers. Caroline Calomme writes about the pinion of Advocate General Saugmandsgaard Øe in Joined Cases C-203/15 and C-698/15 by the Court of Justice, about data retention obligations. Fanny Coudert Opinion discusses an opinion by Advocate General Mengozzi of Court of Justice of the European Union about the bulk transfer of PNR data to law enforcement authorities. Finally, Maša Galič has written about the *RE v the UK* case before the European Court of Human Rights, which tackled the topic of covert surveillance of privileged consultations and the weakening of the legal professional privilege. Finally, there are also four book reviews: Mara Paun - *The Privacy Law Sourcebook*; Alessandro Mantelero - *Privacy Revisited. A Global Perspective on the Right to Be Left Alone;* Irene Kamara - *Enforcing Privacy - Regulatory, Legal and Technological Approaches;* and Bart van der Sloot - *Data Protection & Privacy. Jurisdictional Comparisons*.

For those interested in submitting a paper for the Articles section of EDPL, our special focus in the next editions (which does not mean we exclude papers on other topics) is on:

- EDPL 2017/1: Big Data (submission deadline 1 February 2017);

- EDPL 2017/2: Smart Applications (1 May 2017);

- EDPL 2017/3: Law Enforcement (1 August 2017);
- EDPL 2017/4: Young Scholars Award 2017 (15 October 2017).

For those interested in writing an article, report, case note or book review, please email our executive editor, Nelly Stratieva at <stratieva@lexxion.de>.

We hope you will enjoy reading EDPL's fourth edition of 2016!

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