GDPR: a critical review of the practical, ethical and constitutional aspects one year after it entered into force

Talita-Maria Tsekoura and
Fereniki Panagopoulou*

Panteion University,
136, Syggrou Av., Suite 104,
17671, Athens, Greece
Email: ttsekoura@ttlaw.eu
Email: f_panagop@panteion.gr
*Corresponding author

Abstract: The General Data Protection Regulation (GDPR) aims to reform EU data privacy regulation and personal data processing, both in the private and public sectors, by awarding substantial rights to data subjects and obligations to data controllers and processors. Within the first year of its implementation, a heightened awareness regarding the data protection issues of the data subject has been recorded, while, under the threat of the imposition of heavy penalties, data controllers and processors have accelerated their efforts to achieve an acceptable level of GDPR compliance. Furthermore, other aspects of censure are the amended role of the supervisory authorities, the effect of the implementation of the GDPR on competing constitutional rights, the unprecedented extent of its extraterritoriality, and the highly ambitious consistency mechanism. Finally, the GDPR equally aims to protect the free movement of data within the EU and should not be used to trump other constitutional rights, such as the right to information and freedom of expression.

Keywords: General Data Protection Regulation; GDPR; data protection; constitutional law; human rights; technology law; privacy; data processing; data subjects; data controller; data protection authorities; extraterritoriality; consistency mechanism; public administration; private sector; free movement of data.

Reference to this paper should be made as follows: Tsekoura, T-M. and Panagopoulou, F. (2020) 'GDPR: a critical review of the practical, ethical and constitutional aspects one year after it entered into force', *Int. J. Human Rights and Constitutional Studies*, Vol. 7, No. 1, pp.35-51.

Biographical notes: Talita-Maria Tsekoura is a PhD candidate at the School of Public Administration of Panteion University and a corporate legal practitioner. Her doctoral research is focused on the right to human intervention in automated decision making. She has studied Law at Erasmus University of Rotterdam in the Netherlands [J.D./LL.M.)] as well as Philosophy [Bachelor of Arts in Philosophy of a Specific Discipline (BA)] and holds an LL.M. from Harvard Law School University.

Fereniki Panagopoulou is an Assistant Professor of Constitutional Law at Panteion University and a practicing Data Protection Lawyer. She has served for eight years as a Legal Auditor at the Hellenic Data Protection Authority.

She has studied Law at the Law School of the National and Kapodistrian University of Athens [Law Degree (LL.B.) and Post-Graduate Degree (LL.M.) in Public Law], Law and Public Health at the School of Public Health of Harvard University [Master of Public Health (M.P.H.), Law and Public Health Concentration] and Constitutional Law and Bioethics at the Law School of Humboldt Universität zu Berlin (PhD, Title: "The self-determination of the patient").

1 Introduction

The EU 'General Data Protection Regulation' (GDPR) marks the single most important step towards reforming data privacy regulation in recent years. Indeed, the new regulation has brought about significant changes in terms of how data is processed, spanning across all conceivable sectors – from healthcare to banking and beyond. Nevertheless, ideological as the GDPR may appear, it has evoked a substantial amount of disputation regarding its subject matter and objectives. Disparagement has arisen concerning the principles it promotes, the rights of data subjects, the obligations of data controllers and processors, the consequences it will have for the business community, the public sector and the ordinary citizen. Furthermore, other aspects of censure are the amended role of the supervisory authorities, its effect on competing constitutional rights, the unprecedented extent of its extraterritoriality, and last but not least, the liabilities and very high penalties that may be triggered by its infringement. For a few months now that the GDPR has come into force actually[1], one may wonder to what extent these new data laws have affected our lives.

2 The consequences for the business community

The main aim of the GDPR is to create awareness and change the existing mentality, corporate rules and regulations regarding personal data protection, so that data security measures are applied at all appropriate levels. In order to comply with the GDPR, business entities that collect and process personal data of subjects must gain a better understanding of all the systems in which personal data is stored, the original instance of the data and its entire intra and inter-company data lineage. It is imperative that a business should map and comprehend how personal data is handled across its entire ecosystem. Data controllers and processors will no longer find themselves in a state of quasi-immunity and will be responsible for any leakage of data that takes place under their responsibility.

If applied correctly, GDPR compliance could bring direct advantages to businesses, which will allow them to enhance client contentment, develop operational competence, hone tactics and market segmentation, progress up-sell and cross-sell openings and maybe also improve their corporate image (Guy, n.d.). Having said that, complying with the provisions of the GDPR and the spirit of the noble causes it promotes, is a costly and on-going procedure for business entities that are personal data controllers or processors. Most companies will need to make amendments to their existing modus operandi. According to the GDPR, where there are two or more cooperating controllers or when a

processor carries out processing activities on behalf of a controller, their relationships must be contractually regulated in writing.[2] Company employees will require special personal data protection training, companies' human resources departments might need to adjust their curriculum vitae screening and retention procedures, their hiring policies and their communication styles. Company IT departments may need to encrypt various types of personal data in order to safeguard it, IT systems may need to be revisited and updated with the GDPR in mind, personal data may have to be classified and access limited on a need-to-know basis, taking into account the company's business needs and hierarchy. Even if a complete GDPR compliance system is put into place by a business, it will need to be regularly checked and reviewed in order to ensure that it is still valid and sufficient to protect the personal data it processes.

Companies, as the controllers and/or processors, rarely have the necessary know-how in house to provide sufficient guarantees for the implementation of appropriate technical and organisational measures for the protection of data subjects. They mostly need to outsource these services at a significant cost, whereas GDPR compliance is also not a one-off expense. The GDPR is about on-going self-regulation on behalf of the company and the creation of sustainable corporate mechanisms that will be able to adequately respond to the data subject's GDPR grounded demands. Thus, companies are subjected to a quasi-fixed expenditure, which is even more obvious for companies that are obliged to appoint a data protection officer according to Art. 37 GDPR.

It is not, however, entirely inconceivable that the GDPR compliance cost for a company can spiral out of control if data subjects misuse or abuse their GDPR rights. A company may be faced with hundreds of requests for the erasure of specific personal data, coupled with corresponding requests for portability, access and corrections of personal data. If a company is swamped by GDPR related requests by a large number of individual data subjects or even by organised groups of data subjects, such as labour and consumer unions and NGOs[3], it will either have to organise and finance a designated, large department for this purpose, or it will risk defamation and potentially being obliged to pay disproportionately heavy fines. The GDPR does not provide controllers with any protection in such an eventuality.

Furthermore, according to the GDPR, the controller has to justify the subject's personal data it collects and processes[4], mainly in terms of purpose, lawful basis, kind, extent and duration of retention. Initially, in many cases, this 'enhanced', and for many companies, novel awareness manifested itself into a spontaneous and overzealous attempt at misdirected compliance. A characteristic example was that many companies sent out a message to their entire user list requesting that, in the context of the new regulatory framework, they consent to the processing of their personal data which, to a large extent, was not actually required (Gottlieb, 2017) thus giving a 'false sense of compliance' to both the companies and the data subjects. Another example is that quite a number of companies erased a large number of their contacts, without good reason, thus losing a significant part of their clientele, and consequently, of their business potential. More than a few companies spent a considerable amount of money on sending such 'consent' messages or haplessly erasing data, rather than investing towards ensuring that they were actually compliant with the new rules.

Either way, the GDPR related business expenditure will be passed onto the consumer, driving up the price of goods (Ponsoldt and David, 2007). Moreover, it may deflect the controller's or processor's focus on their main raison d'être, which is the development

and growth of their business. The importance of personal data protection should not be underestimated, but the question remains: Is our society willing to potentially pay such a hefty price for personal data protection? What guarantees are there that GDPR will succeed? Furthermore, what feeds the optimism about the GDPR chances of success, when it raises demands far beyond Directive 95/46/EC, the main objectives of which appear to have failed?

3 The consequences for the public sector

The public sector is a country's largest collector and processor of personal data (Bergou, 2018) and thus, the question that arises is whether the public sector leads by example as regards the implementation of the GDPR, and if not, what the consequences thereof are. Given the nature of the services provided by the public sector, it processes, collects and retains an enormous number and variety of personal data on each of its citizens, in many cases of a sensitive nature. Very often, the relevance of the data processed and stored is questionable, whereas the duration of retention is unnecessarily long.

The obligation on the part of the public sector of each EU member state to fully implement the GDPR is expected to dramatically change the way personal data is processed by public authorities, as well as to enhance data subjects' awareness of their GDPR related constitutional rights. In some aspects, the GDPR sets a higher standard of compliance for public authorities. Contrary to the private sector, government agencies that process personal data are *always* required to appoint a data protection officer, whereas public authorities may not use 'legitimate interest' as a legal ground for processing personal data. The GDPR also does not permit public authorities to exchange data with third countries based on the legal ground of 'consent' without suitable safeguards, i.e., legally binding and enforceable agreements between the government authorities involved.

Notwithstanding the above, it is not always evident or easy, in practice, for public sector organisations to comply with their enhanced GDPR obligations, especially since they need to take their complex legacy systems into account; at the same time, neither is the 'public sector' a single integrated organisation: The public sector is composed of:

a public services, which include both public goods and governmental services, such as public education, public healthcare, defence, fire-brigade, police and public infrastructure

b public corporations, which are mostly self-financing commercial enterprises in which the state has a controlling stake.

Since the public sector does not, and realistically, *cannot* provide for a uniform method of personal data protection for each and every one of its so-varied services and enterprises, it will rely on self-regulation per organisation, similarly to the private sector. Thus, it is to be expected that there will be significant disparity in the level of quality and extent of GDPR compliance that each public service provider and enterprise will develop.

The aforementioned disparity is expected to also depend on the funding that the central government of each EU country is willing to allocate to each public service provider and enterprise for GDPR compliance purposes or on the funds they can secure themselves. As already mentioned, achieving GDPR compliance is costly, especially for

the public sector, since, given the enormous amount of data it processes, it requires significant investments in state-of-the-art technological and physical data storage facilities, potentially new integrated robust IT systems, data mapping, risk assessments, personnel training, obligatory data protection officers, controlling and continuously reviewing the relevancy and the legal basis of data processed. It is questionable whether the public realistically has the means, the facilities and the know-how to achieve an acceptable, if not high, standard of GDPR compliance.

Indeed, neither is it a given that the level of compliance will be of the same standard across the public sectors of the various EU member states. The collection, processing, filing, storage methods and systems, both computerised and manual, differ substantially between the various branches of the public sector. Moreover, the public sector of each EU country is organised in a different way. Therefore, data subject rights, like personal data transferability are by no means standardised within the public sector as a whole, let alone between the public sectors of the various EU countries. Furthermore, the financial means of the public sector per EU member state may also differ tremendously and it would not be surprising if this would be reflected in the GDPR protection and compliance level each country awards: it may well be the case that the public sectors of poorer EU countries might award a lower level of personal data protection to their citizens than rich counterparts.

Although reference is made to the 'public sector' as a whole, as we mentioned here above, it consists of a multitude of very different organisations. When the 'state' or the 'public sector' deems it necessary to access and source personal information on a data subject from multiple data banks, it functions as a uniform entity. The opposite, however, is not the case: if a citizen wishes to evoke his/her GDPR rights vis-à-vis the 'state' or the 'public sector' as whole, he/she cannot do so. If, for example, a citizen wishes to access his/her personal information from the 'state' on request, he/she will have to exercise this right across every single public organisation separately and not with regard to the 'state' as a whole. This is to the detriment of the data subject's ability to exercise his/her right to access and to be informed, in a comprehensive and inclusive manner, regarding the sum of the information that the 'state' has on him/her (Flinders, 2018). Consequently, this difference in particular, between the public sector's and the citizen's ability to access his/her personal information, highlights the relational imbalance between the government and its citizens.

Another issue which remains to be clarified in practice by the EU member states, is whether and to what extent public authorities should be subject to administrative fines for GDPR violations.[5] On the one hand, since the risk of a high penalty is possibly the strongest motivator for GDPR compliance, it would be strange to exempt public organisations from these sanctions. On the other hand, the payment of an administrative fee by a public entity to the state for a GDPR violation would ultimately be a zero-sum transaction and thus of no real significance. It is also not clear if the imposition of such administrative fines will also have repercussions for individual civil servants who were assigned the task of GDPR compliance. It would be unfair for both the public organisation and individual civil servants to be fined for GDPR violations, if the public authority had not been granted the necessary financial, technical and human resources to fully implement a GDPR compliance program. Nevertheless, in many cases non-compliance occurs because of an act or omission of an employee, and as such,

his/her personal liability must be determined. In the event of a different approach to such cases, we would be faced with instances of abuse on the part of employees.

4 The consequences for the data subject (ordinary citizen)

Personal data protection legislation, and consequently the GDPR, was primarily put into place in order to protect the rights of data subjects of from potential abuse and misuse of their personal data. Now that the data subject is, assumingly, 'protected' by the implementation of the GDPR, many questions remain unanswered, such as: how much does the average person really understand and care about the GDPR? What are the consequences of the implementation of GDPR in their everyday existence?

All-conquering time shall be the judge of all this. One will be able to answer these questions and many other related queries only after the GDPR has been enforceable for a few years and the relevant research and data has been collected and analysed. Until then, one can only make assumptions and educated guesses. This, however, does not curtail one's curiosity as a multitude of questions remain unanswered: will GDPR related issues be equally important to all age groups and is its importance also culturally defined? It would be interesting to look into how EU citizens from countries that used to be behind the iron curtain, versus those who have always lived in democratic states, feel about personal data collection and processing and whether the GDPR is more or less important to them. Is the older generation, compared with the younger one, more or less concerned about personal data processing issues and their protection? The degree of computer literacy and the general educational level of persons may also be an important determining factor in how they view the GDPR. The level of dissemination of GDPR related information to the ordinary citizen across the various EU countries may also differ substantially and thus affect the way that he/she perceives the GDPR and his/her relevant rights.

Do individuals really care, or have they 'accepted' the idea that through technology, smartphones and CCTV cameras all of their movements, actions, conversations and even their thoughts, are tracked, monitored, registered and analysed and thus consider the GDPR to be a 'smokescreen' or a 'placebo' to cover up this 'given' far-reaching invasion into their private lives? A data protection notification should not end up as just another annoying 'click of the mouse' a user needs to make in order to get to the desired webpage. Also, the GDPR may just end up becoming a useful tool with which a data subject can 'pressure' or 'threaten' a data controller or processor into addressing or resolving a non-GDPR related issue the data subject may have. Therefore, it remains to be seen if and how the GDPR will affect an ordinary EU citizen's everyday life.

All of the above questions rest on the assumption that the GDPR protects the rights of all data subjects, which means the rights of each and every one of us. Is that, however, really true? Personal data and information are collected and processed from the time we are born until we die. Nevertheless – and with the advances of medical science this will be the norm in the near future – the personal data collection process commences even earlier, i.e., at the stage of conception in case of IVF induced pregnancies or with prenatal ultrasounds and screening. This gives rise to the question of whether and to what extent the nasciturus should be protected under the GDPR or whether the mother's data protection rights extend to the nasciturus. In the latter case, why should not the nasciturus also be protected under the biological father's data protection rights, since it equally

carries his/her father's DNA? It would not be unthinkable that the nasciturus, once born, should obtain full data protection rights in retrospect, i.e., going back to the time of conception.

Having said this, irrespective of the level and depth of information and understanding data subjects have regarding the GDPR and their related rights, the publicity surrounding the GDPR has led to a certain elevated level of awareness. Hopefully, this will make the date subjects more careful in terms of what information they 'willingly' share, for which purposes, and on what legal basis. At the same time, it is equally important that data subjects are consciously aware of the extent and the depth of their personal data they regularly 'unwillingly' share, mainly, but not exclusively, through their smartphones, computers and other technical devices. The 'freedom' and 'willingness' of a data subject to share information about him/herself is, more often than not, fully dominated by the default settings of such devices. Refusal to consent, for example, to an application's access to information on a data subject's smartphone, like photos, contacts, and calendar, which in all likelihood contain a multitude of personal and even sensitive data, automatically prohibits the application's downloading.

5 New industry

The enhanced awareness surrounding personal data protection issues and the fear of high penalties in case of non-compliance have spurred the development of an entrepreneurial GDPR related services industry. The GDPR has rekindled the data protection services related market for lawyers, information technology consultants, business consultants, data protection officers and institutions providing GDPR certification and training. This has been the case not only in the EU, where the GDPR has been implemented, but also worldwide, due its extraterritorial scope as per Article 3 GDPR.

The compliance of data processors and controllers with the GDPR is a costly process, both in terms of time and finances. The main mission of GDPR compliance aims at changing and shaping the existing mentality around personal data protection and making it more 'data subject sensitive and friendly', whereas it provides a platform for avoiding administrative penalties. Most companies, however, will not have the necessary expertise to do this in-house. They will have to either employ specialists in the field of personal data protection or they will have to hire the services of external consultants. Similarly, companies that are obliged to appoint a data protection officer in accordance with Art. 37 GDPR, will have to adequately and continuously train such persons so that they remain up to date with regard to any development in the field of personal data protection.

The services of lawyers and legal professionals are regularly required by data controllers and processors in order to help train and guide their data protection officers. Lawyers are also required to draft the necessary written agreements between the data controllers and processors[6] in order to define the scope of their respective actions and liabilities. They are often engaged in order to draft corporate GDPR related policies and to advise on human resources issues pertaining to employee screening and hiring procedures, the processing of employees' personal data and the scope of their right to confidentiality. Another interesting consequence of the implementation of the GDPR is the generally increased awareness that companies have in terms of the need to provide clear and concise information regarding the processing of personal data. Nevertheless,

companies often do not realise that their idea of 'clear and concise' information does not necessarily meet the high standards for transparency and clarity set by the GDPR (Panagopoulou-Koutnatzi, 2018), hence lawyers are often hired to ensure that corporate documents meet these high standards These are just to name a few examples of GDPR related services that the legal profession is now regularly requested to provide.

According to Article 42, Par. 1 GDPR, the EU member states and their supervisory authorities shall encourage the establishment of data protection certification mechanisms and of data protection seals and marks for the purpose of demonstrating GDPR compliance of processing operations by controllers and processors. Therefore, it was no surprise that this need was immediately met by companies, which either extended their existing business in the field of the certifications, so as to include the provision of data protection certifications, seals and marks, or which were setup for this purpose alone.

Insurance companies also jumped at the opportunity to profit from the fear of exorbitantly high penalties for GDPR violations, by starting to design and sell insurance coverage for certain violations of the GDPR. This, of course, entails a certain expenditure for controllers and processors, but there is also an up-side, at least as regards the level of compliance. The involvement of insurance companies will significantly increase the likelihood and extent of the GDPR compliance of processors and controllers, since insurance companies will demand full GDPR compliance as a condicio sine qua non for entering into an insurance agreement. Insurers will instigate their own checks and controls, by regularly demanding information and updates regarding the level of compliance a company have achieved, and thus they will function as quasi GDPR-controllers and gate-keepers.

In order to make a modern, computerised company, GDPR compliant, one needs to work with a multi-disciplinary team of specialists. IT personal data protection specialists are indispensable members of such teams and the need to make all computer systems, programs and electronic databases GDPR friendly and compliant, will create a lot of work for them. Especially in the public sector and in large private organisations, IT specialists will be required to advise and to install state-of-the-art personal data protection software and systems, including electronic data storage facilities. In many cases, IT specialists will advise companies and also assist them in obtaining information security standards, such as, for example, ISO 27001, so that they can prove they have the appropriate technical controls, policies, procedures and information security protection mechanisms in place. The scope of work for the IT specialists in personal data protection will continuously evolve in parallel both with the business needs of the data controller or processor and the developments in the field of information technology in general.

6 The role of the supervisory authorities

A major differentiation between the legislation existing prior to the GDPR and the provisions that it introduces is the severity of the penalties that may be imposed for GDPR violations. Under the pre-existing EU legal framework, penalties used to have a more 'educational' nature. In the past, it was also not unheard of that data controllers and/or processors would perform a cost-benefit analysis in order to decide whether it made financial sense or not to comply with data protection regulations. It is unlikely that this would still occur under the current GDPR, since administrative fines for GDPR violations can run up to 20 million euro or up to 4% of the annual worldwide revenue of

the prior financial year, whichever is higher. The purpose of such severe fines clearly is to deter GDPR violations.

Under the threat of the imposition of exceedingly high penalties, companies will, in all likelihood, be forced to comply with GDPR legislation and adopt more 'personal data friendly practices', bearing the corresponding on-going cost that goes hand in hand with full compliance. Having said that, GDPR compliance is not an exact science and it is not unthinkable that some companies may unwittingly engage in personal data violations, by for example, omitting to retain certain files, or by underestimating the importance or need of commissioning risk and data protection impact assessments. If in such cases companies are subject to very high penalties, this might endanger their existence, or even trigger their financial downfall.

This, of course, also affects and highlights the importance, the role and the scope of work of the relevant Data Protection Supervisory Authorities or departments in the various EU countries. Although all EU countries have a data protection authority or department of some type, their organisational structures, the number of staff they employ and the level of independence of their members varies substantially. Some data protection authorities may find themselves overwhelmed by their increased authorities and scope of work and find themselves being understaffed. Over the past couple of years, for example, in Greece, many employees of the Hellenic Data Protection Authority (2015) chose to resign from their positions in order to profit from the need for GDPR experts in the free market. Finding and hiring new, qualified staff might prove to be a challenge, whereas the same applies when it comes to securing additional funding for these supervisory authorities.

It will be a challenge for data protection authorities across the EU to obtain a similar high standard of independence, expertise and funding in order to ensure the necessary guidance and controls on the implementation of the GDPR. These are issues that, in all likelihood, will affect the extent, the level and the quality of the compliance controls and checks that will be applied by each EU country.

Alas, although the independence of the members of supervisory authorities should be a taken for granted, this may not always be the case. In an ideal world, the independence of the members of a Data Protection Supervisory Authority is embedded in their personal mores and values, it defines who they are and cannot be affected by any other factor. In real life, however, things tend to me more complex. In order to safeguard the independence of the members of supervisory authorities, it is not only important that they are carefully selected and trained: they also need to be adequately remunerated for the work they do. In certain EU countries, the remuneration of the members and staff of Data Protection Supervisory Authorities is so inadequate, especially compared to similar authorities in other EU member states, that this may be a risk factor that will compromise their independence. Members of supervisory authorities may, in such cases, resort to taking up unofficial free-lancing work in the field of data protection. Without wishing to condone such a choice in any way, whatsoever, it is important not to provoke it by underpaying the members of Data Protection Supervisory Authorities. Furthermore, the mechanisms that already exist for the monitoring, control and deterrence of such compromising behaviour by members of supervisory authorities have not always been adequate and should be amended accordingly (Panagopoulou-Koutnatzi, 2016).

Last but not least, because there has been so much discussion about personal data protection and the high penalties imposed by the GDPR, one tends to forget that the

GDPR is not only about personal data protection, but also about 'the free movement of such data'. This imbalance of attention in favour of personal data protection versus its free movement can be viewed and understood in light of the fact that there are independent supervisory authorities which have the power to enforce the protection of personal data, but there are no equivalent single, independent authorities which protect the freedom to access information. The majority of EU countries only have Data Protection Authorities, as opposed to having Data Protection and Access to Information Authorities[7], which would reflect the objectives of the GDPR and task at hand more correctly.

7 GDPR and extraterritoriality

A quite unique aspect of the GDPR is that its regulatory framework extends beyond the EU as a quasi-global law.[8] Looking into its extensive extra-territoriality, we are entering into unchartered waters. Questions arise as to how and to what extent the GDPR can become applicable, and moreover enforceable, in non-EU countries that have not signed up for it. How can a European authority impose sanctions, for example, on a non-European company for a violation of the GDPR, when the country in which the company is domiciled has not ratified it? Are there adequate enforcement mechanisms in existence? It is interesting to theorise about these questions but, ultimately, they remain to be answered in real life practice.

Nevertheless, it is interesting to see that US companies which initially raised an eyebrow and even went as far as to mock the pre-existing EU data protection legislation and the more recent GDPR with its far-reaching protective scope, are starting to understand and worry about the importance of personal data protection and related compliance issues. Thus, increasingly, mainly large companies in the USA have complied or are at the stage of achieving compliance with the new regulatory framework.

Japan has even gone a step further by incorporating a large part of the GDPR in its national legislation. On 25 April 2018, Japan's Data Protection Authority published draft guidelines relating to adequacy findings for international personal data transfers from Europe to Japan. If these guidelines come into force in their current form, subject to the EU's adequacy decision, they will allow for personal data to be transferred from the EEA (which includes the EU countries, Lichtenstein and Norway) to Japan without measures such as specific data subject consent or standard contractual clauses. These guidelines form part of a broader effort to recognise the principle of 'mutual adequacy' between the EU and Japan, respectively, under the GDPR and Japan's Act on the Protection of Personal Information (APPI).

8 The challenges posed by the consistency mechanism

Another revolutionary and significant change in the field of personal data protection within the EU is the use of a regulation, instead of a Directive 95/46/EC, as was the case previously. The GDPR regulates almost all personal data protection issues directly and

member states no longer have to transpose each and every provision into national law. Only as an exception and provided there is adequate justification for divergence from the aim of a fully harmonised legal framework, may certain limited issues be regulated by each EU member state (Albrecht, 2016). The ambition for legal harmonisation across the EU member states also manifests itself[9] in Article 63 GDPR, which provides that "In order to contribute to the consistent application of this regulation throughout the union, the supervisory authorities shall cooperate with each other and, where relevant, with the commission, through the consistency mechanism."

The idea behind this consistency mechanism is that if a supervisory authority of a certain EU member state intends to adopt a GDPR related measure which can reasonably be expected to significantly affect data subjects in other EU member states, or if a supervisory authority of a member state or the commission requests that a certain matter is dealt with consistently within the whole of the EU, the EU supervisory authorities shall cooperate with each other to this end.

It remains to be seen how the consistency mechanism will apply, for example, to administrative fees for GDPR infringements across the EU member states, according to the ambition set forth in Article 150 of the GDPR Recitals. According to Article 83 GDPR, the supervisory authorities of each EU member state may apply administrative fees in respect of GDPR infringements, provided they are assessed per individual case and are effective, proportionate and dissuasive. For the determination of the amount of the fine, as per Par. 2 of Article 83 GDPR, various factors directly linked to the nature and the circumstances of the specific violation itself should be taken into account. Nevertheless, according to Article 150 of the GDPR Recitals, only if a fee is imposed on a person who is not an undertaking should the general level of income in the member state as well as the economic situation of the person be considered. Therefore, the general rule is that for GDPR violations only the circumstances surrounding the violation itself should be taken into account for the determination of the administrative fine.

Given the very significant discrepancy of the GDP level of each EU country and the educational, economic and cultural disparity between the populations of the various member states, it is questionable whether the ambitions of the consistency mechanism as regards the imposition of administrative fines is realistic. A fine for a specific violation in one EU country may be inappropriate, meaning it may be either too low or too high, for the same violation under similar circumstances in another member state.

The consistency mechanism, however, might also be utilised as a 'justification' or 'alibi' for the introduction of certain practices across the EU. If, for example, the personal Data Protection Supervisory Authority of a certain EU member state permits the monitoring and control of an employee's driving behaviour, this 'permission' could be deemed sufficient for employers in other EU members states to engage in the same behaviour, by evoking the consistency mechanism. This would also mean that a misjudgement or error on the part of one EU supervisory authority, permitting or forbidding a certain practice or activity, may have far-reaching consequences for all data controllers and processors in all other EU member states. The consistency mechanism may indirectly lead to a 'quasi right of seniority' of the supervisory authority which happens to be the first to voice an opinion regarding a GDPR related issue or to impose an administrative penalty for a GDPR infringement, thus 'forcing' others to merely follow. These are important questions that remain to be answered in practice.

9 GDPR in relation to other constitutional rights

It is safe to say that the new GDPR and the extensive publicity it has received over the past months, obviously co-driven by the fear of severe penalties in case of its infringement, have enhanced awareness and sensitivity around data processing. At the same time, it is equally safe to say that the other objective of the GDPR which relates to the protection of the free movement of personal data within the union, has not received the same level of attention, at least not in common perception.

According to Recital No. 4 of the GDPR, it is expressly noted that:

> "The right to the protection of personal data is not an absolute right; it must be considered in relation to its function in society and be balanced against other fundamental rights, in accordance with the principle of proportionality. This regulation respects all fundamental rights and observes the freedoms and principles recognised in the charter as enshrined in the treaties, in particular the respect for private and family life, home and communications, the protection of personal data, freedom of thought, conscience and religion, freedom of expression and information, freedom to conduct a business, the right to an effective remedy and to a fair trial, and cultural, religious and linguistic diversity."

In the same spirit, Art. 85 of the GDPR states that "member states shall by law reconcile the right to the protection of personal data pursuant to this Regulation with the right to freedom of expression and information, including processing for journalistic purposes and the purposes of academic, artistic or literary expression."

In this respect, the GDPR does not constitute a novelty. In fact, it is an updated version of Directive 95/46/EU "on the processing of personal data and on the free movement of such data", which contains the same basic principles and places both the protection and the movement of personal data on equal footing. The directive did not aim at providing an absolute and unquestionable right to personal data protection in order to further promote the right to privacy: its objective was to liberate the movement of data within the union in order to facilitate the free movement of goods, capital, services and labour, to the extent that the fundamental right to privacy permits.[10]

Thus, it is clear that the right to information and the right to the protection of personal data should, primarily, be seen as complimentary rights. These rights should be weighed against each other only if they cannot co-exist. Even though both the previous and the new regulatory framework clearly state that personal data protection should be balanced against other fundamental rights, there are strong indications that this is oftentimes not the case. There is concern that our enthusiasm for personal data protection has led to the neglect of other constitutionally protected rights. The right to data protection does not, and should not, per definition, trump other constitutional rights like the right to information and the right of expression. In other words, it is not an absolute and tyrannical right that dominates all others.

Not only our enthusiasm justifies our, sometimes, nearly by default protection of personal data over other constitutional rights. This might also be explained by the need for cost and time efficiency. If, for example, a number of data subjects demand that their personal data be erased by a newspaper, it is in all likelihood, far quicker and thus cheaper for the newspaper to comply with those requests, rather than to justify their refusal by weighing those demands against other constitutional rights on a case by case basis.

In the same spirit, the perceived imperative need for the protection of personal data that has emerged has also led to a widespread refusal towards the provision of information. It is not uncommon to use personal data protection abusively as an excuse and an obstacle to the right to information. Experience has shown that the most problem-free choice on the part of data controllers is simply to refuse to disclose the data that have been requested. The simple reason for this is because an eventual unjustified *provision* of data will be punished far more stringently than a potential case of unjustified *non-disclosure*.

10 Technology

Lastly, concerns have been raised to the effect that parts of the text of the GDPR itself have already started to become questionable, due to rapid technological progress. A characteristic example to point is the use of information technology, automatisation processes and advanced algorithms in individual decision-making activities. Hence, in actual fact, a computer that has been coded and imbued to contain specific pre-defined and pre-decided algorithms, principles, values and parameters, processes the personal data of a vast number of individuals and comes to a decision or selection concerning them. Such systems, due to their speed, efficiency and supposed neutrality, are widely used for activities like hiring of personnel, granting of loans, the sale of health, life insurance policies, etc. These types of processes have raised many concerns regarding the 'instrumentalisation of the data subject' and the 'dehumanising effect' that they have.

In order to mitigate these concerns, Article 22 was drafted into the GDPR, expressly stipulating that in case of automated individual data processing, including profiling, the data subject has the right to secure human intervention on the part of the data controller. The data subject also has the right to receive information on the logic involved in the making of such an automated decision in the context of the assessment in question, as recognised and set out, in practice, in the context of the information duties enshrined in Articles 13(2)f and 14(2)g. Consequently, the data subject essentially has the right to express an opinion and to question the decision taken.

Still, a multitude of questions arise: is trivial human intervention sufficient in terms of meeting the standards set by Art. 22 GDPR or does the intervention need to be substantial? Is the right to information in this case limited, or will it only be met when a data controller hands over to the data subject all technical specifications and algorithms on which the automated processing relies? Or will the duty to inform be met only if and when "meaningful information about the principles and methodology of the data processing" is provided to the data subject in clear and simple to understand terms?

It is also questionable, whether reasoning is possible in every instance, as the manner in which decisions are made through artificial intelligence is no longer always technically known and verifiable (Knight, 2017). In fact, it is often argued that the text of the regulation is characterised by marked disaffection towards the making of automated decisions, without making any reference to the advantages offered by the use of artificial intelligence in the decision-making process (Gola et al., 2007). Artificial intelligence and deep learning systems like Microsoft Project Oxford, IBM Watson, Google DeepMind, Biadu Minwa and LawGeex are facilitating, expediting and augmenting the accuracy of

activities like the diagnosis of certain types of cancer and the review of standard legal contracts (Pearson, 2016).

One of the hailed advantages of automated processing is that it is neutral and unbiased. But is that actually so? At the 'Think 2018' Conference in Las Vegas in March 2018, Arvind Krishna, Head of IBM Research, stated that one of its scientists' predictions is that within five years "we will have new solutions to counter a substantial increase in the number of biased AI systems and algorithms. As we work to develop AI systems we can trust, it's critical to develop and train these systems with data that is fair, interpretable and free of racial, gender, or ideological biases." With this goal in mind, IBM researchers developed a method to reduce the bias that may be present in a training dataset, such that any AI algorithm that later learns from that dataset will perpetuate as little inequity as possible (Balasubramanyam, 2018).

Also, there has been severe criticism regarding the fact that the text of the regulation only offers protection against the making of decisions on the basis of automated processing, whilst it does not adequately address the issue profiling (Schulz, 2017). Profiling means the automated personal data processing towards the evaluation of certain traits on the person's performance in his/her work, the financial situation of the person, his/her health, personal preferences, interests, reliability or behaviour, as well as the position of movements of a person. Notwithstanding the above, there are a multitude of very important character and personality traits and values that are difficult to accurately, and moreover fairly, measure or evaluate through the use of computer systems. Moreover, individual traits are not only important in and by themselves, but oftentimes they need to be seen in context, as per example with the hiring of personnel, where a candidate's good qualifications and a pleasant character do not automatically mean that that person will fit in well in a specific, existing team of people or department.

11 Conclusions

The GDPR has unequivocally increased awareness regarding personal data protection issues and the related constitutional rights of the data subject. Also, under the threat of the imposition of very heavy administrative fees, data controllers and processors, both in the public and the private sector, have accelerated their efforts to achieve an acceptable level of GDPR compliance. This has taken place at a significant, on-going cost for data controllers and processors.

The supervisory authorities of the EU member states have had to adjust to their new enhanced authorities, but also bear the weight of the corresponding responsibility. Depending on their general attitude and how severely they ultimately sanction GDPR infringements, the level of personal data protection will either increase or decrease. The success or failure of the newly introduced, highly ambitious, consistency mechanism will also help define the degree of protection awarded to the personal data of subjects.

The GDPR does not only pertain to the protection of personal data, but equally aims at the protection of the free movement of personal data within the EU. The GDPR rights of the data subject do not, by default, trump the data subject's other fundamental constitutional rights, such as the right to information and free expression. The principle of proportionality must be applied with care and these rights should be seen as complementary rather than competing ones (Vlachopoulos, 2016, 2007).

The road to GDPR compliance, however, may prove to be long, difficult and even at times treacherous and uncharted. Although the GDPR strives to create and impose a uniform regulatory framework across all EU countries, this may prove to be overly optimistic, since many interpretive questions still remain unanswered. Furthermore, despite the introduction of the aforementioned consistency mechanism, discrepancies in the interpretation of the GDPR and the related questions that arise are not unthinkable. Many of these questions will be answered in practice and over time. The GDPR merely provides a framework for self-compliance and self-regulation: it is not an exact science, neither is it a case of 'one size fits all'. As such, it is clear that there is no per definition right or wrong answer to every GDPR question and only time will tell how GDPR matters will evolve and unfold.

Acknowledgements

We express our sincerest gratitude to Dr. Tania Kyriakou for her very productive input.

References

Albrecht, J.P. (2016) 'How the GDPR will change the world', *European Data Protection Law Review*, Vol. 2, No. 3, p.287, DOI [online] https://doi.org/10.21552/EDPL/2016/3/4.

Balasubramanyam, K.R. (2018) 'Think 2018: in 5 years, quantum computing will be mainstream, predicts IBM', *Economic Times Tech*, 20 March [online] https://tech.economictimes.indiatimes.com/news/corporate/think-2018-in-5-years-quantum-computing-will-be-mainstream-predicts-ibm/63374807 (accessed 29 December 2019).

Bergou, E. (2018) *GDPR "X-ray": The Rights, Obligations and the Adaptability Problems*, 25 May, CNN Greece [online] https://www.cnn.gr/eidhseis/tag/74101/lilian-mhtroy (accessed 29 December 2019).

Flinders, K. (2018) *Public Sector Organizations Ill-prepared for GDPR*, 13 March, ComputerWeekly.com [online] https://www.computerweekly.com/news/252436726/Public-sector-organisations-ill-prepared-for-GDPR (accessed 29 December 2019).

Gola, P. (2017) 'Einleitung', in Gola, P. (Ed.): *Datenschutz-Grundverordnung Kommentar* [online] https://beck-online.beck.de/Dokument?vpath=bibdata%2Fkomm%2Fgolakodsgvo_1%2Fewg_dsgvo%2Fcont%2Fgolakodsgvo.ewg_dsgvo.vor1.htm&anchor=Y-400-W-GOLAKODSGVO_1-NAME-ID_6.

Gottlieb, C. (2017) *The GDPR Soft Opt-in Opt-out*, 11 September [online] https://www.linkedin.com/pulse/gdpr-soft-opt-in-opt-out-carl-gottlieb (accessed 29 December 2019).

Guy, A., (n.d.) *The Impact of GDPR on the Public Sector* [online] http://www.frenchduncan.co.uk/blog/the-impact-of-gdpr-on-the-public-sector (accessed 29 December 2019).

Hellenic Data Protection Authority (2015) *Annual Report 2015*, pp.21–22 [online] http://www.dpa.gr/pls/portal/docs/PAGE/APDPX/ANNUALREPORTS/FILES%20ANNUAL%20REPORTS/ANNUAL%202015%20V2.0%20WEB%20VIEW2.PDF (accessed 29 December 2019).

Knight, W. (2017) 'The dark secret at the heart of AI', *MIT Technology Review*, 11 April [online] https://www.technologyreview.com/s/604087/the-dark-secret-at-the-heart-of-ai/ (accessed 29 December 2019).

Panagopoulou-Koutnatzi, F. (2016) 'Exercising control on independent authorities', *Applications of Public Law 2016*, p.253.

Panagopoulou-Koutnatzi, F. (2017) 'The constitutionally enshrined protection relating to decisions on authorizations issued by the Hellenic Data Protection Authority (DPA) for the granting of data', *Administrative Trial Legal Journal*, Vol. 29, No. 3, pp.340–341.

Panagopoulou-Koutnatzi, F. (2018) 'The principle of transparency on data processing', in Kotsalis, L. and Menoudakos, K. (Eds.): *General Data Protection Regulation*, p.233, Nomiki Vivliothiki Publishers, Athens, Greece.

Pearson, C.C. (2016) 'AI supercomputers: Microsoft Oxford, IBM Watson, Google DeepMind, Baidu Minwa', *KDnuggets News* [online] https://www.kdnuggets.com/2016/02/ai-supercomputers-microsoft-ibm-watson-google-deepmind-baidu.html (accessed 29 December 2019).

Ponsoldt, J.F. and David, C.D. (2007) 'A comparison between U.S. and E.U. antitrust treatment of tying claims against Microsoft: when should the bundling of computer software be permitted?', Winter, *Northwestern Journal of International Law and Business*, Vol. 27, pp.447–449.

Schulz, S. (2017) 'Art. 22: Automatisierte Entscheidungen im Einzelfall einschliesslich Profiling', in Gola, P. (Ed.): *Datenschutz-Grundverordnung Kommentar* [online] https://beck-online.beck.de/?vpath=bibdata/komm/GolaKoDSGVO_1/EWG_DSGVO/cont/GolaKoDSGVO.EWG_DSGVO.a22.htm (accessed 29 December 2019).

Vlachopoulos, S.P. (2007) 'Transparency of state actions and protection of personal data. The boundaries between disclosure and secrecy in the executive powers', *Ant. Sakkoula Editions*, p.74, Athens-Komotini, Greece.

Vlachopoulos, S.P. (2016) 'Access to public documents', in Kotsalis, L. (Ed.): *Personal Data, Analysis-Comments-Application*, pp.111, 124–125, Nomiki Vivliothiki, Athens, Greece.

Notes

1 The GDPR (EU) 2016/679 of the European Parliament and of the Council "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" was published in the *Official Journal of the European Union* on the 27th of April 2016. According to Art. 99 Par. 2, the Regulation came into force on the 25th of May 2018.

2 See Articles 26 and 28 GDPR.

3 See Article 60 GDPR.

4 See Article 24 GDPR that states that the controller, will have to ensure and to demonstrate that the data processing of the subject's data is in accordance to the GDPR.

5 See Article 150 GDPR Recitals.

6 See Article 28 Paragraph 3 GDPR.

7 A classic example of authorities that carry out a dual protection function is the German supervisory authority and the corresponding one in the UK (Der Bundesbeauftragte für den Datenschutz und die Informationsfreiheid and the Information Commissioner's Officer, respectively) (Panagopoulou-Koutnatzi, 2017).

8 In accordance with Article 3 GDPR, the territorial scope of the Regulation applies to the activities of an establishment of a controller or a processor that takes place in the EU, but also to the activities of an establishment of a controller or a processor outside the EU, when the processing concerns data subjects who are in the EU (such as, for example, in cases of e-commerce and profiling).

9 See Recital No. 10 GDPR.

10 Within this framework, the considerations of Recitals 3, 8 and 10 of the Preamble of Directive 95/46/EU, that stipulate the following, are important: "(…) (3) Whereas the establishment and functioning of an internal market in which, in accordance with Article 7a of the Treaty, the free movement of goods, persons, services and capital is ensured require not only that personal data should be able to flow freely from one member state to another, but also that the fundamental rights of individuals should be safeguarded; (…) (8) Whereas, in order to remove the obstacles to flows of personal data, the level of protection of the rights and freedoms of

individuals with regard to the processing of such data must be equivalent in all member states; whereas this objective is vital to the internal market but cannot be achieved by the member states alone, especially in view of the scale of the divergences which currently exist between the relevant laws in the member states and the need to coordinate the laws of the member states so as to ensure that the cross-border flow of personal data is regulated in a consistent manner that is in keeping with the objective of the internal market as provided for in Article 7a of the Treaty; whereas community action to approximate those laws is therefore needed; (…) (10) Whereas the object of the national laws on the processing of personal data is to protect fundamental rights and freedoms, notably the right to privacy, which is recognized both in Article 8 of the European Convention for the Protection of Human Rights and Fundamental Freedoms and in the general principles of community law; whereas, for that reason, the approximation of those laws must not result in any lessening of the protection they afford but must, on the contrary, seek to ensure a high level of protection in the community."