E-ISSN: 2360 – 6754; ISSN-L: 2360 – 6754

European Journal of Law and Public Administration

2017, Volume 4, Issue 2, pp.27-39

https://doi.org/10.18662/eljpa/11

2018 REFORM OF EU DATA PROTECTION RULES

Razvan VIORESCU

Covered in:

CEEOL, Ideas RePeC, EconPapers, Socionet, HeinOnline

Published by:

Lumen Publishing House

On behalf of:

**Stefan cel Mare University from Suceava,
Faculty of Law and Administrative Sciences,
Department of Law and Administrative Sciences**

How to cite: Viorescu, R. (2017). 2018 Reform of EU Data Protection Rules. *European Journal of Law and Public Administration*, 4(2), 27-39. https://doi.org/10.18662/eljpa/11

https://doi.org/10.18662/eljpa/11

2018 REFORM OF EU DATA PROTECTION RULES

Razvan VIORESCU[1]

Abstract

As of May 2018, with the entry into application of the General Data Protection Regulation, there is one set of data protection rules for all companies operating in the EU, wherever they are based. Stronger rules on data protection mean: people have more control over their personal data & businesses benefit from a level playing field. The regulation will become directly applicable on 25 May 2018, 2 years after its adoption and entry into force, replacing Directive 95/46/EC.

This issue recaps the main innovations and opportunities opened up by the new EU data protection legislation; takes stock of the preparatory work undertaken so far at EU level; outlines what the European Commission, national data protection authorities and national administrations should still do for bringing the preparation to a successful completion;Sets out measures that the Commission intends to take in the coming months.

Keywords:

data protection, Data Protection Directive, Rights and Citizenship.

JEL Classification: H1, K3

INTRODUCTION

On 6 April 2016, the EU agreed to a major reform of its data protection framework, by adopting the data protection reform package, comprising the General Data Protection Regulation (GDPR) [2] replacing the

[1] University Associate Professor, PhD., Stefan cel Mare" University of Suceava,The Faculty of Law and Administrative Sciences, Romania, razvan.viorescu@fdsa.usv.ro

[2] Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation), OJ L 119, 4.5.2016.

How to cite: Viorescu, R. (2017). 2018 Reform of EU Data Protection Rules. European Journal of Law and Public Administration, 4(2), 27-39. https://doi.org/10.18662/eljpa/11

twenty years old Directive 95/46/EC[3] ('Data Protection Directive') and the Police Directive[4]. On 25 May 2018, the new EU-wide data protection instrument, the General Data Protection Regulation, ("the Regulation"), will become directly applicable, two years after its adoption and entry into force[5].

The new Regulation will strengthen the protection of the individual's right to personal data protection, reflecting the nature of data protection as a fundamental right for the European Union[6].

Providing for a single set of rules directly applicable in the Member States legal orders, it will guarantee the free flow of personal data between EU Member States and reinforce trust and security of the consumers, two indispensable elements for a real Digital Single Market. In this way, the Regulation will open up new opportunities for businesses and companies, especially the smaller ones, also by making clearer rules for international transfers of data. [1]

PRINCIPLES OF THE NEW EU DATA PROTECTION FRAMEWORK — STRONGER PROTECTION AND NEW OPPORTUNITIES

The Regulation continues to follow the approach of the Data Protection Directive [2], but, building on 20 years of EU data protection legislation and relevant case law, it clarifies and modernises the data protection rules; it introduces a number of novel elements that strengthen the protection of individual rights and open opportunities for companies and business, in particular:

• A harmonised legal framework leading to a uniform application of rules to the benefit of the EU digital single market. This means one single set of rules for citizens and businesses. This will address today's situation where EU Member States have implemented the Directive's rules differently.

[3] Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data, OJ L 281 of 23.11.95.

[4] Directive (EU) 2016/680 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data by competent authorities for the purposes of the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, and on the free movement of such data, and repealing Council Framework Decision 2008/977/JHA, OJ L 119, 4.5.2016.

[5] The Regulation has been in force since 24 May 2016 and will apply as of 25 May 2018.

[6] Article 8 of the EU Charter of Fundamental Rights and Article 16 TFEU.

How to cite: Viorescu, R. (2017). 2018 Reform of EU Data Protection Rules. European Journal of Law and Public Administration, 4(2), 27-39. https://doi.org/10.18662/eljpa/11

To ensure a uniform and consistent application in all Member States, a one-stop-shop mechanism is introduced;

• A level-playing field for all companies operating in the EU market. The Regulation requires companies based outside the EU to apply the same rules as companies based in the EU if they are offering goods and services related to the personal data or are monitoring the behaviour of individuals in the Union. Companies operating from outside the EU and active in the Single market must, in certain circumstances, appoint a representative in the EU that citizens and authorities can address in addition to or instead of the company based abroad;

• The principles of data protection by design and by default creating incentives for innovative solutions to address data protection issues from the start, according to Directive 95/46/EC; [3]

• Stronger individuals' rights: The Regulation introduces new transparency requirements; strengthened rights of information, access and erasure ('right to be forgotten'); silence or inactivity will no longer be considered as valid consent as a clear affirmative action to express the consent is required; protecting children online;

• More control over personal data for individuals. The Regulation establishes a new right to data portability, allowing citizens to ask a company or an organisation to receive back personal data he/she provided to that company or organisation on the basis of consent or contract; it will also allow for such personal data to be transmitted directly to another company or organisation, when it is technically feasible. Since it allows the direct transmission of personal data from one company or organisation to another, this right will also support the free flow of personal data in the EU, avoid the 'lock-in' of personal data, and encourage competition between companies. Making it easier for citizens to switch between different service providers will encourage the development of new services in the context of the digital single market strategy;

• Stronger protection against data breaches. The Regulation lays down a comprehensive set of rules on personal data breaches. It clearly defines what is a 'personal data breach', it introduces an obligation to notify the supervisory authority at the latest within 72 hours when the data breach is likely to pose a risk to the individual's rights and freedoms. In certain circumstances, it obliges to inform the person whose data is concerned by the breach. This greatly reinforces the protection compared to the current situation in the EU, in which only electronic communication service providers, operators of essential services and digital service providers are

How to cite: Viorescu, R. (2017). 2018 Reform of EU Data Protection Rules. European Journal of Law and Public Administration, 4(2), 27-39. https://doi.org/10.18662/eljpa/11

obliged to notify data breaches under the Directive on privacy and electronic communications ('ePrivacy Directive')[7] and the Directive on the security of network and information systems (NIS) Directive[8] respectively;

• The Regulation gives all data protection authorities the power to impose fines on controllers and processors. Currently not all of them have this power. This will allow for better implementation of the rules. The fines can go up to EUR 20 million or, in the case of a company, 4% of the worldwide annual turnover;

• More flexibility for controllers and processors processing personal data due to unambiguous provisions on responsibility (the accountability principle). The Regulation moves away from a system of notification to the principle of accountability. This latter is implemented through scalable obligations depending on risk (e.g. the presence of a Data Protection Officer or the obligation to conduct data protection impact assessments). A new tool is introduced in order to help to assess the risk before one starts with the processing: the data protection impact assessment. The latter is required whenever processing is likely to result in a high risk to the rights and freedoms of individuals. Three situations are specifically mentioned as such under the Regulation: when a company evaluates systematically and extensively personal aspects of an individual (including profiling), when it processes sensitive data on a large scale or systematically monitors public areas on a large scale. National data protection authorities will have to make public the lists of cases requiring a data protection impact assessment[9];

• More clarity on the obligations of processors and the responsibility of controllers when selecting a processor;

[7] Directive 2002/58/EC of the European Parliament and of the Council of 12 July 2002 concerning the processing of personal data and the protection of privacy in the electronic communications sector (Directive on privacy and electronic communications), OJ L 201, 31.7.2002, p. 37–47. According to Article 95 GDPR, the GDPR shall not impose additional obligations on natural or legal persons in relation to matters for which they are subject to specific obligations with the same objective set out in Directive 2002/58/EC. This means, for example, that entities covered by the e-Privacy Directive are subject to that Directive's obligation to notify a personal data breach in as far as the breach concerns a service which is materially covered by the ePrivacy Directive. No additional obligations are imposed on them by the GDPR in that respect.

[8] Directive (EU) 2016/1148 of the European Parliament and of the Council of 6 July 2016 concerning measures for a high common level of security of network and information systems across the Union, OJ L 194, 19.7.2016, p. 1–30. Entities within the scope of the NIS Directive should notify incidents having a significant or substantial impact on the provision of some of their services. The incident notification under the NIS Directive is without prejudice to the breach notification under the Regulation.

[9] Article 35 of the Regulation.

How to cite: Viorescu, R. (2017). 2018 Reform of EU Data Protection Rules. European Journal of Law and Public Administration, 4(2), 27-39. https://doi.org/10.18662/eljpa/11

• A modern governance system to ensure that the rules are enforced more consistently and strongly. This includes harmonised powers for the data protection authorities including on fines and new mechanisms for these authorities to cooperate in a network;

• The protection of the personal data guaranteed by the Regulation travels with the data outside the EU ensuring a high level of protection[10]. While the architecture of the rules on international transfers in the Regulation remains essentially the same as that of the 1995 Directive, the reform clarifies and simplifies their use and introduces new tools for transfers. As regards adequacy decisions the Regulation introduces a precise and detailed catalogue of elements that the Commission must take into account when assessing whether a foreign system adequately protects personal data. The Regulation also formalises and expands on the number of alternative transfer instruments, such as standard contractual clauses and binding corporate rules.

The revised Regulation for EU institutions, bodies and offices and agencies[11] and the Regulation on Privacy and Electronic Communications ('ePrivacy Regulation')[12] which are currently being negotiated, once adopted, will ensure that the EU is equipped with a strong and comprehensive set of data protection rules[13].

ACTIONS BY THE ARTICLE 29 WORKING PARTY / EUROPEAN DATA PROTECTION BOARD

The Article 29 Working Party, which groups all national data protection authorities, including the European Data Protection Supervisor, plays a key role in preparing the application of the Regulation by issuing guidelines for companies and other stakeholders. As enforcers of the

[10] Commission Communication on Exchanging and Protecting Personal Data in a Globalised World, COM(2017)7 final.

[11] Proposal for a Regulation of the European Parliament and of the Council on the protection of individuals with regard to the processing of personal data by the Union institutions, bodies, offices and agencies and on the free movement of such data, and repealing Regulation (EC) No 45/2001 and Decision No 1247/2002/EC, COM(2017) 8 final.

[12] Proposal for a Regulation of the European Parliament and of the Council concerning the respect for private life and the protection of personal data in electronic communications and repealing Directive 2002/58/EC (Regulation on Privacy and Electronic Communications), COM(2017) 10 final.

[13] Until the ePrivacy Regulation's adoption and entry into application, Directive 2002/58/EC applies as *lex specialis* to the Regulation.

How to cite: Viorescu, R. (2017). 2018 Reform of EU Data Protection Rules. European Journal of Law and Public Administration, 4(2), 27-39. https://doi.org/10.18662/eljpa/11

Regulation and direct contacts for stakeholders, national data protection authorities are best placed to provide additional legal certainty regarding the interpretation of the Regulation. [4]

The Article 29 Working Party is working to update existing opinions, including on the tools for transferring data to non-EU countries.

Since it is essential for operators to have a coherent and single set of guidelines, the current guidelines at national level need to be either repealed or brought into line with those adopted by the Article 29 Working Party/European Data Protection Board on the same topic.

The Commission attaches great importance to the fact that those guidelines are subject to public consultation before finalisation. It is essential that stakeholders' input in this process be as precise and concrete as possible as this will help identify best practices and bring industry and sectoral features to the attention of the Article 29 Working Party. The final responsibility for those guidelines remains with the Article 29 Working Party and the future European Data Protection Board, and the data protection authorities will refer to them when enforcing the Regulation.

It should be possible to amend the guidelines in the light of developments and practices. To this end, it is essential for data protection authorities to promote a culture of dialogue with all stakeholders, including businesses.

It is important to recall that, where questions regarding the interpretation and application of the Regulation arise, it will be for courts at national and EU level to provide the final interpretation of the Regulation.

MEMBER STATES TO FINALISE THE SET-UP OF THE LEGAL FRAMEWORK AT NATIONAL LEVEL

The Regulation is directly applicable in all the Member States[14]. This means that it enters into force and applies irrespective of any national law measures: the provisions of the Regulation can normally be directly relied on by citizens, business, public administrations and other organisations processing personal data. [5] Nevertheless, in accordance with the Regulation, Member States have to take the necessary steps to adapt their legislation by repealing and amending existing laws, and setting up national data protection authorities[15], choosing an accreditation body[16] and laying

[14] Article 288 TFEU.

[15] Article 54(1) Regulation

How to cite: Viorescu, R. (2017). 2018 Reform of EU Data Protection Rules. European Journal of Law and Public Administration, 4(2), 27-39. https://doi.org/10.18662/eljpa/11

down the rules for the reconciliation of freedom of expression and data protection[17].

Also, the Regulation gives Member States the possibility to further specify the application of data protection rules in specific fields: public sector[18], employment and social security[19], preventive and occupational medicine, public health[20], archiving purposes in the public interest, scientific or historical research purposes or statistical purposes[21], national identification number[22], public access to official documents[23], and obligations of secrecy[24]. In addition, for genetic data, biometric data and data concerning health, the Regulation empowers Member States to maintain or introduce further conditions, including limitations.[25]

Member States' actions in this context are framed by two elements:

- Article 8 of the Charter, meaning that any national specification law must meet the requirements of Article 8 of the Charter (and the Regulation which builds on Article 8 of the Charter), and
- Article 16(2) TFEU, under which national legislation cannot impinge on the free flow of personal data within the EU.

The Regulation is the opportunity to simplify the legal environment, and so have fewer national rules and greater clarity for operators.When adapting their national legislation, Member States have to take into account the fact that any national measures which would have the result of creating an obstacle to the direct applicability of the Regulation and of jeopardising

16 Article 43(1) Regulation provides for Member States to offer two possible accreditation methods to certification bodies, i.e. by the national data protection supervisory authority established in accordance with data protection legislation and/or by the national accreditation body established under Regulation (EC) No 765/2008 on Accreditation and Market Surveillance. The European Cooperation for Accreditation ('EA', recognised under Regulation 765/2008), which gathers national accreditation bodies, and the supervisory authorities of the GDPR should closely cooperate to this effect.

17 Article 85(1) Regulation.

18 Articles 6(2) Regulation.

19 Articles 88 and 9(2)(b) Regulation. The European Pillar of Social Rights also states that *'Workers have the right to have their personal data protected in the employment context*'. (2017/C 428/09, OJ C 428, 13.12.2017, p. 10–15)

20 Article 9(2)(h) and (i) Regulation.

21 Article 9(2)(j) Regulation.

22 Article 87 Regulation.

23 Article 86 Regulation.

24 Article 90 Regulation.

25 Article 9(4) Regulation.

How to cite: Viorescu, R. (2017). 2018 Reform of EU Data Protection Rules. European Journal of Law and Public Administration, 4(2), 27-39. https://doi.org/10.18662/eljpa/11

its simultaneous and uniform application in the whole of the EU are contrary to the Treaties[26].

Repeating the text of regulations in national law [6] is also prohibited (e.g. repeating definitions or the rights of individuals), unless such repetitions are strictly necessary for the sake of coherence and in order to make national laws comprehensible to those to whom they apply[27]. Reproducing the text of the Regulation word for word in national specification law should be exceptional and justified, and cannot be used to add additional conditions or interpretations to the text of the regulation.

The interpretation of the Regulation is left to the European courts (the national courts and ultimately the European Court of Justice) and not to the Member States' legislators. The national legislator can therefore neither copy the text of the Regulation when it is not necessary in the light of the criteria provided by the case law, nor interpret it or add additional conditions to the rules directly applicable under the Regulation. If they did, operators throughout the Union would again be faced with fragmentation and would not know which rules they have to obey. [7]

At this stage, only two Member States have already adopted the relevant national legislation[28]; the remaining Member States are at different stages in their legislative procedures[29] and have schedules for adopting the legislation by 25 May 2018. It is important to give operators enough time to prepare for all the provisions that they have to comply with.

Where Member States do not take the necessary actions required under the Regulation, are late in taking them or make use of the specification clauses provided for under the Regulation in a manner contrary to the Regulation, the Commission will make use of all the tools it has at its disposal, including recourse to the infringement procedure.

---

[26] Case 94/77 *Fratelli Zerbone Snc v Amministrazione delle finanze dello Stato* ECLI:EU:C:1978:17 and 101.

[27] Recital 8 Regulation.

[28] Austria (http://www.ris.bka.gv.at/Dokumente/BgblAuth/BGBLA_2017_I_120/BGBLA_2017_I_120.pdf); Germany (https://www.bgbl.de/xaver/bgbl/start.xav?start=%2F%2F*%5B%40attr_id%3D%27bgbl117s2097.pdf%27%5D#__bgbl__%2F%2F*%5B%40attr_id%3D%27bgbl117s2097.pdf%27%5D__1513091793362).

[29] For the overview of the state of play of the legislative process in the different Member States see http://ec.europa.eu/transparency/regexpert/index.cfm?do=groupDetail.groupDetail&groupID=3461

How to cite: Viorescu, R. (2017). 2018 Reform of EU Data Protection Rules. European Journal of Law and Public Administration, 4(2), 27-39. https://doi.org/10.18662/eljpa/11

DATA PROTECTION AUTHORITIES TO ENSURE THAT THE NEW INDEPENDENT EUROPEAN DATA PROTECTION BOARD IS FULLY OPERATIONAL

It is essential that the new body established by the Regulation, the European Data Protection Board[30], the successor of the Article 29 Working Party, is fully operational as of 25 May 2018.

The European Data Protection Supervisor, which is the data protection authority responsible for supervising EU institutions and bodies, will provide the secretariat of the European Data Protection Board to enhance synergies and effectiveness. In the past months, the European Data Protection Supervisor has started the necessary preparation to this effect.

The European Data Protection Board will be at the centre of data protection in Europe. It will contribute to a consistent application of data protection law and provide a strong basis for cooperation among data protection authorities, including the European Data Protection Supervisor. The European Data Protection Board will not only issue guidelines on how to interpret core concepts of the Regulation but will also be called on to issue binding decisions on disputes regarding cross-border processing. This will ensure the uniform application of EU rules and prevent the same case being dealt with differently in different Member States. [8]

The smooth and efficient functioning of the European Data Protection Board is therefore a condition for the system as a whole to function well. More than ever before, the European Data Protection Board will have to create a common data protection culture among all the national data protection authorities to ensure that the rules of the Regulation are interpreted consistently. The Regulation fosters the cooperation between the data protection authorities by giving them the tools to cooperate effectively and efficiently: they will notably be able to do joint operations, adopt decision in agreement and resolve divergences they might have concerning the interpretation of the Regulation within the Board by means of opinions and biding decisions. The Commission encourages the data protection authorities to embrace these changes and adjust their functioning, financing and work culture to be able to meet the new rights and obligations.

[30] The European Data Protection Board will be an EU body with legal personality in charge of ensuring the consistent application of the Regulation. It will be composed of the head of each data protection authority and of the European Data Protection Supervisor, or their representatives.

How to cite: Viorescu, R. (2017). 2018 Reform of EU Data Protection Rules. European Journal of Law and Public Administration, 4(2), 27-39. https://doi.org/10.18662/eljpa/11

BUSINESSES, PUBLIC ADMINISTRATIONS AND OTHER ORGANISATIONS PROCESSING DATA TO GET READY FOR THE APPLICATION OF THE NEW RULES

The Regulation did not substantially change the core concepts and principles of the data protection legislation put in place back in 1995. This should mean that the vast majority of controllers and processors, provided that they are already in compliance with the existing EU data protection laws, will not need to make major changes to their data processing operations to comply with the Regulation.

The Regulation impacts most on operators whose core business is data processing and/or dealing with sensitive data. It also impacts on those that regularly and systematically monitor individuals on a large scale. These operators will most probably have to appoint a data protection officer, conduct a data protection impact assessment and notify data breaches if there is a risk to the rights and freedoms of individuals. By contrast, operators, in particular SMEs, which do not engage in high risk processing as their core activity will normally not be subject to these specific obligations of the Regulation.

It is important for controllers and processors to undertake thorough reviews of their data policy cycle so as to clearly identify which data they hold, for what purpose and on what legal basis (e.g. cloud environment; operators in the financial sector). They also need to assess the contracts in place, in particular those between controllers and processors, the avenues for international transfers and the overall governance (what IT and organisational measures to have in place), including the appointment of a Data Protection Officer. An essential element in this process is to ensure that the highest level of management is involved in such reviews, provides its input and is regularly updated and consulted on changes to the business's data policy.

To this end, some operators make recourse to compliance checklists (either internal or external), seek advice from consultancies and law firms and look for products that can deliver on the requirements of data protection by design and by default. Each sector must work out arrangements that are appropriate to the specific nature of its area and are adapted to their business model.

Businesses and other organisations processing data will also be able to take advantage of the new tools provided for in the Regulation as an element to demonstrate compliance, such as codes of conduct and

How to cite: Viorescu, R. (2017). 2018 Reform of EU Data Protection Rules. European Journal of Law and Public Administration, 4(2), 27-39. https://doi.org/10.18662/eljpa/11

certification mechanisms. These constitute bottom-up approaches which come from the business community, associations or other organisations representing categories of controllers or processors and reflect best practice, important developments in a given sector or can inform about the level of data protection required by certain products and services. The Regulation provides for a streamlined set of rules for such mechanisms while taking into account market realities (e.g. certification by a certification body or by a data protection authority).

However, while big companies are actively preparing for the application of the new rules, many SMEs are not yet fully aware of the forthcoming data protection rules.

In short, operators should prepare and adjust to the new rules and see the Regulation as:

- an opportunity to put their house in order in terms of what personal data they process and how they manage it;
- an obligation to develop privacy- and data protection-friendly products and build a new relationship with their customers based on transparency and trust; and
- an opportunity to reset their relations with data protection authorities through accountability and proactive compliance.

TO INFORM STAKEHOLDERS, IN PARTICULAR CITIZENS AND SMALL AND MEDIUM-SIZE BUSINESSES

The success of the Regulation rests on proper awareness of all those affected by the new rules (the business community and other organisations processing data, the public sector and citizens). At national level, the task of raising awareness and being the first point of contact for controllers, processors and individuals lies primarily with the data protection authorities. As enforcers of data protection rules in their territory, data protection authorities are also the best placed to explain the changes introduced by the Regulation to companies and the public sector, and to familiarise citizens with their rights. [9]

Data protection authorities have started informing stakeholders in line with the specific national approach. Some hold seminars with public administrations, including at regional and local level, and run workshops with different business sectors in order to raise awareness about the main provisions of the Regulation. Some run specific training programmes for

How to cite: Viorescu, R. (2017). 2018 Reform of EU Data Protection Rules. European Journal of Law and Public Administration, 4(2), 27-39. https://doi.org/10.18662/eljpa/11

data protection officers. Most of them provide information materials in various formats on their websites (checklists, videos, etc.).

However, there is not yet a sufficiently widespread level of awareness among the citizens of the changes and enhanced right that the new data protection rules will bring. The training and awareness raising initiative set in motion by Data Protection Authorities should be continued and intensified, with a particular focus on SMEs. Furthermore, national sectoral administrations can support the activities of data protection authorities and based on their input do their own outreach among the different stakeholders.

CONCLUSIONS

After 25 May 2018, the Commission will closely monitor the application of the new rules and will stand ready to take action should any significant problems arise. One year after the Regulation enters into application (2019) the Commission will organise an event to take stock of different stakeholders' experiences of implementing the Regulation. This will also feed into the report the Commission is required to produce by May 2020 on the evaluation and review of the Regulation. This report will focus in particular on international transfers and the provisions on cooperation and consistency which pertain to the work of data protection authorities.

On 25 May, a new single set of data protection rules will enter into effect across the EU. The new framework will bring significant benefits to individuals, companies, public administrations and other organisations alike. It is also an opportunity for the EU to become a global leader in personal data protection. But the reform can only succeed if all those involved embrace their obligations and their rights.

Since the adoption of the Regulation in May 2016, the Commission has actively engaged with all concerned actors — governments, national authorities, business, civil society — in view of the application of the new rules. A significant amount of work has been dedicated to ensure widespread awareness and full preparation, but there is still work to do. Preparations are progressing at various speeds across Member States and among the various actors. Moreover, knowledge of the benefits and opportunities brought by the new rules is not evenly spread. There is in particular a need to step up awareness and accompany compliance efforts for SMEs.

The Commission therefore calls on all concerned actors to intensify the ongoing work to ensure the consistent application and interpretation of

How to cite: Viorescu, R. (2017). 2018 Reform of EU Data Protection Rules. European Journal of Law and Public Administration, 4(2), 27-39. https://doi.org/10.18662/eljpa/11

the new rules across the EU and to raise awareness among businesses and citizens alike. The Commission will support these efforts with funding and administrative support and will help raise general awareness, notably by launching the online guidance toolkit.

Data are becoming very valuable for today's economy and are essential to daily lives of the citizens. The new rules offer a unique opportunity for businesses and the public alike. Businesses, especially the smaller ones, will be able to benefit from the innovation-friendly single set of rules and put their houses in order in terms of personal data to restore consumer's trust and use it as their competitive advantage across the EU. Citizens will be able to benefit from the stronger protection of personal data and gain better control over how the data are handled by the companies. [10]

In a modern world with a booming digital economy the European Union, its citizens and businesses must be fully equipped to reap the benefits and understand the consequences of data economy. The new Regulation offers the necessary tools to make Europe fit for the 21st century.

REFERENCES

[1] Communication from the Commission to the European Parliament and the Council Stronger protection, new opportunities - Commission guidance on the direct application of the General Data Protection Regulation as of 25 May 2018 COM(2018)43 final

[2] Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC

[3] Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data

[4] EU Charter of Fundamental Rights

[5] Kolah, A. (2018). *The GDPR Handbook: A Guide to the EU General Data Protection Regulation*. Kogan Page, Limited.

[6] von dem Bussche, A., Voigt, P. (2017). *Data Protection in Germany: Including EU General Data Protection Regulation 2018*. C.H. Beck.

[7] Cushway, B. (2017). *The Employer's Handbook 2017-2018*. Kogan Page Publishers.

[8] Leenes,R., van Brakel,R., Gutwirth, S., De Hert, P. (2017). *Data Protection and Privacy: The Age of Intelligent Machines*. Bloomsbury Publishing.

[9] Lambert, P. (2017). *Understanding the New European Data Protection Rules*. CRC Press.

[10] ITGP Privacy Team (2017). *EU General Data Protection Regulation (GDPR): An Implementation and Compliance Guide* - Second edition. IT Governance Ltd.

How to cite: Viorescu, R. (2017). 2018 Reform of EU Data Protection Rules. European Journal of Law and Public Administration, 4(2), 27-39. https://doi.org/10.18662/eljpa/11