EUROPEAN
COMMISSION

Brussels, 24.1.2018
COM(2018) 43 final

# 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

**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**

## 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) [1] replacing the twenty years old Directive 95/46/EC[2] ('Data Protection Directive') and the Police Directive[3]. 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[4].

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[5].

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.

Even though the new data protection framework has been built on the existing legislation, it will have a wide ranging impact and will require significant adjustments in certain aspects. For this reason, the Regulation provided for a transition period of 2 years - until 25 May 2018 - to give Member States and stakeholders time to fully prepare for the new legal framework.

Over the past two years all stakeholders, from national administrations and national data protection authorities to data controllers and processors, have engaged in a number of activities to ensure that the importance and the scale of the changes brought about by the new data protection are well understood and that all actors are ready for its application. As the deadline of 25 May approaches, the Commission believes that it is necessary to take stock of

[1] 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.

[2] 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.

[3] 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.

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

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

this work and look into any further steps that may be useful to ensure all elements are in place for a successful entry into effect of the new framework[6].

This Communication:

- 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.

Furthermore, in parallel with the adoption of this Communication, the Commission launches an online toolkit to help stakeholders prepare for the application of the Regulation and, with the support of the Representation offices, an information campaign in all Member States.

## 1. THE NEW EU DATA PROTECTION FRAMEWORK — STRONGER PROTECTION AND NEW OPPORTUNITIES

The Regulation continues to follow the approach of the Data Protection Directive, 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. 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;

- **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;

[6] https://ec.europa.eu/commission/sites/beta-political/files/letter-of-intent-2017_en.pdf.

- **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 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

---

[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.

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**;

- **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].

## 2. PREPARATORY WORK UNDERTAKEN SO FAR AT EU LEVEL

The successful application of the Regulation requires cooperation between all those involved in data protection: Member States, including public administrations, national data protection authorities (DPAs), businesses, organisations processing personal data and individuals as well as the Commission.

### 2.1 Actions by the European Commission

Shortly after the Regulation entered into force mid-2016, the Commission has engaged with Member States' authorities, data protection authorities and stakeholders to prepare the application of the Regulation and provide support and advice.

---

[9] Article 35 of the Regulation.

[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.

*a) Supporting Member States and their authorities*

The Commission has been working very closely with the Member States to support their work during the transition period, with a view to ensuring the highest possible level of consistency. To this end, the Commission has set up an Expert Group to accompany the Member States in their effort to prepare for the Regulation. The Group, which met already 13 times, acts as a forum where the Member States can share their experiences and expertise [14]. The Commission also engaged in bilateral meetings with Member States' authorities to discuss issues arising at national level.

*b) Supporting the individual data protection authorities and the creation of the European Data Protection Board*

The Commission has been actively supporting the work of the Article 29 Working Party also in view of ensuring a smooth transition to the European Data Protection Board[15].

*c) International outreach*

The Regulation will further strengthen the EU ability to actively promote its data protection values and facilitate cross border data flows by encouraging the convergence of legal systems globally[16]. EU data protection rules are increasingly recognised at international level as setting out some of the highest standards of data protection in the world. Council of Europe Convention 108, the only legally binding multilateral instrument in the area of personal data protection, is also being modernised. The Commission is working for it to reflect the same principles as those enshrined in the new EU data protection rules and thus help install a uniform set of high data protection standards. The Commission will actively promote the swift adoption of the modernised text of the Convention with a view to the EU becoming a Party to it[17]. The Commission encourages non-EU countries to ratify Council of Europe Convention 108 and its additional Protocol.

Furthermore, several countries and regional organisations outside the EU, from our immediate neighbourhood to Asia, Latin America and Africa, are adopting new data protection legislation or updating the existing one in order to harness the opportunities offered by the global digital economy and respond to the growing demand for stronger data security and privacy protection. While countries differ in their approach and their level of legislative development, there are signs that the Regulation serves increasingly as a reference point and a source of inspiration[18].

---

[14] For a complete list of the meetings, agendas, summary of discussions and overview of the state of play of legislation in the different Member States see http://ec.europa.eu/transparency/regexpert/index.cfm?do=groupDetail.groupDetail&groupID=3461.

[15] For instance, the Commission will provide to the European Data Protection Board the possibility to use the Internal Market Information System (IMI) for the communication between its members.

[16] Reflection Paper on Harnessing Globalisation COM(2017)240.

[17] Council of Europe Convention of 28 January 1981 for the Protection of Individuals with regard to Automatic Processing of Personal Data (ETS No 108) and the 2001 Additional Protocol to the Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data, regarding supervisory authorities and transborder data flows (ETS No 181). The Convention is open to non-members of the Council of Europe, has already been ratified by 51 countries (including by Uruguay, Mauritius, Senegal and Tunisia).

[18] See e.g. Data Protection Standards of the Ibero-American States', http://www.redipd.es/documentacion/common/Estandares_eng_Con_logo_RIPD.pdf

In this context, the Commission is pursuing its international outreach in line with its January 2017 Communication[19] by actively engaging with key trading partners, notably in East and South-East Asia and Latin America to explore the possibility to adopt adequacy decisions[20].

In particular, the Commission is working with Japan towards achieving a simultaneous finding of an adequate level of protection by both sides by early 2018, as announced by President Juncker and Prime Minister Abe in their joint declaration of 6 July 2017[21]. Talks have also been launched with South Korea in view of a possible adequacy decision. The adoption of an adequacy decision would ensure the free flow of data with the concerned third countries while ensuring that a high level of protection applies when personal data is transferred from the EU to these countries.

At the same time, the Commission is working with stakeholders with a view to harnessing the full potential of the GDPR toolkit for international transfers by developing alternative transfer mechanisms adapted to the particular needs of specific industries and/or operators[22].

*d) Engaging with stakeholders*

The Commission has organised a number of events to reach out to stakeholders[23]. A new workshop aimed at consumers is planned for the first quarter of 2018. Dedicated sectoral discussions in areas such as research and financial services have also taken place.

The Commission has also set up a multi-stakeholder group on the Regulation composed of civil society and business representatives, academics and practitioners. This group will advise the Commission in particular on how to achieve an appropriate level of awareness about the Regulation among stakeholders[24].

Finally, the European Commission through its Framework Programme for research and innovation Horizon 2020[25] has funded actions to develop tools supporting the effective application of the rules under the Regulation in relation to consent and on privacy-preserving methods of data analytics such as multi-party computing and homomorphic encryption.

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

---

[19] COM(2017)7.
[20] COM(2017)7 ibid p. 10-11.
[21] http://europa.eu/rapid/press-release_STATEMENT-17-1917_en.htm.
[22] COM(2017)7 ibid p. 10-11.
[23] Two workshops with the industry in July 2016 and April 2017, two business Round Tables in December 2016 and May 2017, a workshop on health data in October 2017, and a workshop with SMEs representatives in November 2017.
[24] http://ec.europa.eu/transparency/regexpert/index.cfm?do=groupDetail.groupDetail&groupID=3537.
[25] https://ec.europa.eu/programmes/horizon2020/h2020-sections

| Guidelines/working documents by the Article 29 Working Party in view of the entry into application of the Regulation[26] | |
|---|---|
| Right to data portability | Adopted on 4-5 April 2017 |
| Data protection officers | |
| Designation of the lead Supervisory Authority | |
| Data protection impact assessment | Adopted on 3-4 October 2017 |
| Administrative fines | Adopted on 3-4 October 2017 |
| Profiling | Work ongoing |
| Data breach | Work ongoing |
| Consent | Work ongoing |
| Transparency | Work ongoing |
| Certification and accreditation | Work ongoing |
| Adequacy referential | Work ongoing |
| Binding corporate rules for controllers | Work ongoing |
| Binding corporate rules for processors | Work ongoing |

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.

[26] All adopted guidelines are available at: http://ec.europa.eu/newsroom/just/item-detail.cfm?item_id=50083.

## 3. REMAINING STEPS FOR SUCCESSFUL PREPARATION

### 3.1 Member States to finalise the set-up of the legal framework at national level

The Regulation is directly applicable in all the Member States[27]. 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. 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[28], choosing an accreditation body[29] and laying down the rules for the reconciliation of freedom of expression and data protection[30].

Also, the Regulation gives Member States the possibility to further specify the application of data protection rules in specific fields: public sector[31], employment and social security[32], preventive and occupational medicine, public health[33], archiving purposes in the public interest, scientific or historical research purposes or statistical purposes[34], national identification number[35], public access to official documents[36], and obligations of secrecy[37]. In addition, for genetic data, biometric data and data concerning health, the Regulation empowers Member States to maintain or introduce further conditions, including limitations.[38]

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

1. 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
2. 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.

---

[27] Article 288 TFEU.
[28] Article 54(1) Regulation
[29] 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.
[30] Article 85(1) Regulation.
[31] Articles 6(2) Regulation.
[32] 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)
[33] Article 9(2)(h) and (i) Regulation.
[34] Article 9(2)(j) Regulation.
[35] Article 87 Regulation.
[36] Article 86 Regulation.
[37] Article 90 Regulation.
[38] Article 9(4) Regulation.

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 its simultaneous and uniform application in the whole of the EU are contrary to the Treaties[39].

Repeating the text of regulations in national law 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[40]. 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.

At this stage, only two Member States have already adopted the relevant national legislation[41]; the remaining Member States are at different stages in their legislative procedures[42] 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.

---

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

[40] Recital 8 Regulation.

[41] 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).

[42] 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

### 3.2 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[43], 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.

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.

### 3.3 Member States to provide the necessary financial and human resources to national data protection authorities

The establishment of fully independent supervisory authorities in each Member State is essential to ensure the protection of natural persons with regard to the processing of their personal data in the EU[44]. Supervisory authorities cannot effectively safeguard individual rights and freedoms unless they act completely independently. Any failure to ensure their independence and the effective exercise of their powers has a wide-ranging negative impact on the enforcement of data protection legislation[45].

---

[43] 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.

[44] Recital 117 and previously stated already in Recital 62 of Directive 95/46.

[45] Communication from the Commission to the European Parliament and the Council on the follow-up of the Work Programme for better implementation of the Data Protection Directive, COM(2007) 87 final, 7 March 2007.

The Regulation codifies the requirement of any data protection authority to act completely independently[46]. It strengthens national data protection authorities' independence and provides them with uniform powers across the EU, so that they are properly equipped to deal effectively with complaints, carry out effective investigations, take binding decisions and impose effective and dissuasive sanctions. It also gives them the power to issue administrative fines on controllers or processors up to EUR 20 million, or in the case of an undertaking, up to 4 % of the total worldwide annual turnover of the preceding financial year, whichever is higher.

The data protection authorities are the natural interlocutors and first point of contact for the general public, businesses and public administrations for questions regarding the Regulation. The data protection authorities' role includes informing controllers and processors of their obligations and raising the general public's awareness and understanding of the risks, rules, safeguards and rights in relation to data processing. It does not mean, however, that controllers and processors should expect to be provided by the data protection authorities with the kind of tailored, individualised legal advice that only a lawyer or a data protection officer can provide.

The national data protection authorities therefore play a central role, but the relative imbalance between the human and financial resources allocated to them in different Member States can jeopardise their effectiveness and ultimately the complete independence required under the Regulation. It can also negatively impact the way the data protection authorities are able to exercise powers such as their investigation powers. Member States are encouraged to fulfil their legal obligation to provide their national data protection authority with the human, technical and financial resources, premises and infrastructure necessary for the effective performance of its tasks and exercise of their powers.[47]

### 3.4 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

[46] Article 52 Regulation.
[47] Article 52(4) Regulation.

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 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.

### 3.5 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.

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 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.

## 4. NEXT STEPS

In the coming months, the Commission will continue actively supporting all actors in preparing for the application of the Regulation.

*a) Work with Member States*

The Commission will continue working with Member States in the lead-up to May 2018. From May 2018 onward, it will monitor how Member States apply the new rules and take appropriate action as necessary.

b) New online guidance in all EU languages and awareness-raising activities

The Commission is making available practical guidance materials[48] to help businesses, in particular SMEs, public authorities and the public to comply with and benefit from the new data protection rules.

The guidance takes the form of a practical online tool available in all EU languages. The online tool will be regularly updated and is intended to serve three main target audiences: citizens, businesses (in particular SMEs) and other organisations, and public administrations. It comprises questions and answers selected based on feedback received from stakeholders with practical examples and links to various sources of information (e.g. articles of the Regulation; guidelines of Article 29 Working Party/European Data Protection Board; and materials developed at national level).

The Commission will regularly bring up to date the tool, adding questions and updating the answers, based on the feedback received and in the light of any new issues arising from implementation.

The guidance will be promoted through an information campaign and dissemination activities in all Member States, targeting businesses and the public.

As the Regulation provides for stronger individual rights, the Commission will also engage in awareness-raising activities and participate in events across the Member States to inform citizens about the benefits and impact of the Regulation.

[48] The guidance will contribute to a better understanding of EU data protection rules, but only the text of the Regulation has legal force. As a consequence, only the Regulation is liable to create rights and obligations for individuals.

*c) Financial support for national campaigns and awareness raising*

The Commission is supporting awareness-raising and compliance efforts undertaken at national level by awarding grants that can be used to provide training within data protection authorities, public administrations, legal professions and data protection officers[49] and to familiarise them with the Regulation.

Around EUR 1.7 million will be allocated to six beneficiaries covering more than half of EU Member States. Funding will be targeted at local public authorities, including data protection officers of local public authorities, of public authorities and from the private sector, judges and lawyers. The grants will be used to develop training materials for data protection authorities, data protection officers and other professionals, as well as 'train the trainer' programmes.

The Commission has also issued a call for proposals specifically aimed at data protection authorities. It will have a total budget of up to EUR 2 million and will support them in reaching out to stakeholders[50]. The objective is to provide 80 % co-financing to measures taken by data protection authorities in 2018-2019 to raise awareness among businesses, in particular SMEs, and reply to their queries. This funding can also be used to raise awareness among the general public.

*d) Assessing the need to make use of the Commission's empowerments*

The Regulation [51] allows the Commission to issue implementing or delegated acts to further support the implementation of the new rules. The Commission will only make use of these empowerments when there is a clearly demonstrated added-value and based on feedback from stakeholders' consultation. In particular, the Commission will look into the issue of certification based on a study contracted with external experts and input and advice on this issue from the multi-stakeholder group on the Regulation established at the end of 2017. The work done by the European Union Agency for Network and Information Security (ENISA) in the field of cybersecurity will also be relevant in this context.

---

[49] Grants provided under the Rights and Citizenship 2016 Programme https://ec.europa.eu/research/participants/portal/desktop/en/opportunities/rec/calls/rec-data-2016.html#c,topics=callIdentifier/t/REC-DATA-2016/1/1/1/default-group&callStatus/t/Forthcoming/1/1/0/default-group&callStatus/t/Open/1/1/0/default-group&callStatus/t/Closed/1/1/0/default-group&+identifier/desc).

[50] http://ec.europa.eu/research/participants/portal/desktop/en/opportunities/rec/topics/rec-rdat-trai-ag-2017.html

[51] Delegated act for information to be presented by the icons and the procedures for providing standardised icons (Article 12(8) Regulation); Delegated act for requirements to be taken into account for certification mechanism (Article 43(8) Regulation); implementing act for laying down technical standards for certification mechanisms and data protection seals and marks, and mechanisms to promote and recognise those certification mechanisms, seals and marks (Article 43(9) Regulation); implementing act for the format and procedures for the exchange of information between controllers, processors and supervisory authorities for binding corporate rules (Article 47(3) Regulation); implementing acts for format and procedures for mutual assistance and for the exchange of information by electronic means between supervisory authorities (Articles 61(9) and 67 Regulation).

*e) Integration of the Regulation into the EEA-Agreement*

The Commission will pursue its work with the three EFTA States (Iceland, Liechtenstein, and Norway) in the European Economic Area (EEA) to integrate the Regulation into the EEA agreement.[52] It is only once the integration of the Regulation into the EEA agreement is in force, that personal data can flow freely between EU and EEA countries in the same way as they do between EU Member States.

*f) Withdrawal of the United Kingdom from the EU*

In the context of the negotiations of a withdrawal agreement between the EU and the United Kingdom on the basis of Article 50 of the Treaty on the European Union, the Commission will pursue the objective to ensure that the provisions of Union law on personal data protection applicable on the day preceding the withdrawal date continue to apply to personal data in the United Kingdom processed before the withdrawal date[53]. For example, the individuals concerned should continue to have the right to be informed, the right of access, the right to rectification, to erasure, to restriction of processing, to data portability as well as the right to object to processing and not to be subject to a decision based solely on automated processing, on the basis of relevant provisions of Union law applicable on the withdrawal date. Personal data referred to above should be stored no longer than is necessary for the purposes for which the personal data was processed.

As of the withdrawal date, and subject to any transitional arrangement that may be contained in a possible withdrawal agreement, the rules of the Regulation for transfers of personal data to third countries will apply to the United Kingdom.[54]

*g) Taking stock in May 2019*

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.

**Conclusion**

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.

---

[52] For information on the state of play, see http://www.efta.int/eea-lex/32016R0679.

[53] https://ec.europa.eu/commission/publications/position-paper-use-data-and-protection-information-obtained-or-processed-withdrawal-date_en

[54] See Commission Notice to stakeholders: withdrawal of the United Kingdom and EU rules in the field of data protection (http://ec.europa.eu/newsroom/just/document.cfm?action=display&doc_id=49245).

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 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.

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.

The Commission will undertake the following actions:

*Towards Member States*

- The Commission will continue working with Member States to promote consistency and limit fragmentation in the application of the Regulation, taking into account Member States' room for specification under the new legislation;

- After May 2018 the Commission will closely monitor the application of the Regulation in Member States and take appropriate actions as necessary, including the recourse to infringement actions;

*Towards data protection authorities*

- Until May 2018 the Commission will support the work of the data protection authorities in the context of the Article 29 Working Party and in the transition towards the future European Data Protection Board; after May 2018, it will contribute to the work of the European Data Protection Board;

- In 2018-2019 the Commission will co-finance (total budget of up to EUR 2 million) awareness-raising actions undertaken by data protection authorities at national level (projects implemented from mid-2018 onwards);

*Towards stakeholders*

- The Commission will launch an online practical guidance tool that includes questions and answers aimed at citizens, businesses and public administrations. The Commission intends to promote this guidance to the target audiences through an information campaign addressed to business and the public in the run-up to May 2018 and afterwards;

- In 2018 and beyond the Commission will continue actively engaging with stakeholders notably through the multi-stakeholder group on the implementation of the Regulation and level of awareness of the new rules;

*Towards all actors*

- In 2018-2019 the Commission will assess the need to make use of its power to adopt delegated or implementing acts;

- In May 2019, the Commission will take stock of the Regulation implementation and will report on the application of the new rules in 2020.