EUROPEAN
COMMISSION

Brussels, 24.7.2019
COM(2019) 374 final

COMMUNICATION FROM THE COMMISSION TO THE EUROPEAN PARLIAMENT AND THE COUNCIL

Data protection rules as a trust-enabler in the EU and beyond – taking stock

Communication from the Commission to the European Parliament and the Council

Data protection rules as a trust-enabler in the EU and beyond – taking stock

I. Introduction

The General Data Protection Regulation[1] (hereafter 'the Regulation') applies across the European Union since over one year. It is at the centre of a coherent and modernised EU data protection landscape that also includes the Data Protection Law Enforcement Directive[2] and the Data Protection Regulation for EU institutions and bodies[3]. This framework is to be completed by the e-Privacy Regulation which is currently in the legislative process.

Strong data protection rules are essential to guarantee the fundamental right to the protection of personal data. They are central to a democratic society[4] and an important component of an increasingly data-driven economy. The EU aspires to seize the many opportunities that the digital transformation offers in terms of services, jobs and innovation, while at the same time tackling the challenges these bring. Identity theft, leaks of sensitive data, discrimination of individuals, in-built bias, sharing illegal content and the development of intrusive surveillance tools are just a few examples of issues that increasingly feature in the public debate where it is clear that people expect their data to be protected.

Data protection has become a truly global phenomenon as people around the world increasingly cherish and value the protection and security of their data. Many countries have adopted or are in the process of adopting comprehensive data protection rules based on principles similar to those of the Regulation, resulting in a global convergence of data protection rules. This offers new opportunities to facilitate data flows, between commercial operators or public authorities, while improving the level of protection for the personal data in the EU and across the globe.

---

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, p. 1): https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A32016R0679.

2 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: https://eur-lex.europa.eu/legal-content/EN/ALL/?uri=celex:32016L0680. The Directive had to be transposed by Member States by 6 May 2018. The Security Union Reports provide the state of play on its transposition.

3 Regulation (EU) 2018/1725 of the European Parliament and of the Council of 23 October 2018 on the protection of natural persons 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, OJ L 295, 21.11.2018, p. 39-98: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A32018R1725. It became applicable on 11 December 2018.

4 The Indian Supreme Court, in a landmark judgment of 24 August 2017, recognised privacy as a fundamental right, an 'essential facet of the dignity of the human being'.

Data protection is taken more seriously than ever before and it has a wide-ranging impact on different stakeholders and sectors. The Commission is determined to lead the EU to a successful implementation of the new data protection regime and to support all aspects of it becoming fully operational. With this Communication, the Commission takes stock of the results achieved so far as in relation to the consistent implementation of the data protection rules across the EU, the functioning of the new governance system, the impact on citizens and businesses and the EU's efforts in promoting global convergence of data protection regimes. It follows-up on the Commission Communication on the application of the Regulation of January 2018[5], and it has been informed by the work of the Multi-stakeholder Group[6], in particular its contribution to the one-year stocktaking exercise as well as the discussions held at the stocktaking event organised by the Commission on 13 June 2019[7]. This Communication is also a contribution to the review that the Commission plans to carry out by May 2020 [8].

The EU data protection legislative framework is a cornerstone of the European human-centric approach to innovation. It is becoming part of the regulatory floor for a widening range of policies including health and research, artificial intelligence, transport, energy, competition and law enforcement. The Commission has consistently emphasised the importance of a proper implementation and enforcement of the new data protection rules, as highlighted in its Communication on the application of the Regulation issued in January 2018 and its Guidance on the use of personal data in the electoral context published in September 2018[9]. At the time of this Communication, a lot of progress had been made towards this objective, although more work is certainly needed for the Regulation to become fully operational.

II. One continent, one law: the data protection framework is in place in Member States

One key objective of the Regulation was to do away with a fragmented landscape of 28 different national laws that existed under the previous Data Protection Directive[10] and to provide legal certainty for individuals and businesses throughout the EU. That objective has been largely met.

---

5 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: https://eur-lex.europa.eu/legal-content/EN/TXT/?qid=1517578296944&uri=CELEX%3A52018DC0043.

6 The Multi-stakeholder Group on the Regulation set up by the Commission involves civil society and business representatives, academics and practitioners: http://ec.europa.eu/transparency/regexpert/index.cfm?do=groupDetail.groupDetail&groupID=3537.

7 http://europa.eu/rapid/press-release_IP-19-2956_en.htm.

8 Article 97 of the Regulation.

9 'Commission guidance on the application of Union data protection law in the electoral context', COM(2018) 638 final: https://ec.europa.eu/commission/sites/beta-political/files/soteu2018-data-protection-law-electoral-guidance-638_en.pdf.

10 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 https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex:31995L0046.

The harmonisation of the legal framework

Although the Regulation is directly applicable in the Member States, it obliged them to take a number of legal steps at national level, in particular to set up and allocate powers to the national data protection authorities[11], lay down rules on specific issues, such as the reconciliation of the protection of personal data with freedom of expression and information, and amend or repeal sectoral legislation with data protection aspects. At the time of this Communication, all but three[12] Member States had updated their national data protection law. Work on adapting sectoral laws is still on-going at national level. Following its incorporation in the European Economic Area Agreement, the application of the Regulation was extended to Norway, Iceland and Lichtenstein which have also adopted their national data protection law.

However, stakeholders are calling for an even higher degree of harmonisation in some areas[13]. Indeed, the Regulation allows Member States some scope to further specify its application in certain areas such as the age of consent by children for online services[14] or the processing of personal data in areas such as medicine and public health. In this case, the action of Member States is framed by two elements:

i) any national specification law must meet the requirements of the Charter of Fundamental Rights[15] (and not go beyond the limits set by the Regulation which builds on the Charter);
ii) it may not impinge on the free flow of personal data within the EU[16].

In some instances, Member States have introduced national requirements on top of the Regulation, in particular through many sectoral laws and this leads to fragmentation and results in creating unnecessary burdens. One example of an additional requirement introduced by Member States on top of the Regulation is the obligation under the German legislation to designate a Data Protection Officer in companies with 20 employees or more permanently involved in automated processing of personal data.

Continuing efforts towards greater harmonisation

The Commission engages in bilateral dialogues with national authorities, where it pays particular attention to the national measures in relation to:

- the effective independence of data protection authorities, including through adequate financial, human and technical resources;
- how national laws restrict the rights of data subjects;

---

11 Such as the power to impose administrative fines.
12 As of 23 July 2019, Greece, Portugal and Slovenia are still in the process of adopting their national law.
13 See report of the Multi-stakeholder Group on the Regulation issued on 13 June 2019: http://ec.europa.eu/transparency/regexpert/index.cfm?do=groupDetail.groupMeeting&meetingId=15670.
14 13 years for Belgium, Denmark, Estonia, Finland, Latvia, Malta, Sweden and the United Kingdom; 14 years for Austria, Bulgaria, Cyprus, Spain, Italy and Lithuania; 15 years for Czechia and France; 16 years for Germany, Hungary, Croatia, Ireland, Luxembourg, the Netherlands, Poland, Romania and Slovakia.
15 Article 8.
16 In line with Article 16(2) of the Treaty on the Functioning of the European Union.

- the fact that national legislation should not introduce requirements going beyond the Regulation when there is no margin for specification, such as additional conditions for processing;
- fulfilling the obligation to reconcile the right to the protection of personal data with freedom of expression and information, taking into account that this obligation should not be misused to creating a chilling effect on journalistic work.

The work of the data protection authorities, cooperating in the context of the European Data Protection Board ('the Board'), is a key driver to a consistent application of the new rules: enforcement actions affecting several Member States go through the cooperation and consistency mechanism[17] within the Board and the guidelines adopted by the Board contribute to a harmonised understanding of the Regulation. There is nevertheless an expectation on the part of stakeholders for the data protection authorities to go further in this direction.

The work of national courts and the Court of Justice of the European Union is also helping to create consistent interpretation of data protection rules. National courts have recently issued judgements invalidating provisions in national laws which depart from the Regulation[18].

III. All the pieces of the new governance system are falling into place

The Regulation created a new governance structure, putting at its centre the independent national data protection authorities, as enforcers of the Regulation and first contact points for stakeholders. While most data protection authorities have benefited in the past year from increased resources, there still remain great differences between Member States[19].

Data protection authorities use their new powers

The Regulation equips the data protection authorities with stronger enforcement powers. Contrary to fears expressed by some stakeholders before May 2018, national data protection authorities have adopted a balanced approach to enforcement powers. They have focused on dialogue rather than sanctions, in particular for the smallest operators which do not process personal data as a core activity. At the same time, they did not shy away from using their new powers effectively whenever this was necessary, including by launching investigations in the area of social media[20] and imposing administrative fines ranging from a few thousand euros to several million, depending on the gravity of the infringements of data protection rules.

---

17 Article 60 of the Regulation provides for cooperation between data protection authorities to apply one interpretation of the Regulation in concrete cases. Article 64 provides that the Board will issue opinions in certain instances so as to ensure consistent application of the Regulation. Finally, the board is given the power to adopt binding decisions addressed to the data protection authorities in case of disagreement between them.

18 This has been the case in Germany and in Spain.

19 https://edpb.europa.eu/sites/edpb/files/files/file1/19_2019_edpb_written_report_to_libe_en.pdf

20 For instance, the Irish Data Protection Commission opened 15 formal investigations in relation to the compliance of multinational technology companies with the Regulation. See page 49 of the 2018 annual report of the Irish Data Protection Commission:

Examples of fines imposed by data protection authorities[21]:

- EUR 5 000 on a sport betting café in Austria, for unlawful video surveillance;
- EUR 220 000 on a data broker company in Poland for failure to inform individuals that their data was being processed;
- EUR 250 000 imposed on the Spanish football league LaLiga, for lack of transparency in the design of its smartphone application;
- EUR 50 million on Google in France, because of the conditions for obtaining consent from users.

When conducting investigations, it is essential that data protection authorities gather relevant evidence, respect all procedural steps under national legislation and ensure due process in often complex files. This requires time and involves a significant amount of work, which explains why most of the investigations launched after the entry into application of the Regulation are still on-going.

That being said, the success of the Regulation should not be measured by the number of fines imposed, but by changes in the culture and behaviour of all actors involved. In this context, data protection authorities have other tools at their disposal such as imposing a temporary or definitive limitation on processing including a ban or ordering the suspension of data flows to a recipient in a third country[22].

Some data protection authorities have created new tools, such as help lines and toolkits for businesses while others have developed novel approaches, such as regulatory sandboxes[23] to assist companies in their compliance efforts. However, a number of stakeholders still consider that they have not received enough support and information, in particular small and medium size enterprises in some Member States[24]. To help remedy this situation, the Commission provides grants to data protection authorities for them to reach out to stakeholders, in particular individuals and small and medium size enterprises[25].

---

https://www.dataprotection.ie/en/news-media/press-releases/dpc-publishes-annual-report-25-may-31-december-2018.

21 Several of the decisions imposing fines are still subject to judicial review.

22 Article 58(2)(f) and (j).

23 https://ico.org.uk/about-the-ico/news-and-events/news-and-blogs/2018/09/ico-call-for-views-on-creating-a-regulatory-sandbox/

24 See report of the Multi-stakeholder Group on GDPR: http://ec.europa.eu/transparency/regexpert/index.cfm?do=groupDetail.groupMeeting&meetingId=15670

25 EUR 2 million allocated to nine data protection authorities in 2018 for activities in 2018-2019: Belgium, Bulgaria, Denmark, Hungary, Lithuania, Latvia, the Netherlands, Slovenia and Iceland: https://ec.europa.eu/info/funding-tenders/opportunities/portal/screen/opportunities/topic-details/rec-rdat-trai-ag-2017;
EUR 1 million to be allocated in 2019: https://ec.europa.eu/info/funding-tenders/opportunities/portal/screen/opportunities/topic-details/rec-rdat-trai-ag-2019.

The European Data Protection Board is operational

The data protection authorities have intensified their work in the European Data Protection Board[26]. This intense work has allowed the Board to adopt around 20 guidelines on key aspects of the Regulation[27]. The future areas of work of the Board are presented in a 2-year programme[28] as required by the Regulation.

In cross-border cases each data protection authority is no longer simply a national authority but is part of a truly EU-wide process across all stages, from the investigation to the decision. Such close cooperation has become daily practice: by end-June 2019, 516 cross-border cases had been managed through the cooperation mechanism.

The Commission contributes actively to the work of the Board[29] to promote the letter and spirit of the Regulation, and recalls the general principles of EU law[30].

Towards the creation of an EU data protection culture

The new governance system still needs to realise its full potential. It is important for the Board to further streamline its decision-making and develop a common EU data protection culture among its members. The possibilities for data protection authorities to pool their efforts[31] on issues affecting more than one Member State, for instance to carry out joint investigations and enforcement measures, can contribute to such an objective while mitigating resources' constraints.

Many stakeholders wish to see even more cooperation and a uniform approach by national data protection authorities[32]. They also request more consistency in the advice provided by data protection authorities[33], and a full alignment of national guidelines with those of the Board. Some also expect further clarifications of key concepts of the Regulation such as the risk-based approach, taking particular account of the concerns notably of small and medium size enterprises.

In this context, allowing stakeholders to better feed into the work of the Board is essential. This is why the Commission welcomes the systematic public consultation organised by the Board on guidelines. This practice, together with the organisation of stakeholder workshops

---

26 The Board has legal personality and is composed of the heads of the national data protection supervisory authorities and the European Data Protection Supervisor.

27 https://edpb.europa.eu/our-work-tools/general-guidance/gdpr-guidelines-recommendations-best-practices_en

28 https://edpb.europa.eu/our-work-tools/our-documents/publication-type/work-program_en

29 As a non-voting participant.

30 The Commission has also helped smooth the establishment of the Board and supports its functioning by providing its communication system.

31 Article 62 of the Regulation.

32 See the report of the Multi-stakeholder Group on the Regulation: http://ec.europa.eu/transparency/regexpert/index.cfm?do=groupDetail.groupMeeting&meetingId=15670. For instance, businesses believe that the national lists of the kinds of processing operations which requires data protection impact assessment under Article 35 of the Regulation could have been better harmonised.

33 Including between the various authorities in federal states.

on targeted topics at an early stage of the reflection, should be continued and amplified to ensure the transparency, inclusiveness and relevance of the work of the Board.

IV. Individuals make use of their rights but awareness-raising should continue

Another key objective of the Regulation was to strengthen individuals' rights. The Regulation is widely considered by civil rights associations and consumer organisations as an important contribution to a fair digital society built on mutual trust.

A stronger awareness of data protection rights

Individuals in the EU are increasingly aware of data protection rules and of their rights: 67% of respondents to a May 2019 Eurobarometer[34] are aware of the Regulation and 57% know that there is a national data protection authority to which they can turn for information or to lodge complaints. 73% have heard of at least one of the rights granted by the Regulation. However, a sizeable number of individuals in the EU still do not take active steps to protect their personal data when they go online. For instance, 44% of individuals have not changed their default privacy settings on social networks.

Individuals increasingly exercise their rights

This increased awareness of rights has led individuals to exercise them more intensively by means of customer queries and by turning more often to data protection authorities to ask for information or lodge complaints[35]. Businesses also report that requests for access to personal data have increased in several sectors, such as banking and telecommunications. Individuals have also more often withdrawn their consent and exercised their right to object to commercial communications[36].

However, some operators reported misunderstandings by individuals about data protection rules, such as the belief that individuals should consent to all processing, or that the right to erasure is absolute (while for instance personal data sometimes have to be kept by the operators due to legal obligations)[37]. On their side, civil society organisations complain about long delays in replying by some business and data protection authorities.

Importantly, several representative actions were launched by non-governmental organisations after being mandated by individuals, making use of the new possibility under the Regulation[38]. The recourse to representative actions would have been easier if more Member States had made use of the possibility provided for by the Regulation to allow non-governmental organisations to launch actions without a mandate[39].

---

34 http://europa.eu/rapid/press-release_IP-19-2956_en.htm
35 https://ec.europa.eu/commission/sites/beta-political/files/infographic-gdpr_in_numbers_1.pdf
36 See report of the Multi-stakeholder Group on the General Data Protection Regulation.
37 See report of the Multi-stakeholder Group on the General Data Protection Regulation.
38 Article 80(1) of the Regulation.
39 Article 80(2) of the Regulation.

The need to continue awareness-raising efforts

The dialogue and awareness-raising efforts focusing on the general public must therefore continue at national and EU level. To this end, the Commission launched a new online campaign in July 2019[40] to encourage individuals to read privacy statements and to optimise their privacy settings.

V. Businesses are adapting their practices

The Regulation aims to support business in the digital economy by offering future-proof solutions. Businesses generally welcome the Regulation's accountability principle which moves away from the previous burdensome *ex ante* approach (elimination of notification requirements, scalability of obligations, and flexibility of the data protection by design and by default principle allowing competition on the basis of privacy friendly solutions). At the same time, some call for more legal certainty and additional or clearer guidelines from data protection authorities[41].

Sound data management

While companies report a number of challenges in adjusting to the new rules[42], many emphasise that it was also an opportunity to bring the issue of data protection to the attention of the company boards, put their house in order in terms of the data they hold, improve security, be better prepared for incidents, reduce exposure to unnecessary risks and build more trusting relationships with their customers and commercial partners. On transparency, business and civil society organisations mention the delicate balance to be struck between giving to individuals all required information under the Regulation while also using clear and plain language and a form that individuals can understand. Operators are developing innovative solutions in this direction.

In general, businesses indicated that they were able to implement the new data subject rights, although it was sometimes challenging to meet deadlines due to an increased number of requests and their more wide-ranging character[43], or to check the identity of the person making the request.

---

40 It follows-up to previous campaign aimed at disseminating information materials for individuals and businesses available on: https://ec.europa.eu/commission/priorities/justice-and-fundamental-rights/data-protection/2018-reform-eu-data-protection-rules_en.

41 See report of the Multi-stakeholder Group on the Regulation.

42 Updating IT system is often mentioned as one of the main challenge, particularly as regards the implementation of the principles of data protection by design and by default, the right to erasure in back-ups, etc.

43 Businesses also plead for guidelines from the Board on unfounded and excessive requests.

Impact on innovation

The Regulation not only allows but encourages the development of new technologies while respecting the fundamental right to protection of personal data. This is the case in areas such as artificial intelligence.

Businesses have started developing their offer of new, more privacy-friendly services. For instance, search engines which do not track users or use behavioural advertising are progressively gaining market shares in some Member States. Other companies are developing services that build on new rights granted to individuals, such as the portability of their personal data. An increasing number of businesses have promoted respect for personal data as a competitive differentiator and a selling point. These developments are not confined to the EU but also concern very innovative foreign economies[44].

The specific situation of 'low risk' micro and small size enterprises

Although the situation varies between Member States, micro and small size enterprises[45] which do not process personal data as their core business have been among the stakeholders with the most questions about the application of the Regulation. While these seem to stem partially from a lack of awareness of the data protection rules, their concerns are also sometimes exacerbated by campaigns from consultancies seeking to provide paid-for advice, by the spread of incorrect information, for instance on the need to systematically obtain consent from individuals[46], and by additional requirements imposed at national level.

In this context, micro and small size enterprises are calling for guidelines that are tailored to their specific situation and that provide very practical information. Some data protection authorities have already done this at national level[47]. To supplement national initiatives, the Commission has issued information material to help such companies comply with the new rules through a series of practical steps[48].

Making use of the toolbox under the Regulation

The Regulation provides for tools to demonstrate compliance, such as standard contractual clauses, codes of conduct and the newly introduced certification mechanisms.

Standard contractual clauses are model clauses which can be included on a voluntary basis in a contract, for instance between a data controller and a data processor, and which lay down the obligations of the contracting parties under the Regulation. The Regulation expands the

---

44 For instance, according to a report published by Israel's cybersecurity industry association, in 2018 the 'Data Protection and Privacy' subsector of Cybersecurity was the fastest growing subsector as a result in part of the entry into application of the GDPR.

45 As defined in the SME definition, available at: https://ec.europa.eu/growth/smes/business-friendly-environment/sme-definition_en.

46 The Regulation, in fact, does not rely only on consent but provides for several legal grounds for processing personal data.

47 For instance, the guide developed by the French data protection authority: https://www.cnil.fr/fr/la-cnil-et-bpifrance-sassocient-pour-accompagner-les-tpe-et-pme-dans-leur-appropriation-du-reglement.

48 https://ec.europa.eu/commission/sites/beta-political/files/ds-02-18-544-en-n.pdf.

possibilities to use standard contractual clauses both for international transfers and within the EU[49]. In the area of international transfers, their broad use indicates[50] that they are very helpful to businesses in their compliance efforts and of particular benefit to companies that do not have the resources to negotiate individual contracts with each of their data processing contractors.

A number of sectors also regard the adoption of standard contractual clauses as a useful way to foster harmonisation, in particular when it is the Commission that adopts them. The Commission will work together with stakeholders to make use of the possibilities provided by the Regulation and to update existing clauses.

The adherence to codes of conduct is another operational and practical tool at the disposal of industry to facilitate demonstrating compliance with the Regulation[51]. Those codes should be developed by trade associations or bodies representing categories of controllers and processors and should describe how the data protection rules can be implemented in a specific sector. By calibrating the obligations with the risks[52], they can also prove to be a very useful and cost-effective way for small and medium size enterprises to meet their obligations.

Finally, certification can also be a useful instrument to demonstrate compliance with specific requirements of the Regulation. It can increase legal certainty for businesses and promote the Regulation globally. The certification and accreditation guidelines[53] recently adopted by the European Data Protection Board will enable the development of certification schemes in the EU. The Commission will be monitoring these developments and, if appropriate, will make use of the empowerment provided under the Regulation to frame the requirements for certification. The Commission may also issue a standardisation request to EU standardisation bodies on elements relevant for the Regulation.

VI. Upward convergence is progressing at international level

The demand for protection of personal data is not limited to the EU. As shown by a recent global survey on internet security, the trust deficit is widening around the globe causing people to change the way they behave online[54]. A growing number of companies are

---

49 See Article 28 of the Regulation. Standard contractual clauses adopted by the Commission, enjoy EU-wide validity. By contrast, those adopted under Article 28(8) by a data protection authority only bind the authority which adopted them and can thus be used as standard contractual clauses for processing operations that fall within the jurisdiction of that authority, according to Articles 55 and 56.

50 They are actually the main tool on which companies rely for their data exports.

51 The European Data Protection Board has adopted guidelines on Codes of conduct on 4 June 2019. They clarify the procedures and the rules involved in the submission, approval and publication of codes at both national and EU level.

52 Recital 98 of the Regulation.

53 https://edpb.europa.eu/our-work-tools/our-documents/guidelines/guidelines-12018-certification-and-identifying-certification_en;
https://edpb.europa.eu/our-work-tools/our-documents/guidelines/guidelines-42018-accreditation-certification-bodies-under_en

54 See 2019 CIGI-Ipsos Global Survey on Internet Security and Trust. According to that survey, 78 % of people surveyed were concerned about their online privacy, with 49% saying their distrust had caused them to disclose less personal information online, while 43% reported taking greater care to secure their device

addressing these concerns by extending of their own volition the rights created by the Regulation to their non-EU based customers.

Moreover, as countries around the world are increasingly addressing similar challenges, they are equipping themselves with new data protection rules or modernising existing ones. These laws often have a number of common features that are shared by the EU data protection regime, such as an overarching legislation rather than sectorial rules, enforceable individual rights and an independent supervisory authority. This trend is truly global, running from South Korea to Brazil, from Chile to Thailand, from India to Indonesia. The increasingly universal membership of the Council of Europe's 'Convention 108'[55] – recently modernised[56] with a significant contribution from the Commission – is another clear sign of this trend of upward convergence.

Promoting safe and free data flows through adequacy decisions and beyond

This developing convergence offers new opportunities to facilitate data flows, and consequently trade as well as cooperation between public authorities, while improving the level of protection for the data of individuals in the EU when it is transferred abroad.

Implementing the strategy laid out in its 2017 Communication on Exchanging and Protecting Personal Data in a Globalised World[57], the Commission intensified its engagement with third countries and other international partners building on and further developing elements of convergence between privacy systems. This included exploring the possibility of adopting adequacy findings with selected third countries[58]. This work has yielded important results, in particular, the entry into force in February 2019 of the EU-Japan mutual adequacy arrangement that created the world's largest area of free and safe data flows. Adequacy negotiations with South Korea are at an advanced stage and exploratory work is ongoing with a view to launching adequacy talks with several Latin American countries – such as Chile or Brazil – depending on the completion of ongoing legislative processes. Developments are also promising in some parts of Asia, such as India, Indonesia and Taiwan, as well as in the

---

and 39% answered that they were using internet more selectively, amongst other precautions. The survey was conducted in 25 economies: Australia, Brazil, Canada, China, Egypt, France, Germany, Great Britain, Hong Kong, India, Indonesia, Italy, Japan, Kenya, Mexico, Nigeria, Pakistan, Poland, Russia, South Africa, Republic of Korea, Sweden, Tunisia, Turkey and the United States.

55 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). This is the only binding multilateral instrument in the field of data protection. The latest countries to ratify the Convention include Argentina, Mexico, Cabo Verde and Morocco.

56 Protocol amending the Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data (ETS No. 108) as agreed in the 128th Session of the Committee of Ministers at Elsinore, Denmark, 17-18 May 2018. The consolidated text of the modernised Convention 108 is available at: https://rm.coe.int/16808ade9d.

57 Communication from the Commission to the European Parliament and the Council 'Exchanging and Protecting Personal Data in a Globalised World', COM/2017/07 final.

58 The Regulation has also created the possibility for adequacy findings also with respect to international organisations, as part of the EU's efforts to facilitate data exchanges with such entities.

European Eastern and Southern neighbourhood, which could open the door to future adequacy decisions.

At the same time, the Commission welcomes the fact that other countries that have put in place transfer instruments similar to the Regulation's adequacy have recognised that the EU as well as countries recognised by the EU as 'adequate' ensure the required level of protection[59]. This has the potential to create a network of countries where data can flow freely.

Alongside this, intense work is ongoing with other third countries, such as Canada, New Zealand, Argentina and Israel to ensure the continuity under the Regulation of adequacy decisions adopted on the basis of the 1995 Data Protection Directive. Meanwhile, the EU-US Privacy Shield has proven to be a useful tool to ensure transatlantic data flows based on a high level of protection, with more than 4,700 participating companies[60]. Its annual review ensures that the correct functioning of the framework is regularly checked and that new issues can be addressed in time.

As there is no one-size-fits-it-all solution for data flows, the Commission is also working with stakeholders and the Board to harness the full potential of the Regulation's toolkit for international transfers. This concerns instruments such as standard contractual clauses, the development of certification schemes, codes of conduct or administrative arrangements for public bodies. In that respect, the Commission is interested in the exchange of experience and best practices with other systems that may have developed a specific expertise in some of these tools. The Commission will consider making use of the empowerments granted under the Regulation with respect to those transfer tools, especially the standard contractual clauses.

Beyond purely bilateral tools, it could also be worth exploring whether like-minded countries could establish a multinational framework in this area at a time when data flows are an increasingly crucial component of trade, communications and social interactions. Such an instrument would allow data to flow freely amongst the contracting parties, while ensuring the required level of protection on the basis of shared values and converging systems. It could be developed, for example, building on the modernised Convention 108 or drawing inspiration from the 'data free flows with trust' initiative launched by Japan at the beginning of this year.

Developing new synergies between trade and data protection instruments

While promoting convergence of data protection standards at international level, the Commission is also determined to tackle digital protectionism. To that end, it has developed specific provisions on data flows and data protection in trade agreements which it systematically tables in its bilateral and multilateral negotiations, such as the current WTO e-commerce talks. These horizontal provisions rule out purely protectionist measures, such as forced data localisation requirements, while preserving the regulatory autonomy of the parties to protect the fundamental right to data protection.

---

[59] This is the approach adopted, for example, by Argentina, Colombia, Israel, and Switzerland.

[60] That means that in its first three years of existence, the Privacy Shield has more participating companies that its predecessor, the Safe Harbour, had after 13 years of operation.

Whereas dialogues on data protection and trade negotiations must follow separate tracks, they can complement each other: the EU-Japan mutual adequacy arrangement is the best example of such synergies, further easing commercial exchanges and in this way amplifying the benefits of the Economic Partnership Agreement. In fact, this type of convergence, based on shared values and high standards and backed-up by effective enforcement, provides the strongest foundation for the exchange of personal data, something which is increasingly recognised by our international partners[61]. Given that companies increasingly operate across borders and prefer to apply similar sets of rules in all their business operations worldwide, such convergence helps create an environment conducive to direct investment, facilitating trade and improving trust between commercial partners.

Facilitating exchange of information to combat crime and terrorism based on appropriate safeguards

Greater compatibility between data protection regimes can also significantly facilitate the much needed exchanges of information between EU and foreign regulatory, police and judicial authorities and, in this way, contribute to more effective and rapid law enforcement cooperation[62]. To that end, the Commission considers to make use of the possibility to adopt adequacy decisions under the Data Protection Law Enforcement Directive to deepen its cooperation with key partners in the fight against crime and terrorism. Moreover, the EU-US 'Umbrella Agreement'[63], which entered into force in February 2017, can be used as a model for similar agreements with other important security partners.

Other examples pointing to the importance of high data protection standards as a basis for stable law enforcement cooperation with third countries are the transfer of Passenger Name Records (PNR)[64], and the exchange of operational information between Europol and important international partners. In this regard, negotiations on international agreements are

---

61 As reflected, for instance, in the reference to the concept of 'Data Free Flow with Trust' in the Osaka G20 Leaders' Declaration: https://www.consilium.europa.eu/media/40124/final_g20_osaka_leaders_declaration.pdf.

62 See the Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions 'The European Agenda on Security', COM(2015) 185 final.

63 Agreement between the EU and the U.S. on the protection of personal data when transferred and processed for the purpose of preventing, investigating, detecting or prosecuting criminal offences, including terrorism, in the framework of police cooperation and judicial cooperation in criminal matters: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex:22016A1210(01) (the 'Umbrella Agreement'). The Umbrella Agreement constitutes the first bilateral international agreement in the law enforcement area providing for a comprehensive catalogue of data protection rights and obligations in line with the EU acquis. It is a successful example of how law enforcement cooperation with an important international partner can be enhanced by negotiating a strong set of data protection safeguards.

64 United Nations Security Council Resolution (SCR) 2396 of 21 December 2017 calls on all the UN Member States to develop the capability to collect, process and analyse PNR data, with full respect for human rights and fundamental freedoms. See also Communication from the Commission 'The European Agenda on Security', COM (2015)185 final: https://ec.europa.eu/home-affairs/sites/homeaffairs/files/e-library/documents/basic-documents/docs/eu_agenda_on_security_en.pdf.

currently ongoing or poised to commence with several countries of the Southern Neighbourhood[65].

Strong data protection safeguards will also be an essential component of any future agreement on cross-border access to electronic evidence in criminal investigations, at bilateral (EU-US agreement) or multilateral level (Second Additional Protocol to the Council of Europe 'Budapest' Convention on Cybercrime)[66].

Promoting cooperation between data protection enforcers

At a time when privacy compliance issues or security incidents may affect large number of individuals simultaneously in several jurisdictions, closer forms of cooperation between supervisory authorities at international level can help ensure both a more effective protection of individual rights and a more stable environment for business operators. Against that background and in close contact with the Board, the Commission will work on ways to facilitate enforcement cooperation and mutual assistance between EU and foreign supervisory authorities, including by making use of the new powers provided in this area by the Regulation[67]. This could cover different forms of cooperation from developing common interpretative or practical tools[68] to exchanging information on on-going investigations.

Finally, the Commission also intends to step up its dialogue with regional organisations and networks, such as the Association of Southeast Asian Nations (ASEAN), the African Union, the Asia Pacific Privacy Authorities forum (APPA) or the Ibero-American Data Protection Network, which play an increasingly important role in shaping common data protection standards, promoting the exchange of best practices and fostering cooperation between enforcers. It will also work with the Organization for Economic Cooperation and Development and the Asian-Pacific Economic Cooperation Organisation to build convergence towards a high level of data protection.

VII. Data protection legislation as an integral part of a wide range of policies

The protection of personal data is guaranteed and integrated in several policies of the Union.

Telecommunications and electronic communication services

The Commission adopted its proposal for a Regulation on Privacy and Electronic Communications in January 2017[69]. The proposal aims to protect confidentiality of communications, as provided for in the Charter of Fundamental Rights, but also to protect

---

65 https://ec.europa.eu/home-affairs/news/security-union-strengthening-europols-cooperation-third-countries-fight-terrorism-and-serious_en

66 http://europa.eu/rapid/press-release_IP-19-2891_en.htm

67 See Article 50 of the Regulation on international cooperation in the field of data protection. This provision covers a wide range of forms of cooperation, from information on data protection legislation to complaint referral and investigative assistance.

68 Such as common templates for breach notifications.

69 https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A52017PC0010

personal data that may be a part of a communication as well as terminal equipment of end-users.

The proposed ePrivacy Regulation particularises and complements the Regulation by laying down specific rules for the abovementioned purposes. It modernises the current EU e-privacy rules[70] to reflect technological and legal developments. It enhances individuals' privacy by extending the scope of the new rules to also cover over-the-top communications service providers, thereby creating a level playing field for all electronic communications services. While the European Parliament adopted a mandate to launch trilogues in October 2017, the Council has not yet agreed on a general approach. The Commission remains fully committed to the ePrivacy Regulation and will support the co-legislators in their efforts to achieve a swift adoption of the proposed Regulation.

Health and research

Facilitating exchanges of health data, which are sensitive data under the Regulation, between Member States is becoming increasingly important in the area of public health for reasons of general interest. These include the provision of healthcare or treatment, protection against serious cross-border threats to health, and ensuring high standards of quality and safety of health care and of medicinal products or medical devices. The Regulation lays down the rules that ensure lawful and trustworthy processing and exchanges of health data across the EU. These rules also apply to access by third parties to the medical data of patients, including to data held in patients summaries, ePrescriptions, and in the long run comprehensive electronic health records, and their use for scientific research purposes. In the specific field of clinical trials, the Commission has also prepared specific Question and Answers on the interplay between the Clinical Trials Regulation[71] and the General Data Protection Regulation[72].

Artificial intelligence ('AI')

As AI gains strategic importance, it is essential to shape global rules for its development and use. In promoting the development and uptake of AI, the Commission has opted for a human-centric approach, meaning that AI applications must comply with fundamental rights[73]. In this context, the rules laid down in the Regulation provide a general framework and contain

---

70 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.

71 https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex%3A32014R0536

72 https://ec.europa.eu/health/sites/health/files/files/documents/qa_clinicaltrials_gdpr_en.pdf

73 Commission Communication of 8 April 2019 on Building Trust in Human-Centric Artificial Intelligence: https://ec.europa.eu/digital-single-market/en/news/communication-building-trust-human-centric-artificial-intelligence.
Ethics Guidelines for Trustworthy AI presented by the High-Level Expert Group (HLEG) on 8 April 2019: https://ec.europa.eu/digital-single-market/en/news/ethics-guidelines-trustworthy-ai. See also the OECD Council Recommendation on Artificial Intelligence: https://legalinstruments.oecd.org/en/instruments/OECD-LEGAL-0449, the G20 AI Principles endorsed as part of the G20 Osaka Leaders' Declaration: https://www.g20.org/pdf/documents/en/annex_08.pdf and G20 Ministerial Statement on Trade and Digital Economy: https://g20trade-digital.go.jp/dl/Ministerial_Statement_on_Trade_and_Digital_Economy.pdf.

specific obligations and rights that are particularly relevant for the processing of personal data in AI. For instance, the Regulation includes the right not to be subject to solely automated decision-making except in certain situations[74]. It also includes specific transparency requirements on the use of automated decision-making, namely the obligation to inform about the existence of such decisions and to provide meaningful information and explain its significance and the envisaged consequences of the processing for the individual.[75] These core principles of the Regulation have been recognised by the High Level Expert Group on AI[76], the Organization for Economic Cooperation and Development[77] and G20[78] as particularly relevant to address the challenges and opportunities arising from AI. The European Data Protection Board has identified AI as one of the possible topics in its 2019-2020 Work Programme[79].

Transport

The development of connected cars and smart cities relies increasingly on the processing and exchanges of large amounts of personal data between multiple parties, including cars, car manufacturers, telematics service providers, and public authorities in charge of road infrastructure. This multi-party environment entails a certain complexity concerning the allocation of the roles and responsibilities of the various actors involved in the processing of personal data, and on how to ensure lawfulness of processing by all actors. Compliance with the Regulation and the ePrivacy legislation are essential for the successful deployment of intelligent transport systems in all modes of transport and the spread of digital tools and services enabling greater mobility of individuals and goods[80].

Energy

The development of digital solutions in the energy sector increasingly relies on the processing of personal data. The legislation adopted as part of the Clean Energy for All Europeans package[81] includes new provisions enabling the digitalisation of the electricity sector and rules on data access, data management and interoperability that allow for the handling of consumers' real-time data for achieving savings and encouraging self-generation and participation in the energy market. Therefore, compliance with data protection rules is of great importance for the successful implementation of these provisions.

---

74 Article 22 of the Regulation.
75 Article 13(2)(f) of the Regulation.
76 https://ec.europa.eu/digital-single-market/en/high-level-expert-group-artificial-intelligence
77 Recommendation of the Council on Artificial Intelligence: https://legalinstruments.oecd.org/en/instruments/OECD-LEGAL-0449.
78 G20 Ministerial Statement on Trade and Digital Economy: https://g20trade-digital.go.jp/dl/Ministerial_Statement_on_Trade_and_Digital_Economy.pdf.
79 https://edpb.europa.eu/sites/edpb/files/files/file1/edpb-2019-02-12plen-2.1edpb_work_program_en.pdf
80 For example by facilitating their planning and use of various means of transportation throughout their journey.
81 In particular the Electricity Directive: https://eur-lex.europa.eu/legal-content/EN/ALL/?uri=CELEX%3A32009L0072.

Competition

The processing of personal data is increasingly an element to be considered in competition policy[82]. Given that data protection authorities are the only authorities entrusted with assessing a violation of the data protection rules, competition, consumer and data protection authorities cooperate and will continue to cooperate when necessary in the intersection of their respective competences. The Commission will foster such cooperation and follow developments closely.

Electoral context

In its Guidance on the use of personal data in the electoral context[83], issued in September 2018 as part of the electoral package[84], the Commission drew attention to rules of particular importance for the actors involved in elections, including issues relating to micro-targeting of voters. This Guidance was echoed in a Statement from the European Data Protection Board[85] and a number of data protection authorities issued guidance at national level. The electoral package also included a call on each Member State to set up a national election network involving national authorities with competence in electoral matters and those responsible for monitoring and enforcing rules, such as data protection, on online activities relevant to the elections. New measures were also adopted to introduce sanctions for infringements of data protection rules by European political parties and foundations. The Commission recommended that Member States adopt the same approach at national level. The evaluation of the 2019 elections to the European Parliament, due to be issued in October 2019, will also take data protection aspects into account.

Law enforcement

An effective and genuine Security Union can only be built on the full compliance with the fundamental rights enshrined in the EU Charter and secondary EU legislation, including appropriate data protection safeguards to enable the secure exchange of personal data for law enforcement purposes. Any restrictions of the fundamental right to privacy and data protection are subject to strict necessity and proportionality test.

---

82 For instance, case M.8788 – Apple / Shazam and case M. M.8124 – Microsoft / LinkedIn.

83 https://ec.europa.eu/commission/sites/beta-political/files/soteu2018-data-protection-law-electoral-guidance-638_en.pdf

84 http://europa.eu/rapid/press-release_IP-18-5681_en.htm

85 https://edpb.europa.eu/sites/edpb/files/files/file1/edpb-2019-03-13-statement-on-elections_en.pdf

VIII. Conclusion

On the basis of information available to date and the dialogue with stakeholders, the Commission's preliminary assessment is that the first year of application of the Regulation has been overall positive. Nevertheless, as shown in this Communication, further progress is necessary in a number of areas.

Implementing and complementing the legal framework:

- The three Member States which have not yet updated their national data protection lawmust do so as a matter of urgency. All Member States should complete the alignment of their sectoral legislation with the requirements of the Regulation.

- The Commission will use all the tools at its disposal, including infringement procedures, to ensure that Member States comply with the Regulation and limit any fragmentation of the data protection framework.

Making the new governance system deliver its full potential:

- Member States should allocate sufficient human, financial and technical resources to national data protection authorities.

- The data protection authorities should step up their cooperation, for instance by conducting joint investigations. Member States should facilitate the conduct of such investigations.

- The Board should further develop an EU data protection culture and make full use of the tools provided for in the Regulation to ensure a harmonised application of the rules. It should continue its work on guidelines, especially for small and medium size enterprises.

- The expertise of the Board's secretariat should be strengthened to support and lead the work of the Board more effectively.

- The Commission will continue to support data protection authorities and the Board, in particular by actively participating in the work of the Board and calling its attention to the requirements of EU law in the course of the implementation of the Regulation.

- The Commission will support the interaction between data protection authorities and other authorities, notably from the competition area in full respect of their respective competencies.

Supporting and involving stakeholders:

- The Board should enhance the way it involves stakeholders in its work. The Commission will continue its financial support to data protection authorities to help them reach out to stakeholders.

- The Commission will continue its awareness-raising activities and its work with stakeholders.

Promoting international convergence:

- The Commission will further intensify its dialogue on adequacy with qualifying key partners, including in the area of law enforcement. In particular, it aims to conclude the ongoing negotiations with South Korea in the coming months. It will report in 2020 on the review of the 11 adequacy decisions adopted under the Data Protection Directive.
- The Commission will continue its work, including through technical assistance exchange of information and best practices, with countries interested in adopting modern privacy laws and foster cooperation with third countries' supervisory authorities and regional organisations.
- The Commission will engage with multilateral and regional organisations to promote high data protection standards as a trade enabler and cooperation facilitator (e.g. under the 'Data Free Flow with Trust' initiative launched by Japan in the context of the G20).

The Regulation[86] requires the Commission to report on its implementation in 2020. This will be an opportunity to assess the progress made and whether after two years of application the various components of the new data protection regime are fully operational. To this end, the Commission will engage with the European Parliament, the Council, Member States, the European Data Protection Board, relevant stakeholders and citizens.

[86] Article 97 of the Regulation.