EUROPEAN
COMMISSION

Brussels, 10.1.2017
COM(2017) 7 final

COMMUNICATION FROM THE COMMISSION TO THE EUROPEAN PARLIAMENT AND THE COUNCIL

Exchanging and Protecting Personal Data in a Globalised World

1. INTRODUCTION

The protection of personal data is part of Europe's common constitutional fabric and is enshrined in Article 8 of the EU Charter of Fundamental Rights. It has been central to EU law for more than 20 years, from the Data Protection Directive in 1995[1] ("the 1995 Directive") to the adoption of the General Data Protection Regulation (GDPR)[2] and the Police Directive[3] in 2016.

As President Juncker stressed in his State of the European Union speech on 14 September 2016, "*[b]eing European means the right to have your personal data protected by strong, European laws. […] Because in Europe, privacy matters. This is a question of human dignity*."

The demand for protection of personal data is however not limited to Europe. Consumers around the world increasingly cherish and value their privacy. In turn, companies recognise that strong privacy protections give them a competitive advantage as confidence in their services increases. Many, especially those with global reach, are aligning their privacy policies with the GDPR, both because they want to do business in the EU, and because they see it as a model to follow.

Likewise, several countries and regional organisations outside the EU, from our immediate neighbourhood to Asia, Latin America and Africa, are adopting new or updating existing data protection legislation to harness the opportunities offered by the global digital economy and respond to the growing demand for stronger data security and privacy protection. While differences exist amongst countries in their approach and the level of legislative development, there are signs of upward convergence towards important data protection principles, in particular in certain regions of the world.[4] Greater compatibility between different data protection systems would facilitate international flows of personal data, whether for commercial purposes or cooperation between public authorities (e.g. law enforcement). The EU should seize this opportunity to promote its data protection values and facilitate data flows by encouraging convergence of legal systems. As announced in the Commission Work Programme[5], the present Communication therefore sets out the Commission's strategic

---

1 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.

2 Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation), OJ L 119, 4.5.2016, p. 1–88. It entered into force on 24 May 2016 and shall apply from 25 May 2018.

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, p. 89-131. It entered into force on 5 May 2016. EU Member States have to transpose it into their national law by 6 May 2018.

4 See "Data protection regulations and international data flows: Implications for trade and development", UNCTAD (2016): http://unctad.org/en/PublicationsLibrary/dtlstict2016d1_en.pdf.

5 Commission Work Programme 2017, Delivering a Europe that protects, empowers and defends, COM(2016) 710 final, 25.10.2016, p.12 and Annex 1.

framework for "adequacy decisions" as well as other tools for data transfers and international data protection instruments.

2. THE EU DATA PROTECTION REFORM PACKAGE – A MODERN LEGISLATIVE FRAMEWORK THAT SUPPORTS INTERNATIONAL DATA FLOWS WITH HIGH PROTECTION

The reform of EU data protection legislation adopted in April 2016 puts in place a system that both ensures a strong level of protection and is open to the opportunities of the global information society. In giving individuals more control over their personal data, the reform strengthens consumer trust in the digital economy. In harmonising and simplifying the legal environment it makes it easier and less burdensome for companies, both domestic and foreign, to conduct their business activities in the EU, including through international data exchanges. The EU today combines openness for international data flows with the highest level of protection for individuals. It has the potential to become a hub for data services which require both free flows and trust.

2.1 A comprehensive, unified and simplified EU data protection framework

The EU reform establishes a comprehensive framework governing the processing of personal data in both the private and public sectors and in both the commercial and law enforcement sectors (the GDPR and Police Directive respectively).

Under the GDPR, as of May 2018, there will be one single pan-European set of rules contrary to 28 national laws today. The newly created one-stop-shop mechanism will ensure that one data protection authority ("DPA") will be responsible for the supervision of cross-border data processing operations carried out by a company in the EU. Consistency of interpretation of the new rules will be guaranteed. In particular, in cross-border cases where several national DPAs are involved, a single decision will be adopted to ensure that common problems receive common solutions. In addition, the GDPR creates a level playing field between EU and foreign companies in that companies based outside the EU will have to apply the same rules as European companies if they are offering goods and services or monitoring the behaviour of individuals in the EU. An increased level of consumer trust will benefit both EU and external commercial operators.

The Police Directive provides common rules for the processing of the personal data of individuals involved in criminal proceedings, be it as suspects, victims, or witnesses, whilst taking into account the specific nature of the police and criminal justice field. Harmonising data protection rules in the law enforcement sector, including rules on international transfers, will facilitate cross-border cooperation between police and judicial authorities, both within the EU and with international partners, and thus create the conditions for a more effective fight against crime. This is an important contribution to the European Agenda on Security.[6]

[6] 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, 28.4.2015.

2.2 A renewed and diversified toolkit for international transfers

From its inception, EU data protection legislation has provided several mechanisms enabling international data transfers. The primary purpose of these rules is to ensure that when the personal data of Europeans are transferred abroad, the protection travels with the data. Over the years, these rules have set the standard on international data flows in many jurisdictions. While the architecture remains essentially the same as under the 1995 Directive, the reform of the rules on international transfers clarifies and simplifies their use and introduces new tools for transfers.

Under EU law, one way to transfer personal data abroad is on the basis of a Commission "adequacy decision" establishing that a non-EU country provides a level of data protection that is "essentially equivalent"[7] to that in the EU. The effect of such a decision is to enable the free flow of personal data to that third country without the need for the data exporter to provide further safeguards or obtain any authorisation. A precise and detailed catalogue of elements that the Commission must take into account when assessing the adequacy of protection of a foreign system is available for interested countries or international organisations.[8] The Commission can now adopt adequacy decisions also for the law enforcement sector.[9] Furthermore, building on practice under the 1995 Directive, the reform explicitly allows for an adequacy determination to be made with respect to a particular territory of a third country or to a specific sector or industry within a third country (so-called "partial" adequacy).[10]

In the absence of an adequacy decision, international transfers can take place on the basis of a number of alternative transfer tools that provide appropriate data protection safeguards.[11] The reform formalises and expands the possibilities to use existing instruments like standard contractual clauses (SCCs)[12] and binding corporate rules (BCRs).[13] For instance, SCCs can now be included in a contract between EU-based processors and processors in a non-EU

---

7 Judgment of the Court of Justice of the EU of 6 October 2015 in Case C-362/14, *Maximillian Schrems v Data Protection Commissioner*, points 73, 74 and 96. See also recital 104 of the GDPR and recital 67 of the Police Directive which refer to the standard of essential equivalence.

8 See Article 45 of the GDPR. As set out in Article 45(2), in its assessment the Commission must take into account, inter alia, the rule of law, respect for human rights and fundamental freedoms and relevant legislation, including in the area of data protection, public security, defence, national security and criminal law and access by public authorities to personal data. These must be underpinned by effective and enforceable rights, including administrative and judicial redress for individuals, and an effectively functioning independent supervisory authority to ensure and enforce compliance with data protection rules. Adherence to legally binding conventions, in particular Council of Europe Convention 108, and participation in multilateral or regional systems dealing with data protection, will also be taken into account.

9 See Article 36(2) Police Directive for the specific adequacy assessment elements.

10 See Article 45(1) GDPR and Article 36(1) Police Directive.

11 See e.g. Communication from the Commission to the European Parliament and the Council on the Transfer of Personal Data from the EU to the United States of America under Directive 95/46/EC following the Judgment by the Court of Justice in Case C-362/14 (*Schrems*), COM(2015) 566 final, 6.11.2015.

12 SCCs lay down the respective data protection obligations between the EU exporter and the third country importer.

13 BCRs are internal rules adopted by a multinational group of companies to carry out data transfers within the same corporate group to entities located in countries which do not provide an adequate level of protection. While BCRs are already in use under the 1995 Directive, the GDPR codifies and formalises their role as a tool for transfers.

country (so-called "processor-to-processor" model clauses).[14] As for BCRs, which until now have been limited to arrangements among entities of the same corporate group, they can now be used by a group of enterprises engaged in a joint economic activity, but not necessarily forming part of the same corporate group.[15] The reform also reduces red tape by abolishing general requirements of prior notification to and authorisation by DPAs of transfers to a third country based on SCCs or BCRs.[16] This is an important simplification of the EU system of international data transfers as the existence of such requirements, which currently vary from one Member State to another, is often perceived as a significant obstacle for data flows, especially for smaller businesses.[17]

In addition, the reform introduces new instruments for international transfers.[18] Controllers and processors will be able to use, under certain conditions,[19] approved codes of conduct or certification mechanisms (such as privacy seals or marks) to establish "appropriate safeguards". This should allow the development of more tailor-made solutions for international transfers, reflecting, for instance, the specific features and needs of a given sector or industry, or of particular data flows. It also offers for the possibility to provide for appropriate safeguards for data transfers between public authorities or bodies on the basis of international agreements or administrative arrangements.[20] Finally, the GDPR clarifies the use of so-called "derogations"[21] (e.g. consent, performance of a contract or important reasons of public interest) on which entities in specific situations can base their data transfers in the absence of an adequacy decision and irrespective of the use of one of the above instruments. In particular, it contains a new, albeit circumscribed, derogation pertaining to transfers that can take place in pursuit of the legitimate interests[22] of a company.

Finally, the reform empowers the Commission to develop international cooperation mechanisms to facilitate the enforcement of data protection rules, including through mutual assistance arrangements.[23] This recognises the contribution that closer forms of cooperation between supervisory authorities at international level could make to ensure both more effective protection of individual rights and more legal certainty for businesses.

---

14 See Article 46(2)(c) and (d) and recital 168 GDPR.
15 See Articles 46(2)(b), 47 and recital 110 GDPR.
16 See Article 46(2) GDPR.
17 That registration requirements create a barrier to trade for many businesses, especially SMEs, was highlighted e.g. in the UNCTAD report, p. 34.
18 See Article 46(2)(e) and (f) GDPR.
19 Non EU-controllers will be able to adhere to an EU code of conduct or certification mechanism by making binding and enforceable commitments, via contractual or other legally binding commitments, to apply the data protection safeguards contained in those instruments. See Article 42(2) GDPR.
20 See Article 46(2)(a) and 46(3)(b) GDPR.
21 See Article 49 GDPR.
22 See Article 49(1), second subparagraph.
23 See Article 50 GDPR.

3. INTERNATIONAL DATA TRANSFERS IN THE COMMERCIAL SECTOR: FACILITATING TRADE BY PROTECTING PRIVACY

Respecting privacy is a condition for stable, secure and competitive global commercial flows. Privacy is not a commodity to be traded.[24] The internet and digitization of goods and services has transformed the global economy and the transfer of data, including personal data, across borders is part of the daily operations of European companies of all sizes, across all sectors. As commercial exchanges rely increasingly on personal data flows, the privacy and security of such data has become a central factor of consumer trust. For instance, two-thirds of Europeans say that they are worried about having no control over the information they provide online while half of the respondents are concerned about becoming a victim of fraud.[25] At the same time, European companies operating in some third countries are increasingly faced with protectionist restrictions that cannot be justified with legitimate privacy considerations.

In the digital era, promoting high standards of data protection and facilitating international trade must thus necessarily go hand in hand. Whereas the protection of personal data is non-negotiable[26] in trade agreements, the EU regime on international data transfers, as outlined above, provides a broad and varied toolkit to enable data flows in different situations while ensuring a high level of protection.

3.1 Adequacy decisions

An adequacy finding allows the free flow of personal data from the EU without the EU data exporter having to implement any additional safeguards or being subject to further conditions. In finding that its legal order provides an adequate level of protection, the decision recognises that the country's system approximates that of the EU Member States. As a result, transfers to the country in question will be assimilated to intra-EU transmissions of data, thereby providing privileged access to the EU single market, while opening up commercial channels for EU operators. As explained above, this recognition necessarily requires a level of protection comparable (or "essentially equivalent")[27] to the one guaranteed in the Union. It involves a comprehensive assessment of the third country's system, including its rules on access to personal data by public authorities for law enforcement, national security and other public interest purposes.

At the same time, as confirmed in 2015 by the Court of Justice in the *Schrems* ruling, the adequacy standard does not require a point-to-point replication of EU rules.[28] Rather, the test lies in whether, through the substance of privacy rights and their effective implementation, enforceability and supervision, the foreign system concerned as a whole delivers the required

---

24 See e.g. Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions on Trade for All Towards a more responsible trade and investment policy, COM(2015) 497 final, 14.10.2015, p. 7.

25 Special Eurobarometer 431 - Data protection, June 2015.

26 President Juncker's political guidelines: *A New Start for Europe: My Agenda for Jobs, Growth, Fairness and Democratic Change*

27 See footnote 7.

28 Cf. point 74 of the *Schrems* ruling.

high level of protection. As the adequacy decisions adopted so far show, it is possible for the Commission to recognise a diverse range of privacy systems, representing different legal traditions, as being adequate. These decisions concern countries that are closely integrated with the European Union and its Member States (Switzerland, Andorra, Faeroe Islands, Guernsey, Jersey, Isle of Man), important trading partners (Argentina, Canada, Israel, the United States), and countries that have a pioneering role in developing data protection laws in their region (New Zealand, Uruguay).

The decisions on Canada and the United States are "partial" adequacy findings. The decision on Canada applies only to private entities falling under the scope of the Canadian Personal Information Protection and Electronic Documents Act. The recently adopted decision on the EU-US Privacy Shield[29] is a specific case in that, in the absence of general data protection legislation in the U.S.,[30] it relies on commitments by participating companies to apply the high data protection standards set out by this arrangement that are in turn enforceable under U.S. law. Moreover, the Privacy Shield builds on the specific representations and assurances made by the U.S. government as regards access for national security purposes[31] that underpin the adequacy finding. Compliance with these commitments will be closely monitored by the Commission and part of the annual review on the functioning of the framework.

In recent years more and more countries around the world have adopted new legislation in the area of data protection and privacy or are in the process of doing so. In 2015, the number of countries that had enacted data privacy laws stood at 109, a significant increase from 76 in mid-2011.[32] Moreover, around 35 countries are currently drafting data protection laws.[33] These new or modernised laws tend to be based on a core set of common principles, including *inter alia* the recognition of data protection as a fundamental right, the adoption of overarching legislation in this field, the existence of enforceable individual privacy rights, and the setting up of an independent supervisory authority. This offers new opportunities, notably through adequacy findings, to further facilitate data flows while guaranteeing the continued high level of protection of personal data.

Under EU law, an adequacy finding requires the existence of data protection rules comparable to the ones in the EU.[34] This concerns both the substantive protections applicable to personal data and the relevant oversight and redress mechanisms available in the third country.

---

29 Implementing Decision EU(2016) 1260 of 12 July 2016.

30 The Commission encourages the U.S. to pursue efforts towards a comprehensive system of privacy and data protection, allowing for convergence between the two systems in the longer term. See Communication from the Commission to the European Parliament and the Council, Transatlantic Data Flows: Restoring Trust through Strong Safeguards, COM(2016) 117 final, 29.2.2016.

31 This includes in particular the application of Presidential Policy Directive 28 (PPD-28), which imposes a number of limitations and safeguards for "signals intelligence" operations, and the appointment of a specific Ombudsperson for complaints by EU individuals in this regard.

32 G. Greenleaf, "Global data privacy laws 2015: 109 countries, with European laws now in a minority", (2015) 133 Privacy Laws & Business International Report, 14-17.

33 UNCTAD study, pp. 8 and 42 (footnote 4 above).

34 In this respect, the Commission also takes into account the third country's obligations arising from legally binding conventions, in particular its accession to Convention 108 and its additional Protocol, when carrying out an adequacy assessment. See Article 45(2)(c) and recital 105 GDPR.

Under its framework on adequacy findings, the Commission considers that the following criteria should be taken into account when assessing with which third countries a dialogue on adequacy should be pursued:[35]

(i) the extent of the EU's (actual or potential) commercial relations with a given third country, including the existence of a free trade agreement or ongoing negotiations;

(ii) the extent of personal data flows from the EU, reflecting geographical and/or cultural ties;

(iii) the pioneering role the third country plays in the field of privacy and data protection that could serve as a model for other countries in its region;[36]and

(iv) the overall political relationship with the third country in question, in particular with respect to the promotion of common values and shared objectives at international level.

Based on these considerations, the Commission will actively engage with key trading partners in East and South-East Asia, starting from Japan and Korea in 2017[37], and, depending on progress towards the modernisation of its data protection laws, with India, but also with countries in Latin America, in particular Mercosur, and the European neighbourhood which have expressed an interest in obtaining an "adequacy finding". In addition, the Commission welcomes expressions of interest from other third countries that are willing to engage on these issues. Discussions on a possible adequacy finding are a two-way dialogue that includes providing any necessary clarifications on the EU data protection rules and exploring ways to increase convergence of the third countries' laws and practice.

In certain situations, rather than taking a country-wide approach, it may be more suitable to make use of other options such as partial or sector-specific adequacy (e.g. for financial services or IT sectors) which may concern geographic areas or industries that form an important part of a particular third country's economy. This will need to be considered in light of elements such as, for instance, the nature and state of development of the privacy regime (stand-alone law, multiple or sectorial laws etc.), the constitutional structure of the third country or whether certain sectors of the economy are particularly exposed to data flows from the EU.

The adoption of an adequacy decision involves the establishment of a specific dialogue and close forms of cooperation with the concerned third country. Adequacy decisions are "living" documents that need to be closely monitored by the Commission and adapted in case of

[35] For countries with respect to which relevant interests for cooperation in the internal security and law enforcement area exist, the Commission will explore the possibility for specific adequacy findings under the Police Directive, see section 4.

[36] This may be particularly relevant for developing and transition countries as the protection of personal data is both a crucial element of the rule of law and an important factor of economic competitiveness.

[37] Japan and Korea have recently adopted or modernised their legislation to put in place comprehensive data protection regimes.

developments affecting the level of protection ensured by the third country in question.[38] To that end, periodic reviews will be held, at least every four years, to address emerging issues and exchange best practices between close partners.[39] This dynamic approach applies also to already existing adequacy decisions, adopted under the 1995 Directive, which will need to be reviewed in case they no longer meet the applicable standard.[40] The third countries concerned are therefore invited to inform the Commission of any relevant change in law and practice that has taken place since the adoption of the adequacy decision relating to them. This is essential to ensure the continuity of these decisions under the new rules of the reform.[41]

The EU data protection rules cannot be the subject of negotiations in a free trade agreement.[42] While dialogues on data protection and trade negotiations with third countries have to follow separate tracks, an adequacy decision, including a partial or sector-specific one, is the best avenue to build mutual trust, guaranteeing uninhibited flow of personal data, and thus facilitate commercial exchanges involving transfers of personal data to the third country in question. Such decisions can therefore ease trade negotiations or may complement existing trade agreements, thus allowing them to amplify their benefits. At the same time, by fostering the convergence of the level of protection in the EU and the third country, an adequacy finding reduces the risk of invocation by that country of personal data protection grounds to impose unjustified data localisation or storage requirements. Beyond this, as indicated in the Trade for All Communication, the Commission will seek to use EU trade agreements to set rules for e-commerce and cross-border data flows and tackle new forms of digital protectionism, in full compliance with and without prejudice to the EU's data protection rules.[43]

---

38 Article 45(4) and (5) GDPR require the Commission to monitor developments in third countries on an ongoing basis and give it the power to repeal, amend or suspend an adequacy decision if it finds that the respective country no longer ensures an adequate level of protection.

39 Article 45(3) GDPR.

40 Article 97(2)(a) GDPR also requires the Commission to submit an evaluation report by 2020 to the European Parliament and the Council.

41 To draw the consequences from the *Schrems* ruling which found that the Commission had exceeded its powers in restricting the powers of DPAs to suspend or ban data flows in the Safe Harbour decision, the Commission on 16 December 2016 adopted an "omnibus" amending decision that deletes similar provisions in existing adequacy decisions and replaces them with provisions that merely provide for information requirements between Member States and the Commission in case a DPA suspends or bans transfers to a third country. The omnibus decision also introduces a requirement for the Commission to monitor relevant developments in the third country. See OJ L355, 17.12.2016, p.83.

42 In particular, an adequacy finding is a unilateral implementing decision by the Commission in accordance with EU data protection law, based on the criteria therein.

43 See Trade for All Communication, p. 12 (footnote 24 above).

The Commission will:

- Prioritise discussions on possible adequacy decisions with key trading partners in East and South-East Asia, starting from Japan and Korea in 2017, but also considering other strategic partners such as India, and with countries in Latin America, in particular Mercosur, and the European neighbourhood.

- Closely monitor the functioning of the existing adequacy decisions. This includes in particular the implementation of the EU-US Privacy Shield framework, notably through the annual joint review mechanism.

- Work with and assist countries interested in adopting strong data protection laws and support their convergence with EU data protection principles.

3.2 Alternative data transfer mechanisms

EU data protection rules have always recognised that there is no one-size-fits-all approach to international data transfers. This is even truer of the rules resulting from the reform. While adequacy findings will be available only to those third countries that meet the relevant criteria, the GDPR provides a diverse set of mechanisms that are flexible enough to adapt to a variety of different transfer situations. Instruments can be developed to take into account the particular needs or conditions of specific industries, business models and/or operators. This could for instance take the form of SCCs targeted at the requirements of a particular sector, e.g. specific safeguards when processing sensitive data in the health sector, or of a specific type of processing activities prevalent in certain third countries, e.g. outsourcing services that are carried out for European companies. This could be done by either adopting new sets of standard clauses or by supplementing existing ones with additional safeguards which could range from technical to organisational to business-model related solutions.[44] Some specific sectorial needs can also be accommodated through BCRs applying to groups of companies involved in a joint economic activity, for instance in the travel industry. International transfers between processors could benefit from the development of processor-to-processor SCCs or/and BCRs for processors. Finally, new transfer mechanisms such as approved codes of conduct and accredited third-party certifications provide industry with the possibility to introduce tailor-made solutions for international transfers while benefiting from the competitive advantages associated, for example, with a privacy seal or mark. Some of these instruments can be developed as transfer-specific mechanisms or as part of more general tools to demonstrate compliance with all the provisions of the GDPR, such as in the case of an approved code of conduct.

The Commission will work with industry, civil society and data protection authorities with a view to harnessing the full potential of the GDPR toolkit for international transfers. The

[44] See Article 46(2)(c) and (d) and recital 109 GDPR which clarify that adaptations to approved model clauses are possible as long as they are not contradictory, either directly or indirectly, to those model clauses or prejudice the fundamental rights or freedoms of individuals.

ongoing dialogue with stakeholders in the context of the implementation of the reform will help identify priority action areas in this respect. This may include completing work that has already started such as on the drawing up, in cooperation with the Article 29 Working Party (to be replaced in 2018 by the European Data Protection Board), of processor-to processor SCCs.[45] It can involve developing new components of the EU compliance infrastructure, for instance through the Commission defining requirements and technical standards for the establishment and functioning of certification mechanisms, including for aspects relating to international transfers.[46] Some of these actions can be complemented by work at international level, in particular with organisations that have developed similar transfer mechanisms. For example, ways could be explored to promote convergence between BCRs under EU law and the Cross Border Privacy Rules developed by the Asia Pacific Economic Cooperation (APEC)[47] as regards both the applicable standards and the application process under each system. This should contribute to promoting high data protection standards globally while bridging differences in approaches to privacy and data protection, helping commercial operators to navigate between different systems and designing policies that comply with them.

The Commission will:

- Work with stakeholders to develop alternative personal data transfer mechanisms adapted to the particular needs or conditions of specific industries, business models and/or operators.

3.3 International cooperation for the protection of personal data

3.3.1. Promoting data protection standards through multilateral instruments and fora

The EU data protection legal framework has often served as a point of reference for third countries developing legislation in this field. The EU will continue to engage actively in dialogue with its international partners, at both bilateral and multilateral level, to foster convergence by developing high and interoperable personal data protection standards globally. This contributes to the more effective protection of individuals' rights and at the same time reduces obstacles to the cross-border flow of data as an important element of free trade.

In particular, the Commission encourages accession by third countries to Council of Europe Convention 108 and its additional Protocol.[48] The Convention, which is open to non-members of the Council of Europe and has already been ratified by 50 countries, including African and

[45] Currently no EU-processor to non-EU processor SCCs are in place.

[46] Article 43(8) and (9) GDPR.

[47] See 2014 APEC/EU Common Referential for the Structure of the EU Binding Corporate Rules and the APEC Cross Border Privacy Rules System (CBPR), comparing the compliance and certification requirements of both systems: http://www.apec.org/~/media/Files/Groups/ECSG/20140307_Referential-BCR-CBPR-reqs.pdf.

[48] Council of Europe Convention of 28 January 1981 for the Protection of Individuals with regard to Automatic Processing of Personal Data (ETS No. 180) 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).

South American States[49], is the only binding multilateral instrument in the area of data protection. It is currently in the process of being revised and the Commission will actively promote the swift adoption of the modernised text with a view to the EU becoming a Party. It will reflect the same principles as those enshrined in the new EU data protection rules and thus contribute to the convergence towards a set of high data protection standards.

The G20 meeting in 2017 will provide a further opportunity for the EU to work towards convergence around the principle that high data protection standards are an essential component of the further development of a global information society capable of promoting innovation, growth and social prosperity.[50]

The Commission is also looking forward to engaging with important new actors, such as the UN Special Rapporteur on the Right to Privacy,[51] and further developing its working relationships with regional organisations such as APEC, to foster a worldwide culture of respect for the rights to privacy and personal data protection.

As part of its broader efforts to improve privacy awareness and raise data protection safeguards internationally, on 15 November 2016, the European Commission approved a project under the Partnership Instrument to strengthen cooperation with partner countries in this area.[52] This will include the financing of activities such as training and awareness-raising. In turn, in the context of implementing the reform, the EU can benefit from the exchange of best practices and the experience of other systems with new challenges for the protection of privacy and emerging legal or technical solutions, including as regards enforcement, compliance tools (e.g. certification mechanisms, privacy impact assessments) or the protections for certain specific data sets (e.g. children's data).

3.3.2. Enforcement cooperation

Enhancing cooperation with relevant privacy enforcement and supervisory authorities of third countries is increasingly necessary given the global reach of multinational companies that process vast amounts of personal data in a large number of countries. Often problems of non-compliance with data protection rules or data breaches simultaneously affect people in more than one jurisdiction. In these cases, the protection of individuals could be made more effective through common action. At the same time, economic operators would benefit from a clearer legal environment where common interpretation tools and enforcement practices are developed at global level.

---

[49] Mauritius, Senegal and Uruguay have ratified the Convention. In addition, Cabo Verde, Morocco and Tunisia have been invited to accede.

[50] See also the OECD Ministerial Declaration on the Digital Economy: Innovation, Growth and Social Prosperity ("Cancun Declaration"), 23 June 2016.

[51] See: http://www.ohchr.org/EN/Issues/Privacy/SR/Pages/SRPrivacyIndex.aspx.

[52] Commission implementing decision C(2016)7198, endorsing the second phase of the Annual Action Programme 2016 (AAP 2016) of the Partnership Instrument.

In the borderless and connected world of data flows, it is therefore time to step up cooperation between enforcers.[53] The EU stands ready to play its part. As recalled above, the GDPR enables the Commission to develop international cooperation mechanisms to facilitate the effective enforcement of data protection legislation, including through mutual assistance arrangements. In this context, the possibility to develop a framework agreement for cooperation between EU data protection authorities and enforcement authorities in certain third countries should be explored, drawing also from the experience gained by the Commission in other enforcement areas such as competition and consumer protection.

The Commission will:

- Promote the swift adoption of the modernised text of Council of Europe Convention 108 with a view to the EU becoming a Party and encourage accession by third countries.
- Use multilateral fora such as the United Nations, G20 and APEC to foster a global culture of respect for data protection rights.
- Develop international cooperation mechanisms with key international partners to facilitate effective enforcement.

4. MORE EFFECTIVE LAW ENFORCEMENT COOPERATION WITH STRONG DATA PROTECTION SAFEGUARDS

Personal data exchanges are an integral part of the prevention, investigation and prosecution of criminal offences. In an interconnected world where crime rarely stops at national borders, the swift exchange of personal data is essential for successful law enforcement cooperation and an effective response to crime. Such exchanges must be underpinned by strong data protection safeguards. This also contributes to building confidence between law enforcement authorities (LEAs) and strengthening legal certainty when information is collected and/or exchanged.

The rules on international transfers in the Police Directive govern data exchanges between EU and non-EU LEAs as well as, in specific situations, transfers from LEAs to other entities. The Directive introduces the possibility for adequacy findings in the criminal law enforcement sector. The Commission will promote the possibility of such adequacy findings with qualifying third countries, in particular with those countries with which close and swift cooperation is required in the fight against crime and terrorism, and where significant personal data exchanges are already taking place. On this basis, the Commission will

[53] Existing networks include the Global Privacy Enforcement Network (GPEN) launched in 2010 under the auspices of the OECD. It is an informal network of Privacy Enforcement Authorities, in which EU DPAs are involved, which is tasked with, among others, law enforcement co-operation, sharing of best practices in addressing cross-border challenges and supporting joint enforcement initiatives and awareness raising campaigns. It does not create any new legally binding obligations amongst the participants and focuses primarily on facilitating cooperation in the enforcement of privacy laws governing the private sector. See https://privacyenforcement.net/.

prioritise discussions on adequacy decisions with third countries that are key partners in this endeavour.

Alternatively, the EU-US Data Protection Umbrella Agreement[54] concluded in December 2016 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. By automatically supplementing existing legal instruments on which data exchanges are based (in particular bilateral agreements at both EU and Member State level), the Umbrella Agreement brings immediate and direct benefits to individuals and strengthens law enforcement cooperation by facilitating the exchange of information. Also, by establishing a baseline for future data transfer arrangements with the United States, the Umbrella Agreement does away with the need to repeatedly renegotiate those same safeguards. The Umbrella Agreement constitutes the first bilateral international agreement with a comprehensive catalogue of data protection rights and obligations in line with the EU acquis. It can therefore serve as a basis for negotiating similar agreements with third countries not only in the field of judicial and police cooperation, but also in other areas of public enforcement (e.g. competition policy, consumer protection). This would cover both government-to-government exchanges and data transfers between private companies and LEAs. It could also facilitate the conclusion by the Union of agreements concerning the exchange of data between relevant EU agencies (notably Europol and Eurojust) and third countries.[55] The Commission will thus explore the possibility to conclude similar framework agreements with its important law enforcement partners.

Moreover, the Police Directive envisages the possibility, under strict safeguards and in specific circumstances, for LEAs in the EU to request information directly from a private company in a third country and to pass on personal information (typically a name or an IP address) in that request.[56] Conversely, the GDPR specifically addresses cases where private entities in the EU transmit personal data to the LEAs of a third country following a request: such transfers outside the EU are permissible only under certain conditions, e.g. based on an international agreement or where disclosure is necessary for an important ground of public interest recognised in Union or Member State law.[57]

This cooperation, which has become central to the successful investigation and prosecution of crime and terrorism, is highlighted in Council conclusions on improving criminal justice in cyberspace. The Council has called on the Commission to take concrete actions, based on a common EU approach, to improve cooperation with service providers, make mutual legal assistance more efficient and propose solutions to the problems of determining and enforcing

---

[54] 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: http://ec.europa.eu/justice/data-protection/files/dp-umbrella-agreement_en.pdf (the "Umbrella Agreement")

[55] The conclusion of operational agreements with Europol and Eurojust has also been a benchmark in visa liberalisation dialogues with certain third countries, including e.g. in the context of the ongoing dialogue with Turkey.

[56] See Article 39 and recital 73 of the Police Directive.

[57] See Article 48 and recital 115 of the GDPR.

jurisdiction in cyberspace.[58] These actions cover both exchanges between LEAs and service providers based in the EU and exchanges with non-EU authorities and companies. The Commission will outline options for access to electronic evidence in June 2017, taking into account the need for swift and reliable cooperation underpinned by the strong data protection standards of the Police Directive and the GDPR both in EU-internal situations and for international transfers.

Finally, in accordance with the new legal basis for Europol, the Commission will assess the provisions contained in those operational cooperation agreements between Europol and third parties, concluded under Council Decision 2009/371/JHA, including their data protection provisions.[59] Moreover, as set out in the 2015 European Agenda on Security, the Union's future approach to the exchange of PNR data with non-EU countries will take into account the need to apply consistent standards and specific fundamental rights protections. The Commission will work on legally sound and sustainable solutions to exchange Passenger Name Records (PNR) data with third countries, including by considering a model agreement on PNR setting out requirements third countries have to meet to receive PNR data from the EU. Any future policy in this area will, however, depend, in particular, on the forthcoming Opinion by the Court of Justice of the European Union on the envisaged EU PNR Agreement with Canada.[60]

---

[58] Conclusions of the Council of the European Union on improving criminal justice in cyberspace, 9 June 2016: www.consilium.europa.eu/en/meetings/jha/2016/06/cyberspace--en_pdf/. The Commission has been tasked to present deliverables on these issues to the Council by June 2017, following its progress report to the Council made in December 2016.

[59] See Article 25(4) of Regulation (EU) 2016/794 of the European Parliament and of the Council of 11 May 2016 on the European Union Agency for Law Enforcement Cooperation (Europol) and replacing and repealing Council Decisions 2009/371/JHA, 2009/934/JHA, 2009/935/JHA, 2009/936/JHA and 2009/968/JHA, OJ L 135, 24.5.2016 (pp. 53-114). The Commission is required to present an assessment report by 14 June 2021 on Europol's cooperation agreements concluded before 1 May 2017.

[60] Opinion of the Court of Justice on the draft 2014 EU-Canada PNR Agreement referred to the Court by the European Parliament (Opinion 1/15). The Court was asked to assess the compatibility of the draft Agreement with the EU Charter of Fundamental Rights.

MORE EFFECTIVE LAW ENFORCEMENT COOPERATION WITH STRONG DATA PROTECTION SAFEGUARDS

The Commission will:

- Promote the possibility for adequacy decisions under the Police Directive with qualifying third countries.

- Promote the negotiation of agreements in the area of law enforcement with important international partners along the model provided by the Umbrella Agreement with the U.S.

- Follow-up the Council Conclusions on improving criminal justice in cyberspace to facilitate the cross-border exchange of e-evidence in conformity with data protection rules.

5. CONCLUSION

Protecting and exchanging personal data are not mutually exclusive. A strong data protection system facilitates data flows by building consumer confidence in those companies that care about the way they handle their customers' personal data. High data protection standards thus become an advantage in the global digital economy. The same holds true for law enforcement cooperation: privacy safeguards are an integral part of the effective and swift exchange of information in the fight against crime, based on mutual trust and legal certainty.

Having completed the reform of its data protection rules, the EU should proactively engage with third countries on this matter. It should strive to seek greater upward convergence of data protection principles internationally, at both bilateral and multilateral levels. This is in the interest and to the benefit of citizens and businesses alike. The new data protection legislative framework provides the EU with the necessary and appropriate tools to achieve these objectives. Based on the strategic approach presented in this Communication, the Commission will actively engage with key third countries to explore the possibility to adopt adequacy findings, starting with Japan and Korea in 2017, with a view to fostering regulatory convergence towards the EU standards and facilitating trade relations. At the same time, the EU will make full use of the range of alternative transfer tools to protect data protection rights and support economic operators when data are transferred to countries whose domestic law does not ensure an adequate level of data protection. Such tools should also be used to further facilitate cooperation between EU supervisory and law enforcement authorities and their international partners. The Commission will ensure coherence of the internal and external dimension of EU data protection policy and promote strong data protection at international level to improve law enforcement cooperation, contribute to free trade and develop high personal data protection standards globally.