Briefing

EU Legislation in Progress

European Parliament

CONTENTS

26 September 2018

Third edition

The 'EU Legislation in Progress' briefings are updated at key stages throughout the legislative procedure.

Please note this document has been designed for on-line viewing.

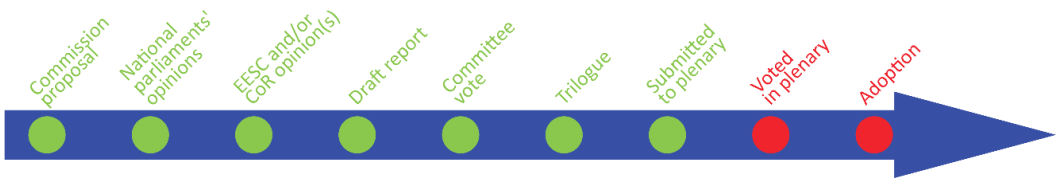
Print

Free flow of non-personal data in the European Union

One of the 16 key elements of the Commission's digital single market strategy, presented in 2015, was a legislative proposal to facilitate the free flow of non-personal data. Although this proposal was not made during 2016, whilst the Commission gathered more supporting evidence, the mid-term review of the digital single market in 2017 identified the data economy as one of the top three priority areas for action in the second half of the strategy's implementation. The European data economy could grow 18-fold, with favourable policy and legislative conditions in place, representing 4 % of EU GDP by 2020.

On 13 September 2017, the Commission tabled a proposal for a regulation aimed at removing obstacles to the free movement of non-personal data across borders. It focuses on removing the geographical restrictions on data storage in the internal market, a move long demanded by stakeholders. In addition, the Commission proposes self-regulation to facilitate switching cloud-service-providers for professional users. Other, less widely agreed aspects, such as access rights and liability are left for future proposals. Within the European Parliament the IMCO committee adopted its report on 4 June along with a mandate to enter into interinstitutional negotiations with the Council. On 19 June a political agreement was reached in trilogue. Parliament is due to vote on this text, in plenary in October 2018.

Proposal for a regulation of the European Parliament and of the Council on a framework for the free flow of non-personal data in the European Union	
COM(2017) 495, 13.9.2017, 2017/0228(COD), Ordinary legislative procedure (COD) (Parliament and Council on equal footing – formerly 'co-decision')	
Committee responsible:	Internal Market and Consumer Protection (IMCO)
Rapporteur:	Anna Maria Corazza Bildt (EPP, Sweden)
Shadow rapporteurs:	Christel Schaldemose (S&D, France); Daniel Dalton (ECR, UK); Dita Charanzová (ALDE, Czech Republic); Julia Reda (Greens/EFA, Germany); Marco Zullo (EFDD, Italy)
Next steps expected:	First-reading vote in plenary



EPRS | European Parliamentary Research Service

Author: Mar Negreiro

Members' Research Service

PE 614.628

EN

Introduction

The amount of machine-generated data being created is increasing at an exponential rate in an increasingly connected world, expected to reach over 30 billion connected devices by 2020. In this context, the value of the European Union's data economy was already more than €285 billion in 2015, representing over 1.94 % of EU gross domestic product (GDP). However, if favourable policy and legislative conditions were put in place, the European data economy could grow 18-fold, representing 4 % of EU GDP by 2020.

Data-driven innovation is underpinned by the free flow of data across borders. To make the most of the data economy, it is essential to enable data to flow across borders and to use data beyond national borders. This would enable growth and job creation, and has the potential to significantly boost European competitiveness in the global market. Firms that adopt data-driven decision-making have been found to have 5-6 % higher output and productivity.

In 2014, the European Commission communication 'Towards a thriving data-driven economy' set out specific measures to support and accelerate the emergence of the data economy. It was followed by the Commission's digital single market (DSM) strategy, in May 2015, which included legislation on the free flow of non-personal data as one of its 16 key measures. However, rather than publishing any related legislative initiative during the first half of the DSM strategy, the Commission instead issued a communication entitled 'Building a European data economy', which specified the rules and regulations impeding the free flow of data and presented options to remove unjustified or disproportionate data storage location restrictions (i.e. national rules that require data to be stored/processed in a specific territory). According to the Commission, further consultation was necessary before proposing any EU legislation.

In May 2017, under the mid-term review of the digital single market strategy, the Commission again identified development of the European data economy as one of its three key priority areas for further EU action in the years to come, and announced a legislative proposal for the second half of 2017. On 13 September 2017, coinciding with President Juncker's State of the Union speech to the European Parliament, the Commission presented its proposal for a regulation on a framework for the free flow of non-personal data.

The European Commission's accompanying staff working document notes that the trend in Europe is towards more, not less data localisation (an increase of 100 % in 10 years), which some studies have linked to the general misconception among administrations and businesses that there is a legal obligation to store data within national borders. In effect, geographical data localisation may weaken security,[1] as centralised data is more vulnerable to targeted attacks. According to the Commission review, many Member States restrict the geographical location and storage of data related to the financial and health sectors, as well as company records, accounting and tax data, telecommunications, and government data.

At present cloud computing service-providers cannot choose competitive locations that might be more suitable when constrained by geographical data localisation rules. The Commission has identified this as a major barrier to the development of cloud computing services and infrastructure, as set out in the European cloud initiative. A recent report estimated that data localisation policies raise the cost of hosting

1 The Commission has noted that data security does not depend on its location but rather on the security of the IT infrastructure and the strength of the encryption and protection techniques used.

data by 30-60 %. For instance the Leviathan Security Group calculates that the cost of data processing in Germany is twice as high as that in neighbouring Belgium. This exacerbates market fragmentation as the costs of storing data vary substantially across Member States: according to some estimates, in 2016 these costs could vary by up to 120 % across the EU.

There would be also environmental advantages to data hosting in countries with cooler weather and greener energy. For instance, Nordic countries have experienced a boom in data storage business as companies might save up to 50 % on hosting infrastructure because of lower temperatures and energy costs.

Existing situation

Even though free flow of data is to some extent already supported by regulations that aim at deepening the EU single market in some sectors,[2] no specific regulation targets the storage of non-personal data alone.. Non-personal data is defined as data other than personal data, i.e. data not relating to an identified or identifiable person, including anonymised data and machine-to-machine data.

It should be noted that there is already a framework in place for personal data.[3] The recently adopted General Data Protection Regulation (GDPR), guarantees the free flow of personal data within the EU. Since 25 May 2018, the regulation requires EU Member States to refrain from establishing data localisation requirements based on the protection of personal data. The GDPR framework also covers the ownership of personal data aspect, but at this time, there is no framework in place for ownership of non-personal data. In other areas, ownership is accounted for in certain specific information goods, such as copyright, patents and trademark law. The DSM midterm review announces that the Commission will continue to assess the need for action in areas such as non-personal data access rights, liability, and portability.

Parliament's starting position

The European Parliament (EP) has asked the Commission to unlock the potential of the data economy on at least two occasions.

In its resolution of 10 March 2016, 'towards a thriving data-driven economy' (2015/2612(RSP)), Parliament specifically asked the Commission to 'develop a regulatory framework to tackle the economic, technological, social and cultural challenges of a data-driven economy' and furthermore 'that the following challenges be addressed: data ownership, possession, management, access and security, interoperability, data limitation

2 Mainly the E-commerce Directive 2000/31/EC, the Services Directive 2006/123/EC, the Directive on the re-use of public sector information (Directive 2003/98/EC, known as the 'PSI Directive', currently under review), the General Data Protection Regulation (GDPR), and the E-privacy Directive 2002/58/EC (currently under review). The general provisions of the Treaty on the Functioning of the European Union (Articles 49 and 56) could be applicable to the totality of data storage and other processing services. However addressing existing barriers through infringement procedures against the Member States concerned has been identified as cumbersome and complicated, yet leaves a situation of legal uncertainty.

3 According to the GDPR Recital 26; Article 4(1), 'Personal data' means any information relating to an identified or identifiable natural person ('data subject'); an identifiable person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that person.

and storage, restrictions on the use and reuse of data across Europe, innovative interrupters in intellectual capital, accessibility and infrastructure, transparent transportation rules, cross-border mechanisms and, where applicable, the creation and dissemination of, and access to, open data, and its availability for public administrations and service providers'.

Similarly, in its resolution of 16 January 2016, towards a digital single market act, the EP also highlighted that a data-driven economy is key to economic growth; emphasised the opportunities that new ICT technologies such as big data, cloud computing, the Internet of Things, 3D-printing and other technologies can bring to the economy and society; recalled that the creation of the digital single market is dependent on the free flow of data within and outside the European Union; and asked for action to be carried out for this to happen.

Council & European Council starting position

In its conclusions of 25 and 26 June 2015 and those of 15 December 2016, the European Council called for EU action to ensure the free flow of data.

Similar calls were made by the Estonian Presidency of the Council of the EU in its vision paper on the free movement of data.

In addition, a letter of 13 December 2016 to the President of the European Council signed by 16 Member States called for a legislative proposal to end data localisation practices (the signatories were: Belgium, Bulgaria, the Czech Republic, Denmark, Estonia, Ireland, Latvia, Lithuania, Luxembourg, the Netherlands, Poland, Slovenia, Slovakia, Finland, Sweden and the United Kingdom).

Proposal

Preparation of the proposal

To underpin the proposal and collect evidence, the Commission ran two public consultations, nine dedicated workshops, and commissioned four dedicated studies, which fed into its impact assessment accompanying the legislative proposal. The related reports' main results are briefly described below.

Public consultations:

The first public consultation was broader and focused on several issues related to the regulatory environment for platforms, online intermediaries, data and cloud computing, and the collaborative economy. It ran for 12 weeks from September 2015 to June 2016. In total, 1 036 responses were received, but not all respondents answered every question or section: around 60 % of the respondents replied to the section on 'data and cloud computing', as per the full report of the results. One main outcome was that two thirds of respondents found that restrictions on localisation affected their strategy for doing business in Europe. A majority of respondents wanted to make a clear distinction between personal and non-personal data. However, detailed answers revealed that making such a distinction is not always easy.

A second public consultation was launched in the context of the European Commission communication on 'Building a European data economy' (COM (2017) 9), which ran from 10 January to 26 April 2017. The online survey received a total of 380 responses and 21 position papers.

The stakeholder consultation confirmed that businesses incur high costs due to current data localisation restrictions, predominantly when carrying out cross-border business in the EU, launching new services, entering new markets, or starting a new business. More than half of the respondents (61.9 %) wanted data localisation restrictions to be removed. A majority of respondents also preferred legislative action to tackle unjustified localisation restrictions. This would bring many benefits to the DSM, such as cost reductions, stronger competition to correct the existing market distortions, improved data security and more legal certainty to encourage the free movement of data.

Respondents also indicated that there are problems with transferring non-personal data between cloud-service-providers if they wish to change provider or bring the data in-house. A majority of SMEs testified to having experienced difficulties when attempting to transfer data. About a quarter of respondents said they were dissatisfied with the conditions under which they can port (i.e. transfer) data, and about a third had experienced difficulties with porting data.

Four studies commissioned:

1. Study on measuring the economic impact of cloud computing in Europe: This study provides an assessment of the likely impacts of cloud computing in Europe for three different groups of stakeholders: professional users; providers; and society as a whole. The study estimated that over the next five years, cloud computing could add a cumulative total revenue of €449 billion to EU-28 GDP (including in the public sector). This will have a positive impact on job creation and employment.

2. Study on facilitating cross border data flow in the DSM: This study investigated restrictions on the free flow of data within the EU by looking at eight Member States (the Czech Republic, Germany, Spain, France, Italy, Lithuania, Luxembourg and the United Kingdom). It concluded that unnecessary geographical requirements to maintain control over the location where data and documents physically reside are an obstacle to the free flow of data within the single market. An important finding is the widespread misinterpretation of the existing legal framework: Many market participants assume data storage and processing within national boundaries is mandatory or advised, when in fact it is not.

3. Study on cross-border data flow in the digital single market: Data location restrictions: The objective of the study was to provide evidence on the scope and magnitude of legal and non-legal barriers in Member State practices that hinder the free flow of non-personal data within the DSM. It was also supposed to provide evidence of the costs of these barriers for the private and public sectors. However, this evidence could not be provided, as very little data exist on the volume and economic value of cross-border data flows within Europe, due to a lack of reliable 'digital trade' statistics.

4. Study on European data market, measuring the size and trends of the EU data economy: This study presented the findings of a monitoring tool measuring the size and trends of the EU data economy for the years 2013-2016, as well as forecasts up to 2020. The results showed that the value of the data economy grew from €247 billion in 2013 to almost €300 billion in 2016 (worth nearly 2 % of EU GDP). By 2020, the EU data economy is expected to increase to €739 billion, with an overall impact of 4 % on EU GDP. According to the monitoring tool, in 2016 there was a gap between total demand and supply of data workers of 420 000 unfilled data-worker positions in the EU, corresponding to 6.2 % of the total demand for skilled data professionals. By 2020, the EU is forecast to face a data skills gap corresponding to 769 000 unfilled positions in the baseline scenario, concentrated in particular in the large Member States (especially Germany and France).

Impact assessment:

An impact assessment in two parts was carried out for this legislative proposal.[4] The following set of options were considered: a baseline scenario (no policy intervention) and three policy options. Option 1 consisted of guidelines and/or self-regulation to address the different problems identified, and entailed strengthening of enforcement vis-à-vis different categories of unjustified or disproportionate data localisation restrictions imposed by Member States. Option 2 would lay down legal principles concerning the different problems identified and would envisage the designation by Member States of single points of contact and creation of an expert group, to discuss common approaches and practices and provide guidance on the principles introduced under the option. A Sub-option 2a was also considered, to allow for the assessment of a combination of legislation establishing the free flow of data framework and the single points of contact and an expert group, as well as self-regulatory measures addressing data porting. Option 3 consisted of a detailed legislative initiative, to establish, inter alia, pre-defined (harmonised) assessments of what constitutes (un)justified and (dis)proportionate data localisation restrictions and a new data porting right.

4 See impact assessment SWD(2017)304/948366 (Part 1) and impact assessment SWD(2017)304/948366 (Part 2).

In the first instance, the Commission showed a preference for Option 2. However, it received two negative reviews from the Regulatory Scrutiny Board (RSB), which criticised a number of shortcomings,[5] the main one being that there was insufficient evidence to justify a new right to the portability of cloud services data, and that the evidence seemed to point to less stringent options. The Commission therefore had to accommodate a lighter legislative proposal through Option 2a, which focuses mainly on removing data storage localisation restrictions, while proposing a self-regulatory approach for the portability aspects for the time being.

The impact assessment showed that Sub-option 2a would ensure the effective removal of existing unjustified localisation restrictions and would prevent future limitations, as a result of a clear legal principle combined with review, notification and transparency, while at the same time enhancing legal certainty and trust in the market. The burden on Member States' public authorities would be modest, leading to approximately €33 000 annually in terms of human resources costs to sustain the single points of contact, as well as a yearly cost of between €385 and €1 925 for the preparation of notifications.

The main economic estimate shows that removing data localisation restrictions is considered the most important factor for the data economy to unlock its full potential. Moreover, removing existing data localisation measures will drive down the costs of data services, provide companies with greater flexibility in organising their data management and data analytics, while expanding their use and choice of providers. Even though the main direct beneficiaries are businesses, it is also expected that these benefits would indirectly reach consumers, through greater choice of hosting service providers at more competitive prices. Positive environmental impacts are also expected, as locating hosting in greener and cooler countries will be possible, leading to less pollution.

EPRS has published an initial appraisal of the Commission's impact assessment. It concludes that the Commission carried out a well-structured analysis although it highlights the scant availability of quantitative data, also highlighted by the RSB in its two negative opinions, which weakens its effectiveness in underpinning the proposal.

The changes the proposal would bring

The general policy objective of the initiative is to achieve a more competitive and integrated internal market for data storage and other processing services and activities. To this aim, the new regulation would bring three main changes:

5. The regulation establishes the principle of free movement of non-personal data in the Union to deepen the internal market: The regulation would prevent any Member State from imposing territorial restrictions or prohibitions regarding the storage or any other processing of data anywhere within the EU. It removes unjustified or disproportionate national rules that hamper or restrict companies in choosing a location for storage or processing of their data. There is always a door open to exceptions based on grounds of public security, which will need to be expressly

5 These are detailed on a table in SWD(2017)304 final, part 2/2.

justified, and notified ex ante to the European Commission for its assessment and approval as provided for the Single Market Transparency Directive.

6. The regulation clarifies the availability of non-personal data for regulatory control. For this purpose, public authorities will retain access to data, when it is located in another Member State, or when it is stored or processed in the cloud, just as they do when the data is stored on their own territory. Private parties cannot therefore refuse access to such data on the basis of the country in which they are stored. To facilitate this access, a single point of contact per Member State will be created to liaise with other Member States' contact points and with the European Commission.

7. The initiative would enable easier switching of cloud-service-providers for professional users. The Commission proposes a self-regulatory approach, encouraging providers to develop codes of conduct regarding the conditions under which users can port data between cloud-service-providers and back into their own IT environments. The Commission proposes a two-year deadline for such codes of conduct to come into force and become fully effective. It would also review the situation within the following two years, to assess if the code is working, or if more stringent solutions are necessary.

The Commission proposes to conduct a review within the regulation's first five years, and to report its findings to the European Parliament, Council and Economic and Social Committee.

Full consistency and synergies are expected with the recently proposed cybersecurity act, including clarification that any security requirements that already apply to businesses storing and processing data will continue to do so when they store or process data across borders in the EU or in the cloud.

Views

Advisory committees

On 15 February 2018, the European Economic and Social Committee (EESC) adopted its opinion on the proposal, in which it states that it cannot endorse the current version and asks the Commission to make a number of changes and improvements. Among other things, the EESC recommends that the Commission revisits its proposal with a view to bringing it significantly closer to the terms defined in the impact assessment under option 3, moving away from the sub-option 2a, as it criticises its lack of ambition. Moreover, the EESC asks the Commission to incorporate the suggestions outlined in the opinion's points 3.4.1 (date of entry into force), 3.4.2 (the absence of an obligatory procedure in cases of non-compliance), 3.6 (the absence of guidelines for drawing up codes of conduct), 3.7 (failure to take into account the classification of metadata) and 3.8 (failure to take account of the global, trans-European nature of the digital economy), especially as regards the need to provide for a specific procedure for cases where Member States do not comply. The EESC also stated that it supports the position adopted by the Council in December.

The European Committee of the Regions (CoR) for its part has not adopted an opinion on the proposal. However both committees had issued an opinion on the Commission's January 2017 communication on building a data economy.

In its opinion on building the data economy, the EESC supported the communication, while asking the Commission to carry out a precise analysis of the state of play of free flow of data in the Member States, in order to remove unjustified barriers and put the right legal and technical provisions in place. It also noted that contractual freedom in the private sector should be respected; supported a general EU framework for standards that do not hamper innovation; and asked for portability of data to be promoted.

In its opinion on building the data economy, the CoR also supported the communication's aims, while pointing out that disadvantaged regions have neither the basic infrastructure nor the expertise needed to establish a digital data-driven economy, and recommended that regulatory assistance be provided for these regions. It also asked for a data protection framework to promote innovation, standards and fight cyber-attacks, which tend to exploit major vulnerabilities of digital technologies central to smart cities and regions.

National parliaments

The deadline for national parliaments to submit reasoned opinions on the grounds of subsidiarity was 6 December 2017.

The French Senate adopted a reasoned opinion on 27 November, which considers that the proposal does not comply with the principle of subsidiarity. Among other things, it criticises the weakness of the Commission's impact assessment and that, in addition to public safety, Member States can also legitimately invoke public security, public order and public health to impose a data location obligation on their territory.

It also regrets that the text does not set out a definition of non-personal data. Moreover the text does not solve the question of databases that include both personal and non-personal data.

The Spanish Senate adopted a resolution on 8 November which concluded that the text complies with the principle of subsidiarity.

The Czech Senate also adopted a resolution on 22 November, which supports the proposal but asks for further clarifications regarding, among other things, the concept of non-personal data, the term 'professional user' and the concept of 'public safety' as a proposed exception. It also underlines that the proposal must not call into question the protection of business secrets and other sensitive data relating to their know-how; or freedom of contract for services. Finally it calls for clarification on the Commission's intentions in the event of its dissatisfaction with the development of self-regulation on data portability.

Stakeholders' views[6]

A majority of stakeholders agree that EU legislative action is needed to remove geographical data localisation restrictions and that any forced data storage localisation requirements should be subject to EU scrutiny and should only be retained if they are proportionate and in line with EU legislation and single market principles.

For instance, during the consultation, the technology industries of Finland and Aalto University requested that decisive EU regulatory action is taken against forced data localisation in Member States. Similarly, in a joint statement, industry associations from several sectors including BusinessEurope, COCIR, ACEA and AIOTI asked the EU to introduce a legal instrument that removes existing national data localisation requirements and prevents the creation of new ones. Similarly, the Netherlands' industry associations VNO-NCW and MKB-Nederland highlighted that localisation requirements conflict with free establishment of business throughout Europe and should be removed. The bodies also asked for clarifications of the exceptions with regard to 'national security', in particular when national security could be a legitimate reason for storing data within national borders. They suggest that the framework covering these exceptions should be made clear. Elements of this framework could include limiting the risk of severe social disruption, i.e. sovereignty, territorial integrity and socio-economic functioning of the state.

Some stakeholders are worried about the blurred distinction between personal and non-personal data for portability purposes, as recognised in Article 20 of the GDPR. As an example, some academics mentioned 'a very close line between non-personal (anonymised) data and machine-generated data which is either personal data – and/or information in which an individual may have a reasonable expectation of privacy' [...] This "grey area" of on-going legal uncertainty for data controllers adds confusion to the decision-making process in deciding which legal regime would apply'.

However, when it comes to other issues related to data economy outside the scope of this legal proposal, such as data ownership, access and liability, there is less consensus for public intervention. Many industry

6 This section aims to provide a flavour of the debate and is not intended to be an exhaustive account of all different views on the proposal. Additional information can be found in related publications listed under 'EP supporting analysis'.

associations prefer to leave these to the market and to the existing legislation for the time being, while further investigating bottlenecks for portability, as these have a chilling effect on firms to innovate.

The Commission's European Political Strategy Centre (EPSC) noted that data portability and interoperability are important in the field of machine-generated data, and accompanying rules are urgently needed so as not to lower services' incentives to invest in data-driven innovation.

Legislative process

Within the European Parliament, the file was assigned to the Committee for the Internal Market and Consumer protection (IMCO), rapporteur Anna Maria Corazza Bildt (EPP, Sweden). The Industry, Legal Affairs, and Civil Liberties Committees (ITRE, JURI and LIBE) have been asked for an opinion. The Legal Affairs and the Civil Liberties Committees decided not to submit an opinion.

On 12 October 2017, the European Commission presented the legislative proposal and impact assessment to the IMCO committee.

On 20 February 2018, the IMCO committee held a workshop on the proposal with experts. The draft report was published on 1 March and the rapporteur presented it to the IMCO committee on 21 March. On 24 April the industry committee adopted its opinion on the proposal.

The deadline for amendments in IMCO was 26 March. Some 20 compromise amendments were presented in IMCO on 17 May, and the committee adopted its report on 4 June, with 28 votes in favour, 3 against and 0 abstentions.

The report aims at making the text legally clearer, easier to apply and 'future-proof'. It focuses on clarifying further some concepts, including the public security exception, the scope of application (including now, for instance, a reference to public-sector entities as users), the issue of mixed data-sets and complementarity with the new Data Protection Directive, the porting of data and access to data for public authorities. Since many localisation requirements originate at various levels of governance and not only at national level, the report proposes that this regulation will apply at all levels of governance, and cover both laws and practices, including in the area of public procurement. On the creation of codes of conduct for the porting of data, the report proposes changes to make it easier for SMEs to port data, and encourages them to participate in the development of codes of conduct. It proposes two phases: one for the development of such codes development and one for their implementation.

The report proposes to shorten the evaluation period (article 9) from five years to three and a half years after the date of publication, to keep the regulation up to date. Considering among other things the evaluation of the regulation's application to mixed data sets, the public security exception's implementation and the development and implementation of the codes of conduct. It also asks the Commission to publish guidelines on how the regulation applies to mixed data sets by six months after the date of publication.

On 19 December 2017, the Council had agreed its position and on a mandate to begin negotiations with the European Parliament as soon as possible. The Council supports the Commission's proposal, and intends to allow Member States to impose data localisation requirements only when these are justified on grounds of public security. It has proposed that the concept of 'public security' is defined within the meaning of Article 52 TFEU and as interpreted by the Court of Justice.

On mixed data sets, where non-personal and personal data are inextricably linked, the Council position is that the General Data Protection Regulation will apply to the personal data part of the set, while the non-personal data will be covered by this regulation. Furthermore, it notes that the regulation does not impose an obligation to store the different types of data separately. The IMCO report follows the same line.

The European Council in October 2017 had called for the co-legislators to reach an agreement on this priority dossier by June 2018. The mandate to start negotiations with the Council was approved in the IMCO committee on 4 June. Inter-institutional negotiations started on 14 June, and an agreement was reached during the second trilogue meeting on 19 June. That provisional political agreement was endorsed by the IMCO committee on 12 July 2018.

The agreed text of the regulation sets out the principle that non-personal data is allowed to be located and processed anywhere in the EU without unjustified restrictions, with some exceptions on the grounds of public security. It abolishes data localisation requirements, while making sure that competent authorities can access data for the purposes of regulatory control. To facilitate competent authorities' access to data, a single point of contact per Member State will be created, to liaise with other Member States' contact points and with the European Commission. Under the agreement, the Commission is to publish guidelines regarding the interaction of this regulation and the GDPR in the context of mixed data sets, before the present regulation becomes applicable. As requested by the Parliament, the agreement establishes that the regulation will apply at all levels of governance, and cover both laws and practices, including in the area of public procurement.

Regarding the development of self-regulatory codes of conduct, it has been agreed that, in four years' time, the Commission will review their implementation (one year earlier than the Commission had proposed) and may propose additional measures if needed.

Parliament is due to vote on the agreed text during in the first plenary part-session of October 2018. Once adopted, it would enter into force twenty days after its publication in the Official Journal of the European Union, and apply six months after that publication.

References

EP supporting analysis

Dalli, H., Free flow of non-personal data in the European Union, Initial Appraisal of a European Commission Impact Assessment, EPRS, European Parliament, February 2018

Davies, R., Big data and data analytics, EPRS, European Parliament, September 2016.

Monteleone, S., Reform of the e-Privacy Directive, EPRS, European Parliament, September 2017.

Monteleone, S., Data protection reform package: Final steps, European Parliament, April 2016.

Big Data and smart devices and their impact on privacy, Policy Department for Citizens' Rights and Constitutional Affairs, European Parliament, 2015.

Negreiro, M., Towards a European gigabit society, EPRS, European Parliament, June 2017.

Negreiro, M., ENISA and the new Cybersecurity Act, EU Legislation in Progress Briefing, EPRS, European Parliament, December 2018

Other sources

Unleashing Internal Data Flows in the EU: An Economic Assessment of Data Localisation Measures in the EU Member States, ECIPE, 2016.

Enter the data economy, EU Policies for a Thriving Data Ecosystem, strategic issue 21, European Political Strategy Center, European Commission, 11 January 2017.

Free flow of non-personal data in the European Union, Legislative Observatory (OEIL), European Parliament.

Disclaimer and Copyright

This document is prepared for, and addressed to, the Members and staff of the European Parliament as background material to assist them in their parliamentary work. The content of the document is the sole responsibility of its author(s) and any opinions expressed herein should not be taken to represent an official position of the Parliament.
Reproduction and translation for non-commercial purposes are authorised, provided the source is acknowledged and the European Parliament is given prior notice and sent a copy.
© European Union, 2018.

eprs@ep.europa.eu | EPRS (intranet) | Thinktank (internet) | Blog