



Brussels, 15.5.2018
COM(2018) 320 final

**COMMUNICATION FROM THE COMMISSION TO THE EUROPEAN
PARLIAMENT, THE EUROPEAN COUNCIL, THE COUNCIL, THE EUROPEAN
ECONOMIC AND SOCIAL COMMITTEE AND THE COMMITTEE OF THE
REGIONS**

Completing a trusted Digital Single Market for all

**The European Commission's contribution to the Informal EU Leaders' meeting on data
protection and the Digital Single Market in Sofia on 16 May 2018**

Everyone has the right to respect for his or her private and family life, home and communications.

Everyone has the right to the protection of personal data concerning him or her. Such data must be processed fairly for specified purposes and on the basis of the consent of the person concerned or some other legitimate basis laid down by law. Everyone has the right of access to data which has been collected concerning him or her, and the right to have it rectified.

Compliance with these rules shall be subject to control by an independent authority.

Articles 7 and 8 of the Charter of Fundamental Rights of the European Union

The European Union should not only preserve our European way of life but empower those living it. Being European means the right to have your personal data protected by strong, European laws. Because Europeans do not like drones overhead recording their every move, or companies stockpiling their every mouse click. Because in Europe, privacy matters. This is a question of human dignity.

President Jean-Claude Juncker
State of the European Union speech on 14 September 2016

*The European Commission welcomes the decision of the President of the European Council to schedule a debate under the Leaders' Agenda on protection of citizens' privacy and personal data and other issues relating to Digital Europe, including the adoption of all the legislative instruments establishing the Digital Single Market. This Communication presents a set of concrete actions to ensure full protection of citizens' privacy and personal data and to accelerate the completion of the Digital Single Market in 2018 and to feed the informal discussion that the Heads of State or Government will hold in Sofia on 16 May 2018.*¹

1. Introduction

In 2015, the European Council endorsed a Digital Single Market Strategy for the Union. Three years on, the Digital Single Market is becoming a reality.² All the planned legislative proposals have been presented by the Commission.³ Proposals on mobile roaming and portability of online content services have already been adopted. The General Data Protection Regulation will become directly applicable across the Union on 25 May. Other major new steps on network and information security and electronic identification will all be in place in a matter of weeks. The next wave of legislative proposals, opening up access to online services, is agreed and will follow before the end of the year. These are all critical steps towards the goal of completing the Digital Single Market.

The Digital Single Market Strategy is the key for making the EU thrive in the emerging global data economy. Data is now a central asset in the digital society. Every second, smart phones, energy networks, cars, home appliances and individuals in their daily activities are generating data on an ever-increasing scale. Manufacturers, platforms and service providers are collecting, processing and using this data to provide new services to users and gain a competitive edge.

The EU has been slow to exploit the opportunities of the data economy: only some 4% of global data is stored in Europe. But it has many assets: a strong manufacturing base, a fast-growing start-up ecosystem, newly digitised industrial processes and a skilled workforce. If these can be harnessed and scaled up, the European data economy can become a powerful lever to drive growth, spur the creation of new jobs and open up new business models and new innovation opportunities.⁴ The value of the European data economy has the potential to top EUR 700 billion by 2020, representing 4% of the EU economy.

However, the data economy revolution brings also challenges for our societies and for the values on which our Union is based, including democracy, human rights and the rule of law. Recent events have shown that data can be collected, processed and used at the expense of privacy. Access to large amounts of data can be used to gain undue advantage over competitors or even to influence media and public opinion. Personal information can be subject to unauthorized access by third parties. Respect for private life and the protection of personal data are fundamental rights in the EU, as established by the EU Charter of Fundamental Rights.⁵ Strong data protection, confidentiality of communications and data

¹ European Council Conclusions of 22 March 2018.

² COM(2015) 192 of 6 May 2015, Communication on 'A Digital Single Market Strategy for Europe'.

³ See Annex.

⁴ COM(2018) 306 'A renewed European Agenda for research and innovation'; COM(2018) 267-272 – Building a stronger Europe: the role of youth, education and culture policies.

⁵ Articles 7 and 8 of the EU Charter of Fundamental Rights.

security are crucial to dispel individuals' doubts about misuse of their data and to create trust. Without this trust, the potential of a thriving data economy will not be met.

This Communication calls on the European Council to address urgently the remaining issues to make the Digital Single Market a reality and ensure that the EU remains a key player in the global race towards a data economy.⁶ This cannot be done without citizens' trust in how their data are protected and used.

2. Protecting personal data, building confidence in the digital economy: General Data Protection Regulation and ePrivacy Regulation

A new data protection regime for individuals in the EU

Two-thirds of Europeans say that they are worried about having no control over the information they provide online, while half are concerned about falling victim to fraud.⁷

Recent revelations around the 'Facebook/Cambridge Analytica' case have raised awareness among citizens that their data could be misused if not properly protected. The EU data protection authorities are taking action under current data protection rules, and investigating the case in a coordinated manner. The Commission has been in touch with Facebook, urging the company to provide more detailed information and to cooperate fully with the Irish and United Kingdom data protection authorities, who are leading the investigation, to understand what happened and whether the almost 3 million EU individuals affected are still at risk.

These events illustrate that the EU was right to adopt strong data protection rules. With the **General Data Protection Regulation**, which will become directly applicable across the Union on 25 May,⁸ the EU will be better equipped to avoid and address such cases in the future.

What will change with the General Data Protection Regulation

Firstly, individuals will gain better control over how their personal data is processed by companies.⁹ The Regulation will in most cases apply where a contract with or clear consent by individuals exist as a precondition for collecting data – silence or inactivity cannot be taken as a consent. Strengthened transparency requirements, and rights of information, access and erasure ('right to be forgotten') are introduced. Further re-use of the data for a new purpose has to be preceded by information to the user in order to obtain a new consent, unless it is otherwise lawful and permitted under the Regulation. For example, a business that has collected client data for customer care purposes will have to inform the client about plans to use the data for exploring his or her purchasing habits, and obtain the relevant consent. The collection of large swathes of personal data, under any contract or consent arrangement, would go against the principles of purpose limitation and data minimisation.

Secondly, the Regulation introduces **stronger protection against data breaches** also through an obligation to notify the supervisory authority at the latest within 72 hours when the data

⁶ Communication on the Mid-Term Review on the implementation of the Digital Single Market Strategy, COM (2017) 228 of 10 May 2017.

⁷ Special Eurobarometer 431, Data Protection Report, June 2015.

⁸ Regulation (EU) 2016/679.

⁹ Lawfulness of processing, Article 6 of the General Data Protection Regulation, Regulation (EU) 2016/679.

breach is likely to pose a risk to the individual's rights and freedoms. In certain circumstances, it obliges to inform the person whose data is concerned by the breach.

Thirdly, the Regulation will make cooperation between national supervisory authorities in cross border cases more effective and will ensure a coherent interpretation and application of rules in the Union, including through a European Data Protection Board (EDPB) which will provide guidance and ensure a consistent interpretation and application, in case several Member States are concerned across the EU.

Finally, enforcement is also strengthened under the new framework, and centred on a network of national data protection authorities which will each have the power to impose fines on controllers and processors that can go up to EUR 20 million or, in the case of a company, 4% of worldwide annual turnover, whichever is higher.

The EU data protection rules enable the free flow of personal data within the Union, from which the critical mass of data essential for a strong data economy can be generated. For example, cross-border approaches when using the data from citizens' smart meters for smart grid applications and improved energy security rely on the free flow of personal data. As explained in the Communication on Artificial Intelligence for Europe,¹⁰ the availability of privately-held data in the wider interest should be encouraged. For instance, sharing data on the outbreak of epidemics across countries could contribute to a more timely response by medical authorities. Sharing of and access to personal health data could improve diagnosis and treatment. Sharing data from cars and transport means could improve traffic management and reduce congestion. All this is possible while securing a high degree of protection for personal data.

Building a genuine European Data Space¹¹ requires a level playing field also for non-personal data, and a proposal to this end is already on the table.¹² Quick finalisation of the Regulation on the **free flow of non-personal data** will also benefit from proposals to boost access to data from the public sector (see below).

The new data protection regime must work on the ground from day one.¹³ During the transition period of two years, national administrations, data protection authorities and private operators have worked to be ready for the new framework. Now an additional effort is required to make sure that everyone is fully prepared. With less than two weeks before the deadline, most Member States still need to take all the measures necessary to ensure that their national regulatory system fully complies with the Regulation and that their national data protection authorities have adequate resources to play in full their role. It is essential that these measures are adopted swiftly. The Commission calls on the Member States to take all necessary actions and to pay particular attention to the needs of smaller enterprises to ensure that their compliance costs do not impair their ability to compete with larger firms.

¹⁰ COM(2018) 237 of 26 April 2018.

¹¹ Communication 'Towards a common European data space', COM(2018) 232 of 25 April 2018; Communication on Building a European Data Economy, COM(2017) 9 of 10 January 2017.

¹² Proposal for Regulation on a framework for the free flow of non-personal data, COM(2017) 495 of 13 September 2017.

¹³ COM(2018) 43 - Stronger protection, new opportunities - Commission guidance on the direct application of the General Data Protection Regulation as of 25 May 2018.

ePrivacy: the confidentiality of communications

The ability to communicate confidentially, both online and offline, is a right recognised in the EU Charter for Fundamental Rights and a major demand of citizens for the digital society.¹⁴ The Union cannot tolerate a situation whereby someone first creates detailed political profiles of its citizens by data-mining their personal communication and location data, and then uses this knowledge to try to manipulate citizens' political behaviour.

This is why, alongside the General Data Protection Regulation, **ePrivacy** rules are essential to ensure that the confidentiality of Europeans' online communication is not breached. This also means that processing electronic communications data by other than the end-user would not be allowed and no service providers would be able to access devices without users' consent. Individuals will be able to take active control of their online presence via browsers, apps and digital devices, and to avoid unauthorised tracking or tapping without consent. This would set the world standard, with a consistent set of rules on data protection and digital privacy.

The new ePrivacy rules, once approved by the legislators, would apply both to traditional telecom operators and to new communication services such as email, instant messaging or internet-based voice services.¹⁵ It would ensure confidentiality of communications and a level playing field for all operators. The Commission calls on the Council to swiftly agree on a common position, in order to start negotiations with the European Parliament and progress towards agreement this autumn.

International Data Flows

The new EU data protection rules also further open the Union to the opportunities of the global data economy. They expand the 'toolbox' for the international transfer of personal data to third countries, by adding certification mechanisms and approved codes of conduct, together with binding and enforceable commitments of the controller or processor, as alternatives for ensuring a strong level of protection to personal data transferred from the EU. Uniform and simplified rules will also make the EU more attractive to inward investment.

The handling by U.S. authorities of the 'Facebook/Cambridge Analytica' events is an important test for the EU-U.S. Privacy Shield, which since 2016 ensures a level of protection equivalent to that in the EU. The Commission welcomes the opening of an investigation by the U.S. Federal Trade Commission and will follow it closely, also in view of the second annual review of the arrangement in September 2018. The Privacy Shield guarantees that any EU individual who considers that his or her data has been unlawfully processed by U.S. companies participating in and applying the Privacy Shield to transferred data benefits from several avenues for redress that are both easily accessible and affordable.¹⁶ The Commission will continue to monitor that this is the case in practice.

More and more countries around the world are realising that robust data protection and privacy rules not only ensure fundamental rights, but generate trust in the digital economy. As a result, many are adopting or modernising privacy laws. And often the General Data

¹⁴ The ability to communicate confidentially, both on-line and off-line, is a right recognized in Article 7 of the Charter for Fundamental Rights of the EU; the right to privacy and the confidentiality of communications is not specifically addressed by the General Data Protection Regulation.

¹⁵ COM(2017)10. Until such approval occurs, from 25 May 2018 when the General Data Protection Regulation starts applying, the references to consent under the current ePrivacy framework - Directive 2002/58/EC - shall be construed as references to consent under the General Data Protection Regulation.

¹⁶ Report on the first annual review of the functioning of the EU-U.S. Privacy Shield, COM(2017) 611 of 18 October 2017.

Protection Regulation serves as an inspiration, with the EU rules setting a global standard for data protection and privacy. Currently the Commission is exploring adequacy decisions with Japan and South Korea, which would mean that personal data transferred to these countries from the EU would enjoy the same level of protection and rights of redress as in the EU itself.

At the same time, the Commission has developed an approach on how the EU can tackle, through trade and investment agreements, protectionist practices as regards cross-border data flows in the digital economy while ensuring that the right to protect personal data and privacy is fully preserved. This approach, once included in the EU's trade and investment agreements, will foster both free flows of data and trust in the way personal data are processed.

In view of the strategic importance of the General Data Protection Regulation for the data sovereignty of the European Union, the European Council should remind all Member States that they should not impede its immediate and direct application as of 25 May 2018, but equip the independent national data protection authorities with all the resources necessary to ensure a full and efficient application of the new legal framework equally and uniformly in all Member States. To ensure a fair level playing field as intended by the EU legislator, the Commission will start immediately after 25 May 2018 infringement procedures where Member States fail to fulfil their obligations under the General Data Protection Regulation.

The Commission calls on the European Parliament and the Council to accelerate its work and to conclude negotiations as soon as possible on the ePrivacy Regulation (proposed by the Commission in January 2017) and on the updated EU regulation on the protection of individuals with regard to the processing of personal data by the Union institutions, bodies, offices and agencies and on the free movement of such data.

3. Accelerating the completion of the Digital Single Market: finalising key proposals

Bringing down the Digital Single Market barriers within Europe could contribute an additional EUR 415 billion to European Gross Domestic Product.¹⁷ Since the launch of the Digital Single Market Strategy in 2015, the Commission has progressed and delivered proposals for all 29 initiatives which were identified as essential for a functional Digital Single Market.¹⁸ The benefits are already being enjoyed by citizens: with no extra mobile phone charges when **roaming**, the year to summer 2017 saw a four-fold increase in data use when travelling to other Member States.¹⁹ **Portability** means that citizens can now watch their favourite audiovisual content and sports events everywhere in the EU. Removing unfair **geo-blocking restrictions** will free consumers in their online shopping, and there will be more transparency and choice on **parcel delivery prices** for online purchases. Together with the new **Value Added Tax framework for e-commerce** and new **contract rules** both for online content and goods, a comprehensive e-commerce framework will be in place by the end of this Commission's mandate, reinforced by strong **consumer protection cooperation**. To ensure this progress, conclusion of negotiations on the **contract rules** proposals are key to allowing consumers to shop online with the confidence that the remedies for any malfunctioning digital content – such as downloaded music or software – are the same no matter where in the EU the purchase is made. Thanks to this improved legal framework, 122,000 more businesses are expected to start selling to consumers in other Member States, providing a EUR 4 million boost to the EU economy.

¹⁷ COM(2015) 192 of 6 May 2015.

¹⁸ See Annex.

¹⁹ International Roaming BEREC Benchmark Data Report, April 2017-September 2017.

The **cybersecurity** of data-based solutions is a key building block for user trust. The full implementation by all the Member States of the first EU-wide cybersecurity law, the Directive on the Security of Network and Information Systems,²⁰ is a first essential step to EU cyber resilience. With the main tools to combat cybersecurity today in national hands, this will help to drive standards higher, while the proposed cybersecurity certification framework²¹ will help to spread secure cyber solutions. Rapid agreement by the European Parliament and the Council would help to quickly roll out higher standards of resilience into products and underpin EU-wide consumer confidence in security by design. Cybersecurity must be underpinned by effective deterrence of criminal activities: swift adoption of an ambitious set of common minimum rules to combat fraud and counterfeiting of non-cash means of payment²² would be essential.

In September 2018, the requirements for **electronic identification** schemes will apply, guaranteeing the interoperability of public electronic identity and other secure services throughout the Union.²³ Together with a **Single Digital Gateway** for accessing information and procedures online, Member States will be able to offer a simpler environment for consumers and businesses when dealing with public administrations in the EU.

The European data economy also depends on high-quality connectivity for the provision of digital content to all corners of the EU, including through satellite communications. This is why agreement between the European Parliament and the Council is needed on the **Electronic Communications Code**, which will guarantee that by 2020, all EU Member States assign the frequencies necessary for the introduction of the next, fifth generation 5G networks.²⁴ It will create a stable regulatory framework for investments into high capacity networks. The upgrading of networks along main transport routes will be needed for the deployment of automated mobility services, and their roll-out in hospitals will be necessary for doctors to conduct remote consultations and surgeries.²⁵

In addition, agreement on the **copyright** proposals is crucial for European culture and identity to flourish in the digital age and to provide remuneration for creators when content is shared through online platforms.²⁶

The European Parliament and the Council now need to accelerate the work to conclude negotiations on all these proposals by the end of 2018 in order to complete the Digital Single Market for the benefit of European citizens.

4. The future of the Digital Single Market: the right environment for growth

Digitisation is key to the preservation and creation of future jobs in the EU. Currently only one out of five European businesses is highly digitised.²⁷ The huge benefits of the Digital

²⁰ Directive 2016/1148 of the European Parliament and of the Council of 6 July 2016 concerning measures for a high common level of security of network and information systems across the Union.

²¹ COM(2017) 477 of 13 September 2017.

²² COM(2017) 489 of 13 September 2017

²³ Regulation (EU) No 910/2014 on electronic identification and trust services for electronic transactions in the internal market (eIDAS).

²⁴ COM(2016) 590 of 14 September 2016.

²⁵ Communication on Connectivity for a Competitive Digital Single Market - Towards a European Gigabit Society, COM (2016) 587 of 14 September 2016; Communication on 5G for Europe: An Action Plan, COM (2016) 588 of 14 September 2016. Communication On the road to automated mobility: An EU strategy for mobility of the future;, COM(2018) 283 of 16 May 2018; Communication on digital health and care, COM(2018) 233 of 25 April 2018.

²⁶ COM (2016) 593 and COM (2016) 594 of 14 September 2016.

Single Market Strategy can only be realised if digitisation spreads across the EU economy. For this to happen, the EU has a key role to play in helping to put the right environment in place.

Social networks and digital platforms

Social networks and digital platforms base their business model in significant part on the data obtained from their users. They offer benefits to users, but some of their data use practices also raise serious questions and require continued vigilance.

The algorithms feeding news to social media users seem often to privilege sensationalist or advertised content and facilitate the targeting of information to specific user groups. This can make it easier to manipulate sections of public opinion, who increasingly avoid the alternative of high-quality and more trustworthy news sources and contribute to polarisation or even radicalisation of views. The result is to spread **disinformation**, with the impact at election time of particular importance. Moreover, laws on electoral advertising and campaign financing rules have become challenging to enforce online, which risks undermining electoral processes.

Recent elections or referenda in the U.S. and in the EU and the ‘Facebook/Cambridge Analytica’ revelations showed these techniques and practices in action. The Commission is taking action to improve content transparency and establish an EU fact-checking network, to help users to assess the credibility of the sources of news as well as their exposure to different sources of information, and will assess by the end of the year whether additional regulatory measures are needed.²⁸

The Commission also discussed best practices with Member State electoral authorities for the identification, mitigation and management of cyber and disinformation risks to the electoral process in preparation of the European Parliament elections in May 2019, and will invite further commitment from stakeholders to addressing these issues, notably at the next annual colloquium on fundamental rights in November 2018, which will be dedicated to democracy.

Europe is also acting to protect citizens from illegal content. The Commission Recommendation on **measures to effectively tackle illegal content online** recommends specific measures for platforms and Member States to improve the detection, removal and prevention of illegal content.²⁹ The Commission is collecting evidence on the effectiveness of the voluntary measures and the scale of the problem and will explore before the end of 2018 possible further measures to improve the effectiveness of combating illegal content online.

Digital platforms often act as online intermediaries for other businesses to reach consumers. They are very important means for reaching customers and their role is essential for the modern economy. To ensure a fair, predictable, sustainable and trusted online business environment, the Commission has proposed **transparency and redress obligations** for such digital platforms.³⁰ These measures would include obligations on platforms to inform business users of the criteria used to rank business users’ content, of upcoming changes to the terms

²⁷ European Commission Digital Scoreboard – 2017.

²⁸ Communication on Tackling online disinformation: a European Approach, COM(2018) 236 of 26 April 2018.

²⁹ C(2018) 1177 of 1 March 2018.

³⁰ For instance avoiding the delisting of companies without notice or clear reasons, having non-transparent data access conditions or giving their own consumer products better visibility than those provided by other businesses using online intermediation services.

and conditions, and of their use data stemming from intermediary services.³¹ The need for any further measures will continue to be assessed. Consideration of this proposal should be prioritised by the European Parliament and the Council.

The ranking transparency obligation complements a proposal made as part of the **New Deal for Consumers** to clearly identify to consumers any promoted search results based on payments, as well as a requirement to inform about the main parameters determining ranking on online marketplaces.³²

Investing in data, artificial intelligence and high performance computing

Connected digital technologies and data applications are at the heart of innovation in all sectors.³³ The EU's strong data protection rules, that apply both online and offline, provide the basis for a world-class regulatory regime for innovation that users can trust and that enables our industry to gain competitive advantages in the data-based global economy.

Data will nurture digital innovation provided that, in parallel, investments are made into the digital capacities necessary to process exponentially growing amounts of data. The recent **Data package** will unlock the power of public and scientific data and open up this data for re-use by European start-ups.³⁴ Allowing the re-use of data is essential for working with the big data analytics which will stimulate economic growth, help innovation and assist in addressing key societal challenges such as in healthcare or public transport. The data package also offers further guidance on sharing private data and will help to free up data key to innovation. For example, to develop new forms of personalised medicines, EU researchers need access to large numbers of human genome³⁵ and personal health records.³⁶

Data is the raw material for **Artificial Intelligence**, and algorithms are the mechanisms through which Artificial Intelligence applications use data and learn new tasks. Machine readability and common data formats are key for Artificial Intelligence applications to develop and self-organise data.³⁷ The Union's values, and the legal certainty provided for by the new data protection regime, help to ensure the right environment to develop machine learning techniques for Artificial Intelligence in the EU – one where algorithms and programmes learning from human behaviour take into account high standards of data protection and fundamental rights, rather than leaving such innovation to those working without such standards.³⁸ The Commission has presented a framework to allow Europe to maximise the benefits of Artificial Intelligence and has put forward an objective of annual investments by private and public players of at least EUR 20 billion annually between 2020

³¹ Regulation on promoting fairness and transparency for business users of online intermediation services, COM(2018) 238 of 26 April 2018.

³² COM(2018) 185 of 11 April 2018.

³³ COM(2018) 306 – A renewed European agenda for Research and Innovation – Europe's chance to shape its technological leadership.

³⁴ Communication 'Towards a common European data space', COM(2018) 232 of 25 April 2018 and the accompanying package.

³⁵ 14 Member States have signed the Declaration of Cooperation 'Towards access to at least 1 million sequenced genomes in the European Union by 2022': <https://ec.europa.eu/digital-single-market/en/news/eu-countries-will-cooperate-linking-genomic-databases-across-borders>.

³⁶ Communication on enabling the digital transformation of health and care in the Digital Single Market; empowering citizens and building a healthier society, COM(2018) 233 of 25 April 2018.

³⁷ By way of example, individuals have the right, under the General Data Protection Regulation, not to be subject to a decision which is based solely on automated processing and which produces legal effects concerning him or her or similarly significantly affects him or her. Certain exceptions apply.

³⁸ Actions in this regard are outlined in the Communication on Artificial Intelligence for Europe, COM(2018) 237 of 26 April 2018.

and 2030 to allow Europe to take full advantage of this key enabling technology.³⁹ The use of Artificial Intelligence alone is expected to boost the global economy by up to EUR 13 trillion by the end of the next decade; the EU needs to invest to be a leader in this growth.⁴⁰ In addition, data and services derived from **space systems**, including Earth observation data, geo-positioning information and satellite communications, can support AI approaches and help open up many business opportunities in all Member States.

The Commission has also tabled a proposal for a **High Performance Computing Joint Undertaking** to pool scarce resources and to procure the high performance computers that are necessary if we want to continue leading on research and innovation, in particular in the area of Artificial Intelligence and other big data applications.⁴¹ The instrument needs to be finally approved by Council in September 2018 for procurements to start from 1 January 2019. Any delay in adopting the proposal would result in international competitors gaining an advantage in bringing breakthrough innovations to the market.

Equally, the EU has important investment gaps in **skills** and **digital connectivity**, including to fully grasp the opportunities of the **Internet of Things**,⁴² which must be intensively tackled in the coming years. Under current investment trends, we have a EUR 155 billion combined public and private investment gap for reaching the agreed connectivity targets by 2025. There are also notable skills gaps and mismatches as around 40% of the workforce in Europe needs digital upskilling⁴³ and 70 million Europeans lack basic literacy and numeracy skills.⁴⁴ Also 40% of the companies trying to recruit digital specialists face difficulties in finding them (Information and Communications Technology professionals represent a shortage occupation in twenty four EU Member states). Further, the demand for Information and Communications Technology professionals is estimated to grow around 10% between 2015-2025, translating into some 400,000 new jobs.⁴⁵

In response to these investment needs, in its **Multiannual Financial Framework** proposal for 2021-2027, the Commission has strongly increased the ambition for supporting digital priorities at EU level by proposing the new Digital Europe Programme, as well as key contributions to the digital economy in areas like research and innovation and cohesion policy and the Connecting Europe Facility.⁴⁶ However, this additional effort from the EU budget needs to be matched by additional investments by Member States and incentivise the private sector, in order to ensure the much needed competitiveness of the European economy and the upskilling of the European work force.

With the 25 April 2018 package of proposals, the Commission delivered all the remaining Digital Single Market actions and presented a framework for the future of Artificial

³⁹ Communication on Artificial Intelligence for Europe, COM(2018) 237 of 26 April 2018.

⁴⁰ 14% of world Gross Domestic Product, Price Waterhouse Cooper report on Sizing the prize: What's the real value of AI, (2017).

⁴¹ COM(2018) 8 of 11 January 2018.

⁴² In this context, the Commission recently put forward an initiative related to Standard Essential patents providing a clearer framework to incentivize the development of key technologies. COM(2017) 712 of 29 November 2017.

⁴³ COM(2018) 306 – A renewed European agenda for Research and Innovation – Europe's chance to shape its technological leadership.

⁴⁴ Communication on a New Skills Agenda for Europe, COM(2016) 381 of 10 June 2016.

⁴⁵ Cedefop Skills Panorama (2016) Information and Communications Technology (ICT) professionals: skills opportunities and challenges.

⁴⁶ COM(2018) 321 of 2 May 2018 – A modern Budget for a Union that Protects, Empowers and Defends – the Multiannual Financial Framework for 2021-2027.

Intelligence. The Commission calls for endorsement of these actions and prioritisation of work in order to ensure swift adoptions of the corresponding legal acts.

5. Conclusion

Step by step, the Digital Single Market is spreading its benefits to citizens and businesses in the EU. An extra effort is necessary to conclude negotiations on the remaining pending proposals and meet the European Council goal of concluding the Digital Single Market Strategy by the end of 2018.

Already, the EU is well equipped with rules to deal effectively with the new data challenges, provided all actors work closely together in effectively implementing and applying the new tools to protect the rights to privacy and data protection of individuals, but also more broadly in order to safeguard the foundations of our democracies, based on free elections, freedom of expression and an open and varied debate where disinformation can be challenged.

In view of the strategic importance of the General Data Protection Regulation for the data sovereignty of the European Union, all Member States should facilitate its immediate and direct application as of 25 May 2018, including through all relevant measures. Negotiations on the ePrivacy Regulation and on the updated EU regulation on the protection of individuals with regard to the processing of personal data by the Union institutions, bodies, offices and agencies and on the free movement of such data should be concluded as soon as possible.

In managing the digital transformation, we should continue pursuing a genuinely European approach, based on our core values and on preventing a self-destructive race to the bottom. The regulatory environment must be designed to support individuals and creators in the online environment as much as they are in the offline environment. This is how the EU can become the global norm setter for personal data protection, cybersecurity, net neutrality, and fairness and responsibility in the platform economy. And it can become the leader in putting them into practice through trusted digital services and innovation.

However, having the regulatory framework in place will not by itself make the EU a leader in the digital economy. For that to happen European governments and businesses – large and small – need to invest into and exploit the vast opportunities provided by technologies like Artificial Intelligence and big data and to use the Digital Single Market as the launchpad for deploying competitive solutions for the global data economy.

The Commission invites Leaders to discuss and give strategic orientations on the above key political priorities with a view to completing the Digital Single Market before the end of this year and to ensuring a strong data protection on which a dynamic digital Europe can be built.

The Commission invites Leaders to discuss and give strategic orientation with a view to:

- 1. Putting in place with utmost urgency all the remaining steps necessary to prepare for the application of the General Data Protection Regulation in all Member States;*
- 2. Urging Council to swiftly agree on its negotiation position on the ePrivacy Regulation, which aims to ensure confidentiality of electronic communications, so that negotiations could start by June 2018, with a view to its adoption by the end of 2018;*
- 3. Ensuring that the Electronic Communications Code and the Regulation on free flow of non-personal data are agreed by co-legislators by June 2018, as well as all other pending*

Digital Single Market proposals by the end of 2018, in line with the call of the European Council of October 2017;

- 4. Mobilising the public and private investments necessary for businesses and the public sector to deploy Artificial Intelligence, cybersecurity measures, 5G connectivity networks, high performance computing and other new digital technologies, and fostering digital skills, which are essential to spur innovation and key to our future competitiveness in a data-based global economy.*



Brussels, 15.5.2018
COM(2018) 320 final

ANNEX

ANNEX

to the

**COMMUNICATION FROM THE COMMISSION TO THE EUROPEAN
PARLIAMENT, THE EUROPEAN COUNCIL, THE COUNCIL, THE EUROPEAN
ECONOMIC AND SOCIAL COMMITTEE AND THE COMMITTEE OF THE
REGIONS**

Completing a trusted Digital Single Market for all

**The European Commission's contribution to the Informal EU Leaders' meeting on data
protection and the Digital Single Market in Sofia on 16 May 2018**

ANNEX - Digital Single Market legislative initiatives 2015-2018

This Annex provides an overview of progress on the legislative initiatives delivered under the Digital Single Market Strategy.

<i>Nr</i>	<i>Legislative initiatives – Adopted</i>	<i>Proposed by Commission</i>	<i>State of publication in Official Journal of the European Union</i>
1	Decision on the use of the 470-790 MHz frequency band	2/2/2016	Published 25/5/2017
2	Regulation on cross-border portability of online content services	9/12/2015	Published 30/6/2017
3	Regulation as regards rules for wholesale roaming markets	15/6/2016	Published 9/6/2017
4	Regulation and Directive on permitted uses in copyright for print-disabled persons and implementing the Marrakesh Treaty	14/9/2016	Published 20/9/2017
5			
6	Regulation to promote Internet Connectivity in local communities (Wi-Fi4EU)	13/9/2016	Published 1/11/2017
7	Regulation on Consumer Protection Cooperation	25/5/2016	Published 27/12/2017
8	Regulation addressing unjustified geo-blocking	25/5/2016	Published 2/3/2018
9	Council Regulation and Directive on Value Added Tax for e-Commerce	1/12/2016	Agreed 13/12/2017; Awaiting publication
10			
11	Regulation on cross-border parcel delivery services	25/5/2016	Published 2/5/2018
12	Audio-Visual and Media Services Directive	25/5/2016	Political agreement 26/4/2018
<i>Nr</i>	<i>Legislative initiatives – Pending adoption</i>	<i>Proposed by Commission</i>	<i>State of negotiations between co-legislators</i>
1	Directive concerning contracts for the supply of digital content	9/12/2015	<i>Ongoing</i>
2	Directive concerning contracts for the distance sales of goods	31/10/2017 (9/12/2015)	<i>Awaiting Council mandate</i>
3	European Electronic Communications Code	14/9/2016	<i>Ongoing</i>
4	Body of European Regulators for Electronic Communications	14/9/2016	<i>Ongoing</i>
5	Directive on copyright in the Digital Single Market	14/9/2016	<i>Awaiting European Parliament and Council mandate</i>
6	Regulation on broadcasting organisations	14/9/2016	<i>Ongoing</i>
7	Council Directive on Value Added Tax for e-publications	1/12/2016	<i>Awaiting Council</i>
8	Regulation on ePrivacy	10/1/2017	<i>Awaiting Council</i>
9	Regulation on protection of personal data by the Union institutions and bodies	10/1/2017	<i>Ongoing</i>

10	Regulation establishing a Single Digital Gateway	2/5/2017	<i>Ongoing</i>
11	Regulation on a framework for free flow of non-personal data	13/9/2017	<i>Awaiting European Parliament</i>
12	Regulation on the EU Cybersecurity Act	13/9/2017	<i>Awaiting European Parliament and Council</i>
13	Directive on the combatting of fraud and counterfeiting of non-cash means of payment	13/9/2017	<i>Awaiting European Parliament</i>
14	Council Regulation establishing the European High-Performance Computing Joint Undertaking	11/1/2018	<i>Awaiting European Parliament and Council</i>
15	Regulation on promoting fairness and transparency for business users of online intermediation services	26/4/2018	
16	Directive on the re-use of public sector information (recast)	25/4/2018	
17	Regulation on the implementation and functioning of the .eu Top Level Domain name	27/4/2018	
29	Total number of legislative initiatives		