



*Power Breakfast*

***DIGITAL SINGLE MARKET  
Which legacy for the future?***

*Background document / Key Issues*

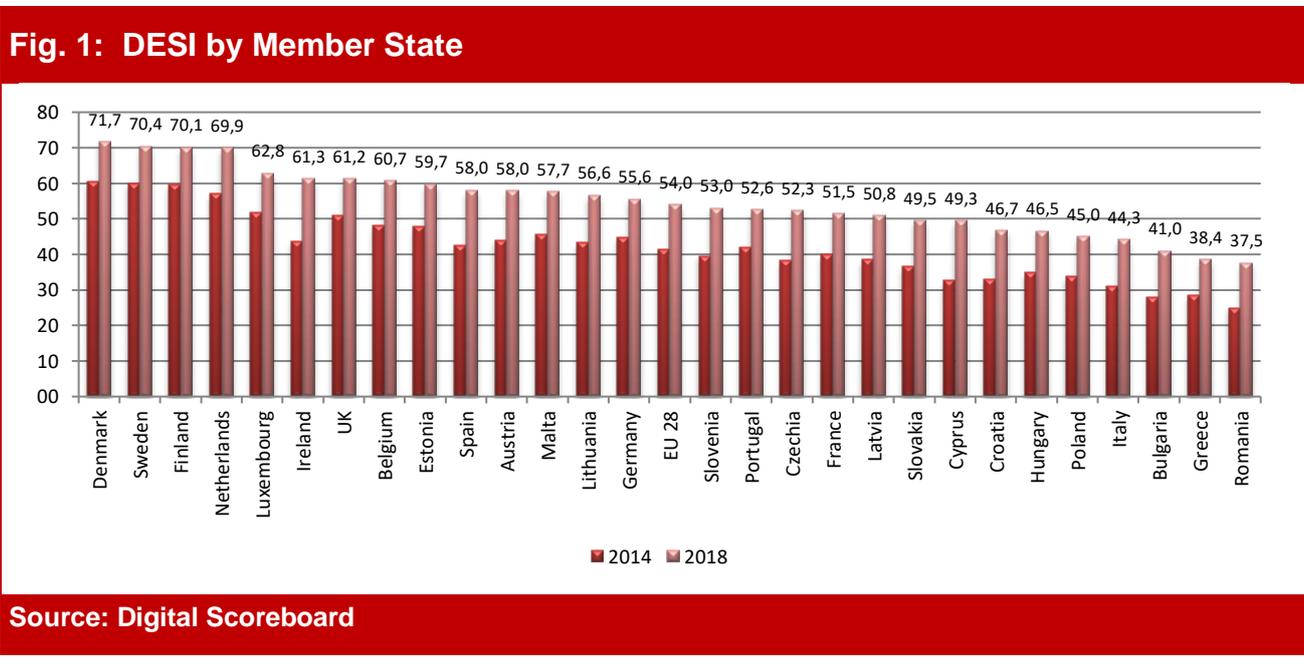
The Internet and digital technologies are transforming our world. The European Commission has identified that an efficiently functioning Digital Single Market could contribute €415 billion per year to our economy and create hundreds of thousands of new jobs. The Digital Single Market aims to open up digital opportunities for people and businesses and enhance Europe's position as a world leader in the digital economy. Connectivity targets for 2025 have been established to create a Gigabit Society and policies are being pursued to address the barriers and seize the opportunities for digital adoption and development in the EU28 Member States.

For this reason, it is important to assess the steps undertaken by the EU.

The European Commission has developed the Digital Economy and Society Index (DESI), a composite measure that examines Europe's digital performance and helps EU countries identify areas requiring priority investments and action in order to create a truly Digital Single Market.

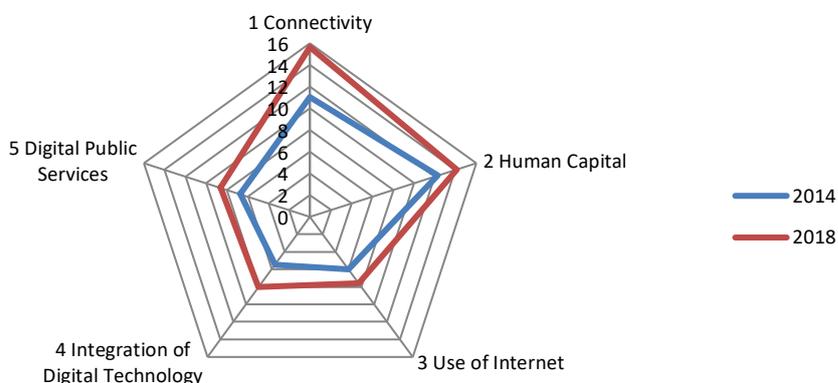
### 1. The Digital Single Market: an analysis within the EU

For the EU as a whole, the DESI score has increased by 12 points, from 42 to 52 (Fig. 1). An increase has been registered in all countries, with the Northern countries remaining at the forefront of the digital market, and the Eastern (Romania and Bulgaria) and Mediterranean (such as Greece and Italy) still lying at the bottom of the ranking. We can see a DESI score ranging from 37.5 for Romania to 71.7 for Denmark, that is a digital divide of 34.2 points, only slightly lower than the 35.3 point digital divide registered in 2014.



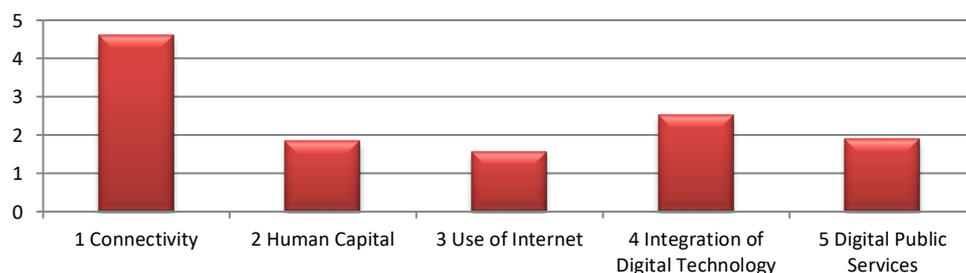
The highest score registered by the EU is in connectivity (Fig. 2), with the greatest progress occurring (Fig. 3) since 2014. This is followed by the integration of digital technology.

**Fig. 2: EU DESI by component**



**Source: Digital Scoreboard**

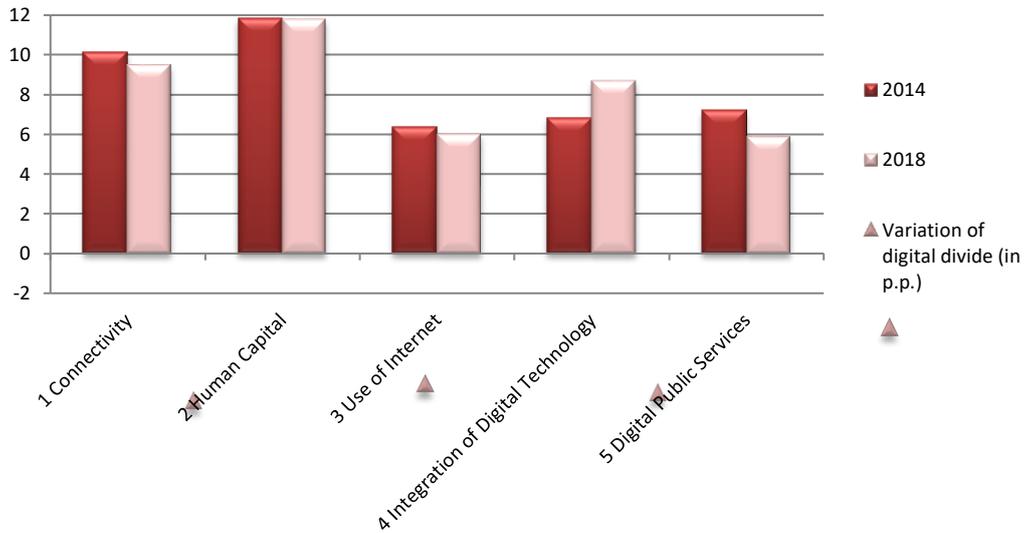
**Fig. 3: Variation 2014-2018 of EU DESI, by component**



**Source: I-Com elaboration on Digital Scoreboard data**

As already mentioned, the digital divide across EU Member States remains very wide, only slightly declining in the 4-year period. This is mainly due to the integration of digital technology (Fig. 4) which, though improving greatly, has seen the divide across countries widen. This means that only certain countries – typically, the best performing ones – improved in this respect, while those lagging behind tended to stagnate or struggle to catch up. Digital Public Services is the sector where the divide shrank the most.

**Fig. 4: EU digital divide by component**



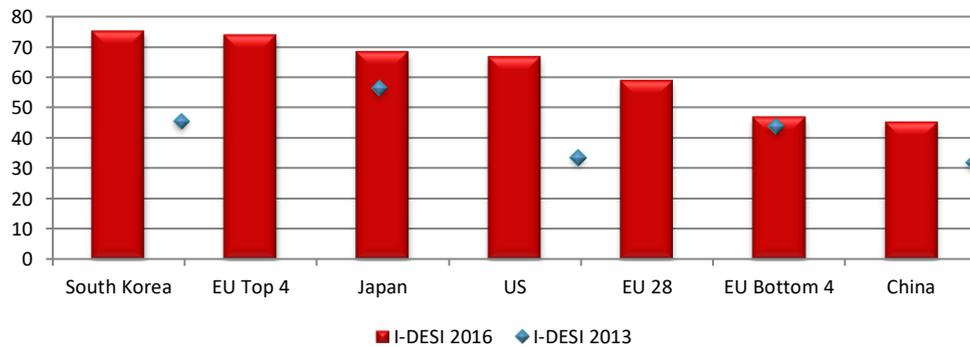
Source: I-Com elaboration on Digital Scoreboard data

## 2. The international context: a benchmark analysis between the EU and the rest of the world

In order to see a more global perspective, the European Commission drew up the International DESI (I-DESI), a composite measure allowing for comparing the EU with some major world economies (the US, South Korea, Japan and China).

South Korea is the most digitally developed economy (Fig. 5), whereas the EU as a whole – with a score of 58.9 – only performs better than China (45.3). Only the best performing EU countries keep up with South Korea, even if the wider gap of 2013 has been narrowed.

**Fig. 5: I-DESI**

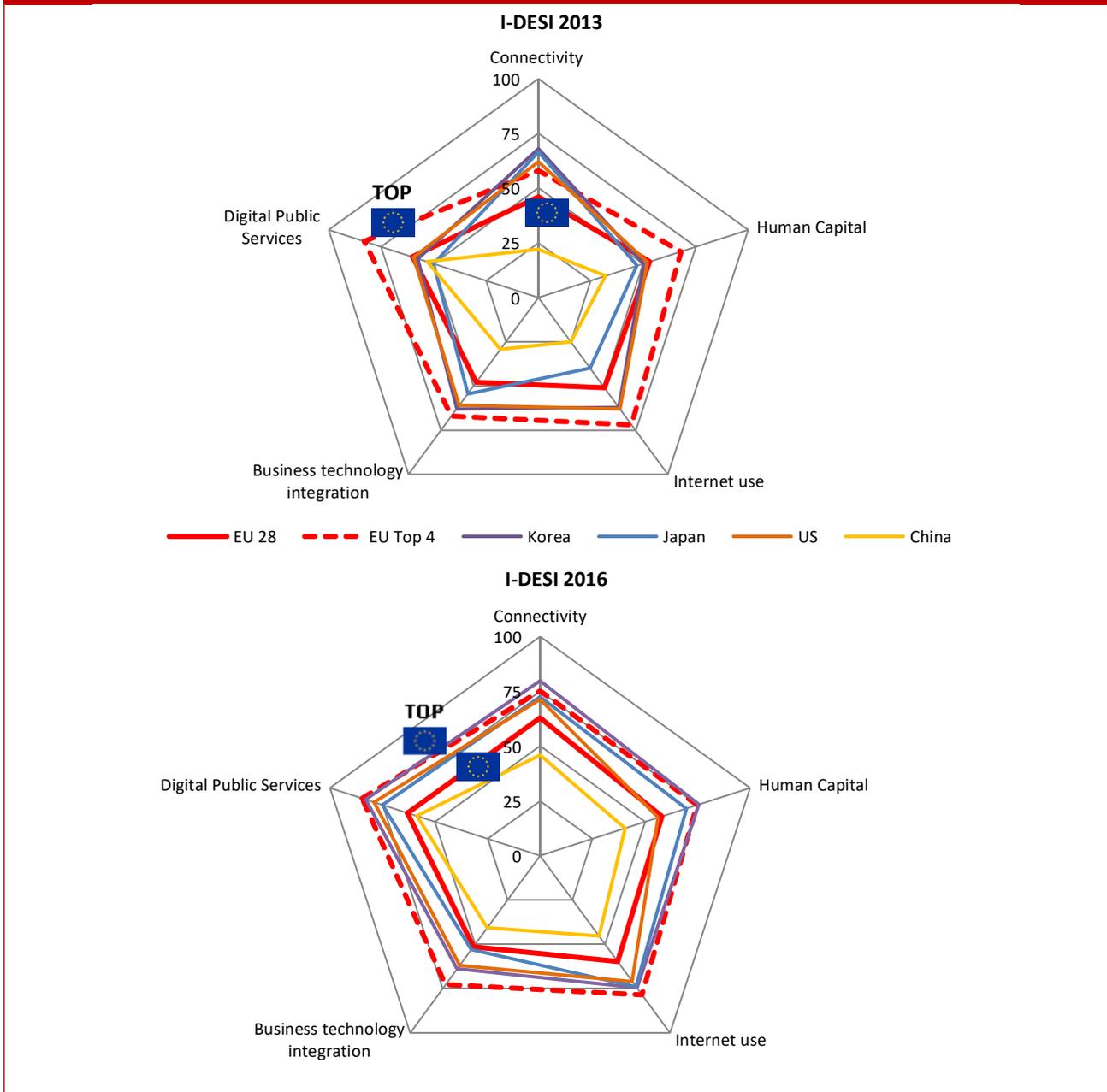


Source: Digital Scoreboard

Looking at the single components of the index (Fig. 6), the EU improved in all in the 3-year period. The largest increase occurred in connectivity (+16.9), followed by Internet usage (+8.7). Less progress was made in digital public services and business technology integration. However, though moving forward, the EU continues to lag behind the major

global economies in all of the components. On the contrary, China, that was way behind in 2013, seems to be catching up quite rapidly.

**Fig. 6: I-DESI by component (2013 vs. 2016)**

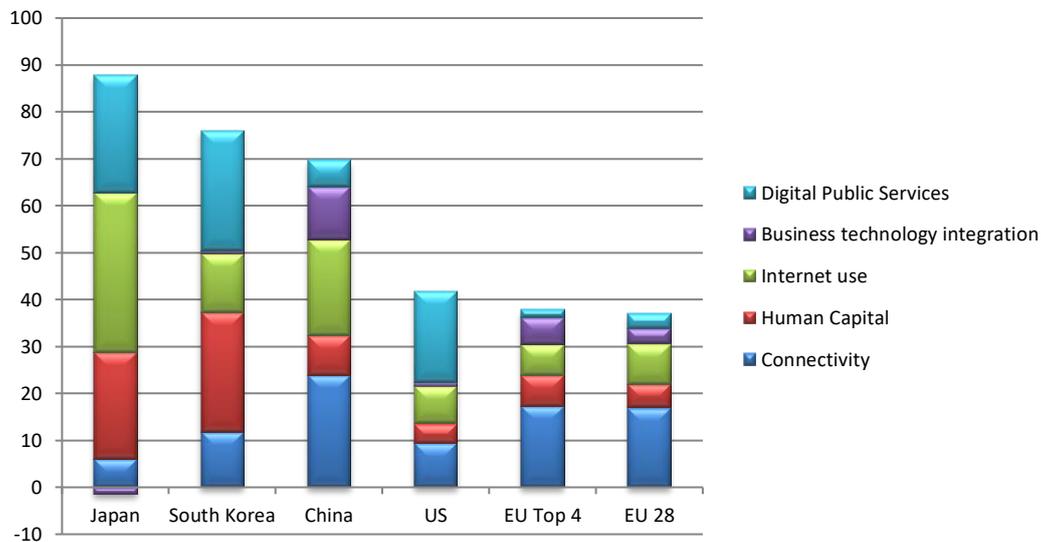


**Source: Digital Scoreboard**

China is one of the countries with the most important variation over time (Fig. 7). However, Japan and South Korea, already the most developed in 2013, are those registering the most progress, especially in digital public services and human capital, the components where the EU only made a small improvement.

In general, faster progress can be noted in the Eastern economies. However, the EU is the least improving economy with the top 4 EU countries not performing much better. Yet, it is more or less at the same level as US performance, showing the slow-paced trend of the major Western major economies compared to their Eastern counterparts.

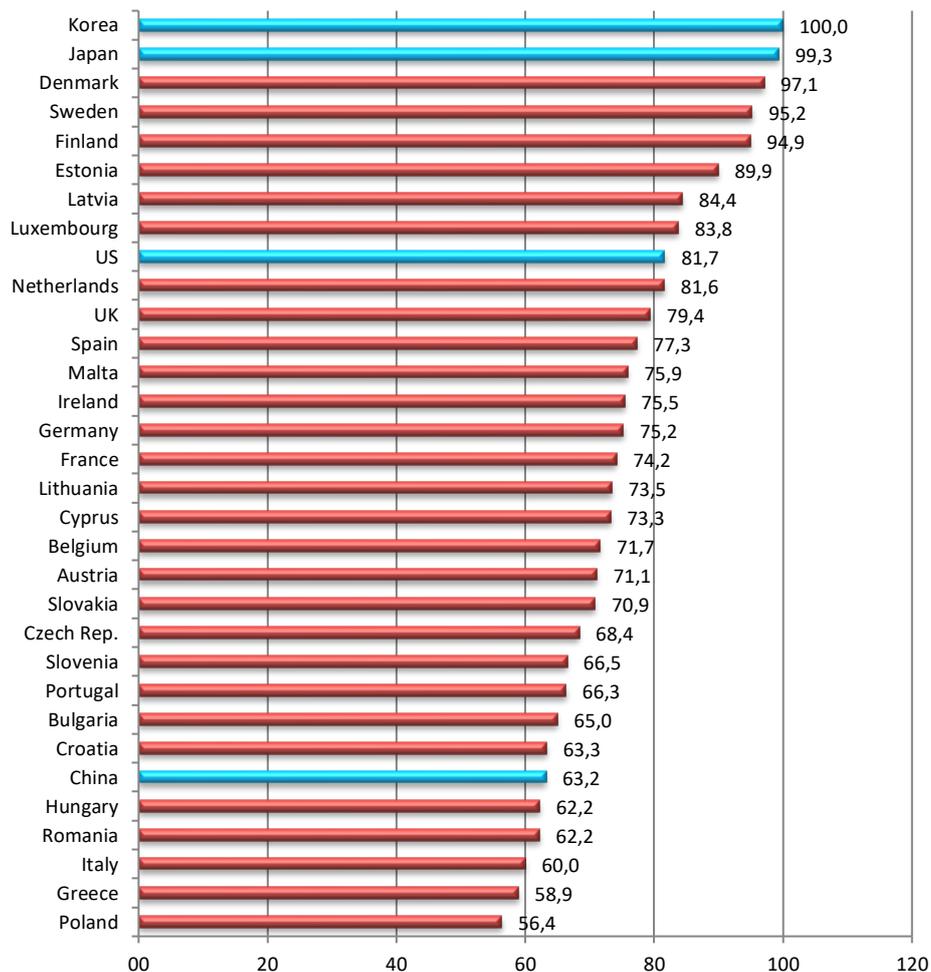
**Fig. 7: Variation in I-DESI score between 2013 and 2016, by country and component**



**Source: I-Com elaboration on Digital Scoreboard data**

In addition, we created an index summarizing the connectivity take-up based on some basic indicators - Internet users, broadband subscriptions (both fixed and mobile) and fiber Internet subscriptions. The index is computed as the mean of the three variables (Fig. 8). Korea and Japan are ahead, but Northern European countries – Denmark, Sweden and Finland - immediately follow. Denmark stands out for its share of Internet users and fixed broadband subscriptions (97% and 43%, respectively). Where mobile broadband is concerned, Finland is the top country with 154 subscriptions per 100 inhabitants; whereas Sweden performs well for fiber connection take-up (21% of population), the best European performer, though lagging behind Korea and Japan. Overall, these 3 countries, together with Estonia, Latvia and Luxembourg, do better than the US. On the other hand, China ranks among the lowest positions. Despite the relatively high share of people with a fiber Internet subscription, only slightly more than one in two people in China use the Internet - thus ranking last - and with only 27% of the population subscribed to a fixed broadband contract. In total, China's score is 63.2. At the bottom of the ranking, below China, we have 5 European countries - Hungary, Romania, Italy, Greece and Poland. Hungary, Romania and Poland especially lag behind in broadband, with Italy and Greece behind in Internet usage and fiber connections.

**Fig. 8: I-Com index on connectivity take-up**



Source: I-Com elaboration on World Economic Forum data

### 3. Police packages for an efficient and competitive Digital Single Market

On 6 May 2015, the European Commission adopted the Digital Single Market strategy. The strategy is built on three pillars, including 16 specific initiatives: 1) **access** - better access for consumers and businesses to digital goods and services across Europe; 2) **environment** - creating the right conditions and a level playing field for digital networks and innovative services to flourish; 3) **economy & society** - maximizing the growth potential of the digital economy.

In the years since the adoption of the strategy, the Commission has made proposals on all the 16 key measures identified. In the following sections some of the most important initiatives will be briefly analyzed.

#### **E-commerce**

The first pillar, specifically, includes initiatives to encourage the development of e-commerce with the boosting of cross-border ecommerce as one of the main objectives of the Digital Single Market.

On this topic, the Commission launched several initiatives. The Communication “*A comprehensive approach to stimulating cross-border e-Commerce for Europe's citizens and businesses*” (25.05.2016) presented a package of measures containing four key DSM proposals to boost the potential for cross-border e-commerce in Europe. They are: 1) a legislative proposal on addressing unjustified **geo-blocking** and other forms of discrimination based on nationality, place of residence or place of establishment within the Single Market; 2) a legislative proposal revising the Regulation on **Consumer Protection Cooperation**; 3) a legislative proposal (Regulation) proposing measures in the area of **parcel delivery**; and 4) a guidance on the implementation/application of the Directive on **Unfair Commercial Practices**.

On 28 February 2018, the **Regulation (EU) 2018/302 addressing unjustified geo-blocking and other forms of discrimination based on a customer's nationality, place of residence or place of establishment within the internal market**, and amending Regulations (EC) No 2006/2004 and (EU) 2017/2394 and Directive 2009/22/EC, was adopted (taking effect from 3 December 2018). It aims to prevent discrimination on the above in cross-border transactions between a trader and a customer relating to the sales of goods and the provision of services within the Union.

To achieve these goals, the regulation prohibits traders to block or limit, through the use of technological measures or otherwise, a customer's access to the trader's online interface for reasons related to the customer's nationality, place of residence or place of establishment (art. 3). The same disposition introduces an exception when the blocking or limitation of access, or the redirection is necessary in order to ensure compliance with a legal requirement laid down by Union law, or by a Member State's laws in accordance with Union law. To ensure compliance with the Regulation, Member States have the power to designate a body or bodies responsible for its adequate and effective enforcement and provide practical assistance to consumers in the case of a dispute between a consumer and a trader arising from the application of this Regulation.

Art. 9 establishes a review clause providing that by 23 March 2020 and every five years thereafter, the Commission shall report on the evaluation of this Regulation to the European Parliament, the Council and the European Economic and Social Committee.

To contribute to fostering growth through the creation of a true Digital Single Market, to the benefit of both consumers and businesses, by eliminating the key contract laws related to barriers hindering cross-border trade, on 9 December 2015, the Commission adopted a **proposal for a Directive of the European Parliament and of the Council on certain aspects concerning contracts for the supply of digital content, and a proposal for a Directive of the European Parliament and of the Council on certain aspects concerning contracts for the online and other distance sales of goods**.

The first, specifically aims to fully harmonize a set of key rules concerning contracts for the supply of digital content setting rules on digital content conformity, remedies available to consumers in cases of lack of conformity of digital content with the contract, as well as certain aspects concerning the right to terminate a long-term contract and the modification of the digital content. This Directive covers the supply of all types of digital content, and not only that supplied for a monetary payment but also in exchange for (personal and other) data provided by consumers, except where the data have been collected for the sole purpose of meeting legal requirements. It lists the remedies available to the consumer in the

case of any failure to supply or lack of conformity of the digital content and establishes the conditions under which the consumer has a right to terminate contracts concluded for an indeterminate duration or for a duration exceeding 12 months and thereby is able to switch provider. The procedure is ongoing (discussions within the Council or its preparatory bodies).

The second, instead, lays down certain requirements concerning distance sales contracts concluded between the seller and the consumer, in particular, rules on conformity of goods, remedies in case of non-conformity and the modalities for the exercising of those remedies (the Directive does not apply to distance contracts for the provision of services).

It prescribes conformity of the goods with the contract also defining requirements establishing that the goods shall be fit for all the purposes for which goods of the same description would ordinarily be used, be delivered along with such accessories. This includes packaging, installation instructions or other instructions as the consumer may expect to receive, and possess the qualities and performance normal in goods of the same type, and which the consumer may expect, given the nature of the goods and taking into account any public statement made by, or on behalf of, the seller or other persons along the supply chain, including the producer. The proposal identifies consumer recourse for lack of contract conformity and the right to obtain a proportionate reduction in the price. The consumer can also choose between repair and replacement unless the option chosen would be impossible, unlawful or, compared to the other options, would impose costs on the seller that would be disproportionate, and can exercise the right to terminate the contract by notice to the seller given by any means. An amended proposal was adopted by the Commission but the procedure is ongoing (discussions within the Council or its preparatory bodies).

**Regulation (EC) 2006/2004 on consumer protection cooperation** (the CPC Regulation) lays down a cooperation framework enabling national authorities from all countries in the EEA to jointly address breaches of Union laws protecting consumer interests in cases where the trader and the consumer are based in different countries. The CPC Regulation links national competent authorities to form a European enforcement network called the “CPC Network”. In each country, a single liaison office is responsible for coordinating the relevant national authorities which cooperate on consumer rules on unfair commercial practices, e-commerce, comparative advertising, package holidays, online selling and passenger rights. On 25 May 2016, to improve the existing mechanism for cooperation between national consumer protection cooperation authorities, the Commission put forward a proposal for the reform of the Consumer Protection Cooperation Regulation and the replacing of the CPC Regulation by a new regulation.

After fruitful negotiations among the co-legislators, the new CPC Regulation (**Regulation (EU) 2017/2394**) was finally adopted and published in the EU Official Journal on 27 December 2017. The Regulation entered into force on 17 January 2018, being applicable from 17 January 2020.

This Regulation sets out a number of improvements that will enable EU consumer protection laws to be better enforced. It provides enforcement authorities with additional powers, setting minimum powers for the competent authorities, that are investigation and enforcement powers. It also identifies the exercise of minimum powers: a) directly by competent authorities under their own authority; b) where appropriate, by recourse to other competent authorities or other public authorities; c) by instructing designated bodies, if

applicable; or (d) by application to courts competent to grant the necessary decision, including, where appropriate, by appeal, if the application to grant the necessary decision is not successful. It also establishes the mutual assistance mechanism, disciplining requests for information and for enforcement measures, the procedure for requests for mutual assistance and particular cases excusing a refusal to comply with a request for mutual assistance. The same Regulation establishes the general principles of cooperation when there is a reasonable suspicion that a widespread infringement or widespread infringement on a Union level is occurring, the launch of a coordinated action and designation of the coordinator. The Regulation also identifies a clearer role of the Commission playing a role of coordinator of the relevant coordinated measures, asking national authorities to jointly investigate bad business practices and address them more efficiently.

A new EU-wide market alert system has been introduced combining the mechanism that already existed under the old CPC Regulation with a wider exchange of relevant and necessary information. As an additional novelty, certain external bodies (such as consumer and trade associations) will also be able to send alerts. Member States will be required to exchange information on their enforcement priorities every 2 years and the Commission will produce an overview of this information making it publicly available.

Concerning measures in the area of parcel delivery, **Regulation (EU) 2018/644 on cross-border parcel delivery services** was adopted on 18 April 2018, entering into force on 22 May 2018. It considers that the tariffs applicable to cross-border parcels and other postal items for low volume senders, particularly for SMEs and individuals, are still relatively high having a direct negative impact on users seeking cross-border parcel delivery services, especially in the context of e-commerce. Art. 1 identifies the subject matter and objectives concerning: a) regulatory controls for parcel delivery services; b) transparency of tariffs, and assessment of tariffs for certain cross-border parcel delivery services for the purpose of identifying those that are unreasonably high; and c) information for consumers made available by traders concerning cross-border parcel delivery services.

The Regulation provides minimum requirements allowing any Member State to maintain or introduce additional necessary and proportionate measures in order to achieve better cross-border parcel delivery services, provided that those measures are compatible with Union law. It sets out information obligations on parcel delivery service providers towards national regulatory authorities and also information obligations to consumers. To evaluate if tariffs are unreasonably high, the national regulatory authority shall take into account the domestic and any other relevant tariffs of the comparable parcel delivery services, any application of a uniform tariff to two or more Member States, bilateral volumes, specific transportation or handling costs, other relevant costs and service quality standards and the likely impact of the applicable cross-border tariffs on individual and SME users.

By 23 May 2020, and thereafter every three years, the Commission shall submit to the European Parliament, the Council and the European Economic and Social Committee an evaluation report on the application and implementation of this Regulation, accompanied, where necessary, by a legislative proposal for its review.

In 2017, the European Commission carried out a thorough analysis of existing regulations which showed that the current EU rules were not being applied and enforced effectively across all countries. For this purpose, on **11 April 2018**, the European Commission launched a **New Deal for Consumers** to ensure that all European consumers fully benefit

from their rights under Union law. In particular, the New Deal will empower qualified entities to submit representative actions on behalf of consumers, introduce stronger sanctioning powers for Member State consumer authorities and also extend consumer protection. The Commission Communication identifies several aims: 1) to modernize existing rules and fill the gaps in the current consumer acquis; 2) to provide better redress opportunities for consumers, support effective enforcement and greater cooperation of public authorities; 3) to increase cooperation with partner countries outside the EU; 4) to ensure equal treatment of consumers in the Single Market and guarantee that national competent authorities are empowered to tackle any problems with 'dual quality' of consumer products; 5) to raise the awareness and strengthen the capacity-building of consumers and traders; and 6) to look at future challenges for consumer policy in a fast evolving economic and technological environment. To achieve the above, this Communication is accompanied by two different proposals. The first, to amend the Council Directive on unfair terms in consumer contracts, the Directive on consumer protection in the indication of the prices of products offered to consumers, the Directive concerning unfair business-to-consumer commercial practices and the Directive on consumer rights, to ensure better enforcement and to modernise EU consumer protection rules, in particular in light of digital developments. The second concerns representative actions for the protection of the collective interests of consumers and repealing the Injunctions Directive 2009/22/EC aimed at improving tools for stopping illegal practices and facilitating redress for consumers where many of them are victims of the same infringement of their rights in mass harm situations.

The first proposal aims to amend four EU Directives that protect the economic interests of consumers. Most of the amendments concern the Unfair Commercial Practices Directive 2005/29/EC<sup>1</sup> and the Consumer Rights Directive 2011/83/EU<sup>2</sup>. For the other two Directives – the Unfair Contract Terms Directive 93/13/EEC<sup>3</sup> and the Price Indication Directive 98/6/EC<sup>4</sup> – only the penalties are amended to ensure greater harmonization and a more consistent application of the rules. Specifically, the proposal prescribes that the penalties provided by Member States (to be communicated to the Commission) must be effective, proportionate and dissuasive and sets out general criteria to be observed by the administrative authorities or courts. Specifically, this involves the nature, gravity and duration or temporal effects of the infringement, the number of consumers affected, including those in other Member States, any action taken by the trader to mitigate or remedy the damage suffered by consumers, where appropriate, the intentional or negligent character of the infringement, any previous infringements by the trader, the financial benefits gained or losses avoided by the trader due to the infringement and any other aggravating or mitigating factor applicable to the circumstances of the case. In the event of the imposition of a fine, annual turnover and net profits must be taken into account in the determination of the amount (the maximum amount shall be at least 4% of the trader's annual turnover in the Member State or Member States concerned).

The second proposal introduces a representative action to ensure an effective and efficient protection of the collective interests of consumers and overcomes the obstacles faced by consumers within individual actions (such as uncertainty regarding their rights and available procedural mechanisms, psychological reluctance to take action and the negative balance of the expected costs and benefits of individual action). The procedure of adoption of these proposals is ongoing.

## **Copyright and Sat-Cab Directive**

Within the “Access” Pillar, topics that are more strictly related to contents are Copyright and the Sat-Cab Directive.

The legislation in force is still Directive 2001/29/EC, with subsequent enforcement (Directive 2004/48/EC on the enforcement of intellectual property rights) and modifications such as on rental and lending rights (Directive 2006/115/EC), on the legal protection of computer programs (Directive 2009/24/EC), on certain permitted uses of orphan works (Directive 2012/28/EU), and on collective management of copyright and related rights and multi-territorial licensing in online musical works (“CRM” Directive 2014/26/EU). Moreover, on 1 October 2018, the EU ratified the Marrakesh Treaty, effectively becoming a party to it as of 1 January 2019. A Directive and a Regulation were adopted in 2017 for the implementation of the treaty in EU law. The first focuses on certain permitted uses of certain works and other subject matter protected by copyright and related rights for the benefit of persons who are visually impaired or otherwise print-disabled (September 2017), while the regulation is focused on the cross-border exchange between the Union and third countries of accessible format copies of certain works and other subject matter protected by copyright for the benefit of “print-disabled”<sup>1</sup> persons.

A new Copyright Directive was proposed by the European Commission in September 2016 as part of the Digital Single Market strategy. On 12 September 2018, the European Parliament adopted its negotiating position, focusing on three main objectives: 1) increasing cross-border access for citizens to copyright-protected content online; 2) giving wider opportunities to use copyrighted material for education, research, cultural heritage and disability; and 3) stimulating creation of high-quality content by introducing clearer rules for a functioning copyright marketplace.

The current debate has slowed down on Article 11 and 13. The former could push publishers to pay for displaying news snippets. However, after snippet taxes were introduced in Spain and Germany in the past, publishers reported plunging traffic on their sites. Article 13 would require online sharing platforms to install filters to prevent users from uploading copyrighted materials.

On February 13, the European Parliament, the Council of the EU and the Commission found a political agreement on an agreed text that must now be formally confirmed by the European Parliament and the Council, before the EP elections taking place in May.

Another goal of the Digital Single Market strategy was to review the Satellite and Cable Directive (93/83/EEC) by assessing if it should include also broadcasters' online transmissions and further measures to improve cross-border access to them within Europe. The new Sat-Cab Directive is also part of the copyright package. The proposed regulation of this topic was based on a retrospective evaluation of the existing Directive, a study and a public consultation. Key topics are the application of the country of origin principle to some online transmissions of broadcasting organizations, and the collective management of rights to retransmissions by means equivalent to cable. Another goal is allowing for a wider access

---

<sup>1</sup> Regulation on the cross-border exchange between the Union and third countries of accessible format copies of certain works and other subject matter protected by copyright and related rights for the benefit of persons who are visually impaired or otherwise print-disabled (Regulation implementing the Marrakech Treaty in the EU), 13 September 2017.

to online contents, in particular those coming from broadcasters, across Europe. EU institutions reached an agreement on the Sat-Cab directive last December. The country of origin principle should enable licensing of rights for program that broadcasters want to offer via their online services (catch-up as well as linear and other on demand services). The content portability will be less extensive than that originally proposed by the Commission and a new mechanism should facilitate the licensing of rights in the case of retransmission of radio and TV program.

### ***European Electronic Communications Code***

In December 2018, the **European Electronic Communications Code** was approved and entered into force. It is an important initiative to guarantee fixed and mobile connectivity for everyone, that is considered key for a competitive economy and an inclusive society. The Code provides incentives for fiber investments for wholesale only operators and incentives for co-investment in fiber networks. There are also new opportunities for national regulators to access civil and core infrastructure elements and longer market review periods for ex-ante regulatory decisions (five years instead of three) to provide greater certainty to operators. At the same time, it will be possible to regulate two dominant network operators on the same market and the EU Commission reserves the right to set the same rate of voice termination for the whole EU. For the first time a ceiling of 19 cents per minute is established for calls and 6 cents for a text message (these rates will be effective from May 15, 2019).

Regarding spectrum management, the Code provides twenty-year licenses and prescribes that 700 MHz (release expected for mobile operators by 2020-22), 3.5 GHz and 26 GHz (release by the end of 2020) will be used for 5G uses allowing each country to set terms and conditions for auctions and licenses. For consumer protection, it is extended to Over, the top part of the regulation that today concerns telecom services. In particular, the Code identifies three types of electronic communication services to be regulated - internet access services (ISPs), interpersonal communication services (also covers the OCs) and the spreading of signals (as in TV or M2M services). The Ott will have to inform customers about the quality of the service offered, just like a telco, and compensation if the service provided does not correspond to that guaranteed. It also introduces the right to keep one's phone number up to one month after termination of the contract and the right to reimbursement of the prepaid credit not used at the time of contract termination, as well as compensation in case of delay or abuse in switching to another operator. The Code introduces another important news - in case of serious emergency or catastrophe, the citizens affected will be notified by text message or mobile applications with the system called 'reverse 112' (Member States will have three and a half years to put the system into operation after the directive's entry into force). Berec will play a key role in helping European countries implement high-capacity networks and will contribute to the smooth and homogeneous application of the measures envisaged by the Code in Europe. Member States will have two years to adopt the necessary provisions for the transposition of the directive.

### ***5G and telecom rules***

The fundamental step was constituted by the Communication "5G for Europe: an Action Plan" (published in September 2016 together with the working document "5G Global Developments") which identifies 8 actions to encourage development. They were mainly

focused on asking Member States to identify 5G pioneer frequencies, adopting national roadmaps, promoting trials, making a global standard available and identifying a city to achieve full 5G by 2020.

The “Gigabit Society” Communication added three new goals related to connectivity by 2025 - 100 Mbps connection for families, even in rural areas; up to 1 Gbps in schools, universities, hospitals; and 5G coverage of urban areas and of the main roads and railways.

The 5G roadmap, signed in December 2017, clarifies timing and deadlines of specific goals:

- harmonization of 3.4-3.8 GHz and 24.25-27.5 GHz bands by 2019
- the provision of a 5G service in at least 1 city in every Member State (2020)
- 700 MHz band allocation in most Member States by 2020 and in all of them by 2022
- 5G infrastructure roll-out by 2025.

According to the 5G Observatory report by Idate, the implementation is resulting in positive and less positive outcomes. Nine countries published precise national 5G roadmaps - Austria, Finland, France, Germany, Luxembourg, Spain, Sweden, The Netherlands and the UK - while thirteen EU MSs have published national 5G roadmaps or global strategy documents.

On the contrary, the Czech Republic., Estonia, Greece, Hungary, Ireland, Latvia and Lithuania did not publish any official documentation on 5G and are still at the internal reflecting phase.

In the middle, four countries have lately launched new public consultations on 5G spectrum (Bulgaria, France, Lithuania and Romania) while three (Croatia, Finland and Slovenia) did not publish a 5G roadmap, but awarded trial licenses or organized round tables. At present, spectrum has been assigned and will be usable in 2020 in 8 Member States.

### ***Audiovisual media framework***

The Commission proposed a revised Audiovisual Media Services Directive in May 2016 that included a new approach to online platforms disseminating audiovisual content. Adopted last November, it includes a strengthened Country of Origin Principle, with certain audiovisual rules extended to video sharing platforms; better protection of minors; reinforced protection on TV and video on demand against incitement to violence or hatred and public provocation to commit terrorist offences; increased obligations to promote European works for on-demand services; more flexibility in television advertising; strengthened provisions to protect children from inappropriate audiovisual commercial communications for foods; and the independence of audiovisual regulators.

### ***Online platforms and illegal content***

The European Commission has drafted various proposals to foster an environment in which online platforms thrive, where consumers are protected whilst competition is enhanced.

The 2016 Communication “Online Platforms and the Digital Single Market - Opportunities and Challenges for Europe”, identifies 4 guiding policy principles:

1. a level playing field for comparable digital services;
2. ensuring that online platforms behave responsibly to protect core values;
3. fostering trust, transparency and ensuring fairness;
4. keeping markets open and non-discriminatory to foster a data-driven economy.

Recently, the European Commission has developed other proposals and recommendations to ensure transparency and consumer protection in online platforms.

A Recommendation on measures to tackle illegal content online (March 2018) enhances and underlines the political commitment of the preceding Communication "tackling illegal content online, towards enhanced responsibility of online platforms", adopted in September 2017.

Moreover, in April 2018 the Commission proposed an EU Regulation on promoting fairness and transparency for business users of online intermediation services trading together with the creation of an Observatory on the online platform economy. This initiative delivers on the commitment made in President Juncker's 2017 State of the Union address to safeguard a fair, predictable, sustainable and trusted business environment in the online economy. By adopting a harmonized framework for minimum transparency and redressing rights, it should protect companies that depend on online platforms for reaching consumers, while crucially safeguarding platform innovation potential. The present proposal aims at ensuring a fair, predictable, sustainable and trusted legal environment for business users, corporate website users, providers of online intermediation services and online search engines alike. This will limit the frequency and impact of harmful platform-to-business trading practices occurring in certain online activities, thereby safeguarding trust in the online platform economy and preventing further legal fragmentation of the Digital Single Market. The choice of a Regulation will facilitate the scaling-up of providers to the benefit of all actors in online intermediated services, as common rules applicable throughout the Union will inherently lower compliance costs and improve legal certainty, particularly for cross-border operations.

### ***Data protection***

Privacy regulation is instrumental in fostering consumer trust in the digital society. In early 2016, the EU reformed the legal framework on data protection and issued the **General Data Protection Regulation (GDPR)** - Regulation 679/16 - entering into force on 25 May 2018, in order to protect all EU citizens from privacy and data breaches in an increasingly data-driven world, vastly different to when the 1995 Directive was presented.

The GDPR sets the foundations for the lawfulness of data processing, clearly indicates times, contents and modalities of information, defines the rights of the interested parties (access, cancellation-forgetting, limitation of treatment, opposition, portability), identifies the subjective characteristics and responsibilities of owners and data controllers and regulates international data transfers.

The key-principle of the discipline is "privacy by design", by which we refer to the choice of guaranteeing data protection rights from the planning and design stage of a treatment preventing possible critical issues (for example, the provision of impact assessments before data processing).

The GDPR establishes the right to erasure ("right to be forgotten"), setting the right of the data subject to obtain from the controller the erasure of personal data concerning them without undue delay and the obligation - in the presence of specific conditions - of the controller to erase personal data without undue delay.

Other important provisions concern the right to data portability and the right of the data subject to receive the personal data in a structured, commonly used and machine-readable format with the right to transmit said data to another controller.

Regarding the controller and the processor, the GDPR establishes features of their responsibility, sets the obligation to implement appropriate technical and organizational measures to ensure a level of security appropriate to the risk, and encourages the drawing up of codes of conduct intended to contribute to the proper application of the Regulation. The same Regulation defines competences, tasks and the powers of authorities, cooperation modality and the characteristics and powers of a European Data Protection Board.

Considering that this regulation required Regulation (EC) 45/2001 to be adapted to the new principles and rules in order to provide a solid and consistent data protection framework in the Union, on 23 October 2018, **Regulation 2018/1725 was adopted by the European Parliament and the Council. This regards the protection of natural persons in the processing of personal data by Union institutions, bodies, offices and agencies and on the free movement of such data, and repealing Regulation (EC) No 45/2001 and Decision No 1247/2002/EC** (it will apply to the processing of personal data by Eurojust from 12 December 2019).

Conforming to the model and the general discipline established by Regulation 2016/679, the regulation identifies the principles applicable to the processing of personal data (lawfulness, correctness, transparency, adequacy, relevance, limitation) and the conditions for consent, regulating the transmission of personal data to recipients, other than Union institutions and agencies, established in the Union and subject to Regulation (EU) 2016/679 or Directive (EU) 2016/680. It identifies the situations in which the processing does not require identification, clearly declines the rights of the data subject (right of access to data, rectification, oblivion, right to limit processing, data portability, objection to processing), obligations and responsibilities, and it introduces, with regard to transfers of personal data to third countries or international organizations, the principle of adequacy and provides specific means of appeal. From an institutional point of view, the regulation establishes a European Data Protection Supervisor, setting tasks and powers and the forms of cooperation with the individual national authorities.

The regulation sets the right to compensation, prescribing that any person who has suffered material or non-material damage as a result of an infringement of this Regulation shall have the right to receive compensation from the Union institution or body for the damage suffered. It also fixes principles relating to the processing of operational personal data, lawfulness of processing operational personal data, distinction between different categories of data subjects, distinction between operational personal data and verification of the quality of operational personal data, with specific processing conditions being set down. The same regulation bans a decision based solely on automated processing, including profiling, which produces an adverse legal effect concerning the data subject or significantly affects them, being prohibited unless authorized by Union law to which the controller is subject and which provides appropriate safeguards for the rights and freedoms of the data subject, and at least the right to obtain human intervention on the part of the controller.

Art. 85 establishes the principle of data protection by design and by default prescribing the adoption by the controller of appropriate technical and organizational measures (including pseudonymization).

The Commission has also launched the **proposal for a regulation concerning the respect for private life and the protection of personal data in electronic communications and repealing the Directive 2002/58/EC regulation on confidentiality and electronic communications** aimed at guaranteeing a greater protection of people's private lives and offering new business opportunities. Furthermore, the proposal, starting from the observation of the importance for Europeans to maintain the confidentiality of emails and online messages and the necessity to define a unitary protection within the Union and the applicability of the current ePrivacy Directive only to traditional telecommunications operators, provides for the extension of privacy rules to new operators supplying electronic communication services (such as WhatsApp, Facebook Messenger, Skype, Gmail, iMessage, Viber). It specifies that this protection covers the contents and the metadata of electronic communications (for example, call time and location).

In order to ensure a greater user control over the settings, allowing for easy acceptance or refusal of the monitoring of cookies and other identifiers in the event of risks to privacy, the proposal provides for the simplification of the so-called "cookie provision" which has resulted in an excessive number of requests for Internet user consent. The proposal clarifies that consent is not necessary for non-intrusive cookies that improve the user experience (for example, those that allow you to remember shopping cart history) and for cookies that count the number of users visiting a website.

The proposal also introduces measures against spam, prohibiting unwanted electronic communications through emails, text messages and, in principle, also telephone calls if users have not given their consent. To complete the set of protections, the proposal imposes the authors of telephone calls for commercial purposes, the obligation to show their telephone number or use a special prefix that indicates the nature of the call.

Considering the close relationship between the ePrivacy Regulation and the GDPR, the proposal intends to align the administrative sanctions established for violations of the ePrivacy Regulation with those provided for by the GDPR, introducing penalties of up to €20 million or up to 4% of total annual turnover, if higher.

The procedure is ongoing. On 20 September 2018, the EU Council published a revised text of the ePrivacy proposal replacing the concept of "electronic mail" with "electronic message". It deleted the application of confidentiality of electronic communications data to the transmission of machine-to-machine electronic communications where carried out via an electronic communications service, strengthening the taxability of cases in which data can be processed by providers of electronic communications, and specifying the necessity to detect security risks and/or attacks in the transmission of electronic communications is specified. The revised text also identifies cases in which metadata can be processed by providers of electronic communications networks and services. On 4 February 2019, the Council published the Interinstitutional File 2017/0003 analyzing in depth some of the outstanding issues for the ePrivacy proposal, namely the impact of ePR on new technologies and the consent requirements, processing of electronic communications data for the purposes of child protection and the exclusion of national security and defense from the scope of ePR.

Returning to the data protection area, on 14 November 2018, **Regulation 2018/1807 of the European Parliament and of the Council on a framework for the free flow of non-personal data in the European Union** was approved.

The regulation aims to ensure the free flow of data other than personal data within the Union by laying down rules relating to data localization requirements, the availability of data to competent authorities and the porting of data for professional users. It: 1) establishes the principle of free movement of non-personal data in the Union (art. 4 - any obligation to locate data is prohibited, except when this is justified for public security); 2) ensures the availability of data for regulatory controls by the competent authorities, prohibiting the refusal on the basis that the data is processed in another Member State; 3) encourages the adoption of self-regulatory codes of conduct that specify information on data portability conditions; 4) provides the designation, by each Member State, of a single point of contact which acts as a link with the contact points of the other Member States and the Commission regarding the application of the Regulation; and 5) establishes that no later than 29 November 2022, the Commission shall submit a report to the European Parliament, to the Council and to the European Economic and Social Committee evaluating the implementation of this regulation.

### **Cybersecurity**

The massive spread of digital services is causing a huge increase in cybercrime, bringing the cybersecurity challenge to center stage.

Since the adoption of the EU Cybersecurity Strategy in 2013, the European Commission has planned actions to better protect Europeans online. In particular, the **EU Cybersecurity Strategy** launched in 2013, established 5 priorities: 1) increasing cyber resilience; 2) drastically reducing cybercrime; 3) developing an EU cyber defense policy; 4) developing the industrial and technological resources for cybersecurity; and 5) establishing a coherent international cyberspace policy for the EU.

On 6 July 2016, **Directive 2016/1148** (NIS Directive) was adopted, setting measures for a common high level security for networks and information systems in the Union. This is of extreme importance as, for the first time, the cybersecurity challenge has been tackled, revolutionizing cybersecurity in Europe. The Directive recognizes that network and information system security is essential for economic and social activities and, above all, for the functioning of the internal market.

To this end, the Directive: 1) has prescribed Member States to adopt a national strategy on network security and information systems; and 2) has established a cooperation group to support and facilitate strategic cooperation and information exchange among Member States and to build trust amongst them, and is made up of representatives from the Member States, the Commission and ENISA and carries out its activities on the basis of two-year work programs; 3) creates a network of cybersecurity action teams in the event of an accident to contribute to the development of trust among Member States and to promote rapid and effective operational cooperation; 4) establishes security and notification obligations for operators of essential services and for digital service providers; and 5) obliges Member States to identify competent national authorities, single contact points and CSIRTs with tasks related to network security and information systems.

In September 2017, the Commission launched the **Strategic Plan for Cybersecurity**. The Plan aims to increase defense, deterrence and the resilience of information systems. It is

based on three fundamental pillars: 1) building a resilient European system increasing the level of cybersecurity in the EU; 2) creating an effective and univocal response to computer crimes, adapting penalties to the seriousness of the criminal action; and 3) encouraging international collaboration.

One of the most important aspects of the proposal concerns the creation of a European Agency on Cybersecurity - the result of the strengthening of the already existing European Information Security Agency and of the Networks (ENISA) – with a full and permanent mandate, with more tools and targets, to come into effect by 2020, when the current Agency mandate will expire. Ongoing training in security systems tops the objectives. The Agency will simulate computer attacks to allow Member States, in coordination with the European institutions and their agencies, to prepare forms of response to potential attacks, improving information and intervention times, thanks also to the creation of a training platform.

Concerning collaboration among Member States, the proposal aimed to set up a research center in 2018, to address the important topic of R&D investment in new technologies.

The EU plan also aims to create a single system certification of cybersecurity to overcome the fragmentation currently existing in the presence of 4 main certifications (CPA, CSPN, BSPA, SOG-ISMRA) and to increase reliability, in terms of security, of purchased products. Last, but certainly not least, a review of the criminal policy in the Member States. Here, the Commission encourages greater uniformity in the penalties applied in the Member States and the affirmation of the right of access to information by the victims of such crimes. It offers an adequate and simple assistance system and the creation of a close collaboration within the Union's whole judicial system, through strengthening existing structures and local Contact Points.

Successively, on 13 September 2018, the Commission launched a **proposal for a Regulation of the European Parliament and of the Council on Enisa, the "EU Cybersecurity Agency", and repealing Regulation (EU) 526/2013, and on Information and Communication Technology cybersecurity certification ("Cybersecurity Act")**. It lays down the objectives, tasks and organizational aspects of ENISA and a framework for the establishment of European cybersecurity certification schemes for the purpose of ensuring an adequate level of cybersecurity of ICT products and services in the Union. The proposal lists Enisa tasks as capacity building, operational cooperation at Union level, the market (cybersecurity certification and standardization), knowledge, information and awareness raising, research and innovation and international cooperation. The same proposal regulates the organization of the Agency providing that the structure is organized in a Management Board, an Executive Board, an Executive Director and a Permanent Stakeholders' Group whose composition and functions are specifically defined. It also prescribes that the Agency shall carry out its operations in accordance with a single programming document containing its multiannual and annual programming, which shall include all of its planned activities and fixes some principles to be observed by the Agency (specifically transparency and confidentiality).

The same proposal also defines a European cybersecurity certification scheme shall attest that the ICT products and services that have been certified in accordance with such scheme comply with specified requirements as regards their ability to resist at a given level of assurance, actions that aim to compromise the availability, authenticity, integrity or confidentiality of stored or transmitted or processed data or the functions or services offered

by, or accessible via, those products, processes, services and systems. The proposal establishes the European Cybersecurity Certification Group composed of national certification supervisory authorities.

The procedure for adoption is ongoing (discussions within the Council).

### ***European free flow of data initiative and Cloud***

In the framework of creating a competitive data economy within the Digital Single Market, free data flow of both personal and non-personal data is crucial. Since GDPR already provides for the free movement of personal data within the Union, the free data flow Regulation extends the framework to non-personal data in three ways:

- equating personal and non-personal data flow in terms of free circulation within the European market;
- allowing to block the data movement for national security reasons only;
- encouraging self-regulation focused on creating a code of conduct which can promote the switch between different cloud providers.

The new regulation was signed in November 2018 and come into effect in May 2019. According to the Commission, the removal of data flow restrictions could push the European data economy up to a global € 740 billion turnover in 2020. Main advantages of the new regulation are related to data duplication and increased competition across European countries and between different services.

### ***Digital skills***

On 17 January 2018, the Commission launched new measures to boost key competences and digital skills. It involves three initiatives: a Council Recommendation on Key Competences for Lifelong Learning (which recommends steps to foster competences in science, technology, engineering and mathematics -STEM - and motivate more young people to embark on a career in these fields; a Council Recommendation on common values, inclusive education and the European dimension of teaching; and a **Communication on the Digital Education Action Plan**. The Digital Education Action Plan builds on the two Communications adopted in May 2017: *A renewed EU Agenda for Higher Education* and *School development and excellent teaching for a great start in life*. It supports the work on the Digital Single Market and the New Skills Agenda for Europe. The Action Plan focuses on implementation and the need to stimulate, support and scale up purposeful use of digital and innovative education practices. It identifies three priorities: 1) making better use of digital technology for teaching and learning (tackling the connectivity divide among EU Member States, supporting the digital readiness of both general and vocational schools and providing a framework for issuing digitally-certified qualifications); 2) developing relevant digital competences and skills for the digital transformation (creating a Europe-wide platform for digital higher education, strengthening open science and citizen science in Europe, bringing coding classes to all schools, tackling the challenges of digital transformation launching an EU-wide awareness-raising campaign targeting educators, parents and learners to foster online safety, cyber hygiene and media literacy and a cybersecurity teaching initiative and supporting measures to further decrease the gender gap in the technology and entrepreneurial sector); and 3) improving education through better data analysis and foresight (building evidence on the uptake of ICT and digital skills in

schools, by publishing a reference study assessing progress in mainstreaming ICT in education, launching artificial intelligence and learning analytics pilots in education as of 2018, initiating strategic foresight on key trends arising from digital transformation for the future of education systems).

### ***E-Government***

The digital transformation of government is a key element to the success of the Single Market. On 19 April 2016, the Commission launched the **EU e-Government Action Plan 2016-2020** which proposes an ambitious vision to make public administrations and public institutions in the European Union open, efficient and inclusive, providing borderless, personalized, user-friendly, end-to-end digital public services to all EU citizens and businesses. The Plan identifies three policy priorities: 1) modernizing public administrations using key digital enablers; 2) enabling mobility of citizens and businesses by cross-border interoperability; and 3) facilitating digital interaction between administrations and citizens/businesses for high-quality public services.

### ***Artificial Intelligence***

Considering the importance of AI and the tremendous opportunities for growth connected to its deployment and usage, on 10 April 2018, 25 European countries<sup>2</sup> signed a Declaration of Cooperation on Artificial Intelligence. Above all, the Member States agreed to work together on the most important issues raised by AI, to ensure Europe's competitiveness in the research and deployment of AI and deal with social, economic, ethical and legal questions.

On **25 April 2018**, the European Commission published a Communication on a **European Approach to Artificial Intelligence**. The European approach is based on three pillars: 1) being ahead of technological developments and encouraging uptake by the public and private sectors; 2) preparing for socio-economic changes brought about by AI supporting business-education partnerships to attract and keep more AI talent in Europe and training and retraining schemes for professionals, also encouraging the modernization of Member State education and training systems and foreseeing changes in the labor market and skills mismatching; and 3) ensuring an appropriate ethical and legal framework.

On **9 March 2018**, the Commission launched a call for the creation of an **IA High-Level Expert Group** with the task, inter alia, to prepare, within the year, a proposal for guidelines on ethical development and use of AI in compliance with the Charter of Fundamental Rights of the European Union, taking into consideration issues such as fairness, security, transparency, the future of the world of work and democracy, as well as "political and investment recommendations". On **18 December 2018**, the High-Level Expert Group delivered a draft proposal of the **"Ethical Guidelines on Artificial Intelligence"** which identifies the essential elements for the creation of a "reliable" artificial intelligence (Trustworthy). The paper is divided into three chapters characterized by a "human-centric" approach aimed at preserving the founding values of our societies and the protection of

---

<sup>2</sup> Austria, Belgium, Bulgaria, the Czech Republic, Denmark, Estonia, Finland, France, Germany, Hungary, Ireland, Italy, Latvia, Lithuania, Luxembourg, Malta, the Netherlands, Poland, Portugal, Slovakia, Slovenia, Spain, Sweden, the UK, Norway.

liberties and rights. It identifies five basic principles to be followed : 1) charity (AI systems should tend to increase individual and collective wellbeing); 2) non-maleficence (AI should not harm human beings); 3) autonomy (AI should not undermine an individual's freedom and self-determination); 4) justice (IA systems should be based on fairness criteria); and 5) transparency (AI should always be understandable and controllable by citizens who should be aware of interacting with them). As well, the document lists the characteristics that IA systems must possess, from the design phase ("by design") to be reliable, and requiring that they be designed so as to avoid discrimination, manage errors, ensure maximum social inclusion, ensure effective human control and effective protection against possible abuses made possible by such technologies, protecting privacy and ensuring the security and transparency of decision-making mechanisms.

#### **4. Power breakfast main highlights**

The EU currently has a long way to go in terms of truly implementing a digital single market, but it is vital to look at how far it has come. Five years ago, the digital world was viewed very differently. Barack Obama was still president of the United States, and most people did not believe that social media would be an important factor in an election. The geopolitical landscape of the EU was very different as well; for example, the EU had just closed its investigation on China. It is now a well known fact that social media has to be taken seriously as a political tool, and it is vital to look at and interact with it.

Digital is a very important part of world trade and also a country's position compared to other world powers. The original priority in the EU was to create a feeling of a singular market, primarily by abolishing digital borders and allowing citizens to access content on their mobile phones anywhere in the EU like they would on their computers at home. With this came an emphasis on the free flow of data and portability. Now, the EU is the data regulator of the world, largely due to necessity. The European Electronic Code was a huge advancement, as it included all of the previous directives in a single act, which sends a powerful political message. In addition, the content is very sophisticated. It is important that all important directives are transposed well and in a uniform way across Europe, and that companies also pass this message, especially those that operate all over Europe.

As the world is becoming more and more digital, cybersecurity is a huge issue. It only took a year for the EU to put the cybersecurity act into place, but Europe is still largely unprepared. Every member state needs to reorganize things, and industry should decide which things are the most important to enact. Although cybersecurity is improving, the functioning in Member States and the exchange of information could be vastly improved. It makes a large difference when Member States and the European Commission work together, as it is vital to move cohesively in a single direction.

A lot also depends on the new Parliament that will be elected in May, especially when it comes to implementing and spending the budget. Now is the time to be serious and ensure that important progress is made, especially in the realms of resilience and more competitive technology. Implementing a digital element is very important, especially in fields such as healthcare and agriculture, and while society will be more technologically advanced, savvy, and competitive, it will also be prepared for cyber attacks. There also needs to be more

focus on competition policy, and the EU largely has to focus more on doing rather than thinking.

Participants in the breakfast also discussed how AI is beneficial for jobs, but there has to be distinct ethics guidelines. However, different Member States often have different responses to things, which makes creating a cohesive plan difficult. Investment in digital in the EU must be higher, especially when it comes to AI, and for the world to take the EU seriously the Member States need to sit down together and figure out a strategy for the future. There needs to be a more European approach to blockchain, and although the EU is doing well it is not well known enough exactly what is happening. The Commission will work together with Member States on blockchain on a voluntary basis, and the Member States should take advantage of that opportunity, especially when it comes to the energy sector. In addition, 5G frequencies need to be assigned. Only 6 Member States have assigned it so far, and it is vital for the future that every country will rapidly award it.

There is also an opportunity for transformative healthcare, but in order to merge technology and healthcare there need to be important advancements in the areas of digital identity, trust, and personal databased. In order to reach the point of personalized medicine, more data is needed, specifically lifestyle and environmental data, and all of the different datasets need to be merged to create a complete picture. Patients need an opportunity to give feedback, and also to receive personalized advice on lifestyle.

Europe should invest in power communities, which are data-driven communities. There needs to be a creation of not only a strong legal framework but also a vibrant community of companies that can be competitive in the world. There also needs to be an organized structure in order to be big in cyber security. The EU needs to identify strategic value chains and form action plans, and do so by looking at the successful examples that are all around. There can be a combination of regional, European, and private funds, and it is also vital to look at what things are failing to avoid making the same mistakes in the future.