Geneva Internet Platform

DigitalWatch
NEWSLETTER

*You receive hundreds of pieces of information on digital policy.
We receive them, too.
We decode, contextualise, and analyse them.
Then we summarise them for you.*

DIGITAL POLICY TRENDS IN MAY

1. The EU's GDPR comes into effect

May was a much-anticipated month, as the EU's General Data Protection Regulation (GDPR) came into effect. It triggered an eleventh-hour rush for companies and organisations to update their privacy policies and bring their e-marketing practices in line.

The GDPR, which replaces the 1995 Data Protection Directive, has reshaped the way in which the personal data of EU citizens is handled and processed. The impact goes beyond EU shores; companies based outside Europe who process the data of EU citizens will also have to comply with the rules.

As soon as it came into effect, the first legal cases emerged. ICANN filed a legal action against Germany-based domain name registrar EPAG over the registrar's decision to stop collecting administrative and technical contact information when domain names are registered. While the registrar believes that collecting such data goes against the GDPR, ICANN argues that the registrar is breaching its contract by not complying with the requirement to continue to collect the data. In its ruling, issued a few days after the case was

filed, the Regional Court of Bonn dismissed ICANN's case. In line with the principle of data minimisation stated in the GDPR, the court opined that the collection and storage of the data of the administrative and technical contacts for a domain name were not necessary, and that the collection of personal data of the domain name registrant was sufficient for purposes related to safeguarding against misuse of domain names.

Austrian privacy campaigner Max Schrems filed complaints against Facebook and Google, accusing them of coercing users into accepting their data collection policies. The complaints, worth €3.9 billion, were filed against Facebook, WhatsApp, and Instagram via data regulators in Austria, Belgium, and Hamburg, while another complaint against Google worth €3.7 billion was filed in France.

The GDPR is also creating a challenge for blockchain technology. Blockchains which were not built with privacy in mind may have a compliance issue. For example, can a blockchain comply with the right to be forgotten if it has no mechanism for removing data?

The EU General Data Protection Regulation entered into force on 25 May 2018, putting in place stronger rules regarding the collection and use of personal data. Its impact goes beyond the EU, affecting business worldwide, as the rules apply to all entities that offer goods or services to, or monitor the behaviour of, users in the EU.

IN THIS ISSUE

BAROMETER

The Internet economy, digital rights, and new technologies are prominent this month. Read our summary of developments.

FACEBOOK SCRUTINY

Facebook's CEO met with leaders of political groups in the European Parliament and faced questions on data protection and content policy, among others.

INCLUSIVE FINANCE

Inclusive finance can accelerate development, and digital technologies and governmental policies have a role to play.

GDPR

Test your knowledge on the main provisions of the GDPR with our crossword.

DigitalWatch
NEWSLETTER

DIGITAL DEVELOPMENTS IN GENEVA

Many policy discussions take place in Geneva every month. The following updates cover the main events of the month. For event reports, visit the Past Events⬀ section on the *GIP Digital Watch* **observatory.**

Keeping Power in Check: Media, Justice, and the Rule of Law

The session, on 3 May 2018, marked the 25th anniversary of the United Nations World Press Freedom Day.⬀ In his opening remarks, UN Secretary-General António Guterres noted the importance of free press for democratic participation. This point was reinforced during the discussions, as participants stressed the important role of governments in upholding the protection of art.19 of the Universal Declaration of Human Rights (i.e., freedom of expression) in the name of democracy. It was also noted that freedom of the press is connected to the sustainable development goal (SDG) #16, which promotes peaceful and inclusive societies through sustainable development. While recognising that digitalisation plays a key role in democratising access to information, participants cautioned against the challenges of online disinformation, and emphasised the role of education and media literacy in countering such challenges.

Commission on Science and Technology for Development – 21st Session

At its 21st session, on 14–18 May 2018,⬀ the Commission addressed two priority themes. The discussion considered the role of science, technology, and innovation in substantially increasing the share of renewable energy by 2030. Although the sessions focused on the potential of technology for development, many speakers also warned of slow policy responses vis-à-vis digitalisation in developing countries. Attention was also drawn to building digital competencies to benefit from existing and emerging technologies, with special focus on gender and youth dimensions. In particular, it emerged that educating women on information and communications technology (ICT) skills is crucial for achieving the SDGs. The meeting reviewed the progress made in the implementation of the outcomes of the World Summit on the Information Society (WSIS). **The Geneva Internet Platform provided reports from several discussions.**⬀

Global Commission on the Future of Work – 3rd Meeting

The Commission, established by the International Labour Organization with a view to examining the future of work, held its third meeting on 15–17 May 2018.⬀ During the meeting, the 28 members of the Commission started working on their final report – due in early 2019 – which will include recommendations on how to achieve a future of work that provides decent and sustainable opportunities for all. Some of the issues tackled during the discussions included digitalisation and the digital divide, and their impact on work, inclusivity, gender equality, skills and lifelong learning, youth employment, income inequality, the measurement of work and wellbeing, and ways to achieve sustainable development. The Commission will reconvene on 15–17 November 2018 to discuss the final draft of its report on the future of work.

AI for Good Global Summit

The summit, held on 15–17 May 2018,⬀ at the International Telecommunication Union (ITU), aimed to identify practical applications of AI as tools for improving the quality and sustainability of life on the planet. The debate was structured along four main tracks. The track on AI and satellite imagery emphasised the potential of using satellite data and AI to achieve the 2030 Agenda. The track on AI and health explored the possible contribution of algorithms and AI to improve the health system, in particular in developing countries. The third track on AI, smart cities, and communities looked, among others, at the importance of including citizens as equally important stakeholders in the development and implementation of such projects. The fourth track, on trust in AI, addressed ways to bridge the policy-technical gap for obtaining a trustworthy AI. **The Geneva Internet Platform provided reports from several sessions at the summit.**⬀

World Health Assembly – 71st Session

Member states of the World Health Organization (WHO) gathered in Geneva on 21–26 May 2018⬀ to discuss current and future policies and programmes of the organisation. Issues related to the use of digital technologies in healthcare were part of the debates. A report on Improving access to assistive technology,⬀ prepared by the WHO Director-General, underlined the need for policies to make assistive technologies more affordable and accessible around the world. Another report on the Use of appropriate digitfal technologies for public health⬀ outlined the role of digital technologies in strengthening the health system, and called on member states to increase their capacities to implement digital health. This call was reiterated in a resolution on digital health,⬀ which urges countries to prioritise the use of digital health solutions in their efforts to enable universal health coverage. The resolution also requests the WHO to develop a global strategy on digital health.

DIGITAL POLICY TRENDS IN MAY

The effectiveness of the GDPR is already visible, but the real test will be its enforceability by the regulators.

2. Scrutiny of Facebook's practices continues

After Facebook's CEO Mark Zuckerberg faced hours of intense scrutiny in the US Congress, the CEO was back to give his testimony, this time at the European Parliament.

His appearance, the questions he was asked, and his replies, were met by mixed reactions. Many thought that the CEO brushed off certain questions; others thought that the politicians were unable to ask the right questions.

For example, unlike the US hearings, there was little mention of regulation in the European hearings. Questions on 'shadow profiles' were dodged. At the same time, some issues were addressed quite comprehensively. For example, three main sources of problems were identified as a roadmap for tackling fake news: managing spam, fighting fake accounts, and tackling people who mean no harm but share false information.

It is likely that companies – especially the Big 4 (Google/ Alphabet, Apple, Facebook, and Amazon) – will continue to be scrutinised, as their data-based business model becomes more valuable. Even if many bullets have been dodged, this trend is likely to continue in the months to come.

3. Artificial intelligence developments prominent again

Developments in artificial intelligence (AI), including new research, the creation of new AI research hubs or centres, and new milestones for AI systems, make headlines regularly.

This month, AI was even more prominent due to French President Macron's intervention at the Viva Technology conference in Paris. Macron suggested that there be a common global structure, which coordinates the regulations and creates a common thinking on AI.

Related to AI is the use of facial recognition technology (FRT), which raised concerns in the UK following the publication of the report *Face off: The lawless growth of facial recognition in UK policing.* The report argues that the use of FRT has led to a 'staggering' number of innocent people being inaccurately flagged as suspects.

Similar concerns have arisen in the USA, as Amazon has been asked to stop selling FRT to the US government. More than 30 US-based civil society organisations signed a letter in which they state the belief that Amazon's technology 'is primed for abuse in the hands of governments', and 'poses a grave threat to communities, including people of colour and immigrants'.

Amazon has been asked to 'stop powering a government surveillance infrastructure that poses a grave threat to customers and communities across the country', and to 'stand up for civil rights and civil liberties'.

Within the ambit of inappropriate use of the technology, the Toronto Declaration, released during RightsCon 2018, highlighted the obligation of governments and tech companies to prevent machine-learning systems discriminating, and in some cases violating, existing human rights law.

The use of facial recognition technologies by governments has given rise to concerns about the possible negative impact on human rights and fundamental freedoms.
Credit: Alexander Baxevanis

DigitalWatch
NEWSLETTER

DIGITAL POLICY: DEVELOPMENTS IN MAY

The monthly Internet Governance Barometer tracks specific Internet governance (IG) issues in the public policy debate, and reveals focal trends by comparing issues every month. The barometer determines the presence of specific IG issues in comparison to the previous month. Read more about each update.

Global IG architecture

same relevance

In a statement on Cybersecurity Cooperation, leaders of the Association of Southeast Asian Nations (ASEAN) countries reaffirmed that international law applies to cyberspace. They tasked the relevant ministers to identify a concrete list of voluntary practical norms of responsible state behaviour in cyberspace that ASEAN countries could adapt and implement.

The Global Commission on the Stability of Cyberspace (GCSC) adopted a Call to Protect the Electoral Infrastructure. The Commissioners made progress on several additional norms that will include barring the insertion of vulnerabilities into essential cyberspace products and services; advocating that governments actively consider disclosing software and hardware vulnerabilities to vendors; and further defining the elements of the public core of the Internet.

Sustainable development

same relevance

At the meeting of the Broadband Commission for Sustainable Development a synthesis report was issued on broadband for national development in four least developed countries (LDCs) – Cambodia, Rwanda, Senegal, and Vanuatu. The report raised concerns that the demand for broadband and its productive use in LDCs has not matched the growing supply.

Security

same relevance

The UK government has introduced new rules to protect the nation's critical infrastructure and digital services from cyber-attacks and computer network failures, among other threats.

E-commerce & Internet economy

increasing relevance

In a meeting with over 50 key figures from the tech industry, French president Macron warned that the industry cannot just be 'free riding' without giving back to society. The issue of taxation was one of the key discussion topics.

Over 40 members of the World Trade Organization (WTO) issued a joint statement calling on states to refrain from adopting protectionism measures, and to resolve their differences through the multilateral system.

The USA and China agreed to take effective measures to substantially reduce the US trade deficit with China. The talks averted planned Section 301 tariffs that Washington was preparing to levy on Beijing. A common Vision Statement on the Australian-French relationship will pave the way for negotiations on an Australia-EU Free Trade Agreement.

The California Supreme Court outlined a series of requirements which companies – including those in the sharing economy – should meet to classify their workers as individual contractors instead of employees. Meanwhile, a federal appeals court ruled that a regulation passed in 2015 by the city of Seattle to allow Uber and Lyft drivers to unionise was not lawful. In Egypt, a new law regulating the provision of ride-sharing services was welcomed by the companies Uber and Careem.

Digital rights

increasing relevance

The EU's GDPR came into effect on 25 May 2018, and the first legal cases immediately emerged. A court in Germany dismissed a case filed by ICANN against domain name registrar EPAG over the registrar's decision to stop collecting administrative and technical contact details when domain names are registered. Austrian privacy campaigner, Max Schrems, filed complaints against Facebook and Google, accusing them of coercing users into accepting their data collection policies.

Facebook's CEO, Mark Zuckerberg, met leaders of the political groups in the European Parliament, drawing mixed reactions about the questions asked, and the CEO's replies.

The Committee of Ministers of the Council of Europe adopted an Amending Protocol which updates its Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data. The change requires personal data processing to apply the privacy-by-design principle and introduces safeguards for individuals concerned in an algorithmic decision-making context.

DigitalWatch
NEWSLETTER

Jurisdiction & legal issues

same relevance

In a continued effort to block the messaging application Telegram, Russian authorities blocked more than 15.8 million IP addresses and some 50 services including VPNs and web anonymisers.

Iran has also banned Telegram after claiming that the app encourages armed uprisings. Mizan, the Iranian judiciary, blocked Telegram's licence to operate in Iran, saying that the app was used for illegal activities.

Infrastructure

same relevance

Facebook and Qualcomm established a partnership to bring high-speed Internet connectivity to cities. The US Computer Emergency Response Team (US-CERT) issued a warning against a newly discovered malware targeting networking equipment. The malware VPNFilter has the potential to cut Internet access for hundreds of thousands of users. It has already infected at least 500 000 devices in 54 countries, according to Cisco's Talos Intelligence Unit.

Net neutrality

increasing relevance

The US Senate has voted in favour of overturning the Federal Communications Commission (FCC) decision to repeal net neutrality rules. In a 52-47 vote, the Senate approved a joint resolution providing for 'congressional disapproval' of the FCC's December 2017 order. To restore the old FCC rules (dating back to 2015), the resolution has to pass in the House of Representatives and be signed into law by the US President.

Meanwhile, the FCC's Restoring Internet Freedom Order, repealing the 2015 net neutrality order, will take effect in June.

New technologies (IoT, AI, etc.)

increasing relevance

The French President has called on countries to agree on a common global structure for AI. The structure would not regulate, but rather coordinate the regulations and create a common thinking on AI.

The Toronto Declaration, released during RightsCon 2018, highlights the obligation of governments and tech companies to prevent machine-learning systems from discriminating and violating human rights law.

In a set of measures to modernise Europe's transport system, the European Commission issued a communication entitled *On the road to automated mobility: An EU strategy for mobility of the future.* The communication outlines actions aimed at achieving the EU's ambition of becoming 'a world leader in the deployment of connected and automated mobility'.
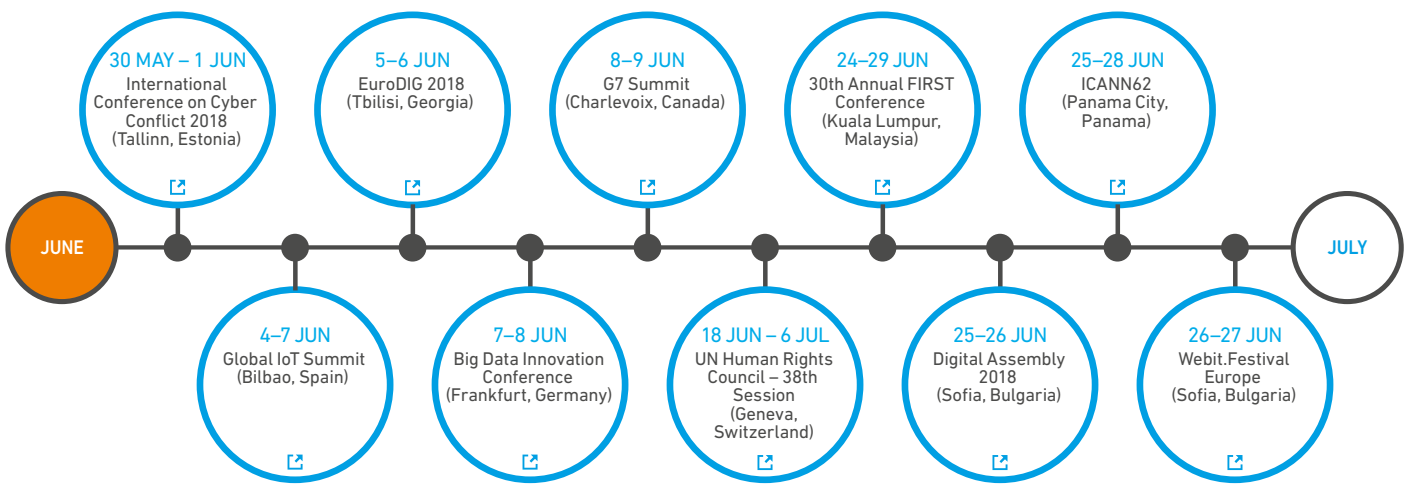
California-based self-driving car company Drive.ai has announced that it is operating fully driverless vehicles, without safety drivers in the driver seat, on public roads in the city of Frisco, Texas, USA. Uber has announced a decision to shut down its self-driving car programme in Arizona, USA, two months after an Uber autonomous car was involved in a fatal accident in the state.

AHEAD IN JUNE

30 MAY – 1 JUN
International Conference on Cyber Conflict 2018 (Tallinn, Estonia)

5–6 JUN
EuroDIG 2018 (Tbilisi, Georgia)

8–9 JUN
G7 Summit (Charlevoix, Canada)

24–29 JUN
30th Annual FIRST Conference (Kuala Lumpur, Malaysia)

25–28 JUN
ICANN62 (Panama City, Panama)

JUNE

JULY

4–7 JUN
Global IoT Summit (Bilbao, Spain)

7–8 JUN
Big Data Innovation Conference (Frankfurt, Germany)

18 JUN – 6 JUL
UN Human Rights Council – 38th Session (Geneva, Switzerland)

25–26 JUN
Digital Assembly 2018 (Sofia, Bulgaria)

26–27 JUN
Webit.Festival Europe (Sofia, Bulgaria)

For more information on upcoming events, visit **https://dig.watch/events**

Digital Watch NEWSLETTER

FACEBOOK CEO MEETS MEPs OVER PRIVACY AND CONTENT POLICY

After testifying for over 11 hours before the US Congress in April, this month Facebook CEO Mark Zuckerberg travelled to Brussels to meet leaders of the political groups in the European Parliament. During the meeting, which lasted less than two hours, the leaders touched on a broad range of issues, including Facebook's potential monopolistic market position, the platform's responsibility with regard to the content it hosts, taxation, and privacy and data protection.

The agreed format for the meeting saw members of the European Parliament (MEPs) addressing questions to Zuckerberg one after another, and the CEO providing answers afterwards. In his replies, the CEO did not provide direct answers to all questions, which left many of the MEPs present unsatisfied, but he committed his team to following up in writing. In the answers he did provide, Zuckerberg reflected on the following points:

Using AI to fight inappropriate content. Facebook's use of AI tools for content policy is not news, and Zuckerberg reiterated this point. Underlining that inappropriate content, such as hate speech, bullying, terrorism-related content, and fake news, has no place on Facebook, the CEO explained that the company is developing and implementing AI tools to improve the process of identifying and removing inappropriate content.

Roadmap for addressing fake news. Facebook is working on tackling fake news by addressing what they have identified as 'main sources of the problem'.

- *Spam*. As spam is mostly driven by financial purposes, Facebook fights it by 'taking away their profit model'.
- *Fake accounts*. When people use fake accounts, there is less accountability, Zuckerberg noted. Facebook has developed tools to identify such accounts while they are being set up or soon after. The company removed around 580 million fake accounts in the first quarter of 2018.
- *People who mean no harm but share false information*. Facebook works with third party fact-checkers to identify news that is probably false and to minimise the possibility of such news being shared over the platform. Once such content is identified, tools are used to show this content less and instead prioritise more accurate content. The company plans to implement this mechanism in as many countries and languages as possible.

Fighting future election interference. Facebook 'is committed' to working more proactively to prevent the platform from being misused by those who wish to interfere in elections. The company's game plan is a combination of building more AI tools to fight fake accounts, co-operating with election commissions, and increasing transparency with regard to political advertising.

Regulation. Reiterating a point made during his testimony before the US Congress, Zuckerberg noted that the question is not whether there should be regulation, but what is the right regulation. 'Some sort of regulation' is important and inevitable, but it is also important to be flexible in order to allow new innovations.

How Facebook sees competition. Zuckerberg spoke about competition from two angles. On the one hand, he explained that Facebook exists in a very competitive space: 'New competitors are coming up every day, so we are trying to stay relevant every day.' On the other hand, the CEO reminded MEPs that the company's business model is based on advertising, and that there are 70 million businesses that use Facebook. By enabling small and large businesses alike to reach customers, Facebook promotes competition, he implied.

Taxes. One of the questions addressed by the MEPs was whether Facebook will commit to pay taxes where it operates and not channel the profits made in one country through tax havens located in other countries. The answer provided was rather general: Facebook has always paid taxes in countries where it has operations set up, including Europe, where it invests heavily.

Platform neutrality and political bias. One concern raised by MEPs was whether Facebook is truly a politically neutral platform for all ideas. 'We are committed to being a platform for all ideas', Zuckerberg replied, while pointing out that his company pledges not to make decisions on content removal or rankings on the basis of political position.

Shadow profiles. Another point on which MEPs sought to get clarity was in relation to Facebook's practices of collecting and transferring the data of individuals who do not have a Facebook account ('shadow profiles'). Reminded about this question towards the end of the meeting, Zuckerberg answered that his company is building a 'clear history' feature allowing users to clear their browsing history data, adding that 'on the security side, we think it's important to protect people in our community.' These replies were seen as an attempt to avoid providing a clear answer to the question, leaving MEPs unsatisfied.

As Zuckerberg committed, his team did provide written follow-up answers to some of the questions raised during the meeting at the European Parliament. What is not clear is whether the MEPs found those answers to be more satisfactory.

INCLUSIVE FINANCE AND DIGITAL POLICY

There is growing interest in inclusive finance as a way to accelerate development and the realisation of the SDGs. Inclusive finance is about economically engaging individuals who are outside the banking and financial systems, through relying on digital technologies such as mobile phones and blockchain. But while technology provides the means, government policies are decisive for the deployment of inclusive finance in economies worldwide.

Individuals' access to banking and financial systems remains a challenge in many parts of the world. This challenge can be addressed through the use of digital technologies, as demonstrated by the M-Pesa mobile payment system in Kenya. But technology in itself is not sufficient. Digital policies are needed to create an enabling environment for the success of inclusive finances. The success of M-Pesa, for example, was possible due to favourable regulations covering three areas: telecommunications, finances, and competition. Here we look at the interplay between inclusive finance and several digital policy areas.

Digital inclusion and mobile/Internet access

Financial inclusion depends on digital inclusion. As is the case with M-Pesa, access to mobile phones facilitates access to financial services. While mobile phone coverage is improving around the world, the next challenge is access to the Internet for more advanced services, including e-commerce. Here, the main obstacle will be to overcome the so-called last-mile problem: providing Internet access to remote and rural communities.

Digital identities

An effective digital identity system is a precondition for financial inclusion. The Aadhaar system in India, which gave a digital identity to 99% of the Indian population, is the cornerstone of the financial inclusion projects in the country. Biometric systems are particularly important when it comes to the financial inclusion of illiterate citizens or citizens without identity documents. Banks and other providers of financial services can use a unique digital identity as the basis for providing financial services.

Big data and AI

As outlined in a recent report by *The Economist*, big data and AI can also facilitate financial inclusion. Decisions to grant financial support are usually based on the so-called credit history of customers. But when customers do not have a credit history, this becomes problematic. Technology can be of help here, too: data related to the use of mobile phones and apps can be analysed by lenders – through a combination of big data and algorithms – to determine whether someone can afford and should be offered a loan. But the use of this kind of analytics also raises concerns about privacy and possible bias in how algorithms work and decisions are made.

Privacy and data protection

The use of data in inclusive financing gives rise to the question of privacy protection. While people are trading their personal data for better access to financial services, they will start to worry about losing control over the use of their data. For example, in China, financial rating is getting closer to a 'social credit rating system' which determines who is a 'good citizen' and who is not.

Monopolies and interoperability

As in other tech industries, monopolies are easy to develop in online finance. New monopolies can drive smaller financial service providers out of the market and limit users' choice. For example, M-Pesa covers 80% of mobile finance in Kenya. To reduce monopolies and increase the possibilities of exchange, the Gates Foundation has developed a free open-source software, Mojaloop, which makes interoperable payment platforms easier to use. Interoperable services will also safeguard the assets of the poor, irrespective of what happens to individual companies.

Security

Security is relevant for digital financial inclusion from several perspectives. First, the resilience and cybersecurity of the infrastructures which enables inclusive finance is a matter of concern. Such infrastructures are vulnerable to cyber-attacks, as demonstrated by the 2016 SWIFT cybercrime incident, when more than USD$100 million was stolen from Bangladesh's Central Bank. Second, inclusive finance is affected by security-related supervision of financial transactions. For example, the fight against terrorism very often requires more detailed control of financial transactions. The stricter security requirements for the financial sector are, the more difficult it is for start-ups and new actors to enter the field of inclusive finance. Third, inclusive finance can affect overall security in countries worldwide. Digital money is much safer for users than cash. Without cash 'under the mattress', robberies and crime are less likely to happen.

Taxation

Inclusive finance can also impact taxation systems. Having online payment systems in place can help improve the collection of taxes and reduce the black economy, by providing immutable evidence of transactions and reducing transaction costs in tax administration.

> **Read more analysis on inclusive finance on the *GIP Digital Watch* observatory.**

Digital technologies provide the tools for inclusive finance in economies worldwide.
Credit: UN SG's Special Advocate for Inclusive Finance/Oktobernardi Salam

GDPR: TEST YOUR KNOWLEDGE

The EU GDPR entered into force this month, introducing stricter rules for how entities within and outside the EU process the personal data of EU citizens. The 99-article regulation outlines new requirements for data processing entities and strengthens the rights of individuals with regard to their privacy and personal data. Test your knowledge on some of the main provisions with our crossword.
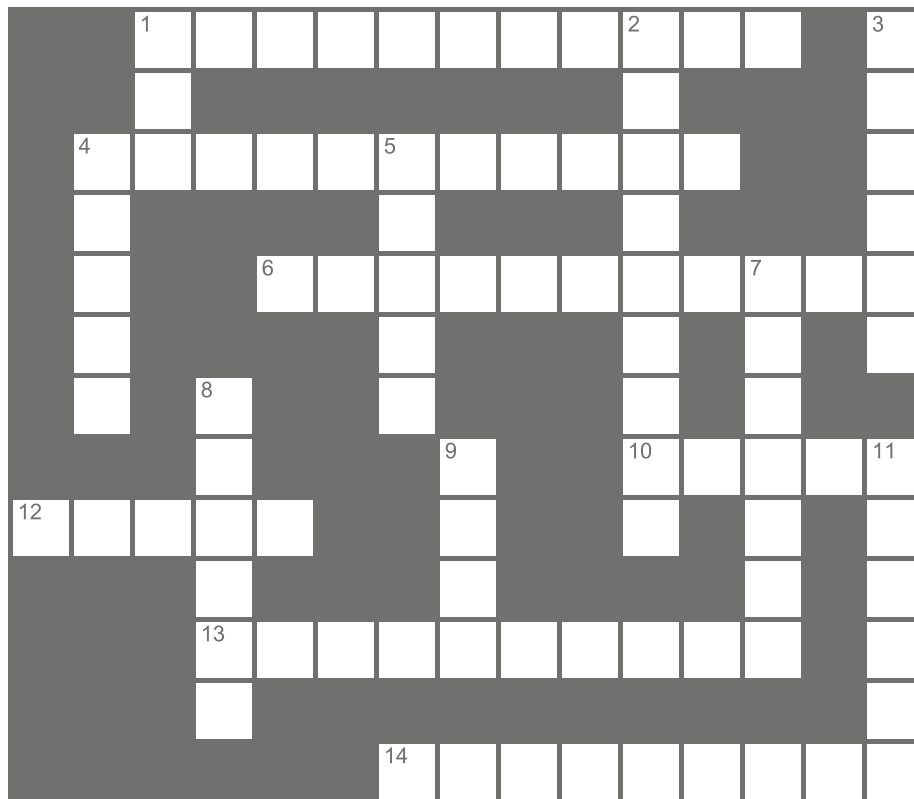
Across

1 The GDPR introduces the concept of extra-_____ appli- cability, as its provisions apply not only to entities based in the EU, but to all entities that offer goods or services to, or monitor the behaviour of, EU data subjects. (11)

4 The right to data _____ gives data subjects the possibility to receive their personal data from one controller and have that data transmitted to another controller. (11)

6 The regulation strengthens the conditions for consent, which should be freely given, specific, informed, and _____. (11)

10 Personal data can be transferred to a ____ country only if the European Commission issues an adequacy decision determining that the country ensures an adequate level of data protection. (5)

12 The GDPR encourages the elaboration of ____ of conduct to assist entities in their efforts to properly apply the provi- sions of the regulation. (5)

13 A data _____ is a natural person or an entity that determines the purposes and means of the processing of personal data. (10)

14 Also known as the right to be _____, the right to erasure enables data subjects to require the removal of their per- sonal data by the data controllers, in certain situations. (9)

Down

1 The GDPR entered into force ___ years after its adoption. (3)

2 Data processors and controllers should take measures to ensure the confidentiality, _____, availability, and resilience of the systems and services used for data processing. (9)

3 The right to ____ empowers data subjects to obtain from the data controller information on whether their personal data is being processed, where, and for what purpose. (6)

4 The concept of ____ consultation requires the data con- troller to consult the data protection authority before start- ing a new type of data processing that could pose a risk to the rights and freedoms of individuals. (5)

5 The GDPR establishes a European Data Protection _____ tasked with 'ensuring the consistent application' of the Regulation across the EU. (5)

7 Entities whose core activities involve regular monitoring of data subjects are required to designate a data protection _____. (7)

8 If a data ____ occurs that is likely to affect the rights and freedoms of individuals, the data controller has an obliga- tion to inform the data subject. (6)

9 The GDPR introduces high penalties for non-compliance, as entities can be fined up to ___ percent of their annual global turnover or €20 million for serious infringements. (4)

11 The concept of privacy by _____ requires the data con- troller to include data protection safeguards when deter- mining the means of data processing, and not only during the processing itself. (6)

Across: 1 Territorial, **4** Portability, **6** Unambiguous, **10** Third, **12** Codes, **13** Controller, **14** Forgotten.
Down: 1 Two, **2** Integrity, **3** Access, **4** Prior, **5** Board, **7** Officer, **8** Breach, **9** Four, **11** Design.