EU Policy News Bulletin

ICT

May 2017

AT A GLANCE : BREXIT NEGOTIATIONS CAN START – DIGITAL SINGLE MARKET MID-TERM REVIEW – MANDATORY SECURITY RULES FOR IOT? – 4 THINGS THAT COULD CRIPPLE EU'S PRIVACY REGIME

EDITION CONTENT:

BREXIT

Brexit negotiations can start

This month the Council, meeting in an EU 27 format, adopted the decision authorising the beginning of talks with the UK. The Commission was nominated as the EU negotiator.

Subsequently to that decision, the Commission spelled out **in two new negotiating papers** how, even when the United Kingdom officially leaves the European Union in March 2019, it will still be entangled in the EU's financial and legal systems for years. Call it "slow Brexit."

The Commission said citizens in the process of acquiring EU rights (such as permanent residency in another country in the bloc) should be allowed to finish doing so, and that the U.K. will be liable for certain financial payments, such as the salaries of British teachers at schools for the children of EU officials, until 2021.

The UK would also remain under the jurisdiction of the European Court of Justice while all pending cases are completed, and the UK would not immediately receive upon departure all the capital it has supplied to the European Investment Bank.

Plus, the EU expects the U.K. to pay all of its financial commitments as part of the seven-year EU budget covering the period 2014-2020.

Source: Dods + Politico Pro

DIGITAL SINGLE MARKET

Mid-term review of Digital Single Market

Since the launch of the DSM strategy in May 2015, the European Commission has delivered 35 legislative proposals and policy initiatives, including on telecoms, e-commerce, copyright, digital rights in general and ePrivacy in particular.

This month the Commission's mid-term review now identified three areas where further action is needed:

- to develop the European Data Economy to its full potential,
- to protect Europe's assets by tackling cybersecurity challenges, and
- to promote the online platforms as responsible players of a fair internet ecosystem.

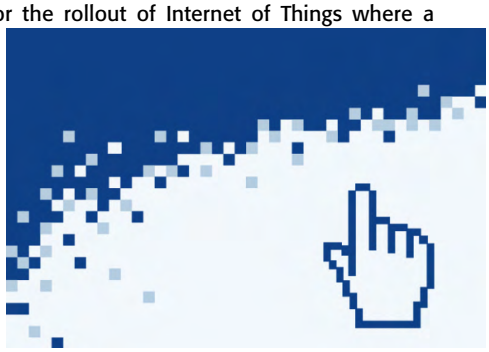
Andrus Ansip, Vice-President for the Digital Single Market, added pressure to the co-legislating bodies in the EU to adopt the legislation as soon as possible.

In the areas of interest to the Working Group, the following measures are being proposed:

Internet of Things

The Commission will consider the possible need to adapt the current legal framework to take account of new technological developments (including robotics, Artificial Intelligence and 3D printing), especially from the angle of civil law liability and taking into account the results of the ongoing evaluation of the Directive on liability for defective products and the Machinery Directive.

Furthermore, the Commission understands that predictability on the access to patent protected technology endorsed in standards (standard essential patents) is key for the rollout of Internet of Things where a broad range of sectors will implement standards on mobile connectivity. The Commission is assessing effective means to ensure a balanced framework for the licensing of this intellectual property respecting the interests of both developers and users of technology.



Cybersecurity

The Commission finds that, with the threat landscape so significantly changed since 2013, the EU Cybersecurity Strategy needs to be reviewed. An evaluation is currently ongoing to assess its effectiveness and to identify gaps in EU action. This will feed into an integrated review.

By September 2017, the Commission will also:

- review the mandate of ENISA to define its role in the changed cybersecurity ecosystem, including aligning it to the requirements of the NIS Directive, based on the recent public consultation and results of the ongoing evaluation;
- develop measures on cyber security standards, certification and labelling, to make ICT-based systems, including connected objects, more cyber-secure.

Artificial Intelligence

The Commission is not envisaging to launch or review any direct legislation in this area, but merely refers to its intention to provide funding for AI. Over the next 3 years, the Horizon 2020 funding instrument will foresee an additional EUR 300 million for activities related to digital innovation hubs, which are essential to support local start-ups and innovation. A continued investment of close to EUR 3.2 billion in key technologies including nanoelectronics, photonics, robotics, 5G, high performance computing, big data, cloud computing, and artificial intelligence and their integration along the value chains with pilot lines, testbeds, is also planned.

Spectrum

With regards to spectrum, the Commission calls on the Member States to have a "*coordinated approach to spectrum policy*". Member States must take coordinated action to make the 700 MHz band available for wireless broadband use. The Commission also noted that the Electronic Communications Code, which is currently being discussed in Parliament and Council, must be "*adopted swiftly*".

Source: European Commission

EU countries agree final stance on digital consumer rules

Digital consumers are entitled to have some non-personal data returned to them if they end a contract with a mobile application or digital service provider, according to a **general approach from EU member countries**.

The Council worked for close to a year-and-a-half on the compromise on digital consumer rules for mobile applications and software. The rules clarify consumers' rights when they pay for digital products with their personal data instead of cash.

In the position, EU member countries clarify that customers buying digital services, like cloud applications and data storage, should also be protected under the new rules.

Physical goods with embedded digital content, like children's dolls connected and operating through Wi-Fi, will not be included in the scope of the rules, the Council said. That contradicts a working compromise being discussed in the European Parliament.

In terms of next steps, the text must be signed off by national ministers at the Justice and Home Affairs Council on June 8 and 9.

Source: Politico Pro

CYBERSECURITY

Call for mandatory security rules for IoT

The EU's cyber agency ENISA and a group of tech companies released a **joint position** urging the Commission to develop "*mandatory staged requirements for security and privacy in the Internet of Things.*"

The European Network and Information Security Agency (ENISA) said an EU "*trust label*" for companies that sell devices that are connected to the internet will help prevent attacks like the denial-of-service attack that took down many internet services in North America and Europe in October 2016.

Companies supporting the position include semiconductor companies Infineon, NXP and STMicroelectronics. The position was agreed upon in December but only published this month.

Tech companies would also be liable should their products be hacked — something ENISA supports but the industry itself is wary about.

The tech lobby DigitalEurope, which represents Google, Microsoft and other tech giants, in March said that mandatory certification schemes will hurt the sector, including smaller businesses.

The Commission has supported initiatives from within the industry, like mobile industry association GSMA's voluntary standards and the IoT Security Foundation for companies to discuss issues but is considering adding mandatory requirements for IoT devices in a new proposal later this year.

Source: Politico Pro

DATA PROTECTION

4 things that could cripple EU's privacy regime

In one year's time all companies and national authorities will have to abide by the EU's strict new privacy law, the General Data Protection Regulation (GDPR).

Businesses, regulators and lawmakers are racing to put national rules and corporate regulations in place to make the EU law effective. That means it's uncertain whether the EU's grand plan of an overarching privacy regime will ever become reality.

Here are four things that could get in the way of the EU's dream of tight privacy protections:

1. National governments making a mess

The German parliament adopted its national version of the GDPR at the end of April, part of the legislative work national governments need to do to implement the law. But Berlin's approach to handling the law displeased some.

"*The Germans have missed the balance,*" a high-level Commission official said, adding that the new German law goes too far in putting burdens on companies dealing with personal data.

The GDPR contains a number of so-called "*opening clauses*" meant to give national governments options in how they roll out the new privacy regime.

National laws like Germany's could end up creating different regimes across the Continent — precisely what the Commission wanted to prevent with the regulation.

2. Watchdogs failing to step up

National data protection authorities will take a lead role in enforcing the new law from May 2018. But the watchdog bodies in national capitals are suffering from a dire lack of funding and, in some cases, expertise to fulfill their role.

The watchdogs are also tasked with drafting guidance for companies on how to set up internal procedures to protect data. But the authorities have been slow in adopting them. Key guidance on things like how to ask users for their approval to store and process data and how companies profile customers still have to be drafted.

3. Businesses having no clue

A series of studies raised alarm over companies' preparedness for the new requirements.

A study commissioned by the company Compuware surveyed 400 chief information officers in the EU's five largest countries and the U.S. and found only 38 percent had a plan in place to comply with GDPR. A survey for cyber firm RSA asked 2,045 U.K. consumers if they had heard of the GDPR: Only 15 percent had.

"*A lot of companies will start implementing it at the last moment,*" said Istvan Lam, CEO of Tresorit, a company specializing in privacy-friendly cloud services. They "*don't have processes to work with data — they'll have to start from scratch,*" he said.

Those that fail to properly respect the law risk being fined 4 percent of their annual turnover — a deterrent business representatives find too drastic.

"*Make no mistake, there will be businesses that will never fully recover from such a fine, if they don't go out of business entirely,*" said Rashmi Knowles, chief technology officer for Europe at RSA.

4. That other privacy law getting in the way

The EU is debating a new e-Privacy Regulation that updates the rules on how telecoms and online communication apps like WhatsApp and Skype can use private communication. The Commission's proposal is all about keeping "*confidentiality of communication*" intact online.

Lawmakers hope to adopt and implement the e-Privacy Regulation by May 2018, in parallel with the GDPR.

European Data Protection Supervisor Giovanni Buttarelli argued for the e-Privacy Directive to come up with separate definitions in the e-Privacy Regulation, in an official opinion last month.

But the e-Privacy Regulation is opening up old wounds between privacy activists and business representatives. If the debate in Parliament and Council gets out of hand, it could create confusion in corporate headquarters and among lawyers about what GDPR really means.

Source: Politico Pro

EDPS asks business to work on ethics

At the beginning of the month European Data Protection Supervisor Giovanni Buttarelli said his office will watch closely how internet companies use big data and artificial intelligence.

"*This issue should be more at the top of the political agenda,*" said Buttarelli at the presentation of the watchdog's **annual report**.

"*We should be, as data protection authorities, more inclusive towards new technologies,*" he said. "*This is why we like to recruit data scientists*" to investigate whether new technologies could discriminate or violate privacy rights.

He also asked whether the business sector is ready to work on ethical principles.

Buttarelli last year pitched a European "**Digital Clearing House**," arguing that big data can pose a threat to privacy, data protection and fundamental rights online. His office is also working on ethical guidance for organizations using big data applications.

In his report, the privacy watchdog also said to focus on new privacy rules for electronic communications, developing new rules for EU institutions on how they treat personal data and setting up a new European Data Protection Board that will take over key privacy oversight in May 2018.

Buttarelli also pledged to watch closely how the EU Commission agrees on data transfer agreements with non-EU countries to allow for personal data to be easily exported outside of the bloc.

"*Privacy is not anymore simple a European Union issue*," said Buttarelli, pointing at the adoption of privacy laws across the globe.

Source: EDPS + Politico Pro

AI & ROBOTICS

EESC calls for code of ethics

At the end of May, the European Economic and Social Committee published its **opinion on artificial intelligence**. The own-initiative report, drafted by the Dutch Catelijne Muller, calls for the development of a standardisation system for verifying, validating and monitoring AI systems. In addition, the report put a strong focus on a code of ethics for the "*development, application and use of AI so that throughout their entire operational process AI systems remain compatible with the principles of human dignity, integrity, freedom, privacy and cultural and gender diversity, as well as with fundamental human rights*."

The EESC highlights the advantage the EU can gain on the global market by developing and promoting "*responsible European AI systems*", complete with European AI certification and labels.

Finally the consultative body also refers to the importance of privacy, real-life test environments and high-quality data sets for developing and training AI systems.

Source: EESC