

European Regional Bureau Newsletter



7 October – 13 October 2017

<http://www.Internetsociety.org/what-we-do/where-we-work/europe>

[Frédéric Donck \(ERB\)](#)

Internet Access

EU: Council ready to start talks with Parliament on telecoms reform

- On October 11, the Council approved a general mandate for the Estonian Presidency to begin trilogue negotiations with the European Parliament on the European Electronic Communications Code.
- The result of these trilogue negotiations will provide the framework for the telecommunications sector for years to come, whether in terms of access to networks, consumer protection rules, or governance.
- The Parliament reached its own position on the telecoms framework just last week.
- Main points of difference between the two institutions include spectrum, whether the Parliament is in favour of greater co-ordination and harmonisation, as well as on co-investment, where the council is in favour of a regime that is more favourable for incumbent telecoms operators.
- The first trilogue discussions will take place on 25 October.

EU: Council adopts WiFi4EU

- On October 9, European ministers for telecommunications adopted the [WiFi4EU](#) regulation. Under this new initiative, the EU will invest up to €120 million to help municipalities, hospitals and other public bodies set up free wireless hot-spots across the region.
- Urve Palo, Estonian Minister for Entrepreneurship and Information Technology, [claimed](#) that the scheme “will make high-quality Internet more accessible for many citizens and could even trigger a virtuous investment cycle.”

EU: DIGITALEUROPE views on 5G spectrum options for the EU

- DIGITALEUROPE, the European organisation representing the digital technology industry, has published a [report](#) providing recommendations on the way forward regarding the allocation and licensing methods for 5G spectrum for Europe.
- DIGITALEUROPE stresses the importance of 5G deployment as a key enabler of digital transformation, and sets out specific recommendations for different 5G bands.
- The paper also claims that licensing mechanisms should be chosen carefully in order to achieve harmonisation of licenses (duration, price, spectrum packaging and availability, regulatory conditions) across Europe.

EU: BEREC addresses net neutrality opt-in tools during plenary session

- During its plenary meeting on October 11, the Body of European Regulators for Electronic Communications (BEREC) decided to develop a net neutrality measurement tool to help National Regulator Authorities (NRAs) and end-users to measure the quality of fixed or mobile Internet access and implement BEREC's guidelines on net-neutrality. BEREC will also provide a tool to detect illegal content online. A public consultation on its proposal runs until November 8.
- BEREC has published a [report](#) on specifications for such tools and plans to launch a tender for the development of the applications in the first quarter of 2018.
- Also during its plenary, BEREC announced the launch of several other public consultations, including on [a report analysing the impact of content and devices on the telecoms market](#); a preliminary report on [monitoring of mobile coverage](#); and its [work programme](#) for 2018.

Trust**EU: New Estonian Presidency text on ePrivacy**

- On October 6, the Estonian Presidency released a revised [text](#) on the draft Regulation concerning the respect for private life and the protection of personal data in electronic communications (ePrivacy Regulation).
- Compared to previous versions, the Presidency tried to clarify the interplay between the ePrivacy Regulation and the General Data Protection Regulation (GDPR), while also making changes to the rules for ancillary services and machine-to-machine communication.
- The text has been provided by the Estonian Presidency ahead of the telecommunications working party meeting on 18 October, at which point negotiations between Member States over the changes to these privacy rules will continue.

EU: Polish PM announces cybersecurity department

- During the [Third European Cybersecurity Forum](#) (CYBERSEC 2017) in Krakow, on October 9, Polish Prime Minister Beata Szydlo [announced](#) her intention to create a department to analyse and monitor cybersecurity.
- The PM added that an expert team was needed in her chancellery in order to be able to better address the current cybersecurity challenges.
- The department will be chaired by Pawel Szefermaker, Secretary of State in the Chancellery of the Prime Minister and a potential successor to Anna Strezynska as Polish Minister of Digital Affairs.

Commissioner for the Security Union addresses Cybersecurity Forum

- Julian King, the Commissioner for the Security Union addressed the European Cybersecurity Forum on October 9.
- He presented the Commission's recent package of cybersecurity measures, explaining the division of priorities between resilience, deterrence, and defence and international cooperation.
- Among other things, he addressed the "cyber security skills gap", a shortfall which is currently estimated to reach 350,000 people by 2022.

Ireland: Data Protection Commissioner receives €4 million additional funding

- With the General Data Protection Regulation (GDPR) set to enter into force in May 2018, the Irish Government has announced an additional funding of €4 million for the Data Protection Commissioner (DPC). The increase brings the total funding allocation for 2018 for the DPC to almost €11.7 million.

- The Irish DPC Helen Dixon stated this will help the DPC to “take on an increasingly leading role in the regulation of the personal data processing activities” and to be more independent.
- The additional funding will also be used for awareness raising campaigns and initiatives.

The Netherlands: Dutch government announces ambitious cyber strategy

- In a coalition agreement released on October 10, the recently formed Dutch government coalition has announced its plan for the next four years, with IT security prominent.
- The Government aims at developing an ambitious cyber strategy, starting by providing €95 million of structural funding to strengthen its digital capacity. An extra €275m a year will be invested into digital forces within the Dutch army, as from 2020, to “increase cyber capacity” in the armed forces.
- Moreover, the government will limit the purchases of the hacking software it uses, and develop standards for Internet of Things products, as well as implementing liability rules for software.

EU: Digital Commissioner Gabriel answers parliamentary question on Microsoft vulnerabilities and the EU

- On October 12, Digital European Commissioner Mariya Gabriel answered a [parliamentary question](#), by Dutch Liberal MEP Marietje Schaake, on the vulnerabilities of Microsoft and the need to secure the European Institutions’ communications, data and critical infrastructures.
- Commissioner Gabriel [said](#) the Commission works to methodically ensure that only vendor supported software is in use and that vulnerabilities are patched as quickly as possible by adopting the necessary relevant updates.
- Commissioner Gabriel also stated that the total amount of the contracts between the Commission and Microsoft is about €6.23 million per year.

EU: Commission presents Cybersecurity package to the EP IMCO Committee

- On October 12, the European Parliament Committee on the Internal Market and Consumer Protection (IMCO) received a presentation from the European Commission on the Cybersecurity package published in September.
- During the discussion, DG CONNECT’s Deputy Director-General Claire Bury [stated](#) that, with regards to the proposed cybersecurity certification framework, the two main problems were the fragmented approach EU countries have on this issue and the lack of practical schemes, given the different needs in different sectors. The Commission believed that a voluntary scheme was the best way to address this.
- Presenting the Proposal for a Regulation on the Free Flow of Non-personal Data, Claire Bury identified the data localisation requirements by EU countries, and the lack of trust due to security risks and legal uncertainties as the main obstacles to data mobility.
- She noted that end-to-end encryption was not covered within the initiatives presented as “it should be dealt with in the telecoms regulation”.