Rechtsanwalt [redacted], 20 December 2018

Steering brief

Scene setter

You will have a 30-minute meeting with [redacted] Vodafone Deutschland and [redacted]

[redacted] took part in the Telecom Roundtable on ePrivacy organised by Vice-President Ansip and Commissioner Gabriel in September 2018. [redacted].

Vodafone is in regular contact with the Commission. T[redacted], met with Commissioner Gabriel in July 2018, and with Vice-President Ansip and Vice-President Katainen in September 2018.

Vodafone is the largest mobile operator in Europe, with operations in 13 European countries and over 25 countries worldwide. Vodafone announced in 2018 an agreement with Liberty Global to acquire their cable networks in Germany, Hungary, the Czech Republic and Romania.

Vodafone requested to discuss the new agenda for digital and the current case Vodafone / certain Liberty Global assets. Other possible topics for the meeting include ePrivacy and cybersecurity.

Objectives

On new agenda on digital and Multiannual Financial Framework

Present the Commission's priorities for the next Multiannual Financial Framework in the digital area.

On ePrivacy

Obtain support of Vodafone for a swift adoption of the ePrivacy Regulation.

Explain that telecom operators will be better off under the ePrivacy Regulation than they are today under the ePrivacy Directive. The Regulation will offer a level playing field between all electronic communications services and will offer more business opportunities to telecom providers.

On Cybersecurity

Inform about Commission's actions in the area of cybersecurity.

Issues for discussion

1. New agenda for Digital and Multiannual Financial Framework

Vodafone recently published their annual Global Trends Barometer 2019 report in which they identified four key trends likely to shape the future based on replies from 1700 businesses worldwide. The four key trends are: (i) Trust in a digital world (cybersecurity); (ii) Prioritising ethics is central to winning the competitive race; (iii) A balance between humans and machines (balance the skills provided by humans versus efficiencies provided by Artificial Intelligence); and (iv) Disruption is placing a renewed focus on customer centricity. These trends and Vodafone's priorities to support sustainable business, people, risk management and governance dovetails with the Digital Europe's priorities in cybersecurity, Artificial Intelligence and Digital transformations of business.

For Vodafone it is important to move away from the funding schemes which reinforce incumbents, towards more pro-competition forms of support, and to invest in future proof technologies (fibre), as well as mobile-fixed convergence (5G).

Vodafone acknowledges that public funding will be necessary to achieve the objectives of the Gigabit Society Strategy by 2025. They pleaded for funding a "EU digital spine and 5G mobile backhaul", similar to our approach regarding socio-economic drivers, more precisely for investing in wholesale only, passive infrastructure (ducts dark fibre open access wholesale networks etc.) connecting all enterprises, schools, government buildings.

Line to take

Multiannual Financial Framework

- While we do not want to pre-suppose the priorities of the next Commission, the proposed budget adopted this Spring hints at some directions, and presents a strong financial component to back our policies and shape global digital markets.
- As the digital transformation gains speed and deeply impacts all sectors of our economy and society, Europe is at a tipping point and needs to invest in its future.
- Therefore, the overall digital objective in the Multiannual Financial Framework proposal is to ensure that Europe drives the digital transformation, and brings benefits to citizens and businesses. More concretely, the proposed Multiannual Financial Framework includes different programmes which aim to:
  - Reinforce the EU's digital capacities in future key technologies such as high performance computing and cybersecurity and ensure their widest possible roll out – through the new Digital Europe Programme;
  - Prepare for and lead the development of next generation technologies – through Horizon Europe;
  - Build a world-leading connectivity infrastructure (e.g. very high capacity digital networks and 5G systems) – through the Connecting Europe Facility;
  - Support creators and ensure the widespread distribution of their works – through Creative Europe.

Future outlook

- Technologies such as Artificial Intelligence, blockchain, virtual and augmented reality will develop further and have the potential to significantly impact our economy and society. This will undoubtedly bring opportunities, but also potential challenges that will require an answer from policy makers.

- Cybersecurity incidents are diversifying both in terms of who is responsible, and what they seek to achieve. Our future security depends on transforming our ability to protect the EU against cyber threats; both civilian infrastructure and military capacity rely on secure digital systems.
- Artificial Intelligence is rapidly becoming the strategic technology of the 21st century, but is raising ethics, privacy and data protection concerns. We must develop policies that allow Europe to be competitive in the Artificial Intelligence landscape; that ensures no one is left behind in the digital transformation; and that core values are embedded in the design and deployment of new technologies.
- In this context, the Commission has published on 18 December 2018 a first draft of the Artificial ethics guidelines (developed by the Artificial Intelligence high-level expert group and with input from telecom operators) which is open for consultation until 18 January 2019.
- We must continue to invest heavily in the digitisation of European industries and skills in order to preserve Europe's prominent role in global value chains.
- By setting up the right framework to exploit the benefits of the data and platform economy, in full respect of fundamental rights and promoting a human-centred approach to digital technology that works for all, the EU can enhance quality of life, ensure affordability and help achieve our climate and sustainable development goals, leading to a better Europe.

Post Digital Single Market strategy - now what?

- The Digital Single Market Strategy adopted May 2015 was set in motion to the to ensure that EU, its governments, businesses and citizens make the most of the digital era to unlock the full potential of the data economy.
- The Commission is fully committed to make sure as requested by the Council June 2018 to implement the Digital Single Market legal and other initiatives fully before the current mandate of this commission and the ongoing legislative cycle will be finalised latest June 2019 to promote competitiveness, jobs and growth.
- The Commission has recently started a study that aims at identifying and prioritising upcoming digital technologies that is required as a new strategic response to make the next wave of digitalization a success story for Europe.
- The study will deliver a condensed list of future disruptive technologies including an assessment on their economic and social impact in the near future and the coming years, but also identifying any possible policy gaps in the current Digital Single Market.
- I would not want to pre-judge anything, but until the necessary analysis is made, and we have some insight into the views of the next Commission, a practical starting point could be found in dividing the future digital policies into three elements:

1. The inherited work; our commitments from the current Digital Single Market Strategy strategy

- We will have to follow-up on our previous work where we are currently proposing non-legislative measures, e.g. Communications on eHealth, Artificial Intelligence and its liability, and we will be following-up on adopted the legislative proposals with review clauses (e.g. geoblocking).

2. Digital trends and tech developments

- We will proactively have to follow up on important technology trends, e.g. Artificial Intelligence, High Performance Computing, Augmented/Virtual Reality to provide a political narrative focusing around :
  - everyone should profit from the digital revolution;
  - managing the digital transformation without losing our core values; and
  - fostering a European digital investment climate, including pushing for European projects where no Member State alone can achieve the necessary scale needed for success.
  - ensuring strategic technological autonomy.

3. Dig deeper into the wider socio/economic effects of technology

- We need to better understand and prepare for the effects technology has on our society:
  - how technology affects citizens and consumers;
  - prepare for and equip our population to make the most of the digital transformation,
  - how technology influences our democracies; a need to make the Internet safer and more trustworthy (eg privacy, cyber security, illegal/hate speech content/fake news),
  - help address our societal challenges such as climate change/energy/mobility
  - how technology impacts the interaction between citizens .
  - deploy an assertive digital diplomacy (values/norms, standards, cyber security, market access).

2. Vodafone / certain Liberty Global assets, (M.8864)

Subject of the case:

On 19 October 2018, Vodafone notified the Commission of the proposed acquisition of sole control of Liberty Global's business in Germany, Czech Republic, Hungary and Romania.

Vodafone provides primarily retail mobile services and to a limited extent fixed telecommunications services in Czech Republic, Hungary and Romania. In Germany, it is active in retail mobile services nationwide, owns the Kabel Deutschland cable network (which covers urban areas within 13 of the 16 Federal States) and offers fixed services in the rest of the country based on access to the Deutsche Telekom fixed network.

Liberty Global primarily offers retail fixed services in the Czech Republic, Germany, Hungary and Romania. In Germany, Liberty Global operates the Unitymedia cable network which covers only the three Federal States (North Rhine-Westphalia, Hesse and Baden-Württemberg) where Vodafone's cable network is not present. In addition, it is active as a mobile virtual network operator in Germany and Hungary.

The Parties argue that the transaction will combine highly complementary telecommunications businesses and create a stronger European player, which will be better placed to compete with the market leaders.

On 7 November 2018, the German Federal Cartel Office made a referral request.

On 11 December 2018, the Commission opened an in-depth investigation (Phase II).

As the Commission opened a Phase II investigation, no formal decision on the pending referral request needed to be taken (according to Article 9(4) of EU Merger Regulation). Should the German Federal Cartel Office re-iterate its referral request in Phase II, the Commission needs to take a formal decision to retain jurisdiction. Should the German FCO not re-iterate its referral request, the Commission will automatically retain jurisdiction.

With regard to Germany, the Commission has concerns that the proposed transaction (i) would eliminate competition between the merging companies, in areas already served by Unitymedia and in Germany as a whole, (ii) could eliminate competition with regard to investment in next generation networks, and (iii) would increase the merged entity's bargaining power vis-à-vis broadcasters. The Commission will investigate these and other less substantiated concerns raised by market participants during its Phase II investigation.

With regard to Czech Republic, the Commission will investigate whether providers of standalone telecommunications services could be marginalised because of the merged entity's converged offers.

At this stage, the Commission has not identified any specific competition concerns relating to the proposed merger for the Hungarian and Romanian markets.

Line to take

- The Commission is concerned that the transaction may reduce competition in Germany and Czech Republic. The Commission will now carry out an in-depth investigation into the effects of the transaction to determine whether its initial competition concerns are confirmed.
- [redacted]
- The current deadline for the phase II investigation is 2 May 2019.

3. ePrivacy

[redacted] *took part in the Telecom Roundtable on ePrivacy organised by Vice-President Ansip and Commissioner Gabriel in September 2018. In* [redacted] *view, telecom operators need rules that would allow them to innovate in the future, and the ePrivacy Regulation should be more flexible.* [redacted] *considers that thanks to the processing of electronic communications metadata, telecom operators could provide services useful for the public interest (e.g. preventing spreading of health diseases; helping a local authority to improve its transportation system by looking where there is high congestion).*

The Commission adopted the proposal for the ePrivacy Regulation in January 2017. The Parliament gave a mandate to the rapporteur to start interinstitutional negotiations in October 2017.

[redacted]

The main novelty for telecom operators added by the Austrian Presidency is a new possibility to process electronic communications metadata for a compatible purpose ('further compatible processing', the concept taken from the General Data Protection Regulation). [redacted]

Line to take

- The ePrivacy Regulation modernises the current rules of the ePrivacy Directive to make them fit for the future. This is why we need the Regulation adopted soon. We trust that the Romanian Presidency will be able to obtain a Council mandate quickly and possibly start trilogues before the European Parliament's elections.
- At this moment, only traditional telecom providers are bound by the ePrivacy Directive. They can only process our electronic communications metadata for billing purposes, or only for value added services if we have given our consent.
- At the same time, the so called "over-the-top" service providers, such as webmail providers and messaging apps, are not bound by the ePrivacy rules. They can read our e-mails and messages, share them with third parties, or use our metadata, all without our consent.
- The proposed ePrivacy Regulation significantly expands the possibilities for providers of electronic communications services to process these types of data (if they have consent for any purpose; to maintain or restore security of the service and process metadata to meet mandatory quality of service requirements). It would help telecom operators develop new services, while at the same time ensuring a high level of protection.
- The Austrian Presidency's compromise proposal would expand the possibilities to process electronic communications metadata even further vis-à-vis the Commission's proposal.
- Finally, the co-existence of the General Data Protection Regulation and the ePrivacy Directive causes significant legal uncertainty for businesses.

4. Cybersecurity

Telecom operators do not fall under the Network and Information Security (NIS) Directive. However, the Electronic Communications Code imposes preparedness and reporting obligations on operators. Apart from being a telecom operator, Vodafone is also a provider of cybersecurity products and services to data, applications, IT and communications network. They provide cybersecurity solutions to utilities, financial institutions and government agencies worldwide.

On 10 December the co-legislators reached a political agreement on the Cybersecurity Act that reinforces the mandate of the European Union Agency for Network and Information Security (ENISA) and establishes an EU framework for cybersecurity certification.

On 12 September 2018, the Commission proposed a Regulation setting up a European Cybersecurity Industrial, Technology and Research Competence Centre with a Network of National Coordination Centres. The Competence Centre will manage funding from the Digital Europe and Horizon Europe programmes to help the Union retain and develop the cybersecurity technological and industrial capacities necessary to secure its Digital Single Market and increase the EU's cybersecurity industry. Industry will be associated to the Competence Centre as part of the Cybersecurity Competence Community and representatives will participate in decision-making via the Industrial and Scientific Advisory Group.

Following recent development and statement by Vice-President Ansip on the alleged dominance of the Chinese telecom vendor Huawei, you may be asked to clarify the Commission's position (more background information in your file).

Line to take

Cybersecurity Competence Centre and Networks

- On 12 September 2018, the Commission proposed a Regulation setting up a European Cybersecurity Industrial, Technology and Research Competence Centre with a Network of National Coordination Centres.
- Industry will be among the main beneficiaries of this support. The Competence Centre and Network will give access to know-how and funding, including to telecom operators who may be both suppliers and users of cybersecurity solutions.
- This initiative should help increase the EU's capabilities to autonomously protect its economy and democracy and to become a leader in the next generation cybersecurity solutions. It should also help assess the security and trustworthiness of telecommunications equipment.

Cybersecurity act

- The agreement on the Cybersecurity Act is a significant step towards enhancing EU's Cybersecurity as well as user and business trust in digital technologies.
- The Act introduces ground-breaking developments as it is the first Union law that takes up the challenge to enhance the security of connected products/ Internet of Things.
- The new Regulation introduces a voluntary EU cybersecurity certification framework for Internet of Things products, services and processes. This framework allows for the creation of various tailored certification schemes, that will be valid across the EU, with clear description of the security requirements to be met and covered.

- Overall, the new framework is expected to encourage an efficient use of the Internet of Things security certification, reduce the fragmentation in this field and increase the level of trust in Internet of Things products and services.

If raised - Huawei issue

- The European Commission monitors the developments closely.
- All companies doing business in the European Union enjoy the benefits of the Single Market but must also comply with the EU's standards and legal framework, such as the EU rules on data protection and consumers' rights.
- EU Member States and relevant national authorities are the ones responsible for the enforcement of EU rules and regulations.
- As regards cybersecurity, the Commission takes this issue very seriously and continues its work to increase cybersecurity in the EU.

Contacts – briefing coordination: **tel.:** .

(CNECT), tel.: **(COMP), tel.:**

Defensive points

E-PRIVACY

Why do we need sector specific rules for the telecommunications sector (ePrivacy rules) on top of the General Data Protection Regulation ?

- The General Data Protection Regulation ensures the protection of personal data. The right to respect for private life and communications is a separate and different right in the Charter of the Fundamental Rights.

- The General Data Protection Regulation does not contain a prohibition to interfere with confidentiality of electronic communications and does not protect communications between two enterprises, or communications between individuals, if they do not include personal data.

- The ePrivacy rules fill this gap and ensure the protection of confidentiality of electronic communications as such.

What is the role of industry and other stakeholders?

- While the Competence Centre and Network is a mechanism for the EU to co-invest and align priorities with Member States, the academic and industrial communities will be the main beneficiaries of this support. These stakeholders will be associated as part of the Cybersecurity Competence Community, and representatives will participate in decision-making via the Industrial and Scientific Advisory Group. Depending on the funding rates, industry will be incentivised to make extensive investment on their side.

How will funding for cybersecurity be allocated?

- The concrete funding priorities and related modalities will be established as part of the Competence Centres annual Work Plan, which is adopted by the Governing Board after having received input from the Industrial and Scientific Advisory Group.

- It is envisioned that the bulk of the funding will be allocated through open calls for proposals and calls for tender. Stakeholders know this system from the past Research & Innovation Framework Programmes. In these cases, the Competence Centre will manage and eventually disburse financial support to recipients, which would typically be academic and research entities, industrial companies, or public authorities.

- The Competence Centre will also seek to promote joint procurement of strategic cybersecurity infrastructures and tools together with one or several other entities – typically public authorities.

- Some funding will be made available directly to National Coordination Centres for them to carry out tasks under this Regulation.

- National Coordination Centres will also be able to financially support their respective national ecosystems through the use of so-called cascading grants.

Huawei issue

Did the US warn the EU on this/similar issues related to cybersecurity before?

- The European Union has regular policy dialogues in place with the US, including on cybersecurity. So far, this issue has not been raised.

If pushed:

- The latest cyber Dialogue took place on 10 September in Brussels. During this dialogue, the EU and the US underlined the need for coordination and cooperation in order to safeguard a global, open, stable and secure cyberspace.

Is there anything planned on our side to take action one way or another?

- The European Union has proposed a wide-ranging set of legislative and non-legislative measures to deal with cyber-attacks and to build strong cybersecurity in the EU. This includes the call from EU leaders in October to introduce measures to combat cyber and cyber-enabled illegal and malicious activities and build strong cyber security, while working on the capacity to respond to and deter cyber-attacks through EU restrictive measures.

- On 10 December, the European Parliament and the Council reached a political agreement on the Cybersecurity Act which reinforces the mandate of the European Union Agency for Network and Information and Security so as to better support Member States in tackling cybersecurity threats and attacks. The Act also establishes an EU framework for cybersecurity certification, boosting the cybersecurity of online services and consumer devices.

- A further measure is the Commission proposal for a European cybersecurity competence centre and network of coordination centres, which aims in particular to provide the EU with scientific excellence and industrial capacity on cybersecurity.

- These are measures which create the right incentives to enhance the cybersecurity of the Information and Communication Technology products and services in the EU for both businesses and consumers alike, and along supply chains.

DISPUTE SETTLEMENT

[redacted]

- [redacted]
- [redacted]
- [redacted]