From: [redacted](CAB-JOUROVA)
To: [redacted](CAB-JOUROVA); TALKO Wojtek (CAB-JOUROVA)
Subject: FW: meeting request with CEOs of TV NOVA Central Europe 18. or 19.2. in Brussles_on elections, desinformation
Date: lundi 14 janvier 2019 18:17:19

Renate agrees to the CEOs of NOVA TVs.

From: NIKOLAY Renate (CAB-JOUROVA)[redacted]
Sent: Monday, January 14, 2019 3:47 PM
To:[redacted](CAB-JOUROVA)[redacted]
TALKO Wojtek (CAB-JOUROVA)[redacted]
[redacted]u>; LADMANOVA Monika (CAB-JOUROVA)
[redacted]>; BRAUN Daniel (CAB-JOUROVA)
[redacted]
Subject: RE: meeting request with CEOs of TV NOVA Central Europe 18. or 19.2. in Brussles_on elections, desinformation

Yep R

Renate NIKOLAY
Head of Cabinet

European Commission
Cabinet of Commissioner Verá Jourová

Commissioner for Justice, Consumers and Gender Equality

[redacted]

From:[redacted]CAB-JOUROVA)
[redacted]
Sent: Monday, January 14, 2019 10:35 AM
To: NIKOLAY Renate (CAB-JOUROVA)[redacted]
TALKO Wojtek (CAB-JOUROVA)[redacted]
[redacted]LADMANOVA
Monika (CAB-JOUROVA)[redacted]
BRAUN Daniel (CAB-JOUROVA)[redacted]
Subject: meeting request with CEOs of TV NOVA Central Europe 18. or 19.2. in Brussles_on elections, desinformation

Dear Renate,

Spokesperson from Prague Rep is offering a meeting with the CEOs of Commercial TV NOVA Central Europe, namely from CZ, RO, SK, BG and SI on EP elections and disinformation. These countries have traditionally low participation in EP elections and these TVs are willing to promote it a bit.

I think it would be very useful for the Cssnr to meet them less formally over a coffee, I would suggest on 19/02, Cssnr is free as of 14.00 onwards.

Would you agree?

Thank you,[redacted]

From:[redacted](COMM-PRAGUE)
[redacted]
Sent: Monday, January 14, 2019 9:53 AM
To:[redacted](CAB-JOUROVA)
[redacted] BRAUN Daniel
(CAB-JOUROVA)[redacted]
Cc: LADMANOVA Monika (CAB-JOUROVA)
[redacted]
Subject: Setkání cmmr s šéfy TV NOVA Central Europe 18. nebo 19.2. v BRUSELU

Ahoj[redacted]ahoj Dane,

bude komisarka **v pondelí 18.2 vecer nebo v úterý 19.2. pres den v Bruselu**?

Bude se tam totiž konat letošní (každorocní) **setkání šéfu televizí skupiny CEM, tzn. TV NOVA v CR**, Slovensku, Rumunsku, Bulharsku a Slovinsku, a šéf **ceské TV NOVY, Christoph Mainusch, by rád pozval komisarku na**

pracovní veceri (ta by byla toho 18.2. vecer). Pokud by to nešlo, tak v úterý nejak pres den kdykoli.

Ta pracovní vecere by trvala cca 1,5-2 hodiny, ale komisarka muže urcite zustat i kratší dobu. Místo a presný cas ješte nemají, ale casove by se jí prizpusobili.

TV NOVA chce hodne vyzývat lidi, aby šli k volbám do EP, výborne s nimi spolupracujeme a i pro komisarku by to byla skvelá príležitost. Všechno jsou to zeme, kde je v EP volbách nízká úcast. Byla by to samozrejme skvelá príležitost k setkání i pro cmmr, a navíc možnost probrat rizika dezinformací a manipulací.

Slíbila jsem mu, že dáme vedet, co nejdrív, jestli bude komisarka moct (aby eventuálne mohli co nejdrív hledat jiného hosta). Pak bych vám dala kontakt, že byste si detaily domluvili už s nimi naprímo.

Moc díky za odpoved!

[redacted]

(2)

COMMISSIONER VĚRA JOUROVÁ

MEETING WITH CEO OF TV NOVA CHRISTOPH MAINUSCH

AND OTHER CEOS OF CME TVS

LOCATION: HOTEL ROCCO FORTE AMIGO, RUE D L'AMIGO 1-3, 1000 BRUXELLES.

DATE AND TIME: 20/02/2019, 14:00

MEETING OBJECTIVE: TO DISCUSS EP ELECTIONS AND DISINFORMATION

MEMBER RESPONSIBLE: TALKO WOJTEK

DG CONTACT & TEL NO: [redacted]
DIRECTOR: IRENA MOOZOVA

VERSION: 16/10/2019 12:27

JUST/123

PARTICIPANTS:

TABLE OF CONTENTS

STEERING BRIEF

CONTEXT/SCENE SETTER

CME is a media and entertainment company operating businesses in primarily four Central and Eastern European markets: Bulgaria, the Czech Republic, Romania and the Slovak Republic. These operations include 26 television channels broadcasting to more than 40 million people across the four markets.

CME was founded in 1994 with the launch of TV Nova in the Czech Republic. CME's television brands are market and audience share leaders in all of its markets with a combined 2017 television advertising spend of approximately US$ 807 million.

CME is a Bermuda company, with subsidiaries in the Netherlands and in each operating country. CME is listed in the United States on the NASDAQ Global Select Market and in the Czech Republic on the Prague Stock Exchange.

Christoph Mainusch is Co-CEO of CME and has served as Executive Director and CEO of the Nova Group since November 2013. Prior to this, Mr. Mainusch was an advisor to the President of Turner Broadcasting International, a wholly-owned subsidiary of Time Warner Inc., where he consulted on various projects from April 2013 until September 2013. From March 2004 to December 2012, Mr. Mainusch was a member of the Operational Management Committee of the RTL Group, a European entertainment network.

From September 2009 to February 2012, Mr. Mainusch served as Chief Executive Officer of the Alpha Media Group in Greece, a terrestrial broadcast company majority owned by the RTL Group. Mr. Mainusch served as Chief Executive Officer of RTL Televizija in Croatia from 2004 to 2009. From 1996 until 2004, Mr. Mainusch served as Chief Executive Officer of ACS Media GmbH. Mr. Mainusch started his career as a freelancer for the public broadcaster Bayerischer Rundfunk before having roles at Tele 5, Sat 1 and RTL2.

OVERALL OBJECTIVES

- EP Elections: inform about our actions to raise participation in EP elections, as well as ensure free and fair elections; enquire about CME Groups' actions undertaken in these areas.
- Understand better the role the TV wants to play in elections and national political debates, especially when it comes to the discourse about the EU.
- Inquire about their views on how EU should be talking to their viewers / what do they need to cover Europe more.

LINE TO TAKE

- Elections are challenging for both politicians and the media. The media are under increased criticism on bias and quality of reporting on the one hand, and under commercial pressure on the other hand.
- The EU is committed to helping the media in an objective way by either funding, defending freedom of information or whistle-blowers.
- I see a big role for the media and journalists to handle disinformation or fake news.

Participation

- The Commission is working with the European Parliament to support the general participation of citizens in the elections to the European Parliament.
- In terms of promoting participation, the Commission recognises the important role broadcasters like CME can play.
- It is important that voters are informed about the practicalities of voting – such as registration dates (which could be different for mobile EU citizens or citizens voting from abroad).
- There will be European level campaign (the so-called spitzen-candidaten process, but the decisive part will be played on national level.
- If you are interested in bring more lights into EU-wide campaign, there will be a number of debates with participation of the media, but mainly in English, French or German.
- The Commission is concerned to ensure that underrepresented voter groups (women, minorities, persons with disabilities etc.) are also addressed and engaged in the elections. One way of achieving this is

through including topics of direct concern for underrepresented groups in the pre-election reporting.

- Election Night – the EP is hosting in Brussels the central election night event in the evening of 26 May. CME Group could consider to discuss with the European Parliament on practicalities of how to include the election night in its coverage.

- ***What are CME Group's plans in relation to covering the European elections 2019? Will it ensure that any voter participation activities are rolled out in line with national election laws and respecting equal treatment of all EU voters?***

Extremist parties

- The extremist and anti-EU parties and candidates should be part of the election campaigns in many Member States. The Commission is interested that bluntly incorrect statements or lies ("myths") about the EU are challenged in the interest of fair and actual reporting. The Commission Representations in the member States, and we in Brussels (spokesperson services), are always ready to provide factual data and information.

- We are also organising so called study visits where journalists could come without reporting to ask questions and understand better quite complex mechanisms of functioning of the EU.

- We would like to avoid scenarios of "he says - she says – journalism" where facts and authoritative sources are put on equal footing with conspiracy theories and outwards lies.

- **What is the CME's plan to make the elections debate about European issues and not about domestic affairs or an expression of sentiment towards the national government?**

Free and fair elections

- The Commission has adopted a number of initiatives aimed at protecting the integrity of the upcoming elections. Most notably, the Election package of 12 September 2018, the Communication on Disinformation and the Action Plan on Disinformation.

- Broadcasters should actively **cooperate with all national authorities** in charge of monitoring that rules related to their activities relevant to the electoral context are respected.

- **Transparency of political advertising** and communication is a crucial element in all these initiatives. The Commission Recommendation has focused on online transparency, as we want to ensure a level-playing field, given that in most member states there are such clear rules already in place for broadcasters. Citizens should know who is behind the ads.

- Basically, we have a lot of rules for broadcasters, as you know, but online media or platforms are often a grey zone. We would want to close as much as possible those loops and extend offline rules to the online world, where possible.

- The Commission has called on online platforms to introduce transparency of political advertising in time for the May 2019 elections. Facebook, and some other platforms, have already indicated they would do so and open a public library of all political ads. The independent journalism will have a role to play in the **public scrutiny** of these commitments and the information provided by political and campaign actors.

-

- Member States should engage with third parties, including media, online platforms and information technology providers, in awareness raising activities aimed at increasing the transparency of elections and building trust in the electoral processes.

- **Disinformation** erodes trust in democracy, institutions and in digital and traditional media. It harms our democracies and impairs freedom of expression by hampering the ability of citizens to take informed decisions. It also affects policy-making by skewing public opinion and affecting social debates in areas like climate change, migration and health. And it can undermine European security and the internal security of Member States, including electoral processes.
- At the same time, the EU considers that actions to address the phenomenon must be fully in line with **freedom of expression**, a fundamental European value and the cornerstone of democracy. Freedom of expression includes the right to receive and impart information and ideas without interference by public authorities. Healthy democracies are strong enough to handle dissenting or shocking speech.

- The **Action Plan on Disinformation** proposes measures framed on: (1) recognition of the threat by Russia specifically and the need for a broader approach, allowing to detect and to expose disinformation from other actors; (2) balance between a pro-active response from the European institutions and governments and the need to safeguard freedom of expression and media freedoms

- The Action Plan offers practical ways to counter disinformation in a coordinated and whole-of-government approach. EU MS, EU institutions, civil society, media and business - all have a role to play.

- One key priority is to put in place **a network of national contact points within a Rapid Alert System** to enable sharing of assessments, data and best experiences tackling disinformation. This would allow better

attribution of attacks and joint responses among the national and Union institutions, taking into account both internal and external dimension. Right now EU MS have very different structures in place who tackle disinformation.

- The Commission will carry out a constant **monitoring of the implementation of the Code of Practice,** which will intensify ahead of the European elections and will push for compliance where needed. One year after the entry into force of the Code, the Commission will also assess its effectiveness. Should such assessment not be satisfactory, it may propose further interventions including of a regulatory nature.

- The Commission and EEAS will **raise awareness of the negative effects of disinformation and conduct communication activities prior the European elections.** The first step was made with the launch of press package for Action Plan, which also included video how to spot fake news, infographic and background briefing for journalists.

- In addition to targeted awareness campaigns, the EU institutions and Member States will promote **media literacy** through dedicated programmes. Support will be provided to national multidisciplinary teams of **independent fact-checkers** and researchers to detect and expose disinformation campaigns across social networks. On 29 January 2019 the European Commission held a conference on countering online disinformation with representatives of industry, regulators, fact-checkers, media, researchers and academia. The launch of the European network of fact-checkers has been announced, which should step up its activities in view of the European elections. A media literacy week will be organised in March 2019.

- We count on strong EU MS political support to build an effective response to the challenge of disinformation. It will require significant

new investments in the short and medium term and more cooperation from the Union institutions and EU Member States.

DEFENSIVES

How can the Commission support increased turnout in elections?

- Following the 2014 elections to the European Parliament, the Commission had pledged in its 2015 post-election report to identify ways of further enhancing the European dimension and the democratic legitimacy of the Union decision-making process, and to examine further, and seek to address, the reasons for the persistently low turnout in some Member States.
- In February 2018, the Commission called for early and ongoing engagement with citizens in debates on European issues, an earlier start to political parties' campaigns for the elections to the European Parliament, including those of their candidates for President of the European Commission, more transparency about the links between national and European political parties and the promotion by Member States of the right to vote, in particular for underrepresented groups.
- We expect from the media to support increased voter engagement and participation. This should be done on an equal basis for all groups of voters and across all Member States.

With five months left before the European elections, what can the Commission hope to achieve in the area of securing free and fair elections?

- Work to combat disinformation and securing fair and free elections is urgent, but we are not starting from scratch.

- A key tool is the EU's strong data protection rules, whose value have already been demonstrated in the Facebook/Cambridge Analytica scandal.

- The EU Institutions and the Member States have long established collaboration in the area of cybersecurity, and notably the Network and Information Security cooperation group recently issued a Compendium on Cyber Security of Election Technology.

- The Code of Practice on disinformation, which emerged from the Commissions April 2018 Communication on Tackling online disinformation, is a set of industry self-regulatory standards to fight disinformation on a voluntary basis, which all the major online platforms have signed up to.

- The Commission's package of measures on securing free and fair elections issued on 12 September 2018 addresses the Member States, and national and European political parties and foundations, providing concrete measures to address the challenge of disinformation and securing fair and free elections in Europe.

- The Action Plan of 5 December of the European Commission and the High Representative provides further specific proposals for a coordinated EU response to the challenge of disinformation.

There have been allegations that online platforms are aggressively removing online political discussion in an effort to avoid being held responsible for the spread of disinformation. Aren't the European measures to combat disinformation liable to made this worse, and is the Commission comfortable with the potential impact on democracy?

- When assessing content published on their platforms, IT companies have to assess it, not only against their rules and community guidelines, but, where necessary, against applicable law and fundamental rights, including the freedom of expression. A priori, the content that is illegal offline should not be allowed to remain legal online.

- The European Commission is continuously monitoring the implementation of its Code of Conduct on countering illegal hate speech online to which many IT companies have signed up.

- The Commission will also carry out a comprehensive assessment of the implementation of the Code of Practice on Disinformation in its first 12 months at the end of 2019. Should the implementation and the impact of the Code of Practice prove unsatisfactory, the Commission may propose further measures, including of a regulatory nature.

What is in the Code of Practice on disinformation?

- The signatories commit to disrupt advertising revenue to go to accounts and websites that misrepresent material information about themselves and to provide advertisers with adequate brand safety tools and information about websites purveying disinformation.

- The signatories will enable public disclosure of political advertising and make effort towards disclosing issue-based advertising. For example, political ads in election campaigns will be clearly marked as such.

- The platforms will have clear and publicly available policy on identity and online bots and take measures to close fake accounts.

- The platforms will provide information and tools to help people make informed decisions when they encounter online news that may be false. They will also make it easier for people to find diverse perspectives about topics of public interest, while giving prominence to reliable sources on their services.

- The platforms will provide privacy-compliant access to data to researchers in order to track and better understand the spread and impact of disinformation.

- By implementing the commitments included in the Code, the signatories will increase transparency for European citizens about political and issue-based advertising and will limit manipulation techniques such as the malicious use of bots and fake accounts.

- The Code should contribute to countering mass online disinformation campaigns that polarise public opinion or sow distrust in the European institutions.

Is the Commission making sure that the actions against disinformation do not unduly interfere with freedom of speech?

- The Commission is of course well aware of the need to protect freedom of expression, which is a core value of the European Union and, as such, is enshrined in the EU Charter of Fundamental Rights and in the national constitutional orders of the EU Member States.

- For these reasons the actions proposed by the Commission do not restrict freedom of speech. Some of the measures to-date proposed, notably the support to fact checkers and to the media literacy, aim at rendering our society more resilient towards disinformation by improving the ability to identify and expose disinformation and by increasing critical thinking on the other side.

- Similarly, the actions to be taken by the on-line platforms in the framework of the code of practice aim at increasing the transparency and the on-line accountability of the internet environment. This means, on the one hand, that users will be better able to know where the news come from, who is the entity sponsoring their circulation whilst, on the other hand, the number of automated bots and trolls that spread disinformation messages on the internet will be reduced.

- Our aim is not to reduce the freedom of EU citizens, but rather to improve their ability to access varied sources of information and to distinguish among these sources the ones that spread malicious disinformation.

Is the Commission planning to intervene with regulatory measures?

- The Commission considered that in a first stage self-regulation by the platforms (notably social media platforms) in this context would be an effective means to target disinformation. Most of the on-line platforms (Facebook, Twitter and Google) are signatories of the code of practice. However the Commission will constantly monitor the implementation of their commitments and will assess their effectiveness. Should the effectiveness of the self-regulatory approach not be

satisfactory, the Commission may decide to intervene including by regulatory measures.

What is the Rapid Alert System and how will it work?

- As part of the Action Plan against disinformation presented by the European Commission and the High Representative in December 2018, the Rapid Alert System will be a hub for Member States, EU institutions and partners to share information on ongoing disinformation campaigns and allow them coordinate their responses. The Rapid Alert System embodies the European approach, in that its purpose is to protect fundamental freedoms and open, democratic debate.
- The system will be based on open-source and unclassified information only. As the Rapid Alert System should be set up by March 2019, Member States are currently working urgently to designate national contact points, map their capacities and draw up collective workflows.

What is the role of the European network of fact-checkers and researchers in tackling online disinformation, and when will it be launched?

- The role of fact-checkers is essential in tackling disinformation. Their work contributes to make the information ecosystem more robust by verifying and assessing the veracity of content based on facts and evidence. The Commission's aim is to facilitate cooperation between European fact-checkers through the creation of a network of European fact-checkers.
- The network will gather fact-checkers operating on the basis of high standards and will be editorially independent.
- The Commission supports a project for a Social Observatory for Disinformation and Social Media Analysis (SOMA), with EUR 1 million, which started its work in November 2018. It is developing a platform that has become operational on the 1 November 2018 and will facilitate cooperation amongst fact-checkers in view of the European elections
- In March, this project organises a meeting with European fact-checkers to foster cooperation ahead of the European elections.
- The Commission will also provide additional funding for the platform (€2.5 million under CEF) which, building on the experience learnt with SOMA, will scale up the joint work between fact-checkers and researchers and provide additional tools for fact-checking and network analysis.
- This digital service infrastructure should scale up the collaboration between fact-checkers and academic researchers in order to ensure full coverage of the Union territory and facilitate the build-up and interconnection of relevant national organisations.
- Meanwhile, the Horizon 2020 support action SOMA (Social Observatory for Disinformation and Social Media Analysis) is providing a platform in order to create a multidisciplinary community, including fact- checkers and academic researchers, to enhance detection as well as analytical capabilities and better understand various types of disinformation threats.

What is the Commission doing to support media?

- The Commission supports quality news media and journalism as an essential element of a democratic society. As confirmed in the progress report of December 2018, the Commission wants to enhance the transparency and predictability of State Aid rules for the media sector; it also launched a call of about €1.9 million for the production and dissemination of quality news content.
- The Commission co-funds, together with initiatives of the European Parliament, independent projects in the field of media freedom and pluralism. These projects, among other actions, monitor risks to media pluralism across Europe, map violations to media freedom, fund cross-border investigative journalism and support journalists under threat. New calls for projects are expected in the coming weeks.
- To support quality journalism, media freedom, media literacy and media pluralism, the Commission proposed a dedicated budget of €61 million in the 2021-2027 Creative Europe programme.
- In addition, in its proposal for Horizon Europe programme (2021-2027), the Commission has foreseen funding for the development of new tools to combat online disinformation; to better understand the role of journalistic standards and user-generated content; and to support next generation internet applications and services including immersive and trustworthy media, social media and social networking. So far around €40 million have been invested in EU projects in the area.

BACKGROUND

On the Commission Recommendation from 12 September 2018

On 12 September 2018, the Commission issued a Recommendation on election cooperation networks, online transparency, protection against cybersecurity incidents and fighting disinformation campaigns in the context of elections to the European Parliament, in line with its priority to ensure fair and free elections to the European Parliament in 2019.

It recommends in particular the establishment of cooperation networks in each Member State, which should involve in particular national authorities with competence for electoral matters, for cybersecurity, media and data protection.

Additionally, a European coordination network on elections is envisaged with representatives from Member States liaising at the European level. The objective is to jointly quickly detect potential threats and gaps, sharing findings and expertise, exchange information and ensure a swift and well-coordinated response including by liaising on the application and enforcement of relevant rules in the online environment.

The Recommendation also elaborates on improving transparency, whereby European and national political parties foundations and campaign organizations and other stakeholders are asked to take appropriate steps to ensure that information is actively disclosed to citizens on the political party, political campaign or political support group behind paid online political advertisements and communications. Member States should also encourage the disclosure of information on campaign expenditure for online activities.

Furthermore, the Recommendation calls on the Member States to put in place the necessary procedures to prevent, detect, manage and respond to cyberattacks, as well as to play a role in raising awareness of the above mentioned issues in advance of the elections.

April Communication on disinformation

The Commission is implementing the actions to counter disinformation announced in its *Communication on Tackling online disinformation*, adopted in April 2018.

One key initiative is the Code of Practice on Disinformation for online platforms and the online advertising sector. This is a self-regulatory instrument, developed by industry stakeholders.

On 16 October, initial signatories subscribed to the Code of Practice. These include the three major platforms (Facebook, Google, Twitter) and Mozilla, plus

trade associations representing other online platforms and the online advertising sector.

The Code includes 15 commitments centred around five chapters: (1) Scrutiny of ad placements; (2) Political advertising and issue-based advertising; (3) Integrity of services; (4) Empowering consumers; and (5) Empowering the research community. Participants identify the commitments relevant to their services and the policies and actions they will take to implement their commitments.

We are also making progress on other actions, including supporting the development of an independent European network of fact-checkers, support to quality journalism and new initiatives to promote media literacy.

The Commission issued a Progress Report on these actions in December.

Action Plan

In response to a June 2018 request, on 5 December 2018 the Commission and the High Representative adopted an Action Plan with further specific proposals for a coordinated EU response to the challenge of disinformation. It was requested and has been endorsed by the European Council. Among other things, it proposes actions to ensure that industry delivers on the Code of Practice on Disinformation as well as actions to raise awareness about disinformation, empower consumers, and support media literacy.

Contact(s): [redacted]

(3)

European Commission

COMMISSIONER VĚRA JOUROVÁ

VISIT TO CROATIA

21-22 FEBRUARY 2019

MEETING OBJECTIVE: BILATERAL MEETINGS AND EVENTS ATTENDANCE

MEMBER RESPONSIBLE: WOJTEK TALKO

DG CONTACT & TEL NO: [redacted]

VERSION: 16/10/2019 12:21

CAB JOUROVA/1437

TABLE OF CONTENTS

6. MEETING WITH BUSINESSES / INDUSTRY ASSOCIATIONS

CONTEXT/SCENE SETTER

The meeting with businesses and industry associations will focus on innovation, data protection and competitiveness. Organisations are starting to share their experience on the application of the GDPR on the ground. The number of complaints received by Data Protection Authorities after 25 May 2018 has considerably risen. NGOs active in the field of data protection have also started to make use of the possibility to bring collective actions before data protection authorities and courts.

On the economic front Croatia is doing well, but the main income comes from tourism. In your meeting with Business Associations, you could try to ask about their plans for the future, innovation and how they perceive not only GDPR but the whole issue of automation, AI and also the role of regional funds

POSITION OF CROATIA ON GDPR

You sent a letter to the Croatian authorities recalling the obligation on Member States to notify a set of GDPR provisions to the Commission. Croatia sent its Notification on 27 June 2018. In its letter, Croatia provides information on the relevant GDPR articles that have been further specified in its domestic legal order.

With regard to the Law Enforcement Directive, the Commission sent a Letter of Formal Notice on 18 July 2018. On 30 July 2018, Croatia sent its Notification, thereby providing the Commission with the national law implementing the Law Enforcement Directive. The Commission officially closed the infringement procedure on 24 January 2018.

The Commission is currently assessing the Croatian national legislation further specifying the GDPR and the Croatian national legislation transposing the Law Enforcement Directive.

With regard to the Evaluation of Croatia on fulfilling the conditions necessary for the application of the Schengen acquis in the field of data protection, during the Council's Working Party on Schengen Matters (Schengen Evaluation) held on 13 February 2019, the Commission announced the successful closure of the Evaluation. The evaluation had taken place on 21 to 26 February 2016.

LINE TO TAKE

- My main objective here is to listen to you rather than to talk. I would like to understand better the opportunities and threats you see this year and the coming future and what role in your view the European Commission should play to help you.
- The global environment around us is changing considerably. The increasing trade tensions between the EU and China, but also between the EU and US are already having some impact, but I want to feel the temperature with you.
- How do you see the economic prospects in relation to countries in the Western Balkans region?
- Last year, the GDPR started to be applicable and I would like to hear from

your experience with these new rules.

- Finally, we have started a lot of discussions on the EU level on the future of business and labour markets, about the digital transformation, AI, automation, block chain. These things will present new opportunities, but also new challenges.
- I know that economic statistics for Croatia look good. You have decent economic growth, low inflation and strong consumption, but I used to have a small business myself so I know this macro data don't always correspond to the real situation on the ground.

On GDPR

- Mishandling of personal data such as in Facebook Cambridge Analytica case or the Facebook September data breach remind us that a strong framework for the protection of personal data is a necessity, not a luxury. In Europe, we made the choice for such a strong legislation, with the new General Regulation on Data Protection that came into application on 25 May 2018. The new legislation modifies and updates data protection rules at EU level to make Europe fit for the digital age.
- I know the GDPR created a lot of stress for companies, in particular for SMEs, also because there was a lot of false rumours about it. In fact, this is not a revolution, but an evolution, as we have data protection rules form 1994.
- The tech revolution creates a lot of uncertainty and the main aim of the GDPR is to ensure that people can trust the innovation.
- But it also promotes innovation by creating one set of rules for the whole EU and by promoting solutions that ensure privacy. This I hope can turn out to be our advantage when we compete with China and the US.

Getting feedback from stakeholders on the GDPR application

- In January 2018, we have issued guidance on GDPR in the form of questions and answers as well as several brochures published on our website. We have allocated grants to support Data Protection Authorities by co-financing their awareness-raising activities towards business, in particular SMEs, and citizens. These activities have started in the autumn and will continue in 2019.
- We are getting feedback from stakeholders on the application of the GDPR on the ground. We are also making use of the multi-stakeholder group on GDPR established last year, involving representatives from businesses, civil society, practitioners and academics.
- Collecting experiences on the practical application of the GDPR will feed into the preparation of the stocktaking event we will organise in June 2019. As foreseen by the GDPR, the Commission will report on the application of the new rules in 2020.

Beyond GDPR on AI and new tech

- For the European Union, it is important to achieve two goals together: one to ensure the take-up and development of the technology within the EU and two, to address people's fear and protect our citizens from the negative side effects.

- I think Europe has found a unique path when it comes to our regulatory approach. It is a liberal path, focused on giving people more control and more freedom, even in the online environment. It is a path where even the governments, or, especially the governments, have to respect limitations and safeguards when it comes to data processing of their citizens.
- But this is also a path where we want to support the innovation, as long as it based on the law or as long as people gave their consent.
- It is an advantage for the EU to be so advanced on modem privacy rules. Because it addresses the big mistrust people have to what's going online with their data.
- But legislation is not the only thing the EU is doing, despite maybe some myths.
- We are also promoting a self-regulatory, or voluntary actions by the companies. Here a good example is the Code of Conduct where we agreed with companies to remove illegal racist of xenophobic content from the platforms like Facebook or Twiiter
- There are also many studies that foresee a big change in the labour market, as many jobs will be replaced by automation and new jobs will appear, but we have to ensure this doesn't create more backlash from the society.
- I am open to hear your views on this and other issues.

DEFENSIVES

What will the Commission do if Member States' actions are late or not in compliance with the General Data Protection Regulation?

[LTT: COM will assess the need to start infringement procedures]

- Where Member States do not take the necessary actions required under the Regulation, are late in taking them or make use of the specification clauses provided for under the Regulation in a manner contrary to the Regulation, the Commission will make use of all the tools it has at its disposal, including recourse to the infringement procedure.

Will the opening clauses in the General Data Protection Regulation lead to fragmentation in the application of data protection rules in the EU?

[LTT: No, MS are to legislate within a strict legal framework; the COM as Guardians of the Treaty will ensure respect of the law]

- The Regulation gives Member States the possibility to further specify the application of data protection rules in specific fields, for example public sector, employment and social security, preventive and occupational medicine, public health, scientific or historical research purposes or statistical purposes, etc. In addition, for genetic data, biometric data and data concerning health, the Regulation empowers Member States to maintain or introduce further conditions, including limitations.

- However Member States' actions are framed by two elements: Article 8 of the Charter, and Article 16(2) TFEU under which national legislation cannot impinge on the free flow of personal data within the EU.
- When adapting their national legislation, Member States have to take into account the fact that any national measures which would have the result of creating an obstacle to the direct effect of the Regulation and of jeopardising its simultaneous and uniform application in the whole of the EU are contrary to the Treaties.
- In the summer 2018, we launched a study to look into the use of some of the specification clauses of the GDPR by the Member States. The results of the study are expected by the end of 2019.

(4)

From: TALKO Wojtek (CAB-JOUROVA)
To: [redacted](CAB-JOUROVA)
Subject: mission report from Zagreb - could you send to the DG?
Date: mardi 5 mars 2019 14:59:35

DAY 1

[redacted]

[redacted]

[redacted]

DAY 2

[redacted]

[redacted]

3) Meeting with business associations

Participants:
Croatian Chamber of Economy - Svjetlana Momciolovic
Croatian Employers Association- Davor Majetic and Milica Jovanoic

The representatives explained that GDPR is a big problem. In Croatia, economy is based on SMEs that don't have time or resources to comply with GDPR. They don't know where to start. They would want a kind of instruction what to do. They would need more time to adopt and expect the government to help with this.

They expressed concerns that without understanding the GDPR it is difficult to think about digitalisation and the single market.

They stressed they would need case studies and examples. DPAs are so general that it is not applicable by businesses.

In general, business environment in HR, SMEs complain about rapidly changing legal environment and long proceedings in front of the courts and taxes. Situation on labour market is difficult because a lot of people leave HR. HR is becoming less and less competitive also because of lack of investment and access to cheap credit.

VJ acknowledged the issues and promised to address them with the EDPB.

[redacted]

[redacted]

(5)

COMMISSIONER VĚRA JOUROVÁ

MEETING WITH HARALD KAYSER
PWC EUROPE CHAIRMAN AND SENIOR PARTNER

LOCATION: BERL 12/176

DATE AND TIME: 15/03/2019, 09H00]

MEETING OBJECTIVE: TO DISCUSS (I) GDPR; (II) GENDER ISSUES

MEMBER RESPONSIBLE: WOJTEK TALKO

DG CONTACT & TEL NO: [redacted]
DIRECTOR: EMMANUEL CRABIT

VERSION: 16/10/2019 12:12

JUST/123

PARTICIPANTS:

TABLE OF CONTENTS

STEERING BRIEF

CONTEXT

Harald Kayser is the Senior Partner and Chairman of PwC Europe. He is a German certified Tax Advisor and Public Accountant and held in the past (2015-2018) the post of Chief Digital Officer within PwC Germany.

On the basis of their websites, PwC provides extensive advisory services related to the GDPR.

The discussions will focus mainly on GDPR implementation.

OVERALL OBJECTIVES

(i) Inform PwC on the ongoing work by the Commission with regards to the GDPR and enquire on PwC experience in the area of data protection;

(ii) Discuss and inform about gender aspects related to digitalisation, in particular online violence and abuse against women.

TOPICS

TOPIC 1: GDPR

CONTEXT

The meeting is taking place roughly 10 months after the entry into application of the General Data Protection Regulation (GDPR).

On the basis of the PwC.com website and other national PwC websites, the company offers extensive advisory services related to the GDPR. PwC has developed a number of tools (example: technical solutions to manage data subject right requests, a completeness assessment tool (CAT) aimed at verifying whether the data controller is able or not to demonstrate compliance, breach readiness assessment tool (BRAT) aimed at ensuring that a data controller has the necessary organisational set up to reach to a data breach) in relation to the GDPR.

In 2016, PwC had created a Readiness Assessment Tool (RAT) aimed at gauging the data controllers data protection maturity in light of the entry into application of the GDPR.

Most of the PwC tools seem to revolve around the following four areas: (i) supporting and developing tools in relation to the role of the data protection officer; (ii) assisting data controllers in the eventuality of a personal data breach; (iii) assisting data controllers in relation to the accountability principle; (iv) assisting data controllers in relation to data subject rights requests.

PwC.com has a Data Protection and Privacy Blog; one finds a variety of issues such as on the role of the data processor, guidance on data protection impact assessment, Brexit and its impact on data flows from and to the UK, AI and GDPR and other relevant topics. The impression one gets reading these blogs is that PwC supports the GDPR in the sense that they view the law as an opportunity to be seized by the companies to increase trust. In one particular blog, issued a year prior to the entry into application of the GDPR, PwC provides reasonable guidance by, for example, stating that PwC does not expect DPAs to start fining as of the 26 of May 2018.

OBJECTIVE

- Stress the importance of the General Data Protection Regulation and of its proper application, in particular in the light of events such as Facebook/Cambridge Analytica and Facebook data breach.
- Inform about the next steps for the Commission, in particular its monitoring of the proper application of the General Data Protection Regulation by the Member States.
- Inquire about their assessment of the GDPR and feedback they get from their clients.

LINE TO TAKE

- We are roughly 10 months after the entry into application of the GDPR. Our efforts now focus on the proper implementation of the GDPR in national law and supporting the new governance system put in place by the GDPR, with at its centre the EDPB and the DPAs. Events such as the Facebook/Cambridge Analytica case demonstrate the importance of the protection of personal data not only for individuals but also for the functioning of our democratic societies as a whole.
- To-date, [24] Member States have adopted their national legislation implementing the GDPR [AT, DE, FR, HR, NL, SE, SK, DK, UK, PL, IE, MT, LT, LV, RO, HU, BE, LU, CY, IT, FI, ES, EE, BG]. On 25 May 2018, the Commission sent letters to the Member States to remind those who are not yet ready of the need to adopt their national laws without delay.
- COM is in the process of analysing the national legislations which have been already adopted by Member States. Our services are in close contact with national authorities. We will take appropriate actions as necessary, including the recourse to infringement actions.
- We made our approach on the monitoring of the application of GDPR very clear in the Communication on GDPR on 24 January 2018 and in the Communication on 'Completing a trusted Digital Single Market for all' on 15 May 2018.

[Working with EDPB and actions by DPAs on GDPR application]

- In parallel, we pursue our active contribution to the work of the European Data Protection Board whose guidelines are of key importance to help stakeholders implement the GDPR. It is essential for the data protection authorities to forge a common EU approach.
- From what we hear from Data Protection Authorities, there has been an increase in the number of complaints they received since the entry into application of GDPR. More than 95,000 complaints have been lodged with national data protection authorities since 25 May 2018 and more than 45,000 data breaches have been notified.
- As concerns cross-border cases, there are around 281 cross-border cases cooperation procedures ongoing. 444 procedures relating to Mutual Assistance have been triggered. 642 procedures have been launched to identify the lead and the concerned Supervisory Authorities.

[Getting feedback from stakeholders on the GDPR application]

- Equally, the Commission is open to get feedback from stakeholders on the application of the GDPR on the ground, in particular in the context of the multi-stakeholder group on GDPR established last year, involving representatives from businesses, civil society, practitioners and academics.

- As announced by Commissioner Jourová and in the Communication of 24 January 2018, the Commission will organise a stock-taking event in June. Collecting experiences on the practical application of the GDPR will feed into the preparation of that event we will organise around June 2019. As foreseen by the GDPR, the Commission will report on the application of the new rules in 2020.

BACKGROUND

- **GDPR**

The General Data Protection Regulation together with the Data Protection Directive for Police and Criminal Justice Authorities ("Police Directive") form the "data protection reform" package. The GDPR entered into force on 24 May 2016 and applies since 25 May 2018 directly in all Member States. The Police Directive entered into force on 5 May 2016 and EU Member States had to transpose it into their national law by 6 May 2018.

The European Data Protection Board has endorsed a number of guidelines, which have been already adopted by the Article 29 Working Party ahead of the application of the GDPR, and adopted further guidelines on key aspects of the GDPR and will pursue this task in the future.

<table>
<tr><td colspan="2">Guidelines/working documents by the European Data Protection Board[1]</td></tr>
<tr><td>Right to data portability</td><td rowspan="3">Adopted on 4-5 April 2017</td></tr>
<tr><td>Data protection officers</td></tr>
<tr><td>Designation of the lead Supervisory Authority</td></tr>
<tr><td>Data protection impact assessment</td><td rowspan="2">Adopted on 3-4 October 2017</td></tr>
<tr><td>Administrative fines</td></tr>
<tr><td>Profiling</td><td rowspan="4">Adopted on 6-7 February 2018</td></tr>
<tr><td>Data breach</td></tr>
<tr><td>Adequacy referential</td></tr>
<tr><td>Binding corporate rules for controllers</td></tr>
</table>

[1] All adopted guidelines are available at: http://ec.europa.eu/newsroom/just/item-detail.cfm?item_id=50083

Binding corporate rules for processors	
Consent	Adopted on 10-11 April 2018
Transparency	
Certification	Adopted on 22 January 2019 – Annex subject to public consultation until 29 March 2019
Accreditation	Adopted on 4 December 2018 – Annex subject to public consultation until 1st February 2019
Codes of Conduct	Adopted on 12 February 2019 and subject to public consultation until 2 April 2019
Derogations for international transfers	Adopted on 25 May 2018
Territorial scope of the GDPR (Article 3)	Preliminary adoption on 23 November 2018 – public consultation concluded on 18 January 2019

The following is a list of topics enlisted in the EDPB's Work Program for 2019/2020: Guidelines on Codes of Conduct and Monitoring Bodies; Guidelines on delisting; Guidelines on PSD2 and GDPR; Guidelines on international transfers between public bodies for administrative cooperation purposes; Guidelines Certification and Codes of Conduct as a tool for transfers; Guidelines on Connected vehicles; Guidelines on video surveillance; Guidelines on Data Protection by Design and by Default; Guidelines on Targeting of social media users; Guidelines on children's data; Guidelines on reliance on Art. 6(1) b in the context of online services; Guidelines on concepts of controller and processor (Update of the WP29 Opinion); Guidelines on the notion of legitimate interest of the data controller (Update of the WP29 Opinion); Guidelines on the powers of DPAs in accordance with Art. 47 of the Law Enforcement Directive.

- **Brexit** (since PwC's Data Protection and Privacy Blog contains articles on the issue of Brexit, the following may be useful)

With the United Kingdom's exit from the European Union, it will become a third country. The disclosure/communication of personal data from business operators or public authorities in the EU/Member States to recipients in the UK would thus in principle be treated as international data transfers, unless the EU and UK conclude a Withdrawal Agreement establishing a transition period during which the EU acquis would continue to apply. In this case, the UK would (for the transition period) be treated like an EU Member State and EU data protection law (with the exception of the rules on the ICO's participation in the EDPB and the consistency mechanism) would continue to apply, meaning that personal data could be exchanged from the EU to the UK as between Member States.

In case of a no-deal scenario, entities in the EU will have to comply with the rules

on international transfers when sending personal data to the UK. While the Commission set out a number of "preparedness" measures in its Communication of 19 December 2018 (COM(2018)890), adequacy is not one of the contingency measures. The European Data Protection Board has issued a guidance paper on transfers of personal data to the UK in case of a no deal Brexit (https://edpb.europa.eu/sites/edpb/files/files/file1/edpb-2019-02-12-infonote-nodeal-brexit_en.pdf).

As part of its 'no deal' preparedness, the UK has adopted a "statutory instrument" that among other things contains transitional provisions on the "roll over" of existing Commission adequacy decisions and Standard Contractual Clauses into UK law and would allow the free flow of data to the EU-27.

DEFENSIVES

Will the specification clauses in the General Data Protection Regulation lead to fragmentation in the application of data protection rules in the EU?

- The Regulation gives Member States the possibility to further specify the application of data protection rules in specific fields, for example public sector, employment and social security, preventive and occupational medicine, public health, scientific or historical research purposes or statistical purposes, etc. In addition, for genetic data, biometric data and data concerning health, the Regulation empowers Member States to maintain or introduce further conditions, including limitations.

- However Member States' actions are framed by two elements: Article 8 of the Charter, and Article 16(2) TFEU under which national legislation cannot impinge on the free flow of personal data within the EU.

- When adapting their national legislation, Member States have to take into account the fact that any national measures which would have the result of creating an obstacle to the direct effect of the Regulation and of jeopardising its simultaneous and uniform application in the whole of the EU are contrary to the Treaties.

- In the summer 2018, we launched a study to look into the use of some of the specification clauses of the GDPR by the Member States (such as the specification clauses in the field of health or scientific research). The results of the study are expected by the end of 2019.

What will the Commission do if Member States' actions are late or not in compliance with the General Data Protection Regulation?

- Where Member States do not take the necessary actions required under the Regulation, are late in taking them or make use of the specification clauses provided for under the Regulation in a manner contrary to the Regulation, the Commission will make use of all the tools it has at its disposal, including recourse to the infringement procedure.

•

Aren't the sanctions foreseen in the GDPR too high? 4% of annual turnover of a company is disproportionate.

- What we have learned from the many recent scandals (Uber data breach, Facebook Cambridge Analytica) is that violations of privacy rules can be very harmful for individuals and for the society as a whole. We need to get serious about data protection compliance and enforcement. As in other areas of law, this requires credible and sufficiently deterrent sanctions.
- The GDPR establishes a range of enforcement tools, from warning to penalties and fines. All these tools must be effective, proportionate and dissuasive. The agreement on fines ensures that they are a deterrent. Each case must be determined in light of its specific circumstances and taking into account 11 different factors listed in the Regulation, including the :
    - gravity/ duration of the violation;
    - number of data subjects affected and level of damage suffered by them;
    - intentional character of the infringement;
    - any actions taken to mitigate the damage;
    - degree of co-operation with the supervisory authority.
- The GDPR sets out two main categories of ceilings of fines for infringements of the Regulation, depending on the gravity of the infringements (2% or 4% of worldwide turnover). These ceilings, as there are expressed in percentage of the company's turnover, ensure that the fine will always be proportionate to the economic weight of the concerned company.
- These are ceilings, meaning maximum amounts. There will therefore apply only to the most serious violations which have taken place over a long period of time, have affected a large number of individuals etc.
- Finally, credible sanctions give value to compliance (compared to a situation where only symbolic sanctions meant that complying or not with data protection rules did not really matter) and avoid situation of free riders (which has just relying on and benefiting from the compliance efforts of others).

GDPR and the FB-Cambridge Analytica scandal

How can EU data protection rules prevent this in Europe?

- There are clear rules in place (1995 Directive), which have been further strengthened since 25 May with the new General Data Protection Regulation.

- The issues these revelations raise relate for instance to data protection principles like lawfulness, fairness and transparency and purpose limitation. They are regulated since 1995.

What would change with the GDPR if such a situation would occur in the future?

- The GDPR harmonises the notion of consent, previously interpreted differently throughout the EU. Consent under the GDPR must be given by a clear and affirmative action. The GDPRs rules out tacit forms of consent (silence, pre-ticked box etc.)
- The GDPR clarifies and develops the transparency obligations, i.e. the information that should be given in a clear and understandable way to individuals on which of their data is processed, for which purposes, whether the company intends to share it with a third party, to transfer it abroad etc.
- Furthermore under the GDPR the conditions under which the personal data can be further shared ("further processed") have been clarified and harmonised.
- The GDPR introduces rules on data breaches, provides when individuals need to be informed when their data has been lost, stolen, hacked or subject to other type of security incidents.
- GDPR reinforces the enforcement mechanisms. It strengthens the role of national data protection authorities by providing Data Protection Authorities (DPAs) with better means of cooperation, clearly dividing the competences between them in cases of cross-border processing, and harmonising their enforcement powers, including the power to impose fines.
- New cooperation tools between supervisory authorities have been created, including the setting up of a European Data Protection Board (EDPB) which will provide guidance and ensure one interpretation in case several Member States are concerned across the EU.
- The GDPR provides also for clear rules for division of competences in cases where the controllers are active in several Member States establishing a "lead supervisory authority" and "other concerned supervisory authorities".

What will the Commission do about the Facebook / Cambridge Analytica case?

- This case highlights the relevance of the new EU-wide data protection rules set by the GDPR. These rules focus on making companies more accountable, more responsible in how they deal with our data.
- The Commission has been in close contact with both the Chair of the EDPB and the Chair of the UK ICO (the UK data protection authority) who has been leading the investigation on Cambridge Analytica since this company is based in the UK. We fully supported the coordinated response of the EU data protection authorities.
- We take note that the ICO released in October its full report and imposed a maximum £500,000 fine on Facebook for two breaches of the Data Protection Act 1998. We understand that Facebook has appealed the fine, which case is

now pending before the UK Court of Appeal. We are awaiting the Court's decision in this case.

Will it still be possible to transfer personal data to the UK in a no deal scenario (and in the absence of an adequacy decision)?

[Yes, different instruments are available to transfer personal data to third countries, which are already widely used with most other countries in the world]

- Yes.
- In case of a no deal scenario, the rules on international transfers under the GDPR and the Law Enforcement Directive will apply to transfers of personal data to the UK as of the withdrawal date.
- The GDPR contains different tools for data transfers to third countries. This includes so-called "appropriate safeguards", which can be provided by, for instance, Standard Contractual Clauses, Binding Corporate Rules and administrative arrangements. In addition, a number of derogations for specific situations exist that allow transfers even in the absence of appropriate safeguards, e.g. with the explicit consent of the individual, for the performance of a contract or when necessary for important reasons of public interest.
- Similar tools are available under the Law Enforcement Directive (e.g. when a legally binding instrument provides for appropriate safeguards). In addition, transfers may take place when an EU entity concludes following a (self-) assessment that such safeguards exist.
- These tools are already being used with most countries in the world for which there is no adequacy decision.

When will the Commission start its adequacy assessment?

[In case of a no-deal Brexit, the Commission will have to decide whether to engage in adequacy talks. Such talks can only start its adequacy assessment once the UK exits the EU]

- In a deal scenario (with Withdrawal Agreement), the Commission is committed to start adequacy talks as soon as the UK exits the EU. We cannot start the assessment while the UK is still a Member State. As regards the completion of the assessment, the Commission shares the UK's interest in ensuring that an adequacy finding is in place by the end of the transition period. We are committed to this objective and will work very hard to make this possible.
- In a no-deal scenario, data transfers could be based on the other available transfer tools, in particular contractual tools (for the commercial field) and the so-called derogations (both in the commercial field and for transfers from EU/MS authorities). This is not different from the situation with most other countries in the world. An adequacy finding is not part of the contingency planning, and it would have to be assessed whether this is an appropriate avenue to pursue in the future.
- In any event, the threshold for an adequacy finding ("essential equivalence") is high, both when it comes to the rules applicable to commercial operators and with respect to the limitations and safeguards applicable to public (UK) authorities, in particular in the area of criminal law enforcement and national

security. Given the strong political and legal scrutiny, this has to be carefully assessed.

- We have already noticed certain differences between the GDPR and the UK's Data Protection Act. For example, the UK provides for broad exceptions on most data subject rights in the area of immigration.

There should be an enforcement moratorium, because companies in the EU do not have enough time to prepare for a no-deal Brexit.

[The GDPR does not allow for an enforcement moratorium: complaints from individuals will be dealt with by the DPAs. Different tools are available for companies to transfer personal data, including model clauses.]

- The data protection authorities are bound by the GDPR and have to handle complaints they receive from individuals. In another case (the application of the GDPR to ICANN/WHOIS databases) the DPAs have made clear that the GDPR does not allow for an enforcement moratorium. Data protection is a fundamental right and individuals may submit complaints to their DPA when they consider their rights under the GDPR have been violated.

Despite the Commission's efforts to negotiate the Withdrawal Agreement, the risk of a no deal Brexit has always remained. Companies therefore had sufficient time to prepare for this possibility. Standard Contractual Clauses are available, which have been approved by the Commission and do not require any additional approval by national data protection authorities. These model clauses have existed for many years and are widely used, including by UK commercial operators for their transfers outside the EU.

ANNEX – GDPR STATISTICS

Statistics in the Member States

Nearly all national data protection authorities report higher (in some cases doubled) workload since the new data protection rules came into force on 25 May.

- Since then, EU citizens submitted at least **95 500 data protection complaints** to the national authorities.
- There were at least **40 000 data breaches** notifications across the EU.
- **Fines** are starting to be imposed: by DPA in the German state of North Rhine-Westphalia, by Austrian DPA, by FR DPA (CNIL).
- Only a few codes of conduct have been officially submitted to Data Protection Authorities pursuant to Article 40 of the GDPR.

National Complaints by countries: (period covering 25 May till 25 January 2019)

France: 7293 complaints
Germany: 27 112 complaints
Estonia: 252 complaints
Romania: 2922 complaints
Belgium: 234 complaints
Czech Republic: 2200 complaints

Denmark: 800 complaints
Cyprus: 130 complaints
Latvia: 1206 complaints
Lithuania: 339 complaints
Luxembourg: 351 complaints
The Netherlands: 3000 complaints
Slovenia: 598 complaints
Sweden: 1400 complaints
Italy: 4704 complaints
UK: 25 791 complaints
Ireland: 1559 complaints
Greece: 562 complaints
Spain: 5500 complaints
Malta: 35 complaints
Austria: 755 complaints
Finland: 8210 complaints

Note that the data from the different countries are not entirely comparable; for instance, some DPAs reported all kinds of actions taken and not only complaints received.

[Source: EDPB, Survey Workload SA, 25/01/2019]

EDPB cooperation mechanisms

There are currently **281 cooperation cross-border cases in the case register.** The breakdown of these is below:

- **194** have been initiating as a result of a complaint;
- **87** cases originating from other sources such as an investigation, a SA initiative, a legal obligation, a media report etc.

From the above cases, the following procedures have been triggered:

- **444** procedures relating to **Mutual Assistance** (Art 61). These procedures may lead in the future to One-stop-shop procedures;
- **45 One-stop-shop procedures** (Art 60) from which **6** are **Final ecision, 16 Draft Decisions, 23 Informal Consultations;**
- **25 Local Case Requests** (Art 56.2);
- **Consistency procedures**: **30** Art.64 procedures, **29** of them concern the DPIA lists.

In addition, **642** procedures have been launched to **identify the lead and concerned SAs** (Art 56.1) (**306** closed). With the number of Art. 56 procedures is less relevant, because at this stage it is still not concluded that a case exists (it may also be possible that several parallel procedures to find a Lead SA will combine into 1 single case; or that a procedure will lead to any case at all (i.e. absence of cross border dimension)).

[Source: EDPB, first overview on the implementation of the GDPR and roles and means of national supervisory authorities, 26/02/2019]

COM Eurobarometer on data protection in elections

Data protection will remain one of the key aspects of the next year's elections. The results of the Eurobarometer show that more than two thirds (67%) of respondents are concerned that the personal data people leave on the Internet could be used to target the political messages they see. 26% are 'very concerned' about this.

[Source: COM press release, 23/11/2018]

Contact: [redacted]

Contact: [redacted]

Quality and language control: [redacted]

TOPIC 2: GENDER ISSUES

OBJECTIVE

Discuss and inform about gender aspects related to GDPR and digitalisation, in particular online violence and abuse against women.

LINE TO TAKE

- Online violence and harassment disproportionately affect women and girls and new forms of online harassment constantly emerge. In addition, women who have experienced violence in real life are often targeted by online violence by the same perpetrators.
- We are also experiencing a global backlash against women's rights and in this context, online harassment has the effect of silencing women and limiting their participation in society, in particular in politics.
- At the 2018 Annual Colloquium on Fundamental Rights on "Democracy in the EU", various participants raised the need for the Commission to address online harassment of women who are in decision-making positions, in particular of women politicians. This issue will be particularly topical in the context of the upcoming European elections.
- EIGE estimates that one in ten women have experienced a form of cyber violence since the age of 15. FRA's study from 2014 on violence against women covered also several forms of online violence and is still referred to as one of the main data sources on this topic. It is still generally agreed that more data on online violence against women is needed. That is why we are now working, together with Eurostat, on an EU-wide survey.
- In May 2016, the Commission launched the "Code of conduct on countering illegal hate speech online" together with Facebook, Microsoft, YouTube and Twitter. We have been happy to see that platform providers have cooperated on countering racist and xenophobic hate speech.
- The approach of this Code of Conduct has been successful, in particular in combination with measures facilitating cooperation between the voluntary stakeholders, such as the platforms and NGOs. The latest results on the application of the Code of Conduct from January 2018 are very positive, with more than 70% of the manifestly illegal content having been removed, and increasingly rapidly.
- At the moment, no EU rule explicitly prohibits online violence against women. It nevertheless is covered by the Istanbul Convention's provisions prohibiting psychological violence, stalking and sexual harassment. So far, 20 EU Member States have ratified the Convention and the EU's accession is ongoing.
- Most forms of online violence have been criminalised or otherwise prohibited in the Member States, in particular as part of the implementation of the Istanbul Convention in the Member States. Due to the lack of international definitions, however, the national prohibitions vary considerably and cover different acts that can be classified as online violence or abuse.

- To improve the protection of victims, we are currently looking at ways in which we could more explicitly address online violence against women and girls. I believe there is room to do more with the online platforms using the Code of Conduct as a model and the platforms have tentatively indicated interest in pursuing such idea.
- The Commission (DG CNECT) is also working on gender equality aspects in communication networks, contents and technology – to get "More Women in Digital", including awareness raising and tackling gender stereotypes in the ICT sector, which are often mentioned as one of the root causes of online violence against women.

Contact: [redacted]

ANNEXES

Curriculum Vitae

Harald Kayser is the Senior Partner and Chairman of PwC Europe SE and was elected with effect from 1 July 2018.

He was a member of the Executive Board of PwC Germany from July 2010 to June 2018 and Chief Operating Officer/Chief Digital Officer (2015-2018) as well as Assurance Leader (2010—2015) of the German firm. He joined the Global Assurance Leadership Team in 2010 where he represented PwC Germany until 2015. He also served as Chief Operating Officer of PwC Europe and as member of the PwC Global Network Operations Team.

From 2007 to 2014 Harald was the Global Relationship Partner for a leading global automobile manufacturer. Prior to this term, he served as the Automotive Cluster Leader, Europe (2009) and Head of the Automotive Segment in Germany (2008). From 2002 to 2007 he had been appointed Global Relationship Partner for a leading global automobile components manufacturer.

Harald is a German certified Tax Advisor and Public Accountant. In 1992 he obtained a degree in Economics following a period of studies at Lüneburg University and Tübingen University in Germany. Harald joined PwC Germany in 1992 and was admitted to the partnership in 2001.

Harald lives in Hanover with his wife and two children. He likes skiing, football and playing tennis.

(source: https://www.pwc.com/gx/en/about/leadership/harald-kayser.html)

(6)

To: TALKO Wojtek (CAB-JOUROVA); CRABIT Emmanuel (JUST);[redacted]

Cc: [redacted](JUST);[redacted](JUST);[redacted](JUST);[redacted](JUST);[redacted](JUST);[redacted](JUST);[redacted](JUST);[redacted](JUST);[redacted]JUST)

Subject: Flash Report: Meeting between Commissioner Jourová and Harald Kayser PwC Europe Chairman, 15 March 2019

Dear all

Kindly find below the Flash Report of the Meeting between Commissioner Jourová and Harald Kayser PwC Europe Chairman, held on 15 March 2019.

Mr. Kayser described the GDPR as a huge success and that it has set golden standards on a global level. Normally, it was US legislation that would set the norm, and others followed; he cited US legislation in the field of audit and in the field of sanctions. In the case of data protection, the GDPR has turned the tables, whereby other jurisdictions are now trying to establish rules similar to the EU ones. He observed that while US legislation was normally rule-based, prescribing in detail the framework and its rules, EU legislation, notably the GDPR, was more principle-based. With regards to the concrete application of the GDPR, Mr. Kayser explained that PwC services were in high demand. PwC has set up tools- mainly for SMEs- and helped multinational companies restructure their governance model in order to comply with the GDPR. The PwC clients varied from SMEs, to multinationals to public authorities. Mr. Kayser explained that they did not offer services to political parties, hence remaining neutral, and did not advise Governments in the drafting of legislation. Mr. Harald touched upon the issues of Blockchain and AI and their respective compliance with GDPR. He called for clear guidelines on the issue of Blockchain and GDPR, especially on the issue of the right to be forgotten and its compatibility with Blockchain. With regard to AI, Mr. Kayser stated that AI worked better when fed with data. In this context, China seemed to have a competitive advantage since processing of personal data was not considered a fundamental right. Mr. Kayser concluded by stating that PwC saw the usefulness of the different tools found in the GDPR to promote compliance, notably Certification and Standard Contractual Clauses.

Commissioner Jourová agreed that the GDPR was a game changer and that it has established global standards. The recent Cambridge Analytica scandal touched people and society on a world-wide basis and are now more aware of the need to protect personal data. She noted that while there may be different legislative techniques between the US and the EU, the most important factor was the end result. Here, the US Cloud Act and the Commission e-Evidence Proposal was cited as an example. With regards to the concrete application of the GDPR, Commissioner Jourová explained that the Commission was currently reviewing the Member State Data Protection Laws which further specify the GDPR, was involved in the EDPB structure and is preparing a One-Year Stock-Tacking event on GDPR to be held in June 2019. Commissioner Jourová explained that the Commission and the EU represents a high level of personal data protection. The experience with Japan, China's neighbor, underlined the importance to ensure a high data protection standard. Protecting personal data ensured trust and thus, in the long run, the competitive advantage argument could be seen in a different light. During the meeting, PwC was informed that the EDPB was currently reflecting on the need to produce Guidelines on the issue GDPR-Blockchain and that this issue was listed as 'Possible' in the EDPB Work Program 2019/2020, and that the Commission was internally reflecting on the way forward with regards to the different tools found in the GDPR, in particular Standard Contractual Clauses.

[redacted]

European Commission
DG JUST. C3

[redacted]

Twitter: https://twitter.com/EU_Justice

Cabinet of Vice-President ANSIP - Minutes of Meeting

MEETING CONCLUSIONS

Title	**Minutes of roundtable with platforms**
Date	**19/03/2019**
Participants	**Participants from the platforms:** representatives of Google, Facebook and Twitter **Participants from the Commission:** VP Ansip, Commissioners King, Jourova and Gabriel
Issues raised & follow-up	VP Ansip introduced the discussion and explained that each Commissioner would discuss in particular the following issues: (i) compliance with the code of practice (Gabriel); (ii) political advertisement in the run up to the EU elections (Jourova); (iii) cooperation with fact-checkers and researchers (King). **1- Compliance with the code of practice** Commissioner Gabriel stressed that more efforts are needed from all platforms in particular on (a) bringing on board more signatories to the code of practice/other players; (b) developing KPIs/clear metrics to better assess the results achieved by each platforms; (c) cover all the Member States (Facebook for instance is for the time being only covering 6 Member States) and provide also a breakdown by Member State of the results achieved. Google stated that compliance with the Code of Practice is important for a company that builds its success over users' trust and public image. It is willing to bring other (smaller) platforms on board but the Commission should help on this by facilitating exchanges among stakeholders and public/private partnerships. As for KPIs/metric, Google has done some efforts in the latest report which seem to be appreciated by the Commissioner, but further input by the Commission on how to shape KPIs/metrics would be helpful to deliver even better. Facebook stated that setting the standards is a way to help smaller platforms to be on board of the initiative. They explained that for the time being they focused on developing the tools to deliver (e.g. AI powered mechanisms to detect inauthentic behaviour, how to better the ad transparency tools to extract the data requested by the Commission), but they will focus now their efforts on improving the reporting in particular in terms of KPIs and metrics. They promised that the next report will show a huge improvement. They explained the difficulty on fake accounts is that they are quickly recreated and it is difficult to eliminate them completely. They explained their work with detecting inauthentic behaviour. They will continue their effort to cover all Member States and improve the breakdown by Member States of the relevant data. Twitter explained their work so far done in particular on transparency, but took note of the need to step up their efforts on different fronts. **2- political advertisement in the run up to the EU elections** Google explained that they put in place a "verification system" aimed at ensuring that only entities established within the EU can upload political advertisement on their platforms (therefore no third country entity is allowed to do so). The enforcement of this system will begin this week and the results (e.g. name of the advertisers, breakdown by Member State targeted by the ads) will be available in the next report. They are also training campaigners and reaching out to Member States to improve their cybersecurity tools. They have access to data on the

sponsors of the ads, but they cannot have access to data on who is funding the parties. This is a competence of the national authorities and they can ask the national authorities to share this info with the platforms (Commission support would help for this). Similar message was reiterated by all platforms.

Facebook explained that they intend to put in place a verification system on a national basis. This system would prevent an entity established in one Member State from uploading political ads referred to/targeting another Member State. However, this would be the safest approach from a legal point of view taking into account the constraints of national legislation.

Twitter stated that they are still working on that.

3- cooperation with fact-checkers and researchers

Commissioner King asked the platforms on their current cooperation with fact checkers and researchers and whether there are ways to improve it and make it more effective (in particular by allowing access to APIs of the platforms, what was the platforms thinking on initiatives like correct the record etc).

Google stated that they are working with the international network of fact checkers. They are also looking on how to expand their cooperation with both fact checkers and researchers. However they would like to receive from the Commission input on how better to develop the approach to this cooperation (e.g. possible involvement also of small organisations). They explained also their media literacy initiatives specifically aimed at journalists. They had mixed views on whether it is better, in terms of impact on the public, to correct the disinformation or just flag it as such.

Facebook explained their work on fact checkers but also their difficulties in selecting reliable ones.

Twitter explained the reasons of its delay and difficulties of working with fact checkers and that they are only working with small and individual ones.

The three stated that they would need to reflect on the possibility to allow the researchers in their internal organisation and cooperate with them to develop better tools.