The General Data Protection Regulation - Issues for the Trilogue, 13th May 2015

This Digital Forum seminar, in cooperation with TechUK and the Coalition for the Digital Economy (COADEC), discussed the main issues likely to be debated during the upcoming trilogue on the General Data Protection Regulation (GDPR) later this year. One particular aim of the seminar was to bring start-ups and entrepreneurs together with regulators to highlight issues faced by small businesses in the context of data protection reform. While the first panel echoed the perspective of start-ups and entrepreneurs on the challenges they face with data management and compliance, therefore questioning the implementability of the GDPR, the second panel gathered officials and representatives from EU institutions in order to give a fresh update and take stock of the evolution of the negotiations.

Panel 1: Challenges of data protection for startups and SMEs

The team of entrepreneurs urged regulators to provide them with legal clarity and questioned the extent to which explicit consent should be balanced with legitimate interests for companies that want to develop useful solutions and personalised services to their customers.

Nathan Salter (COO, OMG) stressed the need to adopt rules on a case-by-case basis and distinguish innovative data analytics from aggressive profiling, unfair tracking and price discrimination practices. His company provides performance marketing and advertising services and typically uses anonymous data. They use IP addresses to count and evaluate the number of generated sales, not to identify end-users. The risk of overly restrictive regulation is that it could hamper the development of the Internet advertising and marketing industry, a source of exponential growth in the EU. In the particular case of OMG, getting consent from every user is unrealistic and meaningless given the amount of data involved. Legislation should rather envision a mechanism for users who want to avoid personalised ads and so-called retargeting practices, but in his view, the risk now is to put an entire industry out of business. Instead, he called for a compromise through self-regulation and co-regulation mechanisms.

Shraddha H. Shetty (CEO, RK Trans2cloud) also advised that the regulatory response should be proportionate to the potential harm to avoid the risk of over-estimation. Her company provides cloud services from data and metadata management and storage services, striving to ensure privacy by design settings and providing to the client a high standard of security. Hence she called for a better analysis of the new business practices to lead policymakers' decisions.

Raphael Van Assche (Managing Consultant, Tunstall Healthcare) outlined how his company provides technology-enabled services to vulnerable, fragile and elderly people such as social alarms, telemedicine and various e-health services. Claiming they would not use profiling for commercial use or price discrimination, instead he explained the rationale lying behind the analysis of patients' behaviours to provide safety and caring services. Trust and confidence, in his view, should be enshrined in regulation in order to avoid suspicion and ensure better perspectives for e-business development in Europe. A greater harmonisation of rules at EU level would help to build a proper European e-health sector, ensure legal certainty to the data-centres spread out across Europe.

Andrey Dokuchaev (COO, Clausematch), representing a utility platform for contract negotiations, follows the evolution of the regulation as they use a lot of data and personal information in order to provide their clients with the most efficient guidance service. The GDPR would provide joint reliability between data controller and data processor, however he thought that the new regulations should not add burdensome procedures because start-ups are already subject to heavy compliance costs such as security requirements, financial management rules and so on.

Aneesh Varma (Founder, Aire), built his company to enable access to financial products, based on algorithms and data mobility. He notably insisted that confidence is a must in his field. In addition, seeing his customers apply for financial services, most of the job consists in profiling. Nevertheless, if clients are convinced that the algorithms are flawed and their data could be used in a harmful way, the activity will not thrive.

Panel 2: Issues for the Trilogue

Beyond the traditional protection versus innovation dilemma, a unified regulation under the Digital Single Market will help data controllers and users to understand their rights and obligations, and will prevent companies from circumventing the rules by locating their main centre of operation in a country with weak data-protection standards. In addition, the GDPR will mean that EU data protection law is valid whenever the European market is targeted – whether from within or outside of the EU. However, the Council and the European Parliament (EP) have conflicting positions on many provisions, including the sensitive "informed consent" issue, set out as a cornerstone by the EP. This principle would require users to be informed about any collection and processing of their data – they must be able to explicitly agree or reject it. Technical standards framing tracking and profiling practices still have to be clarified, notably in view of the EP's willingness to narrow down the so-called 'legitimate interest', where a private company can use personal data without any kind of consent.

Michal Boni (MEP) insisted on the fact that the 16 initiatives of the DSM strategy should have a significant impact on the trilogue discussions. Points focusing on trust and confidence are critical to ensure users' fundamental rights while unleashing innovation potential in the EU. Combined with the review of the privacy directive, the adoption of the GDPR would shape a concrete continental privacy package as an important signal especially in the context of the transatlantic negotiations and revision of the Safe Harbor act. The GDPR should undoubtedly strike the right balance between business interests and users' protection, but should also be easily implementable for SMEs that cannot afford additional red tape. In this respect, the analysis of new data-business models is essential. He also firmly pointed out the question of ownership of data, in particular for sensitive data, and stressed the need to adjust the requirements to each area instead of adopting one-size-fits-all rules. For instance in the e-health sector, secured processing and data portability are important to prevent any misuse whereas in some other sectors the sensitivity of data is lower, and the development of new applications should not be hampered by burdensome regulation. In some cases, some solutions could be found with more flexible regulation and soft laws (codes of conduct, certification scheme and good practice guidance). Pointing out the Commission's better regulation agenda, Mr Boni mentioned the critical need to conduct ex-ante impact assessments but also ex-post evaluations of legislation to assess how implementable are the rules for small businesses. Thus, data collection and policy analysis are critical for adopting evidence-based policies.

Kevin O'Connell (Member of Commissioner Věra Jourová's Cabinet, European Commission) gave his own view on the evolution of the legislative process since the first Commission's proposal in 2012. The initial reform proposed during the previous Commission underlined the need to empower EU citizens, and give greater clarity on data protection laws for all parties involved. The new agenda adopted by this College of Commissioners encompasses a global review of EU rules to improve regulation also for start-ups and entrepreneurs, from e-commerce rules to the revision of the VAT system. Some key aspects have already been agreed by the three institutions such as the nature of the legislative act to reach a greater harmonisation of Member States' laws. He pointed out that the GDPR was certainly the most important variable of the whole DSM strategy, and symbolises the risk of holding back entrepreneurs who have chosen to invest in Europe. Those talents should be given the chance to scale up without moving abroad to achieve success. His cabinet has been studying new kind of business models and routes for innovation; they notably studied the potential impact on start-ups' data-business models to assess the feasibility of the proposal. Being aware of the opportunities offered by digital innovation entails a proportionality principle: some data do not require any consent because it does not put any privacy aspect at stake. Instead, innovative solutions should be found as a compromise to instate more clarity at each stage of the value-chain. Mr O'Connell called for clarifying many areas such as traceability and profiling or tracking practices: setting clear standards in these areas would be beneficial for both users and companies.

Baiba Jugane (Justice Counsellor, Permanent Representation of the Republic of Latvia) enumerated the main steps forward achieved during the Latvian presidency. One of the main achievements was the agreement on the one-stop-shop mechanism for data protection, allowing a company to speak with the regulator of the country where they have their EU headquarters and giving lawful access to the entire EU market on the same basis. In her view, Chapter II on data processing was one of the most debated horizontal issues. She underlined the efforts made to speed up negotiations before the end of the Latvian mandate but expected it would take until the end of 2015 before a consolidated version would be agreed. In her view, the data-subject should be put at the heart of the discussions to ensure their fundamental rights while ensuring the development of the internet-based economy with non-burdensome

regulation, especially regarding machine-to-machine data transfers and text and data mining in order to enable Europe to develop cutting-edge technologies. In her view, over-estimating the matter of consent is dangerous for the future of innovation in the EU; instead technological standards have to ensure that data are not unlawfully breached or harmfully used.

Laure Wagener (Counsellor, Permanent Representation of Luxembourg to the EU) showed her support to her Latvian colleagues in the attempt to reach a broad compromise allowing Europe to reap the benefits from the digital ecosystem without leading to a race to the bottom to the detriment of the data-subject's fundamental rights. In this respect, she shed light on the many single market issues involving data governance and business management, and called for more transparency – pointing out the opportunity for Europe to become a service exporter instead of being an importer and consumer of digital goods and services from other regions of the world. On the disagreement between the European Parliament and the Council as regards explicit or non-explicit consent, she wondered whether privacy policies were really read by users and meaningful for them, or whether explicit consent would in any case prevent users from any harmful use of data. Hence, she also called for innovative and more practical solutions to be adopted as part of the future architecture of the Internet.

Anthony Walker (Deputy CEO, techUK) agreed on this point, also arguing that explicit consent was not a sufficient guarantee for privacy. In addition, asking consent for any use could to a certain extent render the consent meaningless in itself. He cautioned that so-called "informed consent" could seriously backfire on users when terms of use are accepted without really paying attention or because of intangible legalistic terms. Consequently, he called for more pragmatic solutions and advocated self or co-regulation mechanisms. He finally insisted on the idea that as services providers, trust lies at the heart of their business development without excluding that unfair methods leading to any kind of discrimination should be banned – it is a matter of companies' reputation and good practice.

In concluding, the discussions focused on the issues of automated processes, algorithms, profiling practices and anonymity: while some advocate anonymity for better privacy, others argue that anonymity would not prevent from unfair tracking and price discrimination since the IP address gives information on the location and the device of the user. Participants agreed that promotion and awareness on privacy did not exclusively depend on legislation but also raise questions of education and self-conduct. The question of regulating algorithms and defining the place of human decision in technological processes will become central in the future regulatory discussions, in the context of widespread digitization and development of robotics and artificial intelligence. As technological developments will always progress faster than regulatory updates, especially due to the EU architecture, the participants agreed that technological standards based on security by-design and privacy by-default settings should be privileged but also be better defined to ensure the development of a vibrant data-driven economy.