United States Senate Committee on Commerce, Science, and Transportation

Hearing "Consumer Data Privacy: Examining the European Union's General Data Protection Regulation and the California Consumer Privacy Act"

Wednesday, October 10, 2018, 10:00 a.m.

Andrea Jelinek, Chair of the European Data Protection Board

Mr Chairman, Honorable Senators,

My name is Andrea Jelinek, I am the Head of the Austrian DPA and the Chair of the EDPB.

Thank you for inviting me to address you on a piece of legislation that has caused quite a few ripples in Europe and beyond, the European Union's General Data Protection Regulation or GDPR.

As Chair of the European Data Protection Board, which brings together the national supervisory authorities and the supervisor in charge of the European institutions, my task is to make sure we are all on the same page. A key task of the Board is to ensure the consistent application of the GDPR and to provide guidance to this end. My aim today is to shed some

light on how the GDPR works, and the philosophy and concepts behind it. I hope this testimony contributes to the extremely timely debate on the adoption of a comparable law in the US, at federal level.

It is often asserted that the EU and the US have a different approach to privacy and freedom of information, based on different historic backgrounds. In the EU, secrecy of communications and the protection of personal data are enshrined in the European Charter of Fundamental Rights. Europe's complex history has shaped its views on privacy and data protection and caused EU citizens to be in favour of strict data protection rules. Does that mean Americans are less worried about the protection of their personal data than Europeans are? It doesn't seem that way.

24% of social media users in the US are not at all confident in the ability of these platforms to keep their personal information safe. *

And 64% of Americans have experienced a significant data breach pertaining to their personal data or accounts. We can only expect that number to go up with the latest Facebook revelations. *

* Pew Research Centre

The volume of digital information in the world doubles every two years, artificial intelligence systems and data processing deeply modify our way of life and the governance of our societies. If we do not modify the rules of the data processing game with legislative initiatives, it will turn into a losing game for the economy, society and for each individual.

Both in the EU and the US people are more vocal about their right to data protection than ever before. The Facebook data breaches or misuse of data and other revelations have caught people's attention, up to a point where it is necessary to re-establish trust. Trust has always been at the core of the economy and this is even more true in today's digital society.

Businesses have started coming around too. And not just because they need to comply with the GDPR, but because they see that their clients and employees alike expect their personal data to be treated in a safe manner.

More legislators and business leaders are stepping forward to say the time for overarching, federal level privacy legislation in the US has come. I think, for example, of Brendan Eich, CEO of Brave Software and former CEO of Mozilla, who wrote to this very committee making the case for "GDPR-like standards". What shape such a law should take is of course up

to US policy makers to decide. The EU's GDPR and its functioning can perhaps serve as an inspiration.

Is the GDPR the perfect recipe? Maybe not, but it is the result of an intensive consultation and collaboration process with all stakeholders and builds on rules that have been in place in Europe for more than 20 years. The GDPR does not change these rules but ensures greater effectiveness. We often describe this as an evolution rather than a revolution.

The GDPR is designed to ensure, as a single set of rules, the data protection rights and liberties of data subjects in the EU. The harmonisation of the legal landscape means two things: one overarching law rather than sectoral rules and the principle of "one continent, one law". These "common rules of the game" create a level playing field and ensure that data can move easily between operators, while guaranteeing the consistent protection of individuals. The goal is to have one set of privacy rules that are interpreted in a uniform way throughout the continent. This represents a significant reduction in compliance costs for companies active in more than one EU country, as well as increased legal certainty. These are very tangible benefits of the GDPR, especially for foreign operators and smaller companies that do not always

have the resources to deal with complex and diversified legal environments.

Under the GDPR, data can only be processed on the basis of "core principles", including the requirement that data collection and processing shall be lawful, adequate, accurate, transparent, proportionate to the purpose for which it is undertaken and kept only for as long as necessary. Individuals must be informed about the main aspects of the processing of their data, and are empowered to exercise rights on their data, such as to obtain access or demand erasure when the data is incorrect or processed unlawfully.

The philosophy behind the GDPR is to put individuals at the centre of privacy practices, building on human rights and values like dignity. Companies must take a closer look at what data they are collecting, what they use it for, and how they keep and share it.

Accountability is one of the GDPR's core principles and the EU was inspired in this aspect by some of the principles stemming from your common law system. It relies heavily on businesses' capacity to self-regulate. Organisations are responsible for complying with the GDPR and must be able to demonstrate their compliance.

The so-called “risk-based approach” which you find at the heart of the GDPR means that operators that limit the impact of their processing operations are exempt from a number of obligations. This approach reduces the regulatory burden for companies that carry out basic, mundane processing operations. It also creates incentives to develop innovative, privacy-friendly solutions from the earliest stages of development - “privacy by design”. The market offer of new privacy or data security enhancing products is growing. In other words, investing in privacy pays off and creates new commercial opportunities.

One of the greatest achievements of the GDPR is the ‘one-stop-shop’ mechanism, which means a single lead supervisory authority is responsible for drafting a decision in a cross-border case. International or multinational companies operating in different countries have only one interlocutor to deal with: the Lead SA is in the country in which the company has its main EU establishment. Any decisions taken by the lead supervisory authority are valid across the EU.

How does this work in practice? When a cross-border complaint is filed, the cooperation mechanism kicks in. The LSA acts as the main point of contact and drafts a preliminary decision. This decision is then shared with the SAs concerned.

If no objections are raised, the SAs are deemed in agreement with the draft decision.

If objections are raised and the LSA decides to reject them, the so-called consistency mechanism is triggered and the case is referred to the European Data Protection Board. The Board will then act as arbitrator and issue a binding decision. On the basis of this decision, the LSA will adopt its decision (which can be challenged by the courts). The 'one-stop-shop' mechanism significantly reduces the administrative burden for organisations as they do not need to consult with different regulators but receive one single position applicable in all EU countries. Complainants too only have one point of contact, i.e. the supervisory authority in their country.

It is often said that the US approach to data protection promotes technological innovation and economic growth, which is important for people living on both sides of the Atlantic. Let me give you my opinion on that: without trust, there is no economic growth and no innovation at the end of the day. That being said, the GDPR is carefully calibrated so as to not hinder economic development, while keeping in mind the fundamental right of the individuals.

One of the main goals of the GDPR was actually to enable a more functional information economy within the EU with more transparency for citizens, which should lead to more trust. Companies should be allowed to continue to use and share data, as long as they do so in a transparent and lawful manner, respecting the rights of individuals. The key lies in establishing an equilibrium between the respect of personal data and the commercial use of data collection and management. That equilibrium had become impossible to maintain without a new legislative initiative supported by all stakeholders.

It has only been four months since the entry into application of the GDPR, but the first responses from the business community are largely positive. Businesses have made substantial efforts to be compliant and to restore trust with consumers. There are countless examples of businesses asking their customers with straightforward and clear sign-up forms whether they can process customers' personal details with easy-to-understand explanations as to why the company needs these data.

As European data protection authorities, we have "rolled up our sleeves" and actively engaged in a dialogue with stakeholders. This has included the adoption of 18 sets of

detailed guidelines on all novel aspects of the GDPR, following broad public consultations to which many U.S. companies contributed. This work will continue, as new questions will keep emerging.

How do we ensure that the GDPR is enforced? The European supervisory authorities are not the fining machines we've been made out to be by some. The 2% or 4 % numbers that are often reported are maximum ceilings that will only apply to the most serious infringements. Fines are a last resort, just one of the tools which data protection authorities can use to enforce the GDPR and only after a thorough investigation of the facts and always on the basis of the specific circumstances of each case. Fines must be effective, proportionate and dissuasive.

Supervisory Authority corrective powers also include: the issuing of warnings and reprimands, ordering a company to bring processing operations in compliance with the GDPR within a specific time frame; ordering the controller to communicate a data breach to the public and imposing a ban on processing.

I hope and trust that my testimony on the GDPR and its first effects might contribute to your debate on the need for a US

data protection law at federal level. I'm grateful to be here with you today and thank you again for the invitation to share our views. As European data protection authorities we stand ready to share our experience and further discuss these issues with all interested parties.

Let me conclude with the words of one of the greatest U.S. legal experts and one of the founders of modern privacy law, Luis Brandeis: the "right to be left alone [is] the most comprehensive of rights, and the right most valued by free people". Ninety years have passed since Justice Brandeis so eloquently captured what privacy is about but these words have never been truer than they are today in our digital world.