Spring Conference

Austrian Commission of Jurists

Giovanni Buttarelli

31 May 2018

Ladies and gentlemen,

Thank you for this invitation to speak today; much to my dismay I am unable to be with you in person, but nonetheless could not pass up the opportunity to contribute to this dynamic conference.

Given the timing of this event, six days after the full applicability of the General Data Protection Regulation, it seems fitting to review the EU legal order on data protection: where we have come from, and where we might be heading.

It is helpful to consider the manner in which the European ideals and corresponding legislation evolved to emerge as a gold standard for data protection standards globally.

As competition increases between the EU and China, the U.S and India, our founding values play an increasingly pertinent role.

The concrete beginnings of a growing awareness and concern for privacy emerged in the 1970s and 80s with rapid technological advances compared to previous decades in conjunction with widespread automation.

These developments coincided with tumultuous events in the U.S., with incidents such as the Watergate scandal playing also a role in the shaping of privacy legislation emerging.

The cornerstone of European data protection law was laid several years later during the 1980s and 90s; initially commencing with the Single European Act and subsequently the Maastricht Treaty.

Data protection legislation was born from the need to facilitate cross-border data flows within the Union.

These beginnings encapsulate the essence of data protection principles in the EU, which have always been about facilitating the functioning of the internal market, through the creation of a framework of rules specifically engineered to protect the individual, facilitate trade and build trust.

This symbiotic relationship enjoyed between data protection and the growth and success of the European Union serves to underline the inextricable link between the two. It was expressed in the 1995 Directive.

With the turn of the millennium in the year 2000, the proclamation of the European Charter of Fundamental Rights affirmed a separate right to the protection of personal data.

Article 8 of the Charter is relatively detailed. There were discussions about codifying a right to informational self-determination as exists under the German Basic Law, but this was rejected in favour of a right to data protection that corresponded to the principles of the Directive:

- that data must be processed fairly and for specified purposes with a legal base

- individual rights of access and rectification right to see data which have been collected on that individual

- independent supervision

Article 7 on the Right to Privacy duplicates ECHR Article 8 except that it replaces 'correspondence' with 'communication'.

This legal development has far ranging implications.

For instance, in C-617/10 *Akerberg Fransson*, the Court held that (para 17-21) the Charter applies whenever a Member State acts within scope of EU law. In *Melloni* C-399/11 it held that (para 59-60) Member State law in scope of EU law must respect the Charter and the primacy, unity and effectiveness of the EU law at stake. Therefore only the EU's human rights standards, in the form of the Charter, can apply, above and beyond even national constitutional standards (para 64).

The entry into force of the Lisbon Treaty in 2009 made the EU the only jurisdiction in the world to impose upon itself a duty to legislate for this right under Article 16 TFEU.

Within a year, the European Commission adopted a proposal for the General Data Protection Regulation.

Jumping now to 2018- undeniably a milestone year in so far as not only data protection but the regulation of the digital environment is concerned.

The efficiency and enthusiasm of Austria in adapting the national law to the GDPR almost a year in advance of the 25th May this year, is truly something to be applauded.

Like its predecessor, the Austrian Data Protection Amendment Act 2018 appears to focus on what is essential, using some of the possibilities offered by the GDPR to implement provisions that are more stringent.

In addition to legislation, the jurisprudence of the European Court of Justice has evolved our perception of data protection.

Over the course of the last ten years, case law has sculpted the rights to privacy and data protection:

The Snowden revelations and the ensuing striking down of the Safe Harbour Agreement; the Digital Rights Ireland case, striking down the EU Data Retention Directive; and the case law on independent Data Protection authorities in Germany, Hungary and Austria have all left indelible marks on the canvas of European Data Protection law, calling for a new regulation with a suitably robust framework to adapt to future developments.

These cases served to highlight the 'Rubik's Cube' of approaches throughout the EU.

This chronology leads us nicely to attempt to prophesise the near future, an exercise that has rarely been more compelling or enticing.

Companies' willingness to be compliant with data protection rules offers a message of optimism for the future; unfortunately, I doubt this will be sufficient to tackle some of the roots of the various problems which technology has dug into society.

Preserving a diverse democracy and people's autonomy of is of grave concern for the future.

The speed at which technology is evolving and its growing convergence with the everyday lives of citizens, dictates a need for flexibility in our regulatory approach.

Notwithstanding the extensiveness and prescriptiveness of the GDPR, enforcement will not be effective if it happens in silos.

Therefore, a priority in my mandate has centred upon ethics.

In emphasising the principle of accountability, the GDPR casts a wide ethical net. However, incorporating ethics into our approach to technology must go beyond compliance.

Furthermore, when it comes to areas as technically complex as Artificial Intelligence, the inner workings of which only a few comprehend, it is important to have broader ethical standards that act as a benchmark.

Given the volume and sensitivity of data required for processing in order to develop AI, the procedure in general raises basic questions of accountability: if harm is caused by an AI system that had been developed and delivered value for a profit-seeking company, who should be held responsible for such harm?

One thing is clear in this age of algorithms; the perverse incentives in digital markets to treat people like sources of data have to be remedied.

This requires a complete revamp of the system- something that the GDPR alone is not equipped to deal with.

Therefore, it is necessary to complete the regulatory framework with the GDPR's sister legislation, the e-Privacy regulation.

Given Austria's impressive willingness to incorporate the GDPR into national law and ensure full compliance, I feel it is both daring yet legitimate of me to expect Austria, which holds the next Presidency of the Council of Ministers from July, to show leadership in concluding negotiations on the ePrivacy regulation.

The regulation is pivotal not simply to ensure a level playing field, but also to steer companies away from using information that is expected to remain confidential.

This is a prime example of European efforts to change market incentives and encourage innovation.

Now is not the time for complacency simply because the long-awaited GDPR is in place.

In fact, it is the opportune window to build on the success and ensuing reputation of producing a global standard.

One of the seismic changes introduced by the GDPR will be the shift in dynamic between the following entities:

- data controllers putting the new regulation into practice;
    - The obligations of the controller are at the centre of the GDPR, along with provisions like codes of conduct and certification for demonstrating compliance.
- data protection authorities educating on the new requirements demanded by the GDPR;
- the interpretation afforded to the GDPR by the courts through litigation;
    - Moreover, the not so distant future will be shaped by a number of important pending decisions from the CJEU. Both the judgments of the Schrems II case on standard contractual clauses (questions yet to be

submitted) and on the UK referral on boundaries of EU competence in relation to national security will undoubtedly be highly influential.

- In addition, the technology industry will drive innovation in different areas that will by necessity have data protection implications.

The GDPR is explicitly limited in scope to the personal data of natural persons, whereas as it currently stands, the Austrian DSG 2018 expands this remit to include legal persons.

Several solutions exist to bridge this apparent divergence from the GDPR. For example the EU Trade Secrets Directive (2016/943) whose deadline for transposition was this year.

Similarly, a lapse in legal protection arises as the GDPR invalidates the established Austrian regime for 'indirect personal data', covering data relating to a data subject in such a manner that only the data controller can identify the data, subject to legal means.

Nonetheless, indirect personal data is still protected. However, it is simply subject to a less stringent regime.

These solutions highlight the flexibility of the GDPR, allowing national legislatures room to manoeuvre and to mould the regulation to suit their national agendas.

The Big Data ecosystem is remarkably fast-paced, dictating regulators and legislators be likewise.

It is important to bear in mind that the GDPR spent four years in the pipeline.

Its arrival signals a genuine cultural change.

Therein lies the essence of the regulation- far from constituting a standard piece of legislation, its aim is far greater; to incite a change in current business practices and go give control back to citizens.

The GDPR calls for detailed cooperation between Data Protection Authorities. Six substantive articles of the regulation are dedicated to facilitating this; covering topics from information sharing and joint operations to mutual assistance.

The creation of the European Data Protection Board is an ambitious attempt to bring 29 individual regulatory bodies together, united under a general obligation to achieve consensus.

By all means, this will be no small challenge, neither culturally nor legally.

This is particularly true given the patchwork manner in which member states have approached data protection and their level of success at enshrining GDPR in national law.

Moreover, the 'wiggle room' provided within the regulation itself ensures that some legal diversity will persist.

One such example is the Austrian legislature's reservation of the right to render additional regulations for specific areas based on the opening clauses of the regulation in separate, specific laws.

Further, some local special provisions for certain data processing activities (e.g. as regards video surveillance or data processing for purposes of research) are upheld by Austrian law.

In any case, we are offered a fresh start.

With the possibility of reaching binding decisions on disputes regarding cross-border processing, the EDPB will ensure a uniform application of the GDPR.

The large extent of cooperation between Data Protection Authorities demanded by the GDPR is in some ways indicative of data protection law coming full circle.

Initially a tool to facilitate the flow of data within the EU and purely functional, data protection law is now playing a role of further consolidation among member states through the necessity of cooperation between 28 national DPAs along with ourselves.

These developments embraced by Austria and by Europe which have lead us to where we are today, signal our embarking towards a new age of data rights and responsibilities.

Thank you for your kind attention, I wish everyone a thought provoking and stimulating remainder of the conference.