14 May 2018

8th European Data Protection Days (EDPD)

Berlin

Giovanni Buttarelli

Ladies and gentlemen,

Thank you to Euroforum for the invitation.

This event has become one of the unmissable staging posts in the data protection calendar. Unmissable for me personally also.

But this year, 10 days from the launch of the EDPB, I may be permitted to pray forgiveness for not being able to join you in person.

You have a full agenda for the day with so many esteemed speakers lined up, and more important lunch is waiting.

So I have kept these recorded remarks as brief and succinct as possible.

There are so many words which have been printed and spoken about the GDPR that there is not much left to say.

Now is the time for action not words.

And judging by their actions, with two weeks to go you can discern at least three big groups of controllers.

First there are the ones – the majority - which say: "The rules are changing and we are adjusting to them. But basically it is business as usual." These tend to be the firms which are already generally confident that their practices are compatible with EU law on data protection.

Second there are those which say: "You need to agree to our privacy policies before 25 May or you will no longer be able to use our services". These are companies whose main objective is to protect themselves.

Third, there are the growing number of service providers who are saying: "We will probably not be GDPR-compliant so we are getting out of here!"

This category includes a lot of companies – typically 'free' services whose data policies have already been questioned in the past.

In fact there is even a service out there now which promises to allow you to "Avoid the *GDRP*" – yes it actually misspells the acronym. It claims to offer Javascript software which will block all EU users from your website, so you do not need to comply.

Sadly, when I checked last night the website of this ingenious service was unable "due to maintenance downtime or capacity problems".

Joking aside, there are signs of a significant realignment of priorities in the decisions which businesses are taking.

Certain behaviour has become too risky.

But also opportunities are opening for controllers who want to show their customers and potential customers that they care about them.

Caring about customers has come to include caring about what happens to the data about them.

This is a problem for the dominant business model in much of the world outside Europe.

Under this approach there is an assumption that you must first collect as much data as possible and then seek ways to monetise it.

You should worry about the consequences only after the consequences have materialised.

Now, some criticised the GDPR for being too prescriptive.

Rules on when and how to conduct DPIAs, the job description of DPOs, and all the other detailed 'modalities' might be considered as 'gilding the lily'.

But these provisions are a signal of the consumer mistrust which has come to suffuse digital markets.

The EU is trying to steer controllers away from harmful practices. It is trying to incentive greater digital customer care.

That is because it looks like the market on its own is not delivering a fair distribution of the digital dividend.

Now I do not believe that the GDPR, in all its beautiful complexity, can be enough to address this challenge.

Thus we have been experiencing in the last few weeks the *cognitive dissonance* of being confronted on all sides with demands to click to accept new terms and conditions.

It is a lesson that the GDPR was never going to change behaviour overnight. Powerful controllers cannot be expected suddenly to treat ordinary users as equals.

But I predict that as people become more informed about their rights under the GDPR, and of the role of DPAs, they will start to demand changes.

The competitive advantage of treating online customers with respect, and being seen to treat customers with respect, will become more real.

This new dynamic cannot be reduced to a binary question of informed, specific and freely-given consent versus 'legitimate interest'.

Whatever legal basis is settled upon as appropriate for a given processing operation, companies remain accountable for the consequences, including unintended ones.

Consent is not a licence to exploit vulnerable, distracted or addicted data subjects through video games, personality tests, 'life hacks' or any other means of 'eyeball entrapment'.

Equally, legitimate interest is not a blank cheque to permit use of data for any purpose which promises to generate revenue.

The last few weeks have also revealed a need to talk about other aspects of the GDPR which could be interpreted in ways not respectful for the individual. This includes the notion of 'necessary for the performance of a contract' and 'scientific research'.

We are seeing in real time how the right to data protection is meant to complement and safeguard the right to privacy.

There are stricter rules on collecting and using data revealing political views, sexual orientation and religious views, and on data which reveal information about your communications.

The proposed ePrivacy Regulation is essential not just to ensure a 'level playing field': to avoid penalising telcos and giving the amorphous so called 'tech companies' a free pass.

It is essential to steer companies away from using information which people expect to remain confidential.

It is essential to give people more confidence that when they send a message or email that it will not be parsed by the carrier.

It is also essential to free up the market so that people can choose not to be trapped in walled communities where the information served to them is determined by an opaque, unaccountable, revenue-maximising algorithm. This as much as anything is the cause of the 'fake news' and microtargeting scandal.

Publishers and advertisers, as well as individual users, lament their lack of control in the highly concentrated digital information ecosystem.

ePrivacy is essential also to help unblock this system, to de-centralise, and allow different models which do not depend on constant tracking but which give people more control over what happens to their information online.

Again, modern ePrivacy rules will not be a panacea. The systemic problems cannot be fixed by a consent requirement, however tightly we redefine the notion of consent.

But it is an essential missing piece of the puzzle.

With ePrivacy, the EU will have a comprehensive framework for personal data processing and confidentiality of communications for the AI generation.

Our job as regulators is to be predictable and consistent, to focus resources on tackling the most harmful behaviour.

In two weeks we will launch the EDPB. We will be more or less the same faces around the table as when we were the Article 29 Working Party. The architecture – where we meet, the types of sub-groups – will be perhaps more continuity than change.

But it will be a fresh start with a fresh mandate to work in a spirit of collegiality, to reach consensus on all matters of a cross border nature.

EDPS has done its part in providing a world class secretariat which is already in place, in terms of personnel, accommodation, IT and communications facilities.

As a member of the Board, my role will be to support the chair as a loyal colleague, and to place the European perspective is at the heart of all our deliberations.

We are about to enter a new era for digital rights and responsibilities, so fasten your seat belts.

Thank you for listening and best wishes for the rest of the conference.