

Italy's DPO group promotes best practice and GDPR

Laura Linkomies reports from ASSO DPO conference in Milan 8-9 May which gathered together many of Italy's privacy professionals, representatives from other countries' DPO organisations and DPA staff.

Having spoken to many privacy professionals over two days in Milan, the general feeling was that many of Italy's Data Protection Officers (DPOs) feel unprepared for the GDPR. Multinationals are well on their way to full compliance, but for an average Italian company the GDPR is still quite new and it does not help that the adaptation law was not yet ready at the beginning of May.

Opening the conference, ASSO DPO's (Italy's DPO Association) President, *Matteo Colombo* said that we are now establishing the basics of the new DPO position. What should a DPO do? There are mistakes in the interpretation of this GDPR provision, Colombo said. A DPO needs to be a consultant, but also much more.

"The principal objective of ASSO DPO is to support its members. We must take the norms and translate them to the work of DPO. Who needs a DPO? In the private sector it is mostly clear but the Art 29 Working Party guidance is still open to too much interpretation."

Another theme in ASSO DPO's work is that many privacy professionals want to be assured of who has the ultimate responsibility in their organisation.

ASSO DPO has now been accepted as a member of CEDPO, the EU-wide

associations. 25 May is not the end. This is a process. Organisations need to understand this."

Giuseppe Cannella, President of the ASSO DPO Scientific Committee, said that we should focus on potential compensation for data subjects. In many contracts the parties expressly say that they have adopted a code of conduct and each party respects it. But contracts must also make clear who bears liability if individuals claim damages.

Raffaele Provolo from Milan City Council said that ASSO DPO has created a working group on privacy in the public sector. The responsibility of public authorities starts with defining competences, placing people at the centre and being transparent. There is a debate now going on about GDPR, the Right to be Forgotten and deleting some data. "If you delete you respect the Right to be Forgotten. But on the other hand public authorities have a responsibility to govern and offer services. We have to think of the compatibility and convergence with other rules to strike a balance."

Fabio Ferrara, Vice President of the ASSO DPO Scientific Committee spoke about GDPR Article 30 – the duty to present documentation. "This is absolutely central for accountability. The Article 29 WP paper from a few

SWITZERLAND ON ITS OWN PATH

Gianni Cattaneo, a lawyer and member of the Data Protection Commission in the Swiss canton of Ticino provided an update from Switzerland. "We have a very particular system. As Switzerland is not in the EU, many companies are not even considering the GDPR. We have 26 cantons, each with its own Data Protection Authority and the Federal Data Protection Commission in Berne – so many for a small nation. It is therefore not so simple to standardise the practices."

He said it was not yet certain whether there would be a new law by 2020. "We have a draft bill now. There are some differences from the GDPR – for example legal persons are also included. In the future, active consent is needed for all categories of data. The DPA will receive enhanced powers. Now it can only issue recommendations."

New criminal penalties will be created but only up to 250 000 Swiss francs, so far away from GDPR level fines. Data portability is not included in Switzerland's bill, as it is difficult to apply. "Maybe it should be under competition or consumer protection law instead? We wait to see your experiences on this!" Cattaneo said.

DPA PANEL TALKED ABOUT IMPLEMENTATION

Albine Vincent, Head of Data Protection Department at France's DPA, said the CNIL is also preparing internally for the GDPR by training staff, and updating its IT system to exchange information with all other DPAs in the cooperation mechanism.

Organisations must submit details of their DPOs in France to the CNIL – this can be done online. DPO certification is a voluntary mechanism. Certification bodies are to request certification with the CNIL. A public consultation started mid-May. Accredited bodies may issue DPO certifications according

ASSO DPO has now been accepted as a member of CEDPO, the EU-wide DPO Association.

DPO Association. In Italy, ASSO DPO makes representations in legislature, but internationally there needs to be a higher level of visibility for DPOs, Colombo said.

"We cannot immediately reach the same position as the British where DPOs are already well established. But we want to cooperate with other EU

days ago clarifies some issues. This register is not static; we can show how a DPO has approached an issue, and what consultants have done. The DPO is central for keeping records. We need to prove that records are valid but the Art 29 WP says that it is unlikely that keeping the records represents a burdensome task for a company."

to the CNIL's certification scheme.

"There will be no grace period. But account has to be taken of the learning curve in the first few months of the GDPR. We want to be pragmatic."

Michael Kaiser from the Hesse DPA in Germany spoke about the German national consistency mechanism.

"We will accept an Italian certification but the DPO must sometimes provide documents in German. A DPO needs to be appointed in Germany if there are ten or more employees processing personal data."

To satisfy GDPR Art 30 requirements on documentation, English is possible, German could be required, Italian is not sufficient. Exemptions to consent are under discussion. What does 'freely given' mean?

"Are German companies ready? More or less, especially the big ones. A DPO could sit in Italy for example, however it might be better to have one in Germany that can speak German. It is not required under the new German law though."

Spyridon Vlachopoulos, a member of the Greek DPA and law professor, said that he expects companies to challenge fines and take DPAs to court. "I think that many people are well informed. The number of complaints will increase, and they will go to courts to ask for compensation. Will this affect the workload of DPAs? Accountability should reduce red tape. Is this true? We will see. In Greece, some of the old obligations will not exist any longer, for example, prior authorisation. On the other hand, the GDPR creates many new tasks, such as certification."

Sandra Liu of Hong Kong's DPA

said that there is much concern in Hong Kong about the GDPR: the extraterritorial effect has an impact in Hong Kong. There are some differences between the two laws. "We are now conducting a review. One of the major concerns is that under the Hong Kong Data Protection Act, data processors are not regulated. However, under the GDPR they are subject to legal duties, such as record keeping, breach notification, designating DPO and so on."

"We now have a proposal for including processors. The government is not likely to implement this provision. Foreign service providers may analyse data back in Hong Kong, so they now face direct obligations under the GDPR. They are not mentally prepared for this. In Hong Kong, 98 per cent of all businesses are actually SMEs, which complicates the situation."

DPO AND DP LAWYER EXPERIENCE

Anna Poulion, Head of Privacy for Maison Chanel in France spoke about her changing role as a DPO. Having worked in many countries and companies, she had an insight into the development of the profession and the attitudes towards a DPO. At first, management may be indifferent to privacy issues and the GDPR, but then panics and asks for advice. The staff may see the DPO as a friend or a foe, depending on the situation. The DPO needs to stay calm and create trust, also internally.

It is important to adapt the language to the company in question. Most cannot understand legal provisions. Is privacy the new luxury? This statement

was made in Davos and fits a fashion brand perfectly.

Paul Van Den Bulk is a Partner at McGuireWoods LLP in Belgium. Apart from being a solicitor he also works as mediator. His talk explained the possibilities and challenges with the One Stop Shop.

He said it is not as clear as it first seems. Member states work at different speeds. Some DPAs have already said they are not ready, but the EDPB consistency mechanism is ready and will be applied from 25 May.

The One Stop Shop poses some interesting questions, for example the position of a processor. If the processor is in a different member state than the controller, the lead authority will be that of the controller.

"This is explained in the GDPR recitals. But the situation of joint controllers is not mentioned in the GDPR. Maybe there will be two lead authorities? I do not know."

He said that the limits of the One Stop Shop include situations where processing is carried out by public authorities or private bodies acting on the basis of a legal obligation or public interest. Also, complaints will be heard before national courts where the matter substantially affects data subjects only in that member state. Similarly, if an authority concerned thinks there is an urgent need to act in a case to protect the interests of the data subjects, the case can be heard at national level in that country.

BUTTARELLI SAYS THAT EDPB READY TO GO FROM DAY ONE

The European Data Protection Board is ready to start its work immediately on 25 May 2018. Speaking at the ASSO DPO conference in Milan, European Data Protection Supervisor, Giovanni Buttarelli said that the group has now prepared procedural rules, and held discussions about work methods.

"EDPB will not be a successor of EU Article 29 Working Party, we will turn a new page. The DPA group is no longer just a consultative body."

Buttarelli stressed transparency and accountability for the group. "We want to be more accessible and more modern, but also more selective, as we will have to take

more decisions collectively."

Buttarelli said that a quarter of EDPS staff will form the secretariat of the EDPB, but they will work separately as already defined in the Memorandum of Understanding between the two bodies.

He commented on the corrigendum to the GDPR saying that the corrections currently underway do not include anything of substance. There have been some errors of syntax, but essentially there will be nothing new that organisations should be concerned about.

Speaking about the international impact of the GDPR, Buttarelli recognised the work of *PL&B Asia-Pacific Editor*, *Graham*

Greenleaf, for his research in identifying countries globally that have a privacy law.

"GDPR has no grace period. It will stay with us for at least 20 years. In terms of enforcement, those who have done something and made a mistake are in a better position than those who have done nothing."

He said that at the national level the GDPR text has been changed in some countries. Generally the work started too late. In unofficial texts there are very good improvements. But which versions will governments adopt? Certain provisions should be kept for another occasion."