Main topic of the meeting: Directive (EU) 2016/680

1. Transposition progress

Members reported on their transposition process. Most Member States are expected to achieve the goal of transposing the Directive before the deadline (6 May 2018). More details are included in the attached table presenting the state-of-play in the Member States.

2. Data protection officer in the GDPR and in the Directive (Articles 32-34)

On the different status of the data protection officer in the GDPR and the Directive, most of the Members will have one DPO responsible for both the GDPR and the Directive, meeting the GDPR requirements of independence and a line of reporting to the highest management level.

3. International cooperation on data protection (Article 40)

On the obligation to ensure international cooperation on data protection, Members understood it as an obligation of endeavour and most of them will vest their supervisory authorities with the authority and the task to cooperate globally with its counterparts.

4. The right to lodge a complaint with a supervisory authority (Article 52)

Members were of the view that supervisory authorities should be able to verify the identity of the complainant, even though this is not explicitly provided for by the Directive. On the obligation of the supervisory authorities to provide further assistance to the data subject, most of the Members intend to transpose this obligation in very general terms, while some of them envisage more details about matters such as language assistance. Some Members do not intend to specifically transpose this obligation. All of the Members were of the view that, while supervisory authorities should provide information and advice to stakeholders, they should not be expected to provide detailed and tailor-made legal advice.

5. Whether the Directive is applicable to criminal courts

Members agree that the Directive is applicable to the criminal courts, but have differences of approach when it comes to the administrative supervision of courts’ data processing activities. Some Members have a broad interpretation of the exemption from such supervision when courts act in their judicial capacity, while others interpret it narrowly. Moreover, there are differences in approach to the kind of supervision which needs to be in place when this exemption is used. Some Members will set up a separate data protection authority. Others will ensure internal, judicial supervision mechanisms. A third group of Members argues that it is enough to use the existing mechanisms of judicial review in their procedural laws.

6. Penalties (Article 57)

A number of Members plan to transpose this Article by enabling administrative fines against competent authorities, as provided for by Article 83 of the GDPR. The Commission stressed that in Member States where no administrative fines will be possible on the public sector, other types of effective, proportionate and dissuasive penalties will have to be developed by in
national law. Some Members suggested that it would be enough to provide for an exhaustive set of corrective powers of supervisory authorities, similar or identical to the one of the GDPR.

7. The right to access (Articles 14 and 15) and the new architecture of the rights of data subjects (Chapter III)

On the need to remove the blanket restrictions of data subject access rights from national law, due to the new architecture of Chapter III of the Directive, most of the Members agree that there is a need for complete overhaul of the system, providing for both direct access and indirect access through the supervisory authority when restrictions are applied. One Member stated that it plans to keep the current system allowing only indirect access to police databases.

8. The use of logs in criminal proceedings (Article 25)

Some Members argued that such use is restricted to crimes committed by the law enforcement officers (for example unlawful disclosure of a database accessible to him or her), while others argued that the last part of paragraph 2 of Article 25 is very general and open to interpretation.

9. International transfers (Chapter V)

The Commission explained its plans for adequacy under Article 36 of the Directive. It also explained that the self-assessment of the controller, provided under Article 37(1)(b) could conclude that transfers to Interpol are transfers by way of appropriate safeguards. Finally, the discussion on the controller-processor relationship under the Directive, in the context of international transfers, led to the conclusion that processors such as cloud service providers would not be able to carry out international transfers of personal data for their business purposes under binding corporate rules, because such transfers would not be allowed under Article 35 of the Directive. The processor should be able to do only what the controller can, and no more.