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

1. Scope of the Directive

The meeting started with a new round of discussions on the scope of the Directive. The Commission underlined the importance of both the material and the personal scope of the Directive. Only when the two come together is the Directive applicable. As regards the personal scope, there were discussions as to whether a possible interpretation could be to cover only those authorities which have the prosecution, detection, investigation of criminal offences as their main task.

Some Member States supported this interpretation, while others argued that in their national legal systems there is a variety of bodies with prosecutorial powers on variety of offences, without a difference in legal treatment between core criminal offences and other offences. They therefore argued that they all fall within the EU notion of "criminal offence". It is important to focus on the nature of the activity carried out by the competent authority, and the link of that activity with the purposes of the Directive.

Some Member States are testing the idea of applying the GDPR to administrative bodies up until the moment proceedings end up in a criminal/misdemeanour court, at which moment the Directive would become applicable. Some Member States argued that Engel criteria and the case-law of the European Court of Human Rights can help to define a criminal offence, but can also complicate things as such case-law is focused on the independent notion of civil rights, both in the context of civil and criminal law. Some Member States stressed the need to find a framework model that all Member States could use for the delimitation between the GDPR and the Police Directive. The Commission therefore proposed a third round of discussions on the scope, with a smaller group composed of those Member States that are facing difficulties on this issue.

2. Special categories of personal data

The Commission presented Article 10 on special categories of personal data (sensitive data), which differs in approach from the corresponding Article 9 of the GDPR. In the Directive, the legal basis for any processing must be found in law (according to Article 8), and one of the three conditions (authorisation in law, protection of vital interests of the data subject or another natural person, data manifestly made public) must be met in order to process sensitive data, together with legal safeguards. Consent of the data subject is an example of an appropriate safeguard.

One Member State argued that national law must be more specific about the issue of consent, and that it is up for the national law to decide if it wants to have this safeguard. Another Member State raised the attention of the group to the fact that biometric data such as fingerprints and DNA became sensitive data, which was not the case before the Directive entered into force. It was only considered to be identification data.

3. Automated individual decision- making
The Commission presented how Article 11 of the Directive works and the differences between that Article and the corresponding Article 22 of the GDPR. Member States had no comments on this point.

4. Exercise of data subject rights
The Commission presented the difference between the direct and indirect exercise of data subject rights, emphasising that the rule is direct exercise, while indirect exercise comes into play when certain information about the imposed restrictions are not provided to the data subject, for duly justified reasons. It also emphasised that the provisions on the rights of data subject, like the entire Directive, are fully applicable in criminal proceedings.

One Member State wondered about the instances in which the restriction on a data subject right to access has to be lifted. The Commission argued that this depends on the circumstances of each case and the necessity and the proportionality of the restriction, which was supported by another Member State. Some Member States questioned the added value of Article 18. The Commission and one Member State argued that its purpose was to make sure that these important rights can be laid down in the framework of judicial proceedings and criminal investigations and proceedings; i.e. that the same guarantees can be provided elsewhere. One Member State argued that most of the rights already exist in the criminal procedural law, and additional legislation transposing the Directive for criminal proceedings will be necessary only on the right to information and to a limited extent.

The Group also discussed the carve-out for courts acting in their judicial capacity, which are exempt from the administrative supervision of the data protection authorities (DPA). While the Commission and some Member States argued that the independent supervision in such cases should be ensured through a separate judicial body within the judiciary, other Member States argued that the supervision is ensured through the system of judicial review (appellate courts), as one judge cannot, for example, control decisions of another judge on the admissibility of evidence containing personal data. Some Member States noted that data subjects who are not parties in the proceedings would then not be able to raise data protection related complaints.

5. New obligations of controllers and processors
The Commission presented the data protection impact assessment (DPIA) under the Directive, underlining that the notion of high risk should be the same as in the GDPR. The three cases in which DPIA is mandatory under the GDPR should be taken into account as examples where a high risk is considered to exist.

Some Member States wondered if DPIA could be carried out in the context of the legislative impact assessment, as is the case under the GDPR. The Commission will examine this issue and reply later.

One Member State wondered if the obligation for DPIA is not broader than in the GDPR. The Commission took the view that it is not, because in the Directive it is limited to new filing systems. Some Member States wondered to what extent the new obligations of controllers are applicable to the existing databases. The Commission pointed to the recital 96, which states that processing complying with Union law prior to the date of entry into force of the Directive does not entail the obligation of the prior consultation of the DPA. One Member State added that in any case, new obligations can apply only prior to the processing and not to the processing which is already underway.

The Commission also presented the new obligations on notifications of personal data breaches, which are fully aligned with the GDPR. The Commission went on to present the provisions on the data protection officer. Some Member States asked about the possible appointment of one DPO for several controllers, and about the exact meaning of an
organisational structure and size of organisations. The Commission took the view that a joint DPO can be appointed when types of processing and hierarchical structure of controllers are similar as long as the DPO remains easily accessible by data subjects' and by the DPA. One Member State wondered how to integrate a DPO in a structure of an organisation, if he or she is shared by several organisations. One Member State wondered if a DPO can be a contact point in case of joint controllers. One Member State wondered if an organisation can appoint one DPO for both the GDPR and the Directive. The Commission and one Member State took the view that a joint DPO cannot be appointed between controllers falling within different branches of power (e.g. police and judiciary). Functional criteria would prevail. In any case, as the recital points out, several controllers could have a joint DPO through shared resources in central units. The Commission also took the view that the DPO could be a contact point in case of co-controllernesship and that it would be difficult to appoint an external DPO in the context of the Directive. One the other hand, it would be possible to have one DPO for both the GDPR and the Directive, provided that the stricter requirements of DPO’s position within the organisation and independence are met.

The Commission went on to present the obligation to keep logs. One Member State wondered about the timing when the DPA can inspect logs, while another Member State wondered how long logs should be kept. The Commission took the view that the logs should be available for the inspection of the DPA whenever the DPA wants to inspect them. They should be kept as long as the purposes for which they are kept exist and long enough for the DPA to inspect them, if needed.

Some Member States argued that the provision on the logs may require very substantial changes in the architecture of some national databases. In order to use logs for criminal investigations on personal data breaches, some sort of archive of logs may have to be developed and available to DPAs. One Member State mentioned that it already developed national legislation on keeping the logs. Another Member State wondered about differences between operations of consultation and disclosure and other operations for which logs should be kept. The Commission took the view that logs of consultation and disclosure have to include specified data because of their importance. One Member State was critical about the lack of a specific reference to the use of logs for disciplinary proceedings in paragraph 2 of Article 25. The Commission took the view that such use is covered by self-monitoring, which is elaborated further in a recital.

6. Any other business
One Member State raised the issue of the difference between the end of the transposition period for the Directive (6 May 2018) and the entry into application of the GDPR (25 May 2018). Another Member State asked about the activities that fall outside of the scope of Union law. The Commission gave the example of national security. One Member State took the view that the Directive can be nevertheless applicable to matters of national security if that is the wish of a Member State.

Next meeting of the expert group is on the Regulation (EU) 2016/679 (GDPR) and will take place on 14 February 2017.