
4 May 2017

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

1. Scope of the Directive

The discussion on the scope was a follow-up of previous exchanges on this theme and provided an opportunity for the Commission (LS) to clarify that while Member States can, when transposing the Directive, rely on the notion of criminal offence as defined in their national legal systems, they cannot label a situation as a criminal offence only for the specific purpose of including it in the scope of the Directive. Where national legal systems do not provide for a (clear) notion of criminal offence, Member States have the option to decide, on the basis of objective criteria (e.g. use of criminal procedure or application of typical criminal sanctions such as imprisonment), where to draw the line between administrative and criminal offences. While some Member States announced that they will apply the GDPR to all types of administrative proceedings (regardless of whether or not such proceedings may eventually become criminal proceedings), others informed they will apply the Police Directive to all offences qualifying as criminal under their national law, including minor offences. This will lead in some cases to the application of the Police Directive to processing which is presently submitted to the national legislation transposing Directive 95/46/EC. Moreover, in some other Member States, the Police Directive will apply to authorities which otherwise carry out administrative tasks, where such authorities handle infringements that constitute criminal offences (e.g., by obtaining prosecuting powers).

On the relationship between the notions of "competent authority" and "data controller" the Commission clarified that all data controllers under the Directive must be competent authorities but a competent authority can be organised in a way of enclosing more than one data controllers within its structure.

Further, the Commission presented the concept of Public-Private Partnerships (PPPs) under the Directive. This allowed clarifying the rules that apply to different situations of cooperation between public authorities and private partners for law enforcement purposes. It was explained that PPPs can only qualify as data controllers under the Directive if they process data for the purposes of the Directive, they decide on the purposes/means of the data processing and have been entrusted, by law, with public authority and public powers. In other cases, they will qualify as processors either (1) under the Directive where processing is done on behalf of competent authorities for the purposes of the Directive or (2) under the GDPR where the processing is carried out for other purposes. Member States had several questions aimed at identifying different specific situations of cooperation between public and private partners for example, how to qualify cases where attorneys or interpreters process personal data in the context of criminal proceedings, on request from a Court or cases where private detectives process personal data, for the purposes of the Directive, on a police request.
2. Relationship with previously concluded international agreements (Article 61)

On Member States’ obligation to align previously concluded international agreements with the Directive, the Commission noted that Article 61 allows for certain flexibility time-wise but requires, as a first step, that Member States map the existing situation. The Commission also explained that, in many cases, it is possible that no renegotiation or reopening of the agreements in question will be necessary, as an appropriate interpretative solution (as it is often the case in practice in particular for transfers between public authorities) could be sufficient for the alignment of the agreements with the Directive. However, the Commission noted that it cannot be excluded that some agreements may conflict with the Directive and, therefore, will need to be amended (e.g. through an additional protocol or some sort of interpretative understanding, complementary agreement etc.). Concerning the bilateral agreements with the US, the Commission noted that the Umbrella Agreement has solved possible existing problems, as it "retroactively" fills the gap. Several Member States mentioned that they have quite a high number of agreements on transfers of data for law enforcement purposes dating back to the 60's and 70's and are deemed to be non-compliant either with the Union law applicable before May 2016 or with the Directive. Against this backdrop, they sought for clarification on the extent of their obligations under this provision and, in particular, they queried whether the adherence of a third country to the Council of Europe Convention 108 could be used for complementing old data transfer agreements, in order to make them compatible with Union law. The Commission underlined that transposition to the internal legal order of a third country of the obligations arising from the existing Convention 108 and in particular the revised version of that Convention is an important element in an alignment assessment. However, such element might not be, by itself, sufficient. One Member State called for the proposal of a model package that could be used for aligning the international agreements with Union law. Another Member State queried on the limits of flexibility under Article 61 and whether it required Member States to include data protection provisions during the revision of an international agreement. The Commission recalled that conclusion of international agreements on this area is subject to compliance with Art. 3(2) TFEU and noted that the time flexibility provided in article 61 is not open-ended.

3. Legally binding instruments providing for appropriate safeguards

The Commission argued that the Umbrella Agreement is a model of a legally binding instrument providing for appropriate safeguards, as referred to in Article 37(1)(a), because it provides for directly enforceable data subject's rights, judicial redress etc. On the other hand, Convention 108, on its own, cannot probably provide for appropriate safeguards because of (i) its level of generality (it does not go into the details of the rules applying to data processing for criminal law enforcement purposes, such as specific agreements or specific domestic laws) and (ii) it lacks certain important safeguards (e.g. judicial redress or independent DPA, which only applies to those countries which have ratified the additional protocol). However, its conclusion and full implementation by a third country might be taken into account in the assessment carried out under Article 37(1)(b).

4. The periodic review of the need for storage of personal data

Regarding the time-limits for storage or for a review of the need for the storage of personal data, as provided in Article 5 of the Police Directive, the Commission suggested storing data
in different categories (victims, experts, suspects etc., as provided by Article 6) and automatically deleting them after a given period, unless the periodic review reveals the need for prolonging the data retention period. One Member State informed that it has already adopted a system similar to the one described by the Commission. Some Member States pointed to a recurrent need of prolonged data retention period, in particular when it might still be possible to reopen the case. The Commission pointed out that appropriate time limits should be established in accordance with the proportionality principle. A decision to prolong the retention period should be supported by sufficient and valid reasons.

5. Technical solutions for logging (Article 25); the extended transposition period

Concerning the obligation to keep logs (Art. 25), one Member State emphasised the financial burden it creates for competent authorities. It considered the obligation to provide justification for operations of consultation and disclosure as cumbersome for the police and technically difficult to implement. By contrast, another Member State informed that it had a system in place running in an effective manner and, therefore, considered itself to be fully compliant with the said Article. Most Member States are expected to make use of the derogation concerning the extended period for implementation of this obligation (Art. 63(2)). The Commission expressed the view that the justification of consultations and disclosures in logs had not necessarily to be extremely detailed and that the aim is to prevent data disclosures for reasons extraneous to the Directive's purposes. The Commission also proposed the use of log collector machines that generate and compile logs for a long period.

6. Mechanisms for whistle-blowers' protection (Article 48)

The Commission presented examples of mechanisms for whistle blowers (required under Article 48). Several Member States informed that they already have in place whistle blower mechanisms with a broader scope than the Directive and queried whether they could rely on them for the purposes of the Directive or would need to have dedicated systems. In particular, one Member State asked whether an Ombudsperson could act as an intermediary between the whistle blower and the competent authority in the context of Article 48. The Commission noted that the most important feature of those systems should be their effectiveness in encouraging the confidential reporting of infringements of the Directive. The provision of Article 48 requires a competent authority to address an infringement complaint in a confidential way. If an independent authority acts as an intermediary and informs the competent authority on the whistle blower’s behalf, this would be in line with the Directive.

7. Replies to various questions of Members

One Member State asked about “necessary information” in Article 7, the relationship between Article 8 and Article 10, about follow up to data subject requests in Article 12, about the differences between general and specific information in Article 13 and about legislative impact assessments fulfilling the obligation from Article 27 to carry out a data protection impact assessment. The Commission replied that “necessary information” in Article 7 is a sort of metadata helping the recipient assessing the accuracy and reliability of data and advised to
use handling codes\(^1\) for that purposes. The relationship between Article 8 and 10 means that processing of special categories of data always have to be provided for by law, and in addition it is allowed only when strictly necessary and subject to appropriate safeguards, also laid down in law. The follow up to requests in Article 12 means that data subjects always need to receive a reply to their requests. The substance and detail of the reply will depend on possible restrictions applied on the exercise of his or her rights. On Article 13, the Commission explained that general information from paragraph 1 could be provided on a website, while specific information from paragraph 2 need to be given directly to data subject, in specific cases that depend on national law (e.g. after the data subject was subject to covert surveillance). On Article 27, the Commission referred to previous discussions in the Expert Group and explained that legislative impact assessments could meet the requirements of Article 27 if they analysed the same processing operations and meet all the requirements of that Article.

Another Member State asked whether the DPO under the Police Directive could be the same person as the DPO under the EU PNR Directive, given that the DPO under the EU PNR Directive has a higher level of independence than the one appointed under the Police Directive. The Commission replied that this could be the same person provided that this person meets the requirements of both Directives.

Finally, one Member State asked how to ensure the possibility for a mandated representation of data subjects before national DPAs and courts, pursuant to Article 55 of the Directive. Several Member States replied that their national procedural laws already provide for even wider possibilities of *actio popularis* than the ones envisaged under Article 55, so they will have no problems with the transposition of this Article.

8. Way forward

The Commission suggested to the Members to meet again towards October and in the meantime to organise a workshop with practitioners (prosecutors, judges, police). However, most of the Members replied that current meetings are very useful and that the bi-monthly rhythm of meetings should therefore be maintained. They also pointed out that it would be too early to engage in dialogue with the practitioners who will have to work with the national laws transposing the Directive, and not the Directive itself. One Member State suggested a greater involvement of national data protection authorities in the work of the expert group.

\(^1\) For example

(1) – accuracy confirmed
(2) – accuracy confirmed to the source but not to the official in charge
(3) – accuracy not confirmed to the source either
(x) – doubtful accuracy