Council of the European Union

Brussels, 27 November 2014
(OR. en)

DS 1573/14

DATAPROTECT

MEETING DOCUMENT

From:	Presidency
To:	JHA Counsellors
Subject:	Proposal for a regulation of the European Parliament and of the Council on the protection of individuals with regard to the processing of personal data and on the free movement of such data (General Data Protection Regulation) [First reading] - One-stop-shop mechanism = Orientation debate

Further to the COREPER meeting of 26 November 2014, delegations find attached a redrafted version of the discussion note.

ANNEX

I. Introductory remarks

The "one-stop-shop" principle, together with the consistency mechanism, is one of the central pillars of the proposed General Data Protection Regulation. In the 2013 October and December JHA Councils Ministers gave the following main orientations for concluding work on the one-stop-shop mechanism:

- in important transnational cases the draft Regulation should establish a one-stop shop mechanism in order to arrive at a single supervisory decision, which would be fast, ensure consistent application, provide legal certainty and reduce administrative burden;

- experts should explore methods for enhancing the "proximity" between individuals and the decision-making supervisory authority by involving the local supervisory authorities in the decision-making process;

- further work at technical level should include investigating the possibility of providing the European Data Protection Board in some cases with the power to adopt binding decisions regarding corrective measures.

The 2014 June Council mandated the **Presidency** to continue work on the one-stop-shop **(…)**. The EL PRES has strived to further address the issues of efficiency of the mechanism and proximity towards individuals.

The **Presidency** has tackled the two remaining points of the one-stop-shop, namely enhancing effective proximity for individuals and entrusting the Board with binding powers in limited cases **(…)**. Therefore, chapters VI**,** VII **and VIII** of the draft Regulation have been intensively discussed in DAPIX.

II. Current situation – no effective solutions for cross-border cases

Today Directive 95/46/EC does not provide for any detailed obligation to coordinate or cooperate between potentially concerned **supervisory authorities (= data protection authorities** (DPAs)). This situation has generated legal uncertainty for companies and fragmented and ineffective protection for individuals in respect to data processing activities with cross-border impact.

More precisely, when a company operates in more than one Member State it must deal with several DPAs, but without any guarantee that these DPAs coordinate or cooperate when adopting their positions. A data subject affected by processing operations of a company operating in several Member States which addresses its complaint to his/her local DPA asking for a corrective measure, may often be granted a measure with limited effect in terms of protection. In other words, the DPA action may often lack effectiveness and comprehensiveness and therefore not satisfactorily address the impact on the individual's rights. If the data subject seeks a more comprehensive protection in such cross-border cases, he/she will have often no other choice than to submit complaints to several DPAs with no guarantee that these DPAs will coordinate and cooperate in view of a uniform decision binding on all of them.

Moreover, when the processing of a company based in only one Member State affects data subjects in other Member States, only the DPA where the company is established can decide on the processing without any role for the other DPAs which may be concerned by the processing.

III. Situation under the draft Regulation

The **Presidency** has further clarified the categories of cases that DPAs have to address. The aim is to have a system based on objective criteria which reflect realities on the ground and to ensure that the decision taken is effective in terms of both strengthened legal certainty for companies and high level of protection for individuals. The text foresees three types of cases.

1. Local cases (Article 51)

The **Presidency** has further clarified the general principle according to which processing situations affecting only one Member State or persons in only one Member State should continue being dealt with only by the local DPA and not be covered by the specific rules of the one-stop-shop.

More specifically, the **current** text provides the following general criteria as regards what is a local case:

- each supervisory authority shall deal with the cases concerning the territory of its own Member State (territorial competence);

- **each supervisory authority shall deal with the cases where the data controller is a public authority or body of that Member State (functional competence);**

- each supervisory authority shall be competent for processing taking place in the context of the activities of an establishment of a controller or a processor on the territory of its Member State or exclusively affecting data subjects on the territory of its Member State (material competence).

A significant number of cases of day-to-day processing are and will continue being local cases and will be dealt with by the local DPA. The decisions of local DPAs will be challengeable before the courts in the Member State of the local DPA.

2. Cross-border cases – One-stop-shop

Processing operations with a cross-border impact raise challenges for companies, individuals and supervisory authorities. The mechanism of the one-stop-shop is intended to deliver enhanced legal certainty, efficiency for businesses and effective proximity for individuals. The mechanism relies on an enhanced cooperation and coordination between a "lead DPA" and other concerned DPAs.

2.1. Criteria for one-stop-shop cases (Article 51a)

The one-stop-shop mechanism should only intervene in important cross-border cases. The **current** text sets forth the following criteria for these important cross-border cases:

1. processing in the context of the activities of an establishment of the same controller or processor established in more than one Member State - in this case the "lead DPA" will be that of the main establishment of the controller or processor;

2. processing by a controller or processor established only in one Member State, but which substantially affects or is likely to affect substantially data subjects in other or in all Member States - in this case "the lead DPA" will be that of the single establishment of the controller or processor.

2.2. Criteria for concerned DPAs (Article 4(19a))

One key feature of the one-stop-shop mechanism that has been further strengthened by the **Presidency** pertains to the involvement of all concerned DPAs in the decision-making process.

The notion of "concerned DPA" covers DPAs which either are concerned because there is an establishment of the controller or processor in its Member State or because data subjects present in its Member State (e.g.: complainants) are substantially affected by the processing. Depending on the nature of the processing at stake (e.g.: pan-European reach or limited only to some Member States) all or only some DPAs could be involved in the one-stop-shop mechanism.

The controller or processor shall indicate its main establishment to the supervisory authority of the Member State where this main establishment is located. This supervisory authority shall inform the European Data Protection Board of this indication. The EDPB keeps a public register of this information.

2.3. Cooperation and joint-decision making (co-decision) (Article 54a)

The lead DPA cooperates with the other DPAs concerned in an endeavour to reach consensus. The lead DPA after having investigated the case (including, where appropriate, with the support of the other DPAs concerned via mutual assistance and joint operations rules) submits to all DPAs concerned a draft decision for their opinion. There are two possible outcomes: the lead DPA and the DPAs concerned should jointly agree on the decision or cannot reach a joint decision.

The jointly agreed decision should cover the results of the investigation of the case carried out. This includes the determination of whether there has been and infringement of the Regulation or not, the actions to be taken in case of infringement (e.g.: prohibition of a form of profiling) or the rejection of a complaint if there has been no infringement.

2.4. Who gives effect to the jointly agreed decision? (Article 54a)

The **current** text clarifies that the jointly agreed decision will be adopted by the DPA best placed to deliver the most effective protection both from the perspective of the controller/processor and of the data subject. While guaranteeing that a single supervisory decision is taken, the IT PRES has ensured that sufficient proximity is provided for also at this stage of the one-stop-shop mechanism. The **current** text differentiates situations in which the jointly agreed decision will be adopted by the lead DPA from situations in which this decision will be adopted by the local DPA.

First, when the jointly agreed decision fully grants the complaint and concerns measures to be taken vis-à-vis the controller/processor, this decision will be given effect by the lead DPA who is the best placed to provide more effective and comprehensive remedy. This includes, *inter alia*, cases of prohibition of processing or the exercise of the rights of access, rectification or erasure.

The lead DPA **shall adopt and** will notify this single decision to the main or single establishment of the controller/processor. It is then the duty of the controller/processor addressed by this single decision, to ensure compliance as regards all its processing activities in the Union. If the controller/processor does not agree with the decision, it may take legal action against the lead DPA. The competent courts will then be those in the Member State of the main or single establishment of the controller/processor.

Secondly, when the jointly agreed decision adversely affects the individual, notably where his/her complaint is rejected, it will be the local DPA which **adopt and** gives effect to this decision in its national legal system as it is the best placed to ensure effective protection and proximity for the individual concerned. If the complainant does not agree with the decision, he/she may take legal action before his/her domestic courts. The competent courts will thus be those in the Member State where the complaint has been lodged.

In all cases where the decision is only partially satisfactory for the **complainant** it will be **adopted by the lead DPA and the local DPA**, and consequently, in case of legal action against the decision, the competent courts will be all the local courts of the concerned parties.

The local DPA should also remain competent for all actions to be taken on their territory as follow-up of the jointly agreed single decision. In particular, the local DPAs keep the competence to monitor and ensure the implementation of the jointly agreed single decision of an establishment on the territory of their own Member State. **To this end the local DPA shall , as set out above, adopt the jointly agreed single decision.**

The local DPA which is the "single contact point" for the individual will also inform the individual on the positive outcome of the complaint as reflected in the jointly agreed decision taken by the lead DPA.

Finally, in urgent cases, the local DPA can also adopt provisional measure in order to protect the rights and freedoms of the data subjects (Article 61).

3. Dispute resolution system for cross-border cases

3.1. Criteria for triggering the dispute resolution system

The one-stop shop mechanism relies on an enhanced cooperation and coordination between the lead DPA and the concerned DAs and aims at a consistent application of the Regulation. In that context, the development of a cooperative culture and the effect of "peer pressure" should result in reaching consensus in most cases, as similar mechanisms introduced in other fields of European law have shown.

The **current** text has therefore introduced a dispute-resolution system as a back-stop for the rare cases, where

- the case concerns an important cross-border situation; and
- no agreement can be reached between the DPAs involved in the case.

3.2. Scenarios for dispute resolution (Article 57(2a))

The **current** text clearly identifies four situations where a dispute resolution should apply:

- conflicts as to the identification of the lead DPA;
- conflicts as to the functioning of cooperation between DPAs (mutual assistance, joint operations case);
- conflicts as to the merits of the one-stop-shop draft decision, notably whether there is an infringement or no infringement of the Regulation;
- conflicts resulting from failure to ask or to follow the opinion of the European Data Protection Board in cases subject to the consistency mechanism (e.g.: binding corporate rules or codes of conduct with cross-border impact).

3.3. Role of the European Data Protection Board

The **current** text foresees that the appropriate forum for the dispute resolution is the European Data Protection Board, which will be composed of all EU DPAs and will have legal personality. This provides therefore the required independence and the necessary expertise. Furthermore, the **current** text provides that the Board in the above four cases will settle the dispute by adopting a binding decision.

The European Data Protection Board shall decide, by two-third majority, on the issue which is under dispute. This decision shall be binding for all DPAs concerned. The lead DPA or the local DPA depending on the outcome of the case (e.g.: rejection of a complaint or actions against the controller/processor) shall give effect to the binding decision of the Board.

By allowing each DPA concerned the right to raise a dispute to the Board and by granting binding powers to the Board to settle disputes, this model further strengthens the involvement of all concerned DPAs and thereby represents a further element of proximity. It essentially gives each of the DPAs concerned a "veto power".

The system should ensure that the natural/legal persons involved in the procedure (the data subject as well as the controller/processor) enjoy the possibility to have the legality of the Board's decision reviewed when this directly affects them. In this respect, the powers of the judicial authorities (ECJ or national courts) to review the legality of the Board's decision should be fully safeguarded and it should be ensured that the parties may challenge the legality of such decision at any appropriate stage in the procedure, in order to grant the effective judicial protection of the fundamental rights concerning personal data. To this end, it appears appropriate to provide that the Board's decision is brought to the knowledge of the parties.

Orientation debate

In this light, the Presidency invites the Council to endorse the constituent elements of the 'one stop shop' mechanism as set out above and consequently give guidance to the technical working party for further work on this matter.