**COUNCIL OF THE EUROPEAN UNION**

**Brussels, 18 September 2013**

**13643/13**

**Interinstitutional File: 2012/0011 (COD)**

**LIMITE**

**DATAPROTECT 127**
**JAI 781**
**MI 767**
**DRS 169**
**DAPIX 109**
**FREMP 126**
**COMIX 502**
**CODEC 2025**

**NOTE**

| | |
|---|---|
| from: | Presidency |
| to: | COREPER |
| No. prev. doc.: | 12929/13 DATAPROTECT 118 JAI 696 MI 697 DRS 150 DAPIX 104 FREMP 117 COMIX 475 CODEC 1880<br>7565/13 DATAPROTECT 32 JAI 211 MI 211 DRS 52 DAPIX 54 FREMP 30 COMIX 175 CODEC 608 |
| No. Cion prop.: | 5853/12 DATAPROTECT 9 JAI 44 MI 58 DRS 9 DAPIX 12 FREMP 7 COMIX 61 CODEC 219 |
| Subject: | General Data Protection Regulation - The one-stop-shop mechanism |

1. The one-stop-shop principle, as laid down in Section II of Chapter VI, has been discussed by the Working Party on Information Exchange and Data Protection (DAPIX) at meetings of 8-9January, 27 March, 3-4 July and 9-10 September 2013. Various delegations have produced documents on this and the compilation of comments on Chapters VI and VII is set out in 7105/4/13 REV 4 DATAPROTECT 28 JAI 182 MI 170 DRS 42 DAPIX 49 FREMP 24 COMIX 141 CODEC 476 + ADD 1.

**Commission proposal**

2. The one-stop-shop principle together with the consistency mechanism is one of the central planks of the Commission proposal for a General Data Protection Regulation. Where the processing of personal data in the context of the activities of an establishment of a controller or a processor in the Union takes place in more than one Member State, one single supervisory authority should be competent for monitoring the activities of the controller or processor throughout the Union and taking the related decisions, in order to increase the consistent application, provide legal certainty and reduce administrative burden for such controllers and processors. The competent authority, providing such one-stop shop, should be the supervisory authority of the Member State in which the controller or processor has its main establishment (Article 51(2) and recitals 97 and 98).

3. The one-stop-shop principle is linked with the mandatory co-operation between the supervisory authorities through the European Data Protection Board, which is aimed at ensuring the consistent application of this Regulation throughout the Union (Recital 105). The one-stop-shop principle is thus clearly aimed to be an advantage for business within the internal market, which in the international digital economy, should be given the advantage of having to deal only with one supervisory authority throughout the European Union. However, it does not affect the competence of the supervisory authority for the supervision of processing activities of the controller or processor which are limited to one single Member State.

4. The principle sets out the supervision of the processing activities of the controller or the processors in all Member States, but under Article 73(1) data subjects would have the right to lodge a complaint at a supervisory authority in any Member State (e.g.: where he or she has his or her residence or where the controller is established or to another supervisory authority). This would leave, as it is currently the case under the 1995 Data Protection Directive, supervisory authorities the competence to hear complaints by data subjects and data subjects to decide where they want to go. At the same time, only the main-establishment supervisory authority would have the competence to take measures intended to produce legal effects regarding processing by that controller.

**Current situation**

5. Under the 1995 Data Protection Directive, the territorial scope of application of the Directive is governed by Article 4(1), according to which a Member State, as a rule, is to apply the national provisions it adopts pursuant to the Directive to the processing of personal data where there is an establishment of the controller on its territory, or in cases where the controller is not established in the Union, if he makes use of equipment situated on the territory of the Member State for the purposes of processing personal data.

6. This implies that a Member State has jurisdiction to supervise processing of personal data (and, should the processing be in violation of EU law, to have penalties imposed on the controller or processor), only if there is an establishment on the territory of that Member State. The mere fact that one or several individuals (data subjects) in a Member State claim to have been the victim of wrongful data processing operations carried out in another Member State, does, in the current situation, not give jurisdiction to the Member State of the complainant if there is no establishment of the controller/processor in that Member State. Furthermore, Directive 95/46/EC provides no cooperation mechanism between the supervisory authorities of the Member States whose residents are concerned by the processing activities.

**Member States concerns**

7. The Commission proposal for a one stop-shop principle has been the subject of several discussions in the Working Party on Information Exchange and Data Protection (DAPIX). In the course of these discussions the vast majority of delegations have voiced various and detailed criticisms on this principle. The most important concerns can be grouped under the following headings:

***Exercise of individual rights***

8. Probably the most important point of concerns on the one-stop-shop principle is that, while it is intended to bring benefits to businesses, it would risk to be detrimental to the protection of the data protection rights of individuals, because it will have a consequence that supervision functions will be concentrated in the hands of one supervisory authority, which will be the single authority for deciding on (certain) measures. In certain situations measures will be decided upon by the supervisory authority of the main establishment and not by those of the Member States where the controller has other establishments[1].

9. This 'lack of proximity' of the deciding supervisory authority admittedly already exists under the current legal regime as the 1995 Data Protection Directive gives no jurisdiction to the Member State where a person lodges a complaint regarding an, alleged data breach, if there is no establishment or equipment in that Member State.
Regardless of the view one takes of the possibilities that exist currently for supervisory authorities to react to alleged data breaches, several Member States expressed the view that the one-stop-shop principle will reduce the powers for the supervisory authorities of the Member States to which complaints have been lodged, if the supervision will be concentrated in the hands of a single supervisory authority.

10. Another prong of this argument is that, irrespective of whatever legal arrangements the future Data Protection Regulation may contain for concentrating supervision in the hands of the supervisory authority of the main establishment Member State, data subjects who claim to have been the victim of data protection violations may seek remedies through courts of law in other Member States. Various avenues are available to data subjects: they may sue for civil damages or, in those Member States where data protection violations have been criminalised, may lodge a criminal complaint against the alleged offender. These judicial remedies may even be exercised pending a decision under the consistency mechanism. The rules on jurisdiction of the courts hearing those claims may well be much extensive than those contained in the Regulation. In addition, data subjects may ask a court of law to overturn a decision - or even a refusal to take a decision - by a supervisory authority.

[1] Article 74(4) of the Commission proposal did allow for the supervisory authority of the Member State of a complainant to appeal against a decision of the supervisory authority of the main establishment in that Member State.

11. There is thus a distinct risk that any attempts, via the Regulation, to arrive at more unified application of data protection supervision practices by data protection authorities will be undone by judicial decisions. Indeed, this may well be the Achilles' heel of any alternative to the Commission proposal for a one-stop-shop principle, as, under any scenario, it is difficult to see how the Regulation could prevent a court of law from taking a different view than that of the supervisory authority or authorities concerned.

***Transfer of sovereign powers***

12. The Commission proposal for the one stop-shop principle implies a transfer of powers. If the supervisory authority of the Member State where the controller has its main establishment is to be the sole responsible for supervision of that controller, including regarding processing operations carried out by establishment of that controller in other Member States, this implies that decisions can be made only by the supervisory authority of the main establishment and no longer by the supervisory authority of the other Member State. The fact that each Member State will remain exclusively competent for the exercise of powers on the territory of its Member State (see Article 51 (1) of the Commission proposal), does not detract from this. Article 63 of the Commission proposal makes it clear that there is an obligation to enforce decisions by the supervisory authority of one Member State in all other Member States.

13. In the light of those Member State concerns, the latest Presidency redraft of Chapters VI and VII had identified some powers for which the decision could be made solely by the main establishment supervisory authority. Whereas the choice as to which powers of the supervisory authority of the main establishment should exactly be entrusted with, should be the subject of further discussions at expert level, the one-stop-shop principle appears to make this inevitable. Not to do so implies that all other supervisory authorities are able to supervise the establishments located on their territory and the one-stop-shop principle is emptied of any binding character. As will be discussed under point 19 the main-establishment supervisory authority can be turned into a 'lead authority', which should ensure coordination and cooperation between the supervisory authorities concerned, but has no power to impose any binding decisions on supervisory authorities of other Member States.

***Legal uncertainty and defragmentation of oversight***

14. Many delegations have argued that the implementation of the one-stop-shop principle as proposed by the Commission would lead to legal uncertainty. Giving a central role to the supervisory authority of the main establishment Member State and coordinating the positions of other supervisory authorities through the consistency mechanism will inevitably require time. Pending this coordination, there may be legal uncertainty as to whether supervisory action can/should be taken. At times it may be uncertain whether the coordination mechanism will result in a coordinated result. It is already recognised by Member States that such coordination mechanism will need some filters, so there will inevitably cases that will be submitted to the consistency mechanism, but where eventually no decision will be taken via the consistency mechanism.

15. There may also be cases where various supervisory authorities take different views as to where the main establishment of an undertaking or a group of undertakings is located. Pending resolution of these questions there will - to some extent - also be uncertainty regarding the applicable law. Whilst fundamental data protection rules will be laid down in the regulation, other substantive and especially procedural rules will be governed by the law of the supervisory authority which is responsible for supervising the controller.

16. Another argument linked to the legal uncertainty that may flow from the practical implementation of the one-stop-shop principle is that rather than leading to the intended concentration of supervision, it may result in fragmentation of supervision. This can happen due to the fact that, as regarding processing activities carried out in other Member States, the main establishment supervisory authority will exercise some, but not all of the powers that supervisory authorities will be entrusted with further to the Regulation. At least the exercise of investigatory powers will, given the territorial executive jurisdiction, remain with the supervisory authority of the Member State where the processing takes place.

***Red tape: bureaucratic and cost implications***

17. Delegations have voiced concerns on the bureaucratic and cost implication of the consistency mechanism that will need to be followed each time the one-stop-shop principle is to be applied. The particular concerns regarding a need to translate documents for every case to go through the consistency mechanism could probably be addressed by common language arrangements by the European Data Protection Board and the supervisory authorities involved, as it is the case today under Directive 95/46/EC. The fact that the administrative and financial burdens will have to be incurred for every case to be submitted to the consistency mechanism, even where eventually no decision will be taken, compounds these concerns.

**Possible alternatives to the Commission proposal**

18. During the discussions delegations have floated ideas for alternatives to improve or to change the one-stop-shop principle as proposed by the Commission. The Presidency has hereafter endeavoured to succinctly summarise these suggestions, being fully aware that these summaries may not do justice to the way in which some delegations have presented and/or are developing their ideas.

***Restrict the powers of the main establishment supervisory authority***

19. A variation on the one-stop-shop principle as proposed by the Commission is to maintain the exclusive jurisdiction of the main establishment supervisory authority, but to limit it to the exercise of certain powers in relation to the controllers (such as authorisation and consultation powers, e.g. responding to consultation requests by Member State institutions and bodies, establishing and making public a list in relation to the requirement for a data protection impact assessment pursuant to Article 33(2a); authorising contractual clauses referred to in Article 42(2)(d) and approving of binding corporate rules pursuant to Article 43). Other supervisory powers in relation to monitoring compliance with and investigating possible breaches of data protection rules would be in the hands of the supervisory authority of the Member State where the processing takes place. The main advantage of this option is that it both keeps the benefit for companies of having to deal with only one supervisory authority and allows individuals to deal with their own supervisory authority. The obvious disadvantage is the fragmentation of supervisory powers between various supervisory authorities with a risk of conflicting decisions by different supervisory authorities.

***Co-decision by supervisory authorities concerned***

20. In lieu of concentrating certain decision-making powers in the hands of the single supervisory authority of the Member State of the main establishment, it has been suggested that the supervisory authorities of all Member States concerned could decide on the measures to be taken regarding a controller who has processing operations in those Member States. The main advantage of this model is that it avoids the need to have decisions of a supervisory authority of one Member State enforced in another Member State. The main drawback may be that it is difficult to see how supervisory authorities could then be obliged to reach a common decision. Should the Regulation contain some rules on majority voting between the supervisory authorities concerned, this in reality would also allow for a decision being imposed on supervisory authorities.

***Submitting a matter to the European Data Protection Board***

21. Two other alternatives consist of giving a certain role to the European Data Protection Board (EDPB) by allowing to submit (draft) decisions of a supervisory authority to the Board. Under those alternatives every supervisory authority that has jurisdiction with regard to certain processing activity, will be able to exercise its supervisory powers, but under certain circumstances a case could be submitted to the European Data Protection Board for resolution. It has been established that from an EU law point of view, the EDPB as proposed by the Commission cannot be vested with the power to take legally binding decisions. It appears that it would be possible only in a limited way to overcome this.

22. A first way is to provide for the power of the Commission to adopt implementing acts in clearly defined circumstances set out in the Regulation after taking the utmost account[1] of the EDPB opinion. These powers would have to be much more restrictive than the broad powers proposed in Articles 60 and 62(1)(a) of the Commission proposal, which would amount to a simplified infringement procedure without respecting the conditions provided for in Article 258 TFEU. If however, strictly-circumscribed implementing powers were conferred on the Commission, for example in cases where there are conflicting views between supervisory authorities on clearly-defined subjects or where the competent supervisory authority does not submit a certain type of draft measure intended to produce legal effects to the EDBP or does not comply with the obligations for mutual assistance or for joint operations and the EDBP has issued an opinion which the lead authority refuses to follow, the Commission, after taking the utmost account of the EDBP's opinion, could adopt an implementing decision which would bind that supervisory authority.

23. Another way of overcoming the lacking of binding nature of EDPB opinions is to decide to give legal personality to the EDPB, thus transforming it into an "agency". Only clearly defined executive powers which should exclude too broad and discretionary powers involving policy choices (so-called "Meroni" case law[2]) could thus be conferred on this agency. In such case, the EDPB would not only be empowered but would also be obliged to adopt measures where clearly defined criteria laid down in the Regulation are fulfilled. Apart from such cases that could be decided by the EDPB on the basis of clearly defined criteria, any other model could only encourage Member State supervisory authorities to take the utmost account of the EDPB opinion, but would not be able to oblige them to do so.

---

1 See contribution of the CLS in doc. 16204/08.

2 Case 9/56 Meroni v High Authority.

24. The first option for submitting a matter to the EDPB implies enabling a supervisory authority to submit a case to the EDPB prior to a decision becoming final. This may be a supervisory authority that has jurisdiction with regard to the controller or the supervisory authority at which a data subject has lodged a complaint. In such case the Regulation would have to provide for a system by which supervisory authorities are informed, probably via the EDPB Secretariat, that a draft decision is being prepared by a supervisory authority in case with cross-border implications which might affect them. A certain time period would have to be provided during which the supervisory authorities of the Members States concerned could request an opinion from the EDPB. Pending the decision of the EDPB, the decision of the supervisory authority could not become final. The opinion of the EDPB could become binding via Commission's implementing act as set out in paragraph 22.

25. A second option for submitting a matter to the EDPB implies that each supervisory authority has jurisdiction with regard to certain processing activity and will exercise its full supervisory powers and make final decisions. However, in this option supervisory authorities from other Member States would have the possibility to submit a final decision made by the competent authority to the EDPB, as a type of appeal mechanism. Again this possibility of submitting a case to the EDPB could be opened up to the supervisory authority that has jurisdiction with regard to the controller or to the supervisory authority at which a data subject has lodged a complaint. It could also be envisaged to allow a controller which has establishments in several Member States to submit to the EDPB a decision of a supervisory authority with regard to him. The opinion of the EDPB could become binding in the way set out in paragraph 23.

**Questions**

26. In view of the above, the Presidency invites delegations to reply to the following questions.

1. *Do Member States accept that in cases with a cross-border element the supervisory authority of the Member State of the main establishment should have the exclusive power/jurisdiction to take legally binding decisions (after having consulted other concerned supervisory authorities)?*
    - 1.1. *If so, do they accept that such exclusive jurisdiction is valid in all cases or should it be restricted to certain cases, e.g. where the controller has voluntarily subjected itself to the one-stop-shop principle?*
    - 1.2. *If so, should this include administrative fines under Article 79?*

2. *In case Member States do not accept that the supervisory authority of the Member State of the main establishment should have the exclusive competence to take measures intended to produce legal effects, do they see a need for an alternative? If so which of the following alternatives, do they prefer?*
    - 2.1. *Restrict the powers of the main establishment supervisory authority.*
    - 2.2. *A model of co-decision by the supervisory authorities concerned.*
    - 2.3. *A model reinforcing the a priori involvement of the European Data Protection Board (as described in paragraph 24).*
    - 2.4. *A model reinforcing the a posteriori involvement of the European Data Protection Board (as described in paragraph 25).*