



**COUNCIL OF
THE EUROPEAN UNION**

Brussels, 1 October 2013

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

**14074/1/13
REV 1**

LIMITE

**DATAPROTECT 134
JAI 829
MI 802
DRS 177
DAPIX 115
FREMP 137
COMIX 519
CODEC 2128**

NOTE

from: Presidency
to: COREPER

No. prev. doc.: 13643/13 DATAPROTECT 127 JAI 781 MI 767 DRS 169 DAPIX 109
FREMP 126 COMIX 502 CODEC 2025
13808/13 DATAPROTECT 129 JAI 794 MI 776 DRS 171 DAPIX 110
FREMP 128 COMIX 509 CODEC 2058
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: 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)
- The one-stop-shop mechanism

Commission proposal

1. 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).
2. 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.
3. 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

4. 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.
5. 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

6. The Commission proposal for a one stop-shop principle has been the subject of discussions in the Working Party on Information Exchange and Data Protection (DAPIX) at the meetings of 8-9 January, 27 March, 3-4 July and 9-10 September 2013. In the course of these discussions the vast majority of delegations have voiced various and detailed criticisms on this principle. The most important concerns are summarised in 13643/13 DATAPROTECT 127 JAI 781 MI 767 DRS 169 DAPIX 109 FREMP 126 COMIX 502 CODEC 2025. Various delegations have produced documents on this¹.

¹ 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. See also the proposal by the Italian delegation: 12879/13 DATAPROTECT 116 JAI 688 MI 691 DRS 148 DAPIX 102 FREMP 115 COMIX 472 CODEC 1858.

7. At the COREPER meeting of 25 September 2013 it appeared that most Member States were in favour of the philosophy underlying the one-stop-shop mechanism, however, only a few accepted that the main establishment authority could have the exclusive jurisdiction to supervise all the processing activities of the company (controller) concerned and decide exclusively upon all measures (including penalties). The most important point of concern regarding the one-stop-shop principle is that, while it is intended to bring benefits to businesses, it risks to be detrimental to the protection of the data protection rights of individuals. In this regard the main concern is proximity: the individual needs to have the possibility to communicate with and obtain a decision from the supervisory authority closest to him or her, which may not be the case if all supervision functions and the concomitant powers will be concentrated in the hands of the authority of the main establishment. Furthermore, the individual should have the right to go to his or her 'local' supervisory authority as well as use a judicial remedy against a decision - or the omission to take a decision - by his or her supervisory authority before to his or her 'local' court. Moreover, individuals who claim to have been the victim of data protection violations may seek remedies through (civil or criminal) courts of law in other Member States rather than relying on a decision by a supervisory authority.

Improvements to the Commission proposal

8. It is clear that the one-stop-shop principle as proposed by the Commission will need to be improved in order to take account of the Member State concerns. Following the COREPER meeting of 25 September 2013 and the JHA Counsellors meeting of 30 September 2013, the Presidency has endeavoured to outline a number of elements for the further work.

Which powers for the main-establishment supervisory authorities?

9. A first possible variation 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. In order to be able to act as single interlocutor for controller and processors with establishments in other Member States regarding all their processing activities in the European Union, the 'main-establishment' supervisory authority needs to be able to exercise some powers, for example such as authorisation, consultation powers and also certain monitoring powers regarding processing operations in other Member States. These monitoring powers need not necessarily be exercised exclusively by the main establishment supervisory authority, but could also be exercised by the 'local' supervisory authorities. Each supervisory authority should remain competent to receive complaints from data subject, to support them in the exercise of their rights, in relation to monitoring compliance with and investigating possible breaches of data protection rules that took place on their territory. The 'local' authority would also remain competent for imposing fines.

10. The exact description of the powers that should be vested exclusively in the main establishment authority under this model will of course need to be the subject of further discussion at expert level, but the Presidency is inviting the Council to provide some guidelines as to the type of powers that should be exercised exclusively by the main establishment supervisory authority.

Co-decision by supervisory authorities

11. Another possible variation to the Commission proposal has been put forward by the French delegation¹. In lieu of concentrating certain decision-making powers in the hands of the single supervisory authority of the Member State of the main establishment, the French delegation has proposed 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 scope of this model could obviously be restricted to the most important transnational cases and should not be applied in petty cases. The main-establishment authority would still act as a the single interlocutor for a company with various establishments in different Member States, but would not be vested with an exclusive jurisdiction to take certain decisions, as these would be taken by all supervisory authorities involved under a co-decision model.

12. The French proposal contains a number of procedural steps and rules, including deadlines and voting rules by which supervisory authorities should reach a common decision. It would require further detailed discussion at expert level to investigate if and how a national independent supervisory authority could be 'obliged' to adopt and implement a decision through a co-decision procedure. An apparent 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. These decisions would be decisions under national law and an individual or company who disagrees with a final decision under the co-decision model, will therefore have to lodge a remedy with a national court.

¹ 13808/13 DATAPROTECT 129 JAI 794 MI 776 DRS 171 DAPIX 110 FREMP 128
COMIX 509 CODEC 2058.

Enhanced involvement of 'local' supervisory authorities

13. For those cases in which the supervisory authority of the 'main establishment' Member State would have exclusive power and thus act as single supervisory interlocutor, the draft Regulation should provide additional ways of involving authorities from other Member States and in particular from those Member States where an individual has lodged a complaint. This enhanced involvement of 'local' supervisory authorities could contribute to the 'proximity' which is the main concern of Member States. There are different ways in which the 'local' supervisory authorities could be involved.
14. It could be envisaged that the 'main-establishment' supervisory authority could only decide to exercise its exclusive powers after having consulted the other supervisory authorities concerned 'with a view to reaching consensus'.
15. Another alternative is that, with a view to enhancing uniformity of decisions taken by supervisory authorities, the 'local' authority that has received a complaint would be allowed to submit a draft measure to the 'main-establishment' authority. In case the 'main-establishment' authority disagrees on the draft measure, a 'dispute settlement' procedure within the EDPB triggered by any of the two authorities could be envisaged.

Appeal to the European Data Protection Board (EDPB)

16. The risk of conflicting views between different supervisory authorities in transnational cases could potentially be offset by adding a possibility to submit a final decision prepared by a supervisory authority to the EDPB, as a type of appeal mechanism which would increase the efficient and reliability of the system as a whole. This possibility of submitting a case to the EDPB could be open to the supervisory authority that has jurisdiction with regard to the controller and to a supervisory authority at which a data subject has lodged a complaint. Obviously rules would have to be put in place in order to limit the number of cases that could be submitted to the EDPB under such appeals mechanism so as to avoid that the EDPB would be flooded with cases. It could also be envisaged to allow a company (controller) which has establishments in several Member States to submit to the EDPB for an appeal a decision of a supervisory authority with regard to him.

17. However, the EDPB as initially proposed by the Commission cannot be vested with the power to take legally binding decisions. It could be envisaged that the EDPB opinion could become binding firstly by giving legal personality to the EDPB and secondly by conferring upon it clearly defined executive powers which should exclude too broad and discretionary powers involving policy choices (so-called 'Meroni' case law¹). 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. These measures would not be decisions of a normative or political nature, but legally binding administrative decisions on the supervisory authorities. Further discussion at expert level is required in order to decide upon: (1) the cases in which a matter could be submitted to the EDPB by supervisory authorities; and (2) the clearly defined criteria upon which the EDPB should decide. An action for the annulment of a decision by the EDPB would have to be lodged at the General Court of the European Union (cf. Article 263 TFEU).

Questions

18. *In view of the above and with a view to improving the Commission proposal for a one-stop-shop mechanism, it is suggested that COREPER invites the Council to provide guidance for further work at expert level on elements of the one-stop-shop mechanism by indicating:*

(1) Whether, for transnational cases the work should continue along:

- a) a model which restricts the exercise of certain powers for the supervisory authority of the Member State where a company has its main establishment; or*
- b) a co-decision model;*

(2) In case a preference is expressed for the first model, which powers can be exclusively exercised by the supervisory authority of the Member State where a company has its main establishment regarding processing activities anywhere in the Union: only 'authorisation and consultation' powers or also other powers such as 'corrective powers' and 'sanctioning powers';

¹ Case 9/56 Meroni v High Authority.

(3) *How to enhance the involvement/cooperation with concerned 'local' supervisory authorities in decisions of the supervisory authority of the main establishment either by:*

- a) a consensus-seeking model (as described in paragraph 14); and/or*
- b) by providing the 'local' supervisory authority the power to submit a draft decision to the 'main-establishment' supervisory authority (as described in paragraph 15);*

(4) *Whether the competent Working Party should examine which clearly defined executive powers can be entrusted to the European Data Protection Board (EDPB), when given legal personality, in view of increasing the consistency of the application of EU data protection rules, with particular attention to:*

- a) the cases in which a matter could be submitted to the EDPB; and*
- b) the criteria upon which the EDPB should decide.*
