COUNCIL OF THE EUROPEAN UNION

Brussels, 4 December 2013

17025/13

Interinstitutional File: 2012/0011 (COD)

DATAPROTECT 185
JAI 1084
MI 1104
DRS 214
DAPIX 150
FREMP 200
COMIX 646
CODEC 2771

NOTE

from:	Presidency
to:	Council
No. prev. doc.:	16626/3/13 DATAPROTECT 177 JAI 1042 MI 1063 DRS 208 DAPIX 145 FREMP 192 COMIX 625 CODEC 2675
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) - Essential elements of the one-stop-shop mechanism

Background

1. The one-stop-shop principle has been discussed by the Working Party on Information Exchange and Data Protection (DAPIX) at meetings of 8-9 January, 27 March, 3-4 July, 9-10 September, 17-18 October, 7-8 and 20 November 2013. Various delegations have produced documents on this[1]. This note refers to, but is not aimed to seek approval of the latest Presidency draft legal text set out in the annex of 16626/1/13 REV 1 DATAPROTECT 177 JAI 1042 MI 1063 DRS 208 DAPIX 145 FREMP 192 COMIX 625 CODEC 2675.

2. The topic was debated at the Council meeting of 7-8 October 2013, at which the Chair concluded, *inter alia*, that:

a) 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.

b) further expert work on this should continue along a model in which a single supervisory decision is taken by the 'main establishment' supervisory authority but the exclusive jurisdiction of that authority would be limited to the exercise of certain powers;

c) the Working Party 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. This proximity is an important aspect of the protection of individual rights;

d) the competent Working Party should explore which powers could be entrusted to the European Data Protection Board (EDPB),

In this regard, the Council Chair also specified that it should be investigated to what extent elements of the co-decision model could be incorporated.

[1] The compilation of comments on Chapters VI and VII is set out in 7105/6/13 REV 6 DATAPROTECT 28 JAI 182 MI 170 DRS 42 DAPIX 49 FREMP 24 COMIX 141 CODEC 476.

3. The one-stop-shop principle purports to be an advantage for businesses: it aims at ensuring compliance with the Regulation, increasing consistent application and legal certainty for enterprises, data subjects and supervisory authorities.

Proximity and competence of 'local' supervisory authority

4. The one-stop-shop mechanism, as initially proposed by the Commission, covered only the situation of processing in the context of the activities of an establishment of the same controller or processor established on the territory of different Member States. Member States have expressed a clear wish that their data protection authorities could also have legal standing to act - on their territory - in cases where processing which physically takes place outside their territory affects their data subjects.

5. This issue has been approached from the angle of the competence of the data protection authorities. Under the current legal regime, Article 28(4) of the 1995 Directive provides that '[e]ach supervisory authority shall hear claims lodged by any person, or by an association representing that person, concerning the protection of his rights and freedoms in regard to the processing of personal data', means that affected data subject can lodge a complaint at their 'own' supervisory authority. However this does not imply that the processing underlying the complaint is governed by the national law of that Member State. This follows from the definition of territorial applicable law (Article 4(1) (a), (b) and (c) of Directive 95/46/EC). That Directive gives as the main criterion to trigger the applicability of national law the fact that 'the processing is carried out in the context of the activities of an establishment of the controller on the territory of the Member State'. This criterion is thus linked to the presence on the Member State territory of the entity carrying out the processing concerned and not to the data subjects affected.

6. As the Regulation will - by its very nature - not contain any rules on applicable law, the Presidency believes that it is very important to clarify in the future Regulation the question of the competence of the local supervisory authority on its own territory. It has endeavoured to do so by introducing a new paragraph 1 into Article 51, which refers to the following alternative criteria:

- the establishment of the controller or processor;
- the fact that the data processing affects data subjects on its territory; or
- the fact that a controller not established in the Union is processing personal data in the cases referred to in Article 3(2).

7. The proximity, of which the importance was emphasised at the October JHA Council, is ensured by the involvement of the local supervisory authorities in the decision-making process by the main establishment authority, by the fact that that each authority retains jurisdiction in cases affecting individuals within its territory, and the possibility for local authorities to oppose a draft measure and refer the matter to the Board. The possibilities for judicial redress (see para. 28) also contribute to proximity.

8. Proximity may also be further enhanced by clarifying that a supervisory authority is competent whenever data subjects on its territory are affected by the processing of their personal data by a controller or processor, even if it is established in another Member State. Obviously such competence should exist only on the national territory and regarding processing by a controller/processor in another Member State that extends to data subjects in other Member States and should not allow supervisory authorities to 'rule' on processing that took place in the context of the use of services or purchase of goods in another Member State. The criteria for determining the territorial competence of the data protection authorities are thus not only linked to the presence of a processing entity in the territory, but also to that of the data subjects affected. This also chimes in with a remark made by several delegations that in the digital era it does not make sense to link competence exclusively to the geographical location of the processing entity. The argument has also been made that linking the competence of a supervisory authority exclusively to the location of its (main) establishment may allow companies to engage in 'forum shopping' as - in spite of the harmonisation provided by the Regulation - they may choose to establish them in a Member State which they perceive has a more lenient supervisory authority. In the latest Presidency draft, the 'local' supervisory authority will be competent on its territory whenever one of 'its' data subjects has been affected by the processing. Subject to the possible attribution to the main establishment supervisory authority of exclusive competence to adopt corrective measures, 'local' supervisory authorities will be able to perform all their duties and exercise all their powers (monitoring, investigatory, corrective and authorisation) on their territory.

9. When the 'local' authority which investigates a case and finds that the faulty processing needs to be addressed through corrective measures, it will have to transmit the case to the supervisory authority competent for the main establishment of the controller responsible for that faulty processing. Some Member States appear to be of the opinion that it is somewhat contradictory to provide that each 'local' supervisory authority has competence regarding processing affecting 'its' data subjects, when this competence is in reality emptied of its meaning as soon as the authority deems that the corrective powers need to be adopted.

10. These delegations are of the opinion that a supervisory authority of a Member State whose data subjects are affected by processing by a controller established in the territory of another Member State, should merely be given a procedural right to be closely involved in the decision-making by the main establishment supervisory authority. The competence of supervisory authorities would thus - as is the case in the latest Presidency draft - be limited to cases where the entity carrying out the processing concerned is established on the territory of the Member State concerned.

11. In that scenario, the local authority would still have the power under Article 52 to exercise its duties (such as providing information to the data subject and dealing in general terms with complaints received), but it would not be competent to decide on any measures regarding the faulty processing if the establishment carrying out the processing is not on its territory. It could also be foreseen that the lodging of a complaint at a 'local' authority could provide it with same 'procedural' possibilities (such as submitting a draft measure, see para. 23) as provided in the latest Presidency draft (co-operation and consistency mechanism). As in practice it will be very easy to lodge such complaint - certainly for data protection organisations (NGOs) - the procedural requirement of a complaint would in reality not constitute a very high threshold.

Powers of the supervisory authority

12. Regarding the processing activities of a controller or processor that fall within the scope of the one-stop-shop mechanism, the Presidency has paid heed to the call made in the Council by trying to identify which powers should the supervisory authority of the main establishment exercise exclusively, that is excluding the exercise of those powers by local authorities. In the course of previous discussions on the Commission proposal for a one stop-shop principle, one of the criticisms which has been voiced on this principle related to a perceived transfer of powers and the related need to enforce decisions of another Member State. At least one Member State has raised serious constitutional problems as regards the legal effects for citizens and businesses in other Member States of measures adopted by the main establishment supervisory authority, which will need to be further addressed. In view of the discussions held and in view of the analysis of the possible exclusive exercise of different types of power by the main establishment supervisory authority, the Presidency thinks that the one-stop-shop mechanism can be constructed along the elements set out hereafter.

13. *monitoring powers:* to be exercised on its own territory by each supervisory authority regarding processing for which it is competent, that is processing by establishment of the controller or processor on its territory or affecting data subjects on its territory.

14. *investigatory powers:* in accordance with the territoriality principle set out at the beginning of Article 51, these can be exercised by each supervisory authority only on their own territory. In case a main establishment authority needs to have investigations carried out on the territory of another Member State, it will have to request this to the supervisory authority of that Member State via mutual assistance channels.

15. *authorisation powers*: under the latest Presidency draft of the Regulation, the authorisation procedure for Binding Corporate Rules (BCRs - Article 43) and contractual clauses (Article 42(2)(c) and (d)) provides that they need to be submitted by the main establishment supervisory authority to the EDPB. This is not the case for prior consultation (Article 34) which, following authorisation, can be used by the controller. In the future, the Working Party may look into ways of expanding authorisation powers so as to enable controllers to apply for an EU-wide authorisation, taking into account the articulation with prior consultation, certification mechanisms and codes of conduct as well as the possibilities of providing for a confirmation of compliance with the legal requirements of the Regulation.

16. The substantive articles on authorisation should be redrafted as regards EU-wide authorisation. The one-stop-shop mechanism should apply to EU-wide authorisations, for which only the main establishment supervisory authority would be competent. In cases of an EU-wide authorisation or confirmation of compliance, all supervisory authorities will be involved through the European Data Protection Board (EDPB). In this case the controller should directly apply to the supervisory authority of the main establishment, which should forward the application to the EDPB. All supervisory authorities receive the application and a draft measure prepared by the main establishment authority.

17. *corrective powers*: the basic principle here is that these powers need to be exercised by each supervisory authority regarding processing for which it is competent, that is processing by an establishment of the controller or processor on its territory or affecting data subjects on its territory. The inclusion of the latter criterion will on the one hand allow the data subject to have its complaint dealt with by its 'local' supervisory authority (proximity) and on the other hand enable the supervisory authority dealing with the complaint to act 'on the spot'.

18. In trying to identify - as requested by the Council - whether and in which cases corrective measures should be adopted exclusively by the supervisory authority for the main establishment, the Presidency presented the following approach. The Presidency suggested to limit the exclusive power of the main establishment supervisory authority to adopt corrective measures to those cases in which the local authority dealing with a case is not the one competent for the (main) establishment deciding on the impugned processing. The arguments for providing the main establishment supervisory authority with the exclusive power to adopt corrective measures are the following. Were the 'local' supervisory authority to impose sanctions in such case, it would be imposing them on an establishment which is not responsible for the decision leading to the faulty processing. A purely local approach would neither be satisfactory in cases where there is no establishment on the territory of the Member State of the 'local' supervisory authority, as that authority will not have the power to carry out any investigations regarding the controller or processor and neither the power to enforce any sanctions. While it may adopt corrective measures, it will not have the possibility to serve these (not even warnings and/or reprimands) on the controller/processor, as it is not 'present' within the territory of that Member State.

19. It could therefore be envisaged to give the main establishment supervisory authority the exclusive power to adopt corrective measures in the cases where the main establishment was the decision-making establishment, but in all other cases the 'local' supervisory authority should be able to adopt corrective measures. Such approach would also do away with any need for extraterritorial enforcement of corrective measures adopted by the supervisory authority responsible for the main establishment, as these corrective measures would always be served on the main establishment present within its territory.

20. This approach has, however, been criticised. Some Member States are of the opinion that it is not feasible to require the supervisory authorities to determine in each cross-border case which was the 'decision-making' (main) establishment. More importantly, a number of delegations appear to be of the opinion, that even in limited number of cases, to provide the main establishment supervisory authorities with the exclusive power to adopt corrective measures runs contrary to the required proximity in the enforcement of data protection laws. This is also linked with the fact that the judicial review of any corrective measures adopted by the main establishment authority - or the refusal by that authority to adopt a corrective measure - can be subject to judicial review only in the Member State of the main establishment (see paras. 26 and 27). These Member States appear to be opposed to any concentration of corrective powers in the hands of the main establishment authority, notwithstanding the strong cooperation and consistency mechanism provided for in the draft Regulation. The Presidency is, therefore, inviting the Council to express itself clearly as to whether it wants corrective powers to be included in the exclusive powers of the main establishment authority or whether it, on the contrary, deems that to give such exclusive powers even if in limited cases runs counter the principle of proximity.

Strong cooperation between the main establishment supervisory authority and other concerned authorities

21. The Presidency has endeavoured to ensure the proximity to data subject in these cases by involving all concerned supervisory authorities in deciding on the draft corrective measure. The 'local' supervisory authority have the right to trigger the consultation mechanism by submitting a draft corrective measure to the main establishment supervisory authority. Before adopting a corrective measure, the main establishment authority must endeavour to reach consensus with the other concerned authorities. To this end, the main establishment authority shall share all relevant information with the concerned authorities and submit to them the draft measure and take utmost account of their views. Moreover, the local authority should still have the power to adopt corrective measures in case the supervisory authority of the main establishment of the controller or processor does not act within six weeks after the matter has been referred to the to European Data Protection Board.

22. Apart from this type of situation where the 'local' supervisory authority needs to refer the matter to the main establishment supervisory authority, there may also be cases where the problems of compliance with or serious infringements of data protection rules are of such a nature that they have an implication for several Member States. In case the main establishment authority finds that the matter it is dealing with (either on its own behalf or because it has been referred to it by a 'local' authority) is likely to affect substantially or to have substantially affected data subjects in other Member States, it should refer the matter to the European Data Protection Board (EDPB) for an opinion, unless it has already been satisfactorily dealt with under the cooperation mechanism.

23. For the adoption of corrective measures the local authority will in the above-mentioned cases refer the matter to the supervisory authority of the main establishment, with the possibility to submit a draft corrective measure. The co-operation mechanism will allow the supervisory authorities concerned to have input in the decision-making process, but eventually the corrective measure should be adopted by the supervisory authority of the main establishment, in those cases where the main establishment of the controller or processor is the decision-making establishment. It can be envisaged that the supervisory authorities express their views through a so-called silence procedure.

Decision-making process via EDPB

24. For the adoption of EU-wide authorisations the co-operation mechanism via the EDPB under the consistency mechanism can be applied. Regarding cases referred to the EDPB, its opinions are adopted by majority, but not binding on the supervisory authority of the main establishment. It can be envisaged that the supervisory authorities express their views through a so-called silence procedure; if a supervisory authority within the period of one month does not object to the measure proposed, it tacitly agrees with it. Pending this period no measure can be adopted, except under the urgency procedure.

Judicial review and judicial redress

25. A distinction should be made between *judicial review* of the decisions of supervisory authorities by the courts (Article 74) on the one hand, and *judicial redress* (i.e. the direct exercise of a judicial remedy (Article 75) against a controller or processor and/or the seeking of compensation (Article 77)) on the other hand.

26. *Judicial review* is closely linked to the power of the supervisory authority of that Member State and should therefore be possible only in the courts of the Member State of the supervisory authority concerned. At the DAPIX meeting of 7-8 November 2013 the vast majority of delegations agreed that granting the courts (civil or administrative) of the Member State of habitual residence of the data subject jurisdiction to review an administrative decision of the supervisory authority of another Member State would be impossible in view of the constitutional and practical difficulties that this would entail.

27. Therefore there are clearly limits to the degree to which proximity can be ensured regarding judicial review in those cases where the supervisory authority of the main establishment would have the exclusive power to adopt corrective measures. Only the courts of the main establishment Member State will have jurisdiction, not those of other Member States whose data subjects are affected and where they may have lodged a complaint. In all other cases proximity can be ensured among others- as is proposed in the latest Presidency draft - through the competence of any supervisory authority to hear a complaint and act upon it, not only if there is an establishment on the territory of that Member State, but also when data processing affects data subjects on its territory and through the possibility for the data subject to bring action in courts against a controller or a processor in his or her country of residence.

28. Regarding *judicial redress*, it has been established that the general rules on jurisdiction (in particular those flowing from the Brussels I Regulation) provide sufficient grounds of jurisdiction for the courts of the Member state to order measures against the controller or processor responsible for the alleged data protection violation. The articulation of the provisions on jurisdiction in this Regulation with the Brussels I Regulation is clarified in recital 118a.
If the court of habitual residence of the data subject has no jurisdiction over the controller or processor responsible for the alleged data protection violation, the exercise of a judicial remedy against or the seeking of compensation from a controller or processor will result in a judgment that needs to be enforced in the territory of the Member State where the controller or processor has an establishment. This is also possible under the Brussels I Regulation.

29. In the light of the conclusions of the October JHA Council meeting on this point and in particular the need to ensure proximity in the elaboration of the one-stop shop mechanism, delegations are invited:

1) *to indicate whether they agree that the main establishment authority, acting in close cooperation with local authorities, should, in addition to some exclusive authorisation powers, also be given certain exclusive powers to adopt corrective measures;*
2) *in case there would not be sufficient support for giving certain exclusive powers to adopt corrective measures to the main establishment authority, to indicate whether they think the power to decide on corrective measures should remain in the hands of the 'local' supervisory authorities in all cases or whether they could accept that in certain serious transnational cases the European Data Protection Board be given the power to adopt binding corrective measures.*