COUNCIL OF THE EUROPEAN UNION

Brussels, 19 December 2013 (OR. en)

18031/13 LIMITE

Interinstitutional File: 2012/0011 (COD)

JUR 658 JAI 1167 DAPIX 160 DATAPROTECT 205 CODEC 3040

CONTRIBUTION OF THE LEGAL SERVICE(*)

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 (the General Data Protection Regulation)
- Effective judicial protection of data subjects' fundamental rights in the context of the envisaged "one-stop shop" mechanism

I. INTRODUCTION

1. In January 2012, the Commission submitted a 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[1] (the draft Regulation) which will replace the existing legal framework set up by Directive 95/46/EC[2].

---

* **This document contains legal advice protected under Article 4(2) of Regulation (EC) No 1049/2001 of the European Parliament and of the Council of 30 May 2001 regarding public access to European Parliament, Council and Commission documents, and not released by the Council of the European Union to the public.**

1 Doc. 5853/12. The draft text discussed in this Opinion is the latest one presented by the Presidency in doc. 16626/1/13 REV 1.

2 Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data, OJ L 281 of 23.11.1995, p. 31.

2. The one-stop shop mechanism as laid down in Section II of Chapter VII of the draft Regulation is a mechanism whereby, in transnational cases, a single independent supervisory authority is competent to ensure that controllers or processors comply with the General Data Protection Regulation. This mechanism was first debated at the Justice and Home Affairs ("JHA") 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).*"[3]

3. Therefore, the 7-8 October JHA Council left open the question as to which single supervisory authority in transnational cases will be competent to exercise exclusive powers (including corrective powers) and how proximity as an important aspect of the protection of individual rights, would be achieved.

4. In the course of the proceedings in the DAPIX Working Party in October and November and in Coreper of 27 November 2013, the Presidency presented papers outlining the essential elements of a one-stop shop model based on conferring certain powers to one of the national supervisory authorities and presented a draft compromise text on the key provisions of the draft Regulation relating to that model of one-stop shop.[4] In that context, amended provisions on administrative and judicial remedies contained in Chapter VIII (Articles 73 to 77 of the draft Regulation)[5] were also discussed.

[3] Doc. 16626/2/13 REV 2, page 2.
[4] Doc. 16626/1/13 REV 1.
[5] Doc. 16626/1/13 REV 1, pages 47 to 53.

5. In those Presidency papers, the one-stop shop was developed as a mechanism whereby a single supervisory authority in the Member State, i.e. that where the controller or processor has its main establishment, the so-called "lead authority", is exclusively competent to exercise *inter alia* corrective powers, while allowing the data subject to have his/her complaints dealt with by his/her local supervisory authority in the initial stage.

6. In the JHA Council meeting of 6 December 2013, a revised Presidency document on the essential elements of the one-stop shop mechanism[6] was presented. However, this revised Presidency document maintained the key element that the lead authority would have exclusive competence to exercise corrective powers.

7. Both at the Coreper and JHA Council meetings, respectively on 27 November 2013 and 6 December 2013, the legal question was discussed whether the overall mechanism of a one-stop shop, as presented in the above-mentioned Presidency papers, would guarantee the effective judicial protection of data subjects' fundamental rights. This contribution further develops the oral interventions made by the Legal Service at those meetings.

II. LEGAL FRAMEWORK

8. In accordance with Article 8 of the Charter of Fundamental Rights of the European Union (the Charter), the right to the protection of personal data is a fundamental right and compliance with data protection rules shall be subject to control by an independent authority.

9. Article 16 TFEU is the legal basis of the draft Regulation which empowers the Union legislature to lay down the rules relating to the protection of this fundamental right, and the rules relating to the free movement of personal data.

[6] Doc. 17025/13.

10. Article 47 of the Charter, which corresponds in substance to both Articles 13 and 6(1) of the European Convention on Human Rights (ECHR),[7] provides for the right to an effective remedy before a tribunal and a right to a fair trial. Article 52(3) of the Charter provides that "*in so far as this Charter contains rights which correspond to rights guaranteed by the* [ECHR], *the meaning and scope of those rights shall be the same as those laid down by the said Convention. This provision shall not prevent Union law providing more extensive protection*".

11. Article 6(1) of the ECHR provides in particular for a right to a fair trial by an independent and impartial tribunal established by law and Article 13 of the ECHR provides that everyone whose rights and freedoms as set forth in the ECHR (such as the right to respect for private life under Article 8) are violated shall have an effective remedy before a national authority notwithstanding that the violation has been committed by persons acting in an official capacity.

III. LEGAL ANALYSIS

1. Consequences of conferring an exclusive competence to a lead supervisory authority for the imposition of corrective measures

12. The proposed one-stop shop mechanism consists in particular in conferring an exclusive competence to a lead authority, i.e. the supervisory of the main establishment of the controller or processor, to impose corrective measures,[8] in cases where the processing takes place in the context of the activities of an establishment of a controller or processor in the Union and the processing concerned was decided by the main establishment.[9]

---

[7] See in the Explanations relating to the Charter, ad Article 47.

[8] Corrective powers are listed in Article 53(1b) of the draft Regulation (doc.16626/1/13 REV1). They include in particular the following powers:
- ordering the controller or processor to bring processing operations into compliance with the provisions of the Regulation or ordering the rectification, restriction or erasure of data, or
- imposing a temporary or definitive limitation on processing, or
- imposing an administrative fine.

The lead authority is also given a number of authorisation powers in Article 53(1c) (such as authorising binding corporate rules and contractual clauses) for which the interlocutor of the authority is the controller applying for the authorisations and such a controller may challenge such authorisation or refusal decisions in the court of the Member State where the lead authority is established (Article 75(3)). The data subjects are not involved at that stage.

[9] Article 51(1a) of the draft Regulation.

As stated in the Presidency text of 29 November 2013, 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 (…)"[10] (emphasis added).

13. In effect, the proposed mechanism gives a priority to the businesses (as controllers or processors) which will indeed benefit from a one-stop shop in the Member State where they have their main establishment. By contrast, a data subject who alleges that his/her fundamental right to the protection of his/her personal data has been infringed will have to deal with at least the three following authorities having different powers:

- the "local" supervisory authority in the Member State where the data subject has his/her habitual residence for the basic treatment of the complaint before it is forwarded to the lead supervisory authority;

- the lead supervisory authority in the Member State where the controller or processor has its main establishment, which is exclusively competent for the imposition of corrective measures and

- the courts of the Member State where the controller or processor has its main establishment as regards "judicial review"[11] of the decision of the lead supervisory authority as well as the courts of the Member State where the data subject has his/her habitual residence as regards "judicial redress"[12].

14. The proposed one-stop shop mechanism appears thus to be a one-stop shop in the interest of controllers and processors established in several Member States rather than a one-stop shop in the interest of a data subject wishing to protect his/her fundamental rights where they have been infringed. It actually relies on a reversed construction of Article 16 TFEU which is aimed preponderantly at regulating the exercise of the fundamental right to the protection of personal data guaranteed by Article 8 of the Charter (which is mirrored in paragraph 1 of Article 16 TFEU), and not at improving the functioning of the internal market for controllers or processors.

[10] Doc. 16626/2/13 REV 2, paragraph 3.
[11] Article 74(3) of the draft Regulation
[12] Article 75(2) of the draft Regulation

15. The Treaty of Lisbon has added Article 16 in the TFEU, in a Title (Title II of Part One) entitled "*Provisions having general application*", both as a fundamental principle and right (paragraph 1) and as a new horizontal legal basis (paragraph 2) which empowers the EU legislature to adopt rules on the protection of this fundamental right both by EU institutions and bodies and by Member States when carrying out activities falling within the scope of EU law, in any area.[13]

16. Therefore, unlike the legal basis of Article 114 TFEU which requires that the approximating measures laid down by the Union legislature genuinely have as their object the improvement of the conditions for the functioning of the internal market (on the basis of which Directive 95/46/EC was adopted),[14] the rules adopted on the basis of Article 16 TFEU must have as their preponderant object the protection of the fundamental right to the protection of personal data. This is so both because of the actual wording of Article 16 TFEU which does not require the improvement of the conditions for the functioning of the internal market and the fact that the right to the protection of personal data is a fundamental right. For these reasons, the rules relating to the free movement of personal data should not prevail over, or undermine the protection of this fundamental right. What Article 16 TFEU requires at most is that the conditions of exercise of this fundamental right should not impede the free movement of data.

17. As a consequence, it appears that the proposed one-stop shop mechanism falls short of the requirements of ensuring the data subjects' rights to the protection of their personal data as laid down in Articles 16 TFEU and 8 of the Charter.

18. Furthermore, this multi-layer construction makes the overall system of the guarantee of the protection of data subjects' rights very complex and ineffective for the following reasons.

[13] The only exception is Article 39 of the Treaty on the European Union which constitutes a specific legal basis on personal data protection by Member States when carrying out activities which fall within the common foreign security policy (CFSP) Chapter. Personal data protection by EU institutions and bodies in the CFSP area is however covered by Article 16 TFEU.

[14] Case C-491/01, *British American Tobacco*, point 75.

(a) Ineffective administrative remedies both before the "local" supervisory authority where the data subject has his/her habitual residence and before the lead supervisory authority where the controller or processor has its main establishment

19. Under the draft Regulation, a data subject may lodge a complaint to the lead authority but also to another supervisory authority such as the one of his/her habitual residence[15] (the local authority). However, in accordance with Articles 51(1a) of the draft Regulation, the local authority is not competent to impose corrective measures where the processing takes place in the context of the activities of an establishment of a controller or processor in the Union and the processing concerned was decided by the main establishment. In that case, the local authority "(…) *shall ex officio transmit the complaint to the* [lead] *supervisory authority which is competent* (…)" (Article 73(4) of the draft Regulation, emphasis added).

20. This means that if a data subject lodges a complaint because he/she considers that his/her fundamental right has been infringed by a controller or processor whose main establishment is not in the Member State where he/she has his habitual residence, the competent supervisory authority imposing the corrective measures will be the lead authority located in a Member State other than the one of the data subject's habitual residence. The local supervisory authority who has received the complaint will therefore not settle the dispute in a final way but will only forward the complaint to the lead authority for a decision on corrective measures and will participate in the cooperation and consistency mechanisms,[16] for example by having the possibility to object to a draft measure submitted by the lead authority and refer the matter to the European Data Protection Board (EDPB)[17] for an opinion which will not be binding on the lead authority.[18]

---

[15] Article 51(1) of the draft Regulation "*each supervisory authority shall, on the territory of its own Member State, be competent to exercise the powers conferred on it in accordance with this Regulation* (…)", Article 52(1) *"*(…) *each supervisory authority shall on its territory* (…)*. (b) deal with complaints lodged by a data subject* (…)" and Article 73(1): *"*(…) *every data subject shall have the right to lodge a complaint with a supervisory authority competent in accordance with Article 51* (…)*".*

[16] Articles 54a to 63 of the draft Regulation.

[17] Article 54a(3) of the draft Regulation

[18] Article 58(9) of the draft Regulation.

21. The key role of supervisory authorities which are referred to in Article 16(2) TFEU and 8(3) of the Charter has been underlined by the Court of Justice as "(…) *the guardians of* [the] *fundamental rights and freedoms* [on the right to the protection of personal data], *and their existence in the Member States is considered, as is stated in the 62nd recital in the preamble to Directive 95/46* [to be replaced by the draft Regulation], *as an essential component of the protection of individuals with regard to the processing of personal data*".[19]

22. Conferring an exclusive competence for corrective measures to the lead supervisory authority in another Member State than the one where the data subject has his/her habitual residence, while such an authority plays such a fundamental role in the effective protection of the data subject's rights, is problematic. Indeed, as a result of the remoteness, use of foreign languages and complexity of the procedures in another Member State as well as the excessive costs it would entail, such a proposed system, all the more so if considered with the elements below, could render the exercise of the data subject's rights of the defence and the proper conduct of the proceedings before the lead supervisory authority excessively difficult.

b) Ineffective judicial review and judicial redress

(i) Case law of the European Court of Human Rights on the right of access to a court

23. The European Court of Human Rights (the ECoHR) interpreted the right of access to a court as guaranteed in Article 6(1) of the ECHR in the sense that limitations to this right must not restrict or reduce the access left to the individual in such a way or to such an extent that the very essence of the right is impaired.[20] The test used by the ECoHR to assess the effective access to judicial remedies is examined *in concreto* and not theoretically.[21]

[19] Case C-518/07, *Commission v. Germany*, Judgment of the Court of Justice of the EU (Grand Chamber) of 23.3.2010, point 23.

[20] Case of *de Geouffre de la Pradelle v. France*, application No 12964/87, judgment of the ECoHR of 16.12.1992, point 28.

[21] Case of *Weissman and others v. Romania*, application No 63945/00, judgment of the ECoHR of 4.5.2006, point 37.

The ECoHR considers that a complainant is entitled to expect a "*coherent system*" that would achieve a fair balance between the authorities' interests and his/her own; in particular, he/she should have a "*clear, practical and effective opportunity to challenge an act*" that was a direct interference with his/her fundamental right.[22] The ECoHR has already taken into account the "*extreme complexity*"[23] of the law to effectively access a court to conclude that through an overall assessment, the system of judicial redress was not "*sufficiently coherent and clear*".[24]

24. The ECoHR also assesses the effective right of access to the courts in the context of parallel proceedings (e.g. one through an administrative procedure and the other one before ordinary courts) to conclude that "*all in all, the system was not sufficiently clear or sufficiently attended by safeguards to prevent a misunderstanding as to the procedures for making use of the available remedies and the restrictions stemming from the simultaneous use of them*"[25] (emphasis added). Finally, the ECoHR assesses on the basis of the proportionality principle whether litigation costs such as a financial requirement, are "*excessive*". In this regard, the ECoHR considers that a restriction on access to a court is only compatible with Article 6(1) of the ECHR if it pursues a legitimate aim and if there is a reasonable degree of proportionality between the means used and the aim pursued. It has already held that if the amount is very high for any ordinary litigant and was not justified either by the particular circumstances of the case or by the applicants' financial position, it is disproportionate and thus impairs the very essence of the right of access to a court.[26]

(ii) Ineffective judicial review

25. In accordance with Article 74(3) of the draft Regulation, the judicial review of the decision of the lead authority which rejects the data subject's claim will have to be brought by the data subject (or by organisations he/she has mandated)[27] before the courts of the Member State where the supervisory authority is established.

---

[22] Case of *de Geouffre de la Pradelle v. France*, point 34. See also *Bellet v. France*, application No 23805/94, judgment of 4 December 1995, point 36 and *Beneficio Cappella Paolini v. San Marino*, Application No 40786/98, judgment of 13.7.2004, point 28.
[23] Case of *de Geouffre de la Pradelle v. France*, point 33.
[24] Case of *de Geouffre de la Pradelle v. France*, point 35.
[25] Case of *Bellet v. France*, application No 23805/94, judgment of 4 December 1995, point 37.
[26] Case of *Weissman and others v. Romania*, points 36, 37, 39 and 42.
[27] Article 76 of the draft Regulation

The data subject will therefore have a limited access to judicial remedies in the case of controllers/processors having a main establishment in another Member State, as he/she will have to bring his case only before the courts of the Member State of the main establishment which has decided the processing concerned, where he/she may not have his habitual residence.

26. While it is undisputed that "(…) *it is for national courts and tribunals and for the Court of Justice to ensure the full application of European Union law in all Member States and to ensure judicial protection of an individual's rights under that law*",[28] it is a different issue whether a rule of exclusive jurisdiction in favour of one national court renders the exercise of the data subject's rights "*impossible in practice or excessively difficult*"[29] (principle of effectiveness of judicial remedies stemming from Article 47 of the Charter).

27. Compliance with the principle of effectiveness of judicial remedies is assessed by the Court of Justice on a case by case basis depending on the circumstances of the case. Whilst it has been held, in the context of the common agricultural policy, that for evidence purposes, judicial proceedings are not rendered more complicated by the fact that the agricultural parcels concerned are far away from the exclusively competent national court[30] and that the latter at central level has acquired specific expertise,[31] it could be held, in the quite different context of the protection of data subjects' fundamental rights, that bringing a judicial review before a court in a different Member State from the one where the data subject has his/her habitual residence renders those proceedings more complicated. In this regard, it could be argued for example that a data subject would have to incur substantial litigation costs (including through the payment of legal representatives' and translation fees) in a different Member State which applies a different judicial system and which may be far away from the data subject. In practice, this could be a practical deterrent for a data subject to bring any judicial action.

[28] See e.g. Case C-432/05, *Unibet*, paragraph 38 and Opinion of the Court 1/2009 of 8 March 2011, paragraph 68.
[29] See e.g. Case C-93/12, judgment of the Court of Justice of 27.6.2013, points 50 to 61 regarding the application *in concreto* of the effectiveness principle to a rule of territorial jurisdiction.
[30] Case C-93/12, paragraph 52.
[31] Case C-93/12, paragraph 56.

A similar reasoning has been applied by the Union legislature when it introduced rules of jurisdiction for consumer contracts whereby in principle a consumer may choose to bring proceedings in which the other party is domiciled or in the courts for the place where the consumer is domiciled[32] in order to protect the "*weaker party*" by "*more favourable rules of jurisdiction to this interests*".[33]

(iii) Ineffective judicial protection through an very complex system of parallel judicial proceedings leading to a potential conflict of competence

28. In parallel to the system of judicial review provided for in Article 74(3) of the draft Regulation, Article 75(2) allows the data subject to bring other types of judicial proceedings before the courts of the Member State where the controller or processor has an establishment or before the courts of the Member State where the data subject has his/her habitual residence, unless the controller is a public authority acting in the exercise of its public powers.

29. Therefore, on the basis of Articles 74(3) and 75(2) of the draft Regulation, in the event that the rights under the Regulation have been infringed as a result of the processing of personal data in non-compliance with the Regulation, several courts may be competent to assess the non-compliance with the Regulation and to give redress to the data subject which may consist for example in corrective measures. This could lead to a positive conflict of competences, i.e. two courts in different Member States - one in the context of a judicial review of the decision of the lead authority, the other one in the context of a direct judicial action against the controller or processor - may be competent to assess the same alleged non-compliance with the Regulation and/or to order the same type of corrective measures (e.g. ordering the controller or processor to bring processing operations into compliance).

---

[32] Article 18(1) of Regulation (EU) No 1215/2012 of the European Parliament and of the Council of 12 December 2012 on jurisdiction and the recognition and enforcement of judgments in civil and commercial matters ("Brussels I" recast), OJ 20.12.2012, L 351, p. 1.

[33] Recital 18 of Regulation (EU) No 1215/2012.

30. This case of conflict of competences has been partly dealt with in Article 76a which provides for an obligation to contact the competent court in the other Member State and for a mere possibility to suspend proceedings (Article 76a uses the word "*may*"). Therefore, Article 76a does not provide for a binding mechanism of resolution of the "positive" conflict of competences and does not deal with cases where judicial redress (based on Article 75(2)) is conducted in parallel with a judicial review (based on Article 74(3)) brought by different data subjects for a similar infringement of the Regulation.

31. There is therefore a risk of contradiction in the outcome of parallel Court proceedings and a lack of legal certainty in the enforcement of data subjects' rights before the courts of several Member States.

32. The complexity is increased by the fact that judicial review based on Article 74 starts after the lead supervisory authority has conducted investigations on the case[34] and has made a first assessment of non-compliance, possibly after a cooperation and consistency mechanism.[35] The extent of the judicial review by the Court will therefore be circumscribed by the decision of the lead authority and may be subject to further limitations under different national procedural laws.[36]

33. By contrast, in the context of a judicial redress based on Article 75, the data subject will have to bring the evidence to the Court against the controller or processor and the extent of the judicial control over the lawfulness of the processing may be broader. Member States' procedural rules may also provide for time-limits to bring judicial proceedings so that if a data subject chooses one judicial remedy, he/she may be time barred to bring the second judicial remedy before a different court in a different Member State applying different procedural rules.

[34] Article 52(1) of the draft Regulation

[35] Article 54a and Article 57 and subsequent Articles of the draft Regulation.

[36] For example, given the discretion granted to supervisory authorities, the judicial review may be limited in some Member States to the control for example of a manifest error of appreciation of facts, error of law, misuse of powers or infringement of an essential procedural requirement.

34. In the light of the above-mentioned case law of the ECoHR and of the Court of Justice applied in the context of the proposed one-stop shop mechanism, it can be argued that the overall complex system of judicial review of decisions of lead supervisory authorities located in a different Member State from the one where the data subject has his/her habitual residence with a parallel system of judicial redress before other courts - such as civil or criminal courts - in other Member States, to deal with the same infringements of the Regulation and/or the same corrective measures, would not be sufficiently clear and coherent, would be excessively difficult to apply and understand and would be disproportionately costly for any ordinary data subjects. Such an overall system would therefore be disproportionate for the aim pursued which would thus impair the very essence of the right of access to a court in breach of Article 47 of the Charter and Articles 6 and 13 of the ECHR.

2. Conferring on the EDPB, for transnational cases, the power to adopt legally binding corrective measures as an alternative to the exclusive competence of the lead authority

35. In the context of transnational cases, and where certain thresholds or conditions are fulfilled, conferring on the EDPB the power to adopt legally binding corrective measures would constitute an EU-wide alternative which would ensure the protection of data subjects rights to an effective remedy, without undermining the aim of the free movement of data. Such specific competences of the EDPB would come in addition to the usual competences of the local supervisory authorities which would remain in charge of the majority of the cases, in line with the objective of "proximity" for data subjects.

36. The EDPB, which, under the draft Regulation, would be the successor of the current "Article 29 Working Party", is composed of the 28 national independent supervisory authorities and the European Data Protection Supervisor (EDPS) (see Articles 64 to 72 of the draft Regulation). The draft Regulation foresees that it is independent (Article 65) and that its secretariat will be provided by the EDPS (Article 71).

It could become an independent Union body or agency empowered to adopt binding decisions in individual cases. This would overcome the difficulties faced in the "lead authority model" stemming in particular from the fact that the decisions of a lead supervisory authority may not be enforceable in all Member States and may not bind Courts in other Member States. Indeed, contrary to the "lead authority model" which may give rise to legal uncertainties and fragmented application of Union law, the decisions of the EDPB as a Union body or agency, are binding Union decisions which will have a direct effect and will ensure the uniform application of Union law on the territory of all Member States.

37. Under the so-called "*Meroni*" case law,[37] executive powers can be given to such an EU body or agency, provided they are clearly defined and they do not encompass too broad and discretionary powers involving policy choices. In such a 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.

38. The *Meroni* test could be satisfied in this case if the EDPB were empowered and obliged to adopt corrective measures where a certain threshold is reached or certain conditions are met. Many options can be considered by the co-legislators. Among those options, two "plausible" options are presented below.

39. In the first option, it could be envisaged that the EDPB intervenes in transnational cases where a controller has several establishments or has one establishment but the processing affects data subjects in several Member States and the matter has been referred to it under a clearly-defined procedure, for example after the cooperation mechanism[38] between the national supervisory authorities concerned has not resulted in a solution by consensus between them.

[37] Case 9/56 *Meroni v High Authority*. It should be noted that the Court of Justice (in Case C-270/12) is expected to hand down a judgment on 21 January 2014 on the application of this *Meroni* case law in a concrete case after the entry into force of the Lisbon Treaty.

[38] Article 54a of the draft Regulation

In this scenario, the local authority where the data subject lodged his or her complaint would be strongly involved as it would have the power to refer the matter to the EDPB which in turn would have the power to reverse a draft decision proposed by the lead authority and to follow the opinion of the majority of other supervisory authorities including the local one.

40. In the second option, it could be envisaged that the local authority is even more involved. After preparing draft corrective measures, the local authority would refer transnational cases directly to the EDPB. The supervisory authority where the controller/processor has its main establishment would no longer be in the "lead" but would be involved like any other supervisory authorities which are members of the EDPB.

41. All these organisational options where the corrective measures are adopted by the EDPB, comply with the *Meroni* test, since they are individual decisions not involving policy choices and which the EDPB has to adopt where the matter is referred to it and it has concluded that the General Data Protection Regulation has been infringed in a specific case. The proximity with data subjects will be ensured by the key role given to the local authority which would refer individual cases to the EDPB and by the fact that the EDPB applies Union rules uniformly, any of the Union official languages chosen by the data subject would be accepted and possible translation costs would be borne by the EDPB.

42. As regards the judicial remedies against the binding decisions that would be taken by the EDPB in this context, it results from the first paragraph of Article 263 TFEU that the Court of Justice ("ECJ") will be competent to review the legality of such decisions. Effective judicial remedies would thus be ensured uniformly at Union level.

43. As regards "proximity", unlike the situation which would prevail in the system of judicial review of lead authorities' decisions according to the model discussed at the JHA Council of 6 December 2013, in the model of EDPB adopting legally binding corrective measures subject to judicial review before the ECJ, data subjects would be able to choose a legal representative from any Member State including from the Member State where he/she has his/her habitual residence and, when applying to the ECJ, could choose any of the Union official languages as the language of the case[39]. Furthermore, unlike the judgments of national courts in the context of judicial review[40] of "lead" authorities' decisions which may influence but do not bind other national courts seized in the context of judicial redress[41], ECJ judgments are always published[42] and binding[43] in all Member States of the Union. Such ECJ judgments would also develop case law on the interpretation of a provision of the draft General Data Protection Regulation thus ensuring a uniform interpretation of that Regulation in the Union and improving legal certainty for data subjects and controllers/processors.

44. This new model would thus create for transnational cases both a one-stop shop at Union level for controllers and processors, an effective judicial remedy for data subjects against decisions of the EDPB before the ECJ in Luxembourg and would enable a more uniform interpretation and application of the new General Data Protection Regulation in the Union.

[39] See Article 35 of the Rules of Procedure of the General Court
[40] Article 74(3) of the draft Regulation.
[41] Articles 75(2) and 76a of the draft Regulation ; see also paragraph 30 above.
[42] Article 86 of the Rules of Procedure of the General Court
[43] Article 83 of the Rules of Procedure of the General Court

IV. CONCLUSIONS

45. In view of the above, the Legal Service concludes that:

1) conferring an exclusive competence for the imposition of corrective measures to the lead supervisory authority where the controller or processor has its main establishment:

   (a) is a one-stop shop in the interest of controllers and processors as it only improves the free movement of data without ensuring an adequate protection of data subjects' fundamental rights and is therefore in contradiction with the objectives of Articles 16 TFEU and 8 of the Charter;

   (b) leads to ineffective administrative remedies in contradiction with Articles 16(2) TFEU and 8(3) of the Charter;

2) conferring an exclusive competence for judicial review of decisions by lead supervisory authorities to the courts of the Member State where the controller or processor has its main establishment and, as a consequence of the above, introducing an overall complex system of parallel judicial proceedings - judicial review of lead authorities' decisions and judicial redress against controllers or processors - whereby several courts in several Member States may be competent to assess the same infringement of the General Data Protection Regulation and possibly to apply the same corrective measures, would render the exercise of the data subject's rights impossible in practice or excessively difficult and could lead to positive conflicts of competences, to disproportionate costs for data subjects and as well as to lack of clarity and coherence; such an overall system of judicial remedies would therefore be disproportionate for the aim pursued which would thus impair the very essence of the right of access to a court in breach of Article 47 of the Charter and Articles 6 and 13 of the ECHR;

3) as an alternative one-stop shop model to the currently proposed one, the EDPB could become an independent Union body or agency empowered and obliged to adopt legally binding corrective measures in transnational cases where a matter has been referred to it and it has concluded that the General Data Protection Regulation has been infringed in a specific case. The EDPB decisions would then be subject to judicial review before the ECJ, pursuant to Article 263 TFEU. This would ensure an effective judicial remedy and a more uniform interpretation and application of the new General Data Protection Regulation in the Union, thereby improving legal certainty both for data subjects and controllers/processors.